Carmen Ionela Rotună, Ionuț Eugen Sandu,
Mihail Dumitrache, Adrian Victor Vevera

Reputația Domeniilor de Internet

Fundamente, metode de evaluare și practici operaționale



EDITURA ICI

REPUTAȚIA DOMENIILOR DE INTERNET

Fundamente, metode de evaluare și practici operaționale

Coordonatori
Carmen Ionela Rotună, Ionuț Eugen Sandu, Mihail Dumitrache, Adrian Victor Vevera

Colectiv de autori
Carmen Ionela Rotună, Ionuț Eugen Sandu, Mihail Dumitrache, Adrian Victor Vevera,
Carmen Elena Cirnu, Alexandru Gheorghiță, Dragoș Smada

REPUTAȚIA DOMENIILOR DE INTERNET
Fundamente, metode de evaluare și practici operaționale

EDITURA IC

București, 2026

Copyright © 2026, Editura ICI



Procesare PC
Daniela Coroleucă

Copertă
Alexandru Mihai Manolescu

Layout & Prepress
Iuliana Panciu

ISBN ONLINE 978-606-95858-9-4

Prefață

Numărul numelor de domenii este în continuă creștere, iar incidentele de securitate cresc exponențial (Ruposky, 2022). Evaluarea reputației numelor de domenii reprezintă o problemă de securitate informatică în care interpretarea datelor este la fel de importantă ca disponibilitatea instrumentelor tehnice. Un domeniu poate fi asociat, în momente diferite, cu servicii legitime, configurații vulnerabile sau activități abuzive. Înțelegerea acestor situații presupune examinarea contextului în care sunt obținute informațiile și a limitelor concluziilor formulate pe baza lor. Din această perspectivă, reputația se construiește prin observații verificabile și necesită reevaluare pe măsură ce condițiile de utilizare se modifică.

Volumul „Reputația numelor de domenii" abordează această problematică prin corelarea fundamentelor infrastructurii DNS cu metodele de analiză și cerințele utilizării operaționale. Demersul urmărește modul în care informațiile administrative și observațiile tehnice pot contribui la evaluarea unui domeniu, precum și condițiile în care rezultatul devine util pentru investigarea unui posibil incident. Atenția acordată relației dintre observație, estimare și decizie oferă coerență întregii lucrări și susține o interpretare prudentă a rezultatelor automatizării.

O preocupare centrală a cărții este calitatea informației pe care se întemeiază evaluarea. Datele de registru, răspunsurile DNS, metadatele certificatelor și listele externe de reputație au scopuri și grade de acoperire diferite. Utilizarea lor împreună presupune păstrarea provenienței, a momentului observării și a regulilor de prelucrare. În acest cadru, lipsa unei informații, dezacordul dintre surse sau existența unor observații istorice constituie aspecte metodologice care trebuie examinate explicit. Această abordare permite cititorului să înțeleagă de ce un rezultat numeric poate fi interpretat corect numai în raport cu datele și ipotezele care l-au produs.

Metodele de învățare automată sunt analizate în legătură cu definirea problemei și cu validitatea evaluării experimentale. Alegerea algoritmului este însoțită de examinarea modului de constituire a corpusului, a semnificației etichetelor și a independenței observațiilor. Interpretabilitatea și calibrarea completează analiza performanței, oferind repere pentru înțelegerea scorurilor și a erorilor. Studiul de caz asupra domeniilor .ro conferă acestei discuții un context

aplicativ, în care rezultatele sunt raportate la particularitățile colecțiilor analizate și la limitele protocolului utilizat. Relevanța sa constă și în evidențierea întrebărilor care rămân deschise atunci când un model experimental este avut în vedere pentru utilizarea curentă.

Perspectiva arhitecturală extinde analiza către organizarea sistemului și distribuirea responsabilităților. Separarea colectării datelor de evaluarea automată și de adoptarea unei măsuri permite verificarea etapelor și identificarea cauzelor unor rezultate necorespunzătoare. Relațiile dintre registru, registrar, operatorul DNS și titularul domeniului sunt relevante pentru stabilirea competențelor și a informațiilor disponibile fiecărui participant. În același timp, procedurile de înregistrare și validare a cazurilor oferă suportul necesar pentru documentarea dovezilor și reconstituirea deciziilor.

Dimensiunea operațională a reputației presupune păstrarea unui rol activ pentru specialist. Un scor poate orienta investigația, însă alegerea unei intervenții necesită aprecierea contextului și a consecințelor posibile. O clasificare eronată poate afecta servicii legitime, în timp ce o evaluare insuficient fundamentată poate întârzia identificarea unui abuz. Din acest motiv, cartea acordă atenție verificării ipotezelor alternative, reevaluării cazurilor și posibilității de corectare a concluziilor. Instruirea utilizatorilor și monitorizarea continuă sunt integrate în această perspectivă, alături de protecția datelor și trasabilitatea operațiunilor.

Lucrarea se adresează cercetătorilor și cadrelor didactice interesate de securitatea infrastructurilor Internet, precum și analiștilor, administratorilor și specialiștilor implicați în gestionarea numelor de domenii. Pentru cititorul aflat în formare, ea oferă un parcurs de la conceptele de bază către problemele de modelare și utilizare. Pentru practician, propune repere de examinare a surselor și de organizare a unui proces de evaluare care poate fi verificat și revizuit.

Prin reunirea perspectivei tehnice cu exigențele cercetării și ale practicii operaționale, volumul susține dezvoltarea unor sisteme de reputație ale căror rezultate pot fi explicate și utilizate responsabil. Valoarea acestor sisteme depinde de capacitatea de a transforma informația disponibilă în evaluări argumentate, păstrând vizibile incertitudinea și responsabilitatea deciziei.

CUPRINS

INTRODUCERE 9

1. FUNDAMENTELE REPUTAȚIEI DOMENIILOR DE INTERNET 11

2. AMENINȚĂRI ASUPRA DOMENIILOR ȘI INFRASTRUCTURII DNS 21

3. SISTEME DE REPUTAȚIE ȘI SURSE DE INFORMAȚII 31

4. DATE ȘI INDICATORI PENTRU REPUTAȚIA NUMELOR DE DOMENII 49

5. ALGORITMI ȘI VALIDAREA EVALUĂRILOR DE REPUTAȚIE 57

6. ANALIZA OPERAȚIONALĂ A REPUTAȚIEI 75

7. INTERPRETAREA RESPONSABILĂ ȘI BUNELE PRACTICI 79

8. UTILIZARE, INSTRUIRE ȘI MONITORIZARE CONTINUĂ 93

9. PROCEDURA DE ÎNREGISTRARE ȘI VALIDARE A INFORMAȚIILOR DESPRE DOMENII MALIȚIOASE 105

10. ARHITECTURĂ PENTRU SISTEME DE EVALUARE A REPUTAȚIEI 113

11. STUDIU DE CAZ. DOMENIILE .RO 131

12. CONCLUZII 139

BIBLIOGRAFIE 143

Introducere

Reputația unui nume de domeniu este o evaluare contextuală, construită din observații tehnice și istorice, care sprijină aprecierea riscului unei interacțiuni. Cartea examinează principiile generale ale acestei evaluări, independent de extensia numelui: calitatea dovezilor, proiectarea sistemelor și interpretarea rezultatelor. Publicul vizat cuprinde cercetători, administratori, analiști de securitate și operatori care înregistrează sau verifică informații despre domenii.

Firul central este relația dintre observație, estimare și decizie. Datele de registru, răspunsurile DNS, metadatele certificatelor și sursele de reputație descriu aspecte diferite ale aceluiași obiect. Un scor sintetizează numai informațiile disponibile, în condițiile unei metode și ale unui moment determinate. Reputația nu constituie o proprietate permanentă a numelui și nici o garanție generală asupra tuturor resurselor accesibile prin acesta.

Primele trei capitole prezintă fundamentele, amenințările și sursele. Urmează datele, algoritmii, analiza operațională, bunele practici, monitorizarea și procedura de evidență. Capitolul 10 reunește arhitectura și perspectivele TOGAF. Penultimul capitol prezintă studiul de caz asupra celor două corpusuri .ro iar ultimul formulează concluziile.

Terminologie și convenții

Prin domeniu se înțelege obiectul înregistrat la registrul competent, iar prin FQDN numele complet al gazdei analizate. O adresă URL identifică o resursă. În text, blacklist (listă neagră) desemnează surse de indicatori negativi, iar whitelist (listă albă) desemnează o sursă de referință pentru exemple considerate benigne. Apartenența la aceste liste este o observație contextuală și temporală.

DNS desemnează Domain Name System; DNSSEC, extensiile de securitate DNS; TLS, Transport Layer Security; ML, învățarea automată; API, interfața de programare; IoC, indicatorul de compromitere; TOGAF, cadrul de arhitectură al The Open Group; ADM, metoda de dezvoltare a arhitecturii. Termenul SSL apare în denumiri de câmpuri istorice, în timp ce analiza conexiunilor moderne este exprimată prin SSL/TLS sau TLS.

1. Fundamentele reputației domeniilor de Internet

1.1. Sistemul de nume de domenii de Internet

Sistemul de nume de domenii (DNS) constituie infrastructura distribuită prin care numele utilizate de aplicații sunt asociate informațiilor necesare localizării serviciilor. Evoluția standardelor DNS a permis dezvoltarea unei infrastructuri comune pentru rezoluția numelor la scară globală.

Sistemul de nume de domenii are un rol central în funcționarea Internetului. Rezoluția directă asociază nume de domenii cu adrese IP iar rezoluția inversă utilizează spații dedicate pentru asocierea adreselor cu nume. Infrastructura poate fi exploatată în campanii de phishing, rețele botnet și operațiuni de impersonare a unor servicii legitime.

Spațiul online necesită o modalitate rapidă, fiabilă și automată de a evalua și raporta nivelurile de risc ale domeniilor, astfel încât să poată fi adoptate măsuri de securitate adecvate. Conceptul de reputație, așa cum este aplicat domeniilor, adreselor IP și adreselor URL, permite operatorilor sau tehnologiilor de securitate automatizate să ia decizii cu privire la posibilitatea de a permite, de a refuza sau de a permite condiționat diferite tipuri de conexiuni.

În investigațiile cibernetice, reputația ajută la prioritizarea domeniilor care necesită examinare. O listă de blocare exprimă o apartenență la o categorie definită de furnizor, în timp ce un scor permite diferențierea priorităților. Niciuna dintre aceste reprezentări nu înlocuiește analiza dovezilor. Măsura adoptată depinde de scopul interacțiunii, de impactul unei erori și de posibilitatea revizuirii deciziei.

Sistemele Notos, Exposure și Kopis ilustrează abordări de analiză a datelor DNS pentru identificarea domeniilor potențial malițioase (Antonakakis et al., 2010; Antonakakis et al., 2011; Bilge et al., 2011). Performanțele lor nu pot fi reduse la o singură valoare de acuratețe, deoarece datele, condițiile de observare și protocoalele diferă. În plus, complementul acurateței reprezintă proporția totală a erorilor, nu rata rezultatelor fals pozitive. Listele de blocare rezultate din astfel de analize pot sprijini alertarea și filtrarea, cu păstrarea sursei și a momentului observației.

1.2. Infrastructura DNS

Sistemul de nume de domeniu (DNS) este un sistem descentralizat care traduce numele de domenii în adrese IP. Acesta joacă un rol crucial în funcționarea Internetului, permițând utilizatorilor să acceseze site-uri web și servicii folosind nume de domenii ușor de reținut, în locul adreselor IP numerice.

DNS funcționează pe un model ierarhic și distribuit. Sistemul este alcătuit din mai multe servere DNS care stochează și distribuie mapările numelor de domenii și adresele IP. Aceste servere sunt organizate într-o structură ierarhică, cu serverele

rădăcină (root) în vârf, urmate de servere de domeniu de nivel superior (TLD) și apoi servere de nume autoritative pentru domenii individuale.

Când un utilizator introduce un nume de domeniu în browser-ul său, începe procesul de rezoluție DNS. Dispozitivul utilizatorului trimite o interogare DNS unui resolver recursiv, care acționează ca intermediar între utilizator și infrastructura DNS. Resolver-ul își verifică cache-ul pentru adresa IP corespunzătoare numelui de domeniu. Dacă informațiile nu sunt disponibile, începe procesul iterativ de rezolvare a domeniului.

Resolver-ul contactează serverele DNS rădăcină pentru a obține informații despre serverele DNS autorizate responsabile pentru TLD-ul domeniului solicitat. Apoi contactează serverul TLD pentru a obține serverul de nume autorizat pentru domeniul specific. În cele din urmă, acesta comunică cu serverul de nume autorizat pentru a prelua adresa IP asociată cu numele de domeniu.

DNS utilizează diverse protocoale, inclusiv protocolul DNS (UDP sau TCP), pentru a facilita comunicarea între serverele DNS și clienți. Protocolul DNS definește formatul mesajelor DNS și regulile pentru schimbul lor.

DNS acceptă, de asemenea, diferite tipuri de înregistrări de resurse (RR) care stochează diferite tipuri de informații. Cele mai comune tipuri de RR includ înregistrările de adresă (A), care mapează numele de domenii la adrese IPv4 și înregistrările AAAA, care mapează numele de domenii la adrese IPv6. Alte tipuri de RR includ înregistrările Mail Exchange (MX), înregistrările Name Server (NS) și înregistrările Canonical Name (CNAME).

DNS este o infrastructură critică pentru Internet și este esențială pentru buna funcționare a multor servicii, precum e-mailul, navigarea pe web și tranzacțiile online. Oferă un mijloc scalabil și eficient de traducere a numelor de domenii în adrese IP, permițând utilizatorilor să acceseze cu ușurință site-uri web și servicii.

Sistemul DNS are multiple utilizări esențiale în infrastructura Internet. Câteva dintre cele mai importante utilizări ale acestuia sunt următoarele:

- Traducerea numelor de domenii în adrese IP. DNS permite traducerea numelor de domenii ușor de reținut și de utilizat de către oameni (precum www.example.com) în adrese IP numerice (precum 192.0.2.1) folosite de calculatoare pentru a se identifica și a comunica între ele. Aceasta facilitează accesul utilizatorilor la site-uri web și alte servicii online.
- Navigarea pe Internet. Atunci când utilizatorii introduc un nume de domeniu într-un browser web, sistemul DNS convertește numele de domeniu în adresa IP corespunzătoare a serverului web care găzduiește acel site. Astfel, utilizatorii pot accesa și vizualiza conținutul site-urilor pe care le vizitează.
- Livrarea e-mail-urilor. DNS este utilizat pentru a direcționa trimiterea și primirea de e-mail-uri. Atunci când un utilizator trimite un e-mail către o anumită adresă, sistemul DNS este folosit pentru a găsi serverul de e-mail corespunzător domeniului destinatarului, astfel încât mesajul să poată fi livrat corect.

- Găzduirea de site-uri web și servicii online. Sistemul DNS este utilizat pentru a atribui adrese IP domeniilor și subdomeniilor pe serverele web unde sunt găzduite site-uri web și alte servicii online. Aceasta permite utilizatorilor să acceseze aceste resurse prin intermediul numelui de domeniu.
- Redirecționarea traficului. Prin intermediul sistemului DNS, se pot configura înregistrări de tipul "Record-uri de resursă" (Resource Records) care permit redirecționarea traficului către alte adrese IP. Aceasta este utilă, de exemplu, în situații în care un site web este mutat pe un alt server sau atunci când se dorește echilibrarea încărcării pe mai multe servere.
- Securitate și filtrare. DNS este utilizat și în implementarea măsurilor de securitate și filtrare la nivelul rețelelor și serviciilor. De exemplu, se pot utiliza servicii DNS bazate pe blacklists pentru blocarea accesului la site-uri web cu conținut rău intenționat sau nedorit.
- Gestionarea infrastructurii. Administratorii de rețea utilizează sistemul DNS pentru a gestiona și a configura infrastructura de rețea. Ei pot adăuga, modifica sau șterge înregistrări DNS pentru a asigura o funcționare eficientă și sigură a rețelei.

Acestea sunt doar câteva exemple de utilizări ale sistemului DNS în cadrul infrastructurii Internet. Sistemul DNS este o componentă esențială pentru funcționarea eficientă a Internetului.

Cu toate acestea, DNS nu este lipsit de provocări. Poate fi o țintă pentru diferite tipuri de atacuri, precum alterarea cache-ului DNS, atacurile distribuite de tip denial-of-service (DDoS) și deturnarea DNS. Pentru a atenua aceste riscuri, au fost dezvoltate diverse mecanisme de securitate, precum DNSSEC (DNS Security Extensions), pentru a asigura integritatea și autenticitatea datelor DNS.

Infrastructura Domain Name System este distribuită la nivelul Internetului. Spațiul numelor este organizat ierarhic: rădăcina este reprezentată prin punct, sub aceasta se află domeniile de nivel superior, iar nivelurile următoare sunt administrate prin delegare. DNS deservește mai multe tipuri de servicii și nu se confundă cu World Wide Web.

Pentru www.example.com, acesta află de la nivelul rădăcină serverele pentru .com, apoi serverele autoritative pentru example.com și, în final, înregistrarea solicitată. Figura 1 simplifică acest schimb; cache-ul și eventualele aliasuri pot modifica numărul efectiv de interogări.

Administrarea unei zone DNS și operarea serverelor care o publică pot implica entități distincte. Pentru reputație contează ce sursă a furnizat răspunsul, din ce perspectivă a fost observat și la ce moment. Delegarea oferă o structură administrativă și nu certifică legitimitatea conținutului publicat ulterior de un domeniu.

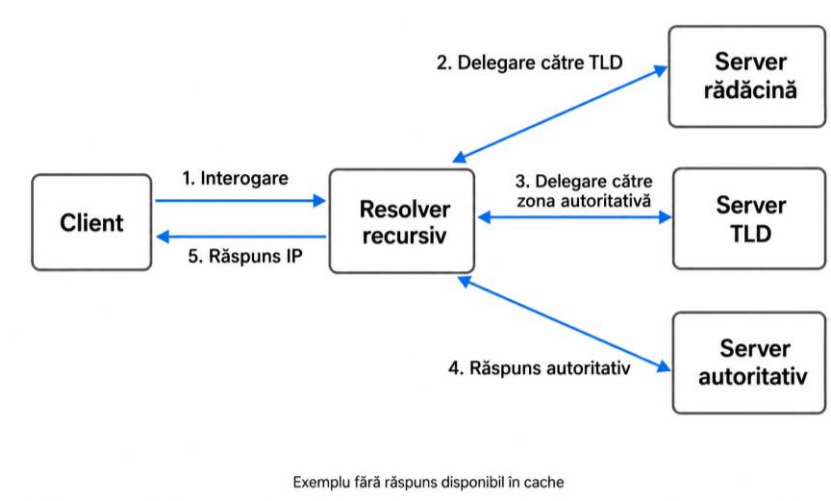


Figura 1. Rezoluția DNS prin delegări succesive

Protejarea rezoluției necesită măsuri complementare la nivelul operatorilor DNS, registrelor, registrarilor și registranților (deținători de domenii). Validarea DNSSEC, controlul accesului la administrare, monitorizarea modificărilor și securizarea resolverelor reduc categorii diferite de risc. Niciun control izolat nu acoperă toate formele de abuz și nici nu justifică atribuirea automată a unei reputații favorabile.

Prin arhitectura sa ierarhică și distribuită, DNS rezolvă numele de domenii și joacă un rol crucial în facilitarea comunicării și a accesului la resursele online.

1.3. Cadrul conceptual al evaluării reputației

Un sistem de reputație trebuie să precizeze obiectul evaluării. Numele, un subdomeniu, o adresă IP și o adresă URL sunt entități corelate, dar diferite. Un incident limitat la o cale web nu demonstrează compromiterea tuturor serviciilor domeniului, iar un IP partajat nu transferă automat reputația negativă tuturor clienților găzduiți.

Evaluarea este definită de obiect, interval temporal, surse și scop operațional. Același domeniu poate avea un istoric benign și un incident recent iar datele disponibile pentru e-mail pot diferi de cele relevante pentru navigare. Prin urmare, formularea unei concluzii trebuie să indice exact serviciul și perioada pentru care există dovezi.

Reputația, riscul și încrederea în evaluare nu sunt sinonime. Reputația sintetizează observații și antecedente. Riscul exprimă posibilitatea unor consecințe nedorite în contextul unei utilizări. Încrederea în evaluare descrie cât de bine este susținută concluzia de date. Un rezultat cu risc ridicat și dovezi incomplete poate necesita investigație urgentă fără a justifica o confirmare definitivă.

Metodologia poate fi organizată în etape verificabile, independente de produsul software utilizat:

- Definirea întrebării de analiză: detectarea phishingului, identificarea infrastructurii malware, urmărirea compromiterilor sau prioritizarea unui portofoliu. Clasele și criteriile de succes se stabilesc înainte de colectare și se raportează la acțiunile pe care evaluarea trebuie să le susțină.
- Stabilirea unității de observație și normalizarea identificatorului, cu păstrarea formei originale și a relațiilor dintre domeniu, gazdă și URL.
- Selectarea surselor în funcție de acoperire, actualitate, proveniență și independență. Două servicii care redistribuie aceeași listă nu reprezintă două confirmări independente.
- Definirea schemei de date, a momentului colectării și a stării fiecărei interogări. Lipsa răspunsului trebuie distinsă de absența unui indicator.
- Construirea unei referințe de evaluare din cazuri documentate. Etichetele trebuie să includă criteriul de atribuire, perioada și eventualele dezacorduri dintre evaluatori.
- Separarea datelor pentru dezvoltare și evaluare. Domeniile corelate prin campanie, infrastructură sau interval temporal necesită atenție specială, deoarece împărțirea aleatorie poate produce o estimare optimistă a generalizării.
- Selectarea unei metode de bază și a unor alternative comparabile. Reguli explicite, liste de indicatori și modele statistice pot fi evaluate pe aceleași date, cu aceleași definiții ale claselor. Complexitatea tehnică nu reprezintă, în sine, o dovadă de utilitate operațională.
- Stabilirea pragurilor în funcție de costul erorilor și capacitatea de analiză. Un prag destinat triajului poate fi diferit de cel utilizat pentru o măsură cu impact asupra accesului.
- Evaluarea separată a preciziei, recuperării cazurilor relevante, calibrării scorului și volumului alertelor. O singură metrică agregată poate ascunde rezultate slabe pentru categorii rare.
- Validarea fluxului complet, inclusiv erorile surselor, expirarea datelor, contestarea concluziilor și posibilitatea revenirii asupra unei decizii. Monitorizarea ulterioară a distribuției datelor și a erorilor confirmate în exploatare. Actualizarea regulilor și a modelelor trebuie versionată și verificată înainte de înlocuirea configurației active.

Aceste etape susțin interpretarea a cinci dimensiuni complementare:

- Identitatea obiectului specifică ce nume, serviciu sau resursă a fost observată și până unde poate fi extinsă concluzia.
- Temporalitatea arată când a fost observat semnalul, cât timp rămâne relevant și ce modificări au intervenit ulterior.
- Proveniența ilustrează cine a produs observația, prin ce metodă și cu ce posibilitate de reproducere.
- Incertitudinea arată ce informații lipsesc, ce surse se contrazic și cât de stabilă este clasificarea.
- Acțiunea exprimă ce măsură este justificată de dovezi și cine are responsabilitatea validării sale.

O observație tehnică trebuie interpretată împreună cu explicațiile alternative. Un domeniu recent poate aparține unei organizații legitime, iar un domeniu vechi poate fi compromis. Un certificat valid descrie un aspect al conexiunii și nu atestă intenția operatorului serviciului.

Corelarea crește valoarea analizei numai dacă se cunoaște dependența dintre semnale. Numărarea repetată a aceleiași informații poate produce o falsă impresie de confirmare.

Scorurile provenite din sisteme diferite nu se compară direct fără definiția scalei, sensului, intervalului și modelului. Valoarea 0,9 poate însemna reputație favorabilă într-un sistem și risc ridicat în altul.

Când datele sunt insuficiente, rezultatul adecvat este o stare explicită de incertitudine. Atribuirea implicită a unei clase benigne transformă indisponibilitatea surselor într-o eroare de interpretare.

Concluzia finală păstrează legătura cu observațiile inițiale și cu versiunea metodei. Această trasabilitate permite reevaluarea, analiza erorilor și aplicarea procedurii de evidență descrise în capitolul 9.

1.4. Sisteme de monitorizare existente

Pentru organizații, preluarea controlului de către infractorii cibernetici asupra unui domeniu deținut este o preocupare majoră deoarece aceștia îl pot exploata în scopuri rău intenționate precum găzduirea de programe malware și obținerea credențialelor utilizatorilor. În aceste cazuri, reputația domeniilor este compromisă (OWASP Foundation, 2026).

Dacă nu este securizat corespunzător, sistemul de nume de domenii (DNS) poate fi vulnerabil la exploatarea de către persoane rău intenționate. Dezvoltatorii de programe malware sunt conștienți de importanța accesibilității DNS și caută în mod activ modalități de a perturba funcționarea DNS și a serverele asociate (Scalzo, 2017).

În prezent, există mai multe tehnici care pot fi folosite pentru a îmbunătăți acuratețea și eficacitatea unui sistem de reputație a numelor de domenii. Aceste tehnici includ:

- Monitorizarea în timp real implică monitorizarea continuă a comportamentului domeniilor în timp real și actualizarea scorurilor reputației acestora în consecință. Acest lucru poate ajuta la identificarea și atenuarea rapidă a noilor amenințări pe măsură ce acestea apar.
- Listele de blocare și listele de referință benignă oferă observații utile, dar dependente de criteriile furnizorului și de momentul actualizării. Prezența într-o listă nu înlocuiește validarea, iar absența dintr-o listă de blocare nu demonstrează siguranța domeniului.
- Reputația IP ajută la identificarea activităților rău intenționate care pot fi asociate cu o anumită adresă IP.

În general, un sistem eficient de reputație a numelor de domenii trebuie să încorporeze o combinație de tehnici care, împreună cu algoritmi avansați de învățare

automată și capabilități de monitorizare în timp real, conlucrează pentru a identifica domenii cu potențial malițios. Procedând astfel, un astfel de sistem poate oferi informații exacte și fiabile asupra reputației unui anumit nume de domeniu, ajutând la protejarea utilizatorilor de potențiale amenințări și asigurând un mediu online rezilient și securizat (Udroiu & Vevera, 2018). În prezent există o serie de sisteme concepute pentru a determina reputația numelor de domenii.

Exposure este un sistem conceput pentru a detecta domeniile rău intenționate prin analiza datelor DNS. Utilizează tehnici de analiză DNS pasivă la scară largă pentru a identifica domeniile care sunt implicate în activități rău intenționate (Bilge et al., 2011).

Notos este un sistem de reputație pentru DNS care identifică domeniile rău intenționate pe baza caracteristicilor lor unice, utilizând date de interogare DNS pasive și analizând caracteristicile de rețea și zonă ale domeniilor. Datele sunt folosite pentru a dezvolta modele de domenii de încredere și domenii rău intenționate (Antonakakis et al., 2010). Sistemul funcționează prin analizarea comportamentului domeniilor de-a lungul timpului și identificarea tiparelor care indică o activitate rău intenționată. Notos ia în considerare o gamă largă de factori, inclusiv topologia rețelei și fluxul de trafic, datele de înregistrare și expirare ale domeniilor și utilizarea anumitor tipuri de înregistrări DNS.

Kopis utilizează o abordare pasivă pentru a observa traficul DNS la nivelurile superioare ale ierarhiei DNS. Analizând modelele de rezoluție a interogărilor DNS la nivel mondial, poate identifica cu precizie domeniile rău intenționate. Spre deosebire de sistemele de reputație DNS anterioare, precum Notos și Exposure, care depind de monitorizarea traficului de la serverele DNS recursive locale, Kopis oferă o perspectivă nouă și încorporează noi caracteristici de trafic care valorifică vizibilitatea globală obținută prin observarea traficului de rețea (Antonakakis et al., 2011).

Odată cu complexitatea tot mai mare a sistemelor IT, apare nevoia de monitorizare și analiză a sistemelor care se dezvoltă continuu, precum sistemele de nume de domenii. Una dintre problemele identificate la operarea sistemelor de date de dimensiuni mari este monitorizarea lor într-o manieră eficientă datorită complexității lor. Pentru a maximiza beneficiile monitorizării datelor, acestea trebuie să fie stocate pentru o perioadă extinsă de timp pentru analize ulterioare într-un sistem care poate susține rate mari de date.

Un prim pas al procesului de monitorizare este achiziționarea de date din surse de date predefinite, precum informații despre numele de domenii și filtrarea acestora astfel încât să nu fie eliminată nicio informație utilă.

Aspectul important este identificarea și adnotarea comportamentului normal pentru fiecare componentă din ecosistem iar apoi, pe baza acestuia, identificarea abaterilor și anomaliilor operaționale. Acest proces, combinat cu analiza tranzacției, va evidenția dacă există o problemă (de exemplu, fluctuații nejustificate), iar dacă se descoperă o problemă, se va identifica cauza și se vor lua măsuri pentru rezolvarea acesteia.

Algoritmii ML sunt antrenați să facă clasificări și/sau predicții, prin găsirea de informații cheie în proiecte care implică seturi mari de date. Informațiile preluate sunt utilizate de părțile interesate pentru a lua decizii în cadrul proceselor de business.

Un proces de învățare automată implică crearea de algoritmi matematici și statistici care pot accepta date de intrare și pot utiliza un proces de analiză a datelor pentru a face o predicție. Primul pas este colectarea datelor pentru setul de date care urmează să fie analizat. Odată colectate datele, se selectează tipul de algoritm de utilizat, apoi se construiește un model. Modelul este antrenat pe datele de antrenare; selecția configurației utilizează date de validare, iar evaluarea finală se realizează pe un set de testare separat.

Calitatea datelor depinde de diversitate, reprezentativitate și corectitudinea etichetelor. Un volum mare nu compensează duplicarea, contaminarea între partiții sau etichetarea necorespunzătoare. Procesarea la scară facilitează analiza, însă performanța trebuie verificată pe date relevante pentru mediul real de utilizare.

1.5. Obiectul reputației și nivelurile de analiză

Reputația devine interpretabilă numai dacă obiectul evaluat este definit explicit. Numele de domeniu, serviciul accesat prin acesta și organizația care îl utilizează sunt entități legate între ele, dar nu echivalente. Un incident observat la nivelul unui serviciu nu descrie automat toate utilizările domeniului. În mod similar, identitatea unei organizații nu poate fi dedusă exclusiv din asemănarea lexicală dintre un nume și o denumire comercială. Cadrul conceptual trebuie să stabilească ce anume primește scorul și asupra căror entități poate fi aplicată o eventuală măsură.

La nivel lexical, analiza privește structura numelui: etichetele, lungimea, secvențele de caractere și relațiile de asemănare. La nivel administrativ, contează existența înregistrării și evenimentele asociate acesteia. La nivel tehnic, sunt observate delegarea, rezoluția și configurația serviciilor. La nivel comportamental, sunt analizate activitățile semnalate. Asocierea acestor perspective susține evaluarea, însă fiecare răspunde unei întrebări diferite. Un nume neobișnuit lexical poate fi legitim, iar o configurație tehnică obișnuită poate servi unei activități abuzive.

Pentru un domeniu care oferă mai multe servicii, reputația poate fi reprezentată prin evaluări distincte. Un verdict privind livrarea mesajelor electronice nu trebuie transformat, fără justificare, într-un verdict asupra conținutului web. Agregarea rămâne posibilă, dar cere o regulă declarată ce arată ce categorii sunt reunite, ce perioadă este acoperită și ce informație se pierde. Cititorul unui raport trebuie să poată reveni de la scorul agregat la observațiile care l-au determinat.

Sistemele de reputație prezentate anterior folosesc observații DNS și relații între infrastructuri în moduri diferite (Antonakakis et al., 2010; Antonakakis et al., 2011; Bilge et al., 2011; Mishsky, Gal-Oz & Gudes, 2015). Din perspectiva metodologică a acestei cărți, această diversitate impune separarea unității de colectare de unitatea de decizie. O observație poate privi o adresă, un nume complet sau o relație temporală, în timp ce decizia privește un domeniu. Trecerea dintre

niveluri trebuie explicată, nu presupusă. Această regulă previne atât extinderea nejustificată a suspiciunii, cât și pierderea indiciilor utile prin agregare prematură.

1.6. Reputația în ciclul de viață al unui domeniu

Un nume de domeniu poate traversa perioade de utilizare activă, inactivitate, schimbare a serviciilor și modificare a administrării. Reputația trebuie raportată la acest parcurs. Continuitatea numelui nu garantează continuitatea operatorului, iar continuitatea operatorului nu garantează stabilitatea infrastructurii. De aceea, o observație istorică trebuie păstrată împreună cu momentul și condițiile în care a fost produsă. Fără aceste informații, un incident vechi poate fi atribuit incorect unei utilizări ulterioare.

O distincție utilă este cea dintre momentul evenimentului și momentul înregistrării lui. O sursă poate publica astăzi o observație realizată anterior, în timp ce un operator poate importa mâine acea publicare. Cele trei momente nu sunt interschimbabile. Într-o analiză retrospectivă, ordonarea numai după data importului poate crea impresia unei schimbări recente, deși activitatea descrisă aparține unei perioade încheiate. Într-o analiză predictivă, aceeași confuzie poate introduce informație care nu era disponibilă la data deciziei simulate.

Actualizarea reputației poate fi tratată ca revizuire a unei ipoteze. O observație nouă poate confirma evaluarea precedentă, o poate contrazice sau poate arăta că informația existentă a devenit insuficientă. Absența unor semnale recente nu demonstrează, prin ea însăși, remedierea. Totuși, nici păstrarea permanentă a unei clasificări negative nu este justificată fără reevaluare. Procedura trebuie să distingă expirarea valabilității unei evaluări de ștergerea istoricului care a susținut-o.

Ca exemplu conceptual, se poate considera un domeniu legitim compromis temporar și ulterior remediat. Înregistrarea istorică a incidentului rămâne relevantă pentru cercetare, dar starea curentă trebuie să reflecte dovezile verificării ulterioare. Raportul poate consemna simultan existența incidentului și absența confirmării sale la reevaluare. Această reprezentare este mai precisă decât înlocuirea unui verdict absolut cu un altul. Principiile de actualitate, trasabilitate și reevaluare din materialele de bune practici susțin o asemenea separare.

1.7. De la reputație la încredere și risc

Reputația, încrederea și riscul sunt concepte apropiate, însă au funcții diferite. Reputația rezumă evaluări rezultate din observații. Încrederea exprimă disponibilitatea de a permite o interacțiune în anumite condiții. Riscul include atât posibilitatea unui eveniment nedorit, cât și consecințele sale pentru contextul analizat. Un scor identic poate conduce la decizii diferite dacă serviciile protejate, resursele disponibile sau efectele unei erori sunt diferite.

Într-un proces de prioritizare, scorul poate ordona domeniile pentru verificare fără să stabilească o interdicție. Într-un proces de filtrare, același scor poate contribui la aplicarea unei restricții. A doua utilizare cere o justificare suplimentară, deoarece

efectele unei clasificări greșite sunt diferite. Definirea utilizării precede alegerea pragului. Un prag adoptat exclusiv deoarece produce o distribuție convenabilă a alertelor, nu constituie, singur, o demonstrație a adecvării sale.

Încrederea trebuie acordată unei afirmații delimitate. Afirmația că o observație a fost colectată corect poate avea un nivel ridicat de susținere, în timp ce interpretarea ei ca dovadă de abuz poate rămâne incertă. De exemplu, verificarea existenței unui certificat și interpretarea legitimității serviciului sunt două operații distincte. O explicație bună păstrează această diferență și arată unde intervine judecata evaluatorului. Astfel, încrederea în instrument nu se transformă automat în acceptarea tuturor concluziilor produse de acesta.

Pentru proiectarea unui sistem, consecința este separarea componentei de observare, a componentei de estimare și a politicii de acțiune. Prima furnizează date verificabile, a doua formulează evaluări, iar a treia stabilește utilizarea permisă a acestora. Separarea facilitează revizuirea unei politici fără modificarea istoricului și compararea mai multor metode pe aceleași observații. În această perspectivă, reputația reprezintă un suport pentru decizii documentate, iar valoarea sa practică se apreciază în raport cu scopul concret al evaluării.

2. Amenințări asupra domeniilor și infrastructurii DNS

2.1. Atacuri asupra sistemului DNS ce permit alterarea rezoluției

Sistemul DNS are un rol crucial în conversia numelor de domenii în adrese IP. O vulnerabilitate în acest proces ar putea conduce la redirecționarea utilizatorilor către site-uri web malițioase sau compromiterea securității comunicațiilor online.

2.1.1. Spoofing DNS

Un atacator furnizează informații DNS false unui resolver DNS, determinându-l să memoreze informații incorecte. Interogările ulterioare pentru același domeniu pot fi direcționate către servere malițioase.

DNS Cache Poisoning este o tehnică de manipulare utilizată de atacatori pentru a influența conținutul unei memorii cache DNS. Scopul este de a introduce informații false în memoria cache, determinând resolverele DNS să asocieze adrese IP incorecte cu nume de domeniu legitime. Această manipulare poate avea consecințe grave, incluzând redirecționarea utilizatorilor către site-uri web malițioase, interceptarea informațiilor sensibile sau facilitarea atacurilor de tip man-in-the-middle. Toate aceste consecințe ale DNS Cache Poisoning poartă denumirea de Spoofing DNS.

Un atacator interceptează cererile DNS efectuate de un utilizator sau un resolver DNS care încearcă să rezolve un nume de domeniu într-o adresă IP. Un exemplu simplificat de cum se poate face interceptarea cererilor într-un atac DNS Spoofing implică manipularea răspunsurilor DNS pentru un anumit domeniu. În acest scenariu vom lua în considerare un atacator care dorește să redirecționeze traficul pentru domeniul "www.exemplu.com" către o adresă IP controlată de el.

Acceptarea răspunsului fals poate determina furnizarea unei adrese incorecte aplicației. Figura 2 ilustrează efectele posibile, fără a descrie condițiile tehnice necesare realizării atacului.

Falsificarea răspunsurilor DNS urmărește acceptarea unor date furnizate de atacator în locul datelor legitime. Poluarea cache-ului DNS apare atunci când datele false sunt acceptate și păstrate în memoria cache a unui resolver. Cele două noțiuni sunt legate: un răspuns fals poate constitui mijlocul prin care este poluat cache-ul. Redirecționarea traficului reprezintă un efect posibil al folosirii datelor incorecte. Într-un scenariu de atac, rezoluția unui nume legitim poate conduce către o adresă controlată de atacator. Efectul asupra aplicației depinde și de verificările efectuate de aceasta; de exemplu, validarea certificatului TLS rămâne un control separat. O prezentare a riscului trebuie să distingă datele DNS falsificate de rezultatul interacțiunii cu serviciul accesat.

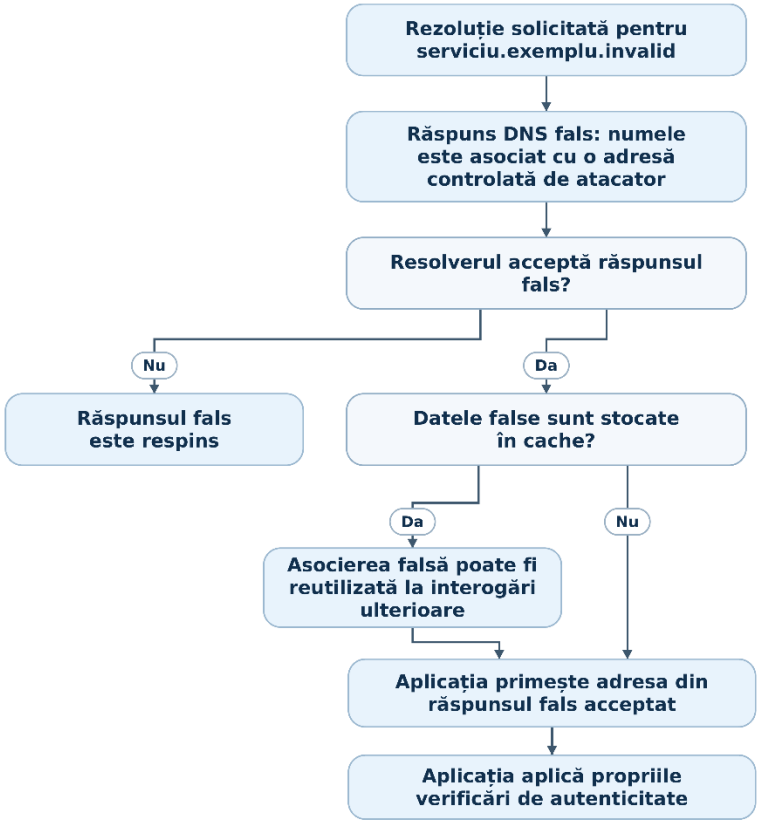


Figura 2. Acceptarea unui răspuns DNS fals și efectele asupra cache-ului și aplicației

2.1.2. Atacuri Man-in-the-Middle

Un atac de interpunere, denumit man-in-the-middle, presupune intervenția unui adversar în comunicarea dintre părți. Într-un scenariu DNS, acesta poate observa sau altera schimbul de mesaje dacă are poziția și capabilitățile necesare. Falsificarea răspunsurilor poate apărea însă și în alte condiții, inclusiv prin încercarea de a determina resolverul să accepte răspunsuri injectate. Mecanismele trebuie prezentate separat, în funcție de poziția atacatorului și de verificările protocolului.

Atacatorul se plasează între două părți care comunică, precum și între un utilizator și un server sau între două dispozitive care schimbă date. Acesta devine "man in the middle" (omul în mijloc), interceptând fluxul de date dintre cele două părți.

Atacul Man-in-the-Middle poate fi pasiv sau activ. Într-un atac pasiv, atacatorul doar ascultă și interceptează comunicațiile. Într-un atac activ, atacatorul poate modifica și manipula datele transmise.

Atacatorii pot folosi diverse tehnici pentru a intercepta comunicațiile, inclusiv sniffing-ul rețelei, atacurile de tip ARP spoofing (modificarea tabelei de rezoluție a

adreselor), sau chiar prin intermediul malware-ului instalat pe dispozitivele victimelor.

În cazul atacurilor active, atacatorul poate modifica sau adăuga date în fluxul de comunicații. Acest lucru poate include injectarea de conținut malițios în pagini web, schimbarea destinatarului unui mesaj sau alterarea informațiilor de autentificare. Atacatorul poate obține acces neautorizat la informațiile sensibile, precum nume de utilizator, parole, informații de card de credit sau alte date confidențiale.

Scenarii comune ale atacului Man-in-the-Middle:

- Atacuri Wi-Fi publice nesigure. În rețelele Wi-Fi publice nesigure, atacatorii pot crea puncte de acces false și intercepta comunicațiile utilizatorilor neavizați.
- Atacuri SSL/TLS. Prin compromiterea certificatelor SSL/TLS, atacatorii pot realiza atacuri Man-in-the-Middle asupra conexiunilor securizate, interceptând informații criptate.

Măsuri de Prevenire a atacului Man-in-the-Middle sunt:

- Folosirea protocoalelor de securitate precum SSL/TLS pentru a cripta comunicațiile și a preveni interceptarea datelor.
- Verificarea validității și autenticității certificatelor TLS contribuie la prevenirea atacurilor asupra conexiunilor securizate.

Rezistența resolverului la răspunsuri falsificate depinde de verificarea corespondenței dintre interogare și răspuns și de imprevizibilitatea parametrilor relevanți ai tranzacției. Randomizarea identificatorilor și a porturilor sursă îngreunează acceptarea unor răspunsuri injectate. Aceste controale completează validarea criptografică a datelor acolo unde aceasta este disponibilă.

2.1.3. Deturnare DNS (DNS Hijacking)

Deturnarea DNS (DNS Hijacking) este o formă de atac cibernetic în care atacatorii încearcă să modifice setările DNS ale unui dispozitiv sau ale unei rețele pentru a redirecționa traficul către servere DNS controlate de aceștia. Redirecționează interogările DNS legitime către servere malițioase, permițând atacatorilor să controleze comunicarea.

Scopul principal al acestui tip de atac este de a dirija utilizatorii către pagini web false sau de a intercepta comunicările în mod neautorizat. Iată o descriere mai detaliată a atacului de deturnare DNS: atacatorii obțin acces la dispozitive sau la infrastructura de rețea și modifică setările DNS ale acestora. Aceasta poate fi realizată prin compromiterea dispozitivelor individuale, a routerelor sau a serverelor DNS. Odată ce setările DNS sunt modificate, traficul care ar trebui să fie direcționat către serverele DNS legitime este redirecționat către serverele DNS controlate de atacatori. Ulterior, aceștia pot să intercepteze și să monitorizeze comunicările utilizatorilor, inclusiv accesul la site-uri web, trimiterea de date și autentificarea.

Deturnarea DNS poate fi folosită în cadrul atacurilor de phishing, redirecționând utilizatorii către site-uri web false care imită site-urile legitime pentru

a obține informații de autentificare sau alte date sensibile. Atacatorii pot redirecționa utilizatorii către site-uri web care distribuie malware sau pot furniza actualizări false de software pentru a infecta dispozitivele cu programe malițioase.

Scenariile de utilizare a deturnării DNS includ:

- Furtul de informații de autentificare, iar atacatorii pot redirecționa utilizatorii către pagini de autentificare false pentru a colecta nume de utilizator și parole.
- Atacuri asupra serviciilor bancare online prin deturnarea DNS pentru a redirecționa traficul către site-uri false de servicii bancare online, unde atacatorii încearcă să obțină informații financiare.

2.2. Atacuri asupra sistemului DNS ce afectează disponibilitatea

2.2.1. Amplificare DNS

Atacatorii utilizează servere DNS configurate incorect pentru a amplifica o simplă interogare DNS într-un răspuns mai mare, inundând ținta cu trafic. Atacul de amplificare DNS este o tactică cibernetică în care atacatorii exploatează serverele DNS pentru a amplifica volumul de trafic trimis către o victimă, astfel încât aceasta să fie supraîncărcată și să devină inaccesibilă. Acest tip de atac se bazează pe caracteristica de amplificare a unor interogări DNS, unde o cerere relativ simplă poate genera un răspuns mult mai complex. Iată o descriere mai detaliată a atacului de amplificare DNS:

- Atacatorul alege servere DNS care sunt configurate să permită interogări de tipul "ANY" (toate) sau alte interogări care pot produce răspunsuri voluminoase. Aceste servere sunt cunoscute sub denumirea de "servere amplificatoare."
- Atacatorul își ascunde identitatea falsificând adresa IP sursă a cererilor trimise către serverele DNS amplificatoare. În acest fel, răspunsurile vor fi direcționate către adresa IP a victimei, nu către cea reală a atacatorului.
- Atacatorul trimite cereri DNS malițioase către serverele amplificatoare, solicitând informații despre un domeniu specific. Cu toate acestea, adresa IP sursă a cererii este falsificată pentru a indica adresa IP a victimei.

Deoarece serverele amplificatoare produc răspunsuri mult mai mari decât cererile inițiale, atunci când răspunsurile sunt trimise la adresa IP a victimei, aceasta primește o cantitate semnificativ mai mare de date decât a solicitat inițial. Volumul de date trimise către adresa IP a victimei poate duce la supraîncărcarea infrastructurii acesteia, provocând indisponibilitatea serviciilor online sau a serverelor.

2.2.2. Atacul DNS DDoS

Un atac DNS DDoS (Distributed Denial of Service) reprezintă o formă de atac cibernetic îndreptat către Sistemul de Nume de Domenii (DNS), o componentă fundamentală a infrastructurii de Internet responsabilă de traducerea numelor de

domenii în adrese IP. Prin întreruperea funcționării normale a DNS-ului, aceste atacuri urmăresc să facă sistemul incapabil să răspundă la solicitările DNS legitime, ceea ce duce la indisponibilitatea serviciului.

Etapele unui atac DNS DDoS:

- Descoperire în care atacatorii identifică servere DNS vulnerabile sau soluții DNS deschise care pot fi exploatate pentru amplificare.
- Amplificarea presupune ca atacatorii să folosească tehnici de reflecție pentru a-și amplifica traficul de atac, făcându-l mai puternic și mai dificil de urmărit până la sursă.
- Lansarea atacului DDoS coordonat împotriva infrastructurii DNS țintă depășește capacitatea acesteia de a gestiona interogări DNS legitime.
- Refuzarea serviciului întrucât sistemul DNS este copleșit de traficul rău intenționat, răspunzând lent, incorect sau devenind complet indisponibil.

Atacurile DNS DDoS reprezintă o amenințare semnificativă la adresa disponibilității și integrității serviciilor de Internet. Organizațiile trebuie să implementeze măsuri proactive pentru a atenua impactul acestor atacuri, asigurând rezistența infrastructurii lor DNS.

O combinație de filtrare a traficului, Anycast DNS, limitarea ratei, servicii de atenuare a DDoS, corecție regulată și monitorizare cu detectarea anomaliilor pot întări DNS împotriva amenințărilor cibernetice în evoluție. Pe măsură ce peisajul Internetului continuă să evolueze, protejarea integrității DNS devine primordială pentru menținerea unui mediu digital sigur și de încredere.

2.2.3. Atac NXDOMAIN DNS

Atacul NXDOMAIN (Non-Existent Domain) în cadrul DNS (Domain Name System) este o tactică prin care un atacator încearcă să exploateze protocolul DNS pentru a crea condiții de supraîncărcare a resurselor sau pentru a efectua atacuri de tip denial-of-service (DoS) asupra unui server DNS sau a unei infrastructuri DNS. În acest tip de atac, atacatorii generează intenționat cereri pentru domenii inexistente (NXDOMAIN) pentru a forța serverul DNS să proceseze cereri inutile, consumând astfel resursele serverului și, potențial, afectând disponibilitatea acestuia.

Atacatorii generează o cantitate masivă de cereri DNS pentru domenii care nu există (NXDOMAIN). Aceste cereri pot fi trimise către un server DNS specific sau pot viza mai multe servere DNS, în funcție de tipul de atac.

În anumite situații, atacatorii pot falsifica adresele IP sursă ale cererilor DNS, ascunzându-și identitatea sau încercând să inducă în eroare serverele DNS cu privire la proveniența cererilor.

În unele scenarii, atacul NXDOMAIN poate fi folosit ca o diversiune sau acoperire pentru alte atacuri asupra infrastructurii sau rețelei, deoarece atenția și resursele echipei de securitate sunt concentrate pe gestionarea acestui volum mare de cereri DNS.

2.3. Atacuri ce implică folosirea abuzivă a DNS

2.3.1. Tunelare DNS

Tunelarea DNS reprezintă o tactică de securitate cibernetică în care traficul neautorizat sau ilegitim este ascuns în cadrul protocolului DNS (Domain Name System). Astfel, se încapsulează traficul non-DNS în interiorul pachetelor DNS pentru a evita măsurile de securitate și a exfiltra datele.

Acest tip de atac exploatează funcționalitățile protocolului DNS pentru a transfera date între un sistem compromis și un server de comandă și control. Tunelarea DNS este adesea folosită de atacatori pentru a evita detecția și a transfera informații sensibile în mod necunoscut.

Atacatorul încapsulează datele pe care dorește să le transfere în cereri DNS. Aceste date pot include comenzi pentru malware, informații furate sau alte activități ilegale.

Cererile DNS care conțin date sunt ascunse în traficul DNS obișnuit, care este adesea considerat inofensiv. Aceasta poate fi realizată prin adăugarea datelor în sub-domenii sau înregistrări DNS care sunt puțin probabile să atragă atenția. Atacatorul poate utiliza resolvere DNS compromise sau servere DNS controlate de el pentru a procesa cererile și a extrage datele ascunse.

Tunelarea DNS este concepută pentru a evita măsurile de securitate care monitorizează și filtrează traficul, deoarece cererile DNS sunt adesea considerate esențial nepericuloase. Totodată, permite un transfer bidirecțional de date între sistemul compromis și serverul de comandă și control. Astfel, atacatorii pot trimite comenzi la sistemul compromis și pot extrage informații furate fără a fi detectați în mod facil.

2.3.2. Atacuri DNS Flux Rapid (Fast Flux)

Atacurile DNS de tip Flux Rapid (Fast Flux DNS) reprezintă o tactică cibernetică avansată în care atacatorii își ascund infrastructura malițioasă în spatele unei rețele dinamice de adrese IP și domenii DNS. Modificarea constantă a adreselor IP asociate cu un domeniu îngreunează urmărirea și prevenirea atacului. Scopul principal al acestui tip de atac este de a evita detecția și de a menține disponibilitatea serviciilor cibernetice folosite în activități ilegale.

Atacatorii configurează o rețea de resurse, precum servere web, servere de comandă și control (C&C), sau servere proxy, care sunt asociate cu o gamă largă de adrese IP și domenii DNS. Această infrastructură dinamică permite atacatorilor să schimbe rapid adresele IP și domeniile pentru a evita blocarea sau identificarea lor.

Atacatorii rotesc continuu adresele IP și domeniile folosite în atac, schimbându-le la intervale scurte de timp. Această rotire rapidă face dificilă identificarea și blocarea infrastructurii malițioase. De asemenea, pot utiliza servere proxy pentru a ascunde adevărata sursă a traficului malițios. Traficul este direcționat printr-o serie de servere proxy, îngreunând astfel urmărirea înapoi către sursa inițială.

Atacul DNS Fast Flux poate fi folosit în cadrul unor atacuri cibernetice mai vaste, precum atacurile distribuite de tip denial-of-service (DDoS), atacurile de tip phishing sau distribuirea de malware. Prin schimbarea rapidă a IP-urilor și domeniilor, atacatorii încearcă să evite detectarea și blocarea prin intermediul măsurilor de securitate convenționale, precum filtrele de trafic și listele negre de domenii.

Scenarii de utilizare a atacurilor DNS Fast Flux includ:

- Distribuirea de malware în care atacatorii pot utiliza Fast Flux DNS pentru a distribui malware prin intermediul unor site-uri web sau link-uri aparent legitime.
- Atacurile de tip phishing pot beneficia de Fast Flux DNS pentru a crea și distribui rapid site-uri web false, folosind diferite adrese IP și domenii pentru a evita detectarea.
- Evaziunea în atacuri DDoS tactică utilizată pentru a evita blocarea surselor atacurilor DDoS, schimbând rapid adresele IP asociate cu traficul malițios.
- Ascunderea serverelor de comandă și control. Fast Flux DNS poate ascunde infrastructura de comandă și control utilizată în atacuri cibernetice, îngreunând investigarea și neutralizarea acesteia.

2.4. Atacuri ce vizează vectori și infrastructuri suport ale sistemului DNS

2.4.1. Atacuri DNS bazate pe Botnet

Atacurile DNS bazate pe botnet sunt tactici cibernetice în care un grup de dispozitive compromise, cunoscute sub numele de botnet, sunt coordonate pentru a lansa atacuri asupra sistemelor DNS (Domain Name System). Atacuri DNS coordonate lansate de la o rețea de calculatoare compromise (botnet). Aceste atacuri pot avea diferite scopuri, precum suprasolicitarea resurselor serverelor DNS, distrugerea disponibilității serviciilor online sau chiar manipularea informațiilor DNS pentru a redirecționa traficul către site-uri web malițioase.

Atacatorii infectează și preiau controlul asupra unui mare număr de dispozitive conectate la Internet, precum computere personale, servere, routere sau dispozitive IoT (Internet of Things). Aceste dispozitive compromise formează un botnet.

Atacatorii trimit instrucțiuni botnet-ului, care poate fi format din mii sau chiar milioane de dispozitive, pentru a lansa atacuri coordonate împotriva unuia sau mai multor servere DNS. Botnet-ul este folosit pentru a efectua atacuri distribuite de tip Denial-of-Service (DDoS) asupra serverelor DNS. Aceste atacuri constau în inundarea serverelor cu un volum masiv de cereri DNS, depășind capacitatea acestora de a răspunde la întrebări legitime.

Prin generarea unei cantități imense de cereri DNS sau prin exploatarea altor vulnerabilități, atacatorii încearcă să supraîncarce resursele serverelor DNS, determinându-le să devină inaccesibile sau să funcționeze lent.

În unele cazuri, botnet-urile pot fi folosite pentru a manipula informațiile DNS. Aceasta poate include distribuirea de informații DNS false pentru a redirecționa traficul către site-uri web malițioase sau pentru a efectua atacuri de tip cache poisoning.

Scenarii specifice ale atacurilor DNS bazate pe Botnet includ:

- Indisponibilitatea Serviciilor Online prin supraîncărcarea serverelor DNS cu cereri false, atacatorii pot face site-uri web și servicii online inaccesibile pentru utilizatori.
- Manipularea informațiilor DNS poate duce la redirecționarea traficului către site-uri web controlate de atacatori, unde pot fi efectuate atacuri de phishing sau se pot distribui programe malware.
- Atacuri asupra infrastructurii critice sau asupra organizațiilor importante pentru a cauza daune semnificative.

Prevenirea implică actualizarea și patching-ul regulat al sistemelor pentru a preveni infectările cu botnet și implementarea monitorizării traficului de rețea pentru a detecta și atenua activitatea botnet.

2.4.2. Atacuri de inginerie socială

Atacurile de inginerie socială presupun manipularea indivizilor pentru a divulga informații sensibile legate de DNS. Aceste incidente pot fi prevenite prin realizarea regulată a sesiunilor de instruire privind conștientizarea securității, pentru a educa utilizatorii cu privire la amenințările potențiale.

Este crucială combinarea mai multor măsuri preventive. Menținerea informării cu privire la amenințările emergente este esențială pentru o securitate DNS eficientă. Organizațiile ar trebui să evalueze și să actualizeze regulat strategiile lor de securitate DNS pentru a aborda riscurile în evoluție.

2.5. Asocierea amenințărilor cu măsurile de prevenire și atenuare

Măsurile de securitate trebuie alese în funcție de mecanismul amenințării, componenta afectată și responsabilitățile entității care le aplică. Protejarea integrității răspunsurilor DNS, menținerea disponibilității serviciului, securizarea accesului administrativ și investigarea comportamentelor suspecte urmăresc obiective distincte. Eficacitatea fiecărei măsuri depinde de configurația infrastructurii și de condițiile în care aceasta este utilizată.

2.5.1. Protecția împotriva răspunsurilor falsificate și a poluării cache-ului

Reducerea riscului de acceptare a unui răspuns DNS fals începe cu verificarea corespondenței dintre răspuns și interogarea aflată în așteptare. Resolverul trebuie să

verifice identificatorul tranzacției, numele solicitat, tipul și clasa înregistrării, precum și adresele și portul relevante pentru schimbul de mesaje. Randomizarea identificatorului tranzacției și a portului sursă al interogării îngreunează anticiparea acestor valori de către un atacator care nu poate observa traficul. Aceste verificări sporesc rezistența la falsificare, fără a oferi, singure, autentificarea criptografică a datelor (Hubert & van Mook, 2009).

Pentru datele protejate prin DNSSEC, resolverul cu validare verifică semnăturile și construiește un lanț de încredere până la o ancoră configurată. Simpla prezență a unei înregistrări DS, DNSKEY sau RRSIG nu demonstrează că validarea a fost realizată cu succes. În analiza unui domeniu trebuie diferențiate observarea acestor înregistrări și rezultatul verificării criptografice. Protecția depinde de semnarea și administrarea corectă a zonelor, de continuitatea lanțului de încredere și de funcționarea resolverului cu validare. DNSSEC autentifică originea datelor DNS și integritatea acestora; nu certifică legitimitatea activității desfășurate prin domeniul respectiv (Arends et al., 2005).

2.5.2. Reducerea utilizării abuzive a serverelor DNS ca reflectoare

În atacurile prin reflexie, serverele DNS pot transmite răspunsuri către o victimă a cărei adresă IP a fost falsificată în interogări. Pentru resolverele destinate unei organizații sau unei categorii determinate de utilizatori, o măsură principală este restrângerea recursiei la clienții autorizați. Configurația trebuie să evite expunerea neintenționată a unui serviciu recursiv deschis. Această restricție privește serviciul recursiv; serverele autoritative care publică date DNS pentru zone publice trebuie să poată răspunde interogărilor externe legitime (Damas & Neves, 2008).

Pe serverele autoritative, mecanisme precum Response Rate Limiting — RRL pot reduce volumul răspunsurilor repetitive exploatate pentru amplificare. Rolul lor este limitarea traficului de răspuns care contribuie la abuz. Pragurile trebuie adaptate traficului normal și monitorizate pentru a evita afectarea clienților legitimi. RRL nu validează autenticitatea datelor DNS și nu înlocuiește controlul accesului la recursie (Internet Systems Consortium, 2018).

La nivelul rețelelor, filtrarea adreselor sursă necorespunzătoare contribuie la reducerea posibilității de utilizare a adreselor IP falsificate. Această filtrare nu trebuie prezentată ca autentificare a solicitantului realizată de serverul DNS (Damas & Neves, 2008). Pentru disponibilitate, distribuirea infrastructurii, utilizarea Anycast și capacitatea adecvată de procesare pot completa măsurile de atenuare, fără a elimina toate formele de suprasolicitare (Rose, Liu & Gison, 2026).

2.5.3. Prevenirea accesului neautorizat la administrare

Protecția administrării domeniilor și a serviciilor DNS presupune limitarea accesului la persoanele autorizate, utilizarea autentificării multifactor, protejarea credențialelor și revizuirea periodică a drepturilor acordate. Modificările datelor de înregistrare, ale delegărilor și ale configurației DNS trebuie urmărite prin notificări

și înregistrări de audit. Pentru domeniile critice pot fi utilizate mecanisme de blocare a transferului sau a modificărilor, acolo unde acestea sunt disponibile (ICANN SSAC, 2010).

Responsabilitățile trebuie precizate pentru fiecare rol. Registrul administrează evidența domeniilor și delegările la nivelul TLD-ului; registrarul gestionează relația de înregistrare cu titularul și transmite operațiunile către registru; operatorul DNS administrează serviciul și înregistrările zonei pentru care este responsabil; titularul autorizează administrarea domeniului și protejează accesul la conturile proprii. Aceste funcții pot fi îndeplinite de aceeași organizație, dar rămân distincte.

Prin urmare, investigarea unei modificări neautorizate trebuie să identifice contul, interfața și entitatea prin care aceasta a fost efectuată (ICANN SSAC, 2010). icann.org

2.5.4. Investigarea traficului și a infrastructurii suspecte

Identificarea comportamentelor suspecte necesită observații repetate și corelarea mai multor categorii de informații. Pot fi analizate evoluția adreselor asociate unui domeniu, valorile TTL, distribuția temporală a interogărilor și utilizarea infrastructurii partajate. Aceste caracteristici trebuie interpretate împreună. De exemplu, un TTL redus și schimbarea frecventă a adreselor pot apărea atât în infrastructuri abuzive de tip fast flux, cât și în servicii legitime care urmăresc disponibilitatea ridicată sau distribuirea conținutului (Bilge et al., 2011).

Jurnalele DNS pot fi corelate cu evenimentele aplicațiilor, modificările administrative și alte observații de securitate, păstrând momentul și sursa fiecărei informații (Rose, Liu & Gison, 2026). Un indicator izolat justifică verificări suplimentare, fără a confirma automat abuzul. Analiza trebuie să păstreze explicațiile alternative, inclusiv migrarea unui serviciu, schimbarea furnizorului sau utilizarea legitimă a găzduirii partajate. În sistemul de reputație, scorul rezultat sprijină prioritizarea investigației; măsura aplicată trebuie justificată prin dovezile disponibile și revizuită atunci când apar informații noi.

3. Sisteme de reputație și surse de informații

3.1. Sisteme de reputație existente studiate

Pentru a consolida un punct de plecare în dezvoltarea unei metodologii de stabilire a reputației unui domeniu, au fost analizate și comparate patru soluții existente: Notos, Exposure Kopis și MaldomDetector.

3.1.1. Notos

Reprezintă o soluție de stabilire a reputației care se bazează pe analiza pasivă a datelor din cadrul serverelor de DNS. Aceasta are capacitatea de a detecta un domeniu malițios înaintea sistemelor clasice de *blacklist*, cu o acuratețe de 96,8% *true-positive* și doar 0.38% *false-positive*.

Sursa principală a sistemului o reprezintă informații colectate pasiv din cadrul serverelor de DNS prin analizarea istorică a IP-urilor rezolvate de către un domeniu. Această bază de date, numită de către autori pDNS, prelua date de la doi mari provideri de Internet (ISP) din Atlanta și San Jose, având acces la aproximativ 30.000 de interogări DNS pe secundă. O a doua sursă de informații o reprezenta listele de tipul *blacklist* ce conțineau domenii cunoscute ca fiind malițioase și în final o sursă de domenii cunoscute ca fiind legitime, Alexa.com.

Scorul de reputație este calculat în funcție de activitățile pe care domeniul vizat le găzduia. În cazul în care sunt descoperite acțiuni catalogate ca fiind malițioase, scorul domeniului era redus, iar dacă se constată că domeniul este asociat unor activități legitime, scorul este crescut.

O limitare importantă a sistemului Notos o reprezintă incapacitatea de a stabili nivelul de reputație pentru un domeniu nou deoarece nu există destule informații istorice aflate în bazele de date pasive ale serverelor de DNS. Astfel, dacă un atacator continuă să achiziționeze domenii noi pentru activități ilegale, acesta poate eluda foarte ușor sistemul de detecție.

3.1.2. Exposure

Reprezintă o soluție cu o abordare similară celei utilizate de Notos pentru stabilirea reputației unui domeniu. Diferența majoră o reprezintă capacitatea sistemului Exposure de a detecta inclusiv domenii noi folosind metode diferite de analiză, în speță, analiza zonei în care este înregistrat domeniul și nu neapărat activitatea IP-urilor rezolvate de către acesta în rețea.

Exposure a reușit să identifice domenii care au avut durată de viață în medie de 1-2 zile, atenuând astfel tehnica atacatorilor de a înregistra un număr mare de domenii zilnic pentru a fi folosite drept paravan pentru acțiunile ilicite ale acestora.

Un alt avantaj deținut de către soluția Exposure este acela că nu necesită un volum mare de date pentru a demara analiza unui domeniu, fiind necesare doar câteva zile de analiză asupra traficului acestuia.

Limitarea principală a soluției Exposure o reprezintă publicarea metodologiei de analiză prin care este determinată reputația unui domeniu, fapt ce poate permite unui atacator să schimbe strategiile de utilizare a domeniilor malițioase și astfel să eludeze sistemul de detectare.

3.1.3. Kopis

Reprezintă o soluție de stabilire a reputației care vizează analiza traficului de DNS la cel mai înalt nivel al ierarhiei serverelor de DNS. Astfel soluția poate accesa la nivel global informații referitoare la activitățile unui domeniu, spre deosebire de soluțiile prezentate anterior Notos și Exposure, care abordează analiza traficului pe plan local, în cadrul providerilor de Internet (ISP).

Analiza este efectuată strict peste informațiile disponibile în cadrul serverelor de DNS și nu sunt luate în calcul reputațiile adreselor de IP-uri, precum în cazul soluțiilor prezentate anterior. Acest lucru decuplează notarea unui domeniu de notarea adreselor de IP, permițând aplicarea unui scor chiar și în cazul în care nu există date despre IP-urile rezolvate de către domeniu.

Rata de succes a soluției este de 98.4% true-positives și doar 0.3 - 0.5% false-positives. Adițional sistemul Kopis are capacitatea de a detecta domenii malițioase cu zile sau săptămâni înainte ca acestea să fie înregistrate în listele publice de tip *blacklist*.

3.1.4. MaldomDetector

MaldomDetector este un sistem eficient de detectare, dezvoltat pentru a detecta numele de domenii rău intenționate generate algoritmic. MaldomDetector folosește algoritmul RMA, pentru a măsura caracterele aleatorii ale numelor de domeniu. MaldomDetector alimentează ieșirile RMA împreună cu un set de caracteristici de bază și derivate extrase din cererea inițială DNS către un clasificator de învățare automată pentru procesare și clasificare. Au fost explorați mai mulți algoritmi de clasificare pentru a construi clasificatorul.

Bazându-se pe ultimă generație privind detectarea numelor de domenii rău intenționate, MaldomDetector nu folosește niciun model de limbaj probabilistic. Acesta utilizează o abordare bazată pe caractere pentru a detecta numele de domenii bazate pe DGA. Efectuează măsurători numai pe pachetul de solicitare DNS și nu trebuie să aștepte răspunsul DNS pentru a extrage caracteristici suplimentare sau pentru a solicita informații din orice sursă externă.

Rezultatele evaluării arată că MaldomDetector poate detecta în mod eficient diferite tipuri de domenii bazate pe DGA generate de mai multe tipuri de malware, iar acuratețea detectării este de ~ 98%. MaldomDetector poate fi folosit pentru a declanșa alarme timpurii despre potențialele comunicări DNS rău intenționate, menținând în același timp o precizie ridicată.

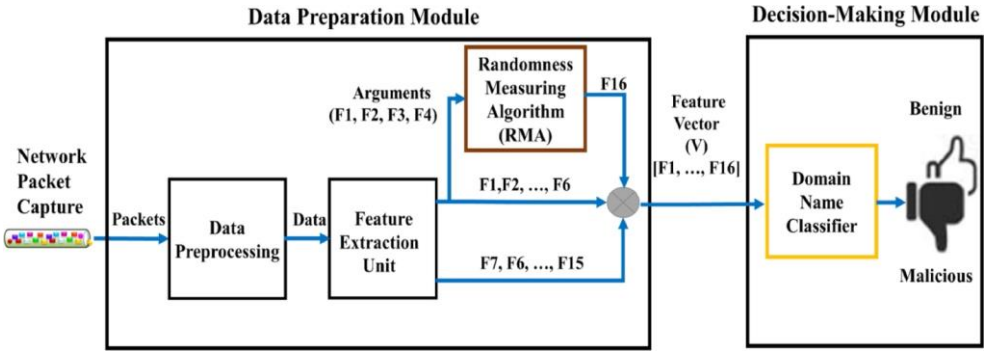


Figura 3. Funcționalitatea MaldomDetector (Almashhadani et al., 2020)

Majoritatea sistemelor existente de reputație a domeniilor nu oferă o soluție dinamică de monitorizare în timp real bazată pe Machine Learning, care poate fi utilizată de ccTLD-urile (Country Code Top Level Domain) sau registrari pentru a scana zilnic nume de domenii, permițând astfel detectarea numelor de domenii compromise.

Un sistem de evaluare a reputației poate corela istoricul numelui de domeniu cu date administrative și observații provenite din surse externe. Tehnicile de învățare automată permit estimarea riscului pe baza atributelor disponibile și prioritizarea cazurilor pentru analiză. Aplicabilitatea metodei depinde de accesul la date, de calitatea etichetelor și de populația evaluată, nu de o anumită extensie. Verificarea unui domeniu suspect necesită analiza dovezilor. Scorul nu constituie, singur, temeiul unei decizii de suspendare.

Comparația sistemelor de reputație trebuie să distingă tipul surselor, nivelul de vizibilitate DNS și obiectivul detecției. Funcțiile descrise în tabelul următor sunt caracteristici ale soluțiilor prezentate în documentația de referință; nu constituie un experiment comparativ pe date comune.

Tabelul 1 compară caracteristicile sistemelor existente:

Tabel 1. Caracteristicile sistemelor de reputație a domeniilor

System	Real Time Analysis	Active DNS Analysis	Uses TLD Domain Registry Database	Continuous Domain Scanning and Alerting	Machine Learning use
Exposure	No	No	No	No	Yes
Notos	No	No	No	No	Yes
Kopis	No	No	No	No	Yes
MaldomDetector	No	No	No	No	Yes

3.1.5. Alte tipuri de sisteme de monitorizare

Rețelele de servicii Fast Flux (FFSN) sunt un tip de rețea folosit de infractorii cibernetici pentru a evita detectarea și pentru a menține disponibilitatea infrastructurii rău intenționate. FFSN-urile sunt caracterizate de multe adrese IP în schimbare constantă, ceea ce le poate face dificil de detectat folosind tehnicile tradiționale de analiză a rețelei.

Cu toate acestea, analiza DNS pasivă poate fi o modalitate eficientă de a identifica FFSN-urile și de a detecta activitățile rău intenționate. Algoritmii de învățare automată pot fi utilizați pentru a detecta FFSN-urile pe baza datelor DNS pasive.

Prin antrenarea modelelor de învățare automată pe seturi mari de date de FFSN-uri cunoscute, cercetătorii pot dezvolta modele care pot detecta cu precizie FFSN-urile în timp real (Caglayan et al., 2009; Lombardo et al., 2018).

Modelul de flux bazat pe topologie propus de Mishsky (Mishsky, Gal-Oz & Gudes, 2015) oferă o abordare promițătoare a reputației domeniului. Utilizând topologia rețelei și analiza fluxului, modelul are potențialul de a oferi o protecție mai precisă și mai eficientă împotriva domeniilor rău intenționate.

3.2. Blacklists și whitelists

În contextul sistemului de reputație a numelor de domenii de Internet, termenii "blacklist" și "whitelist" se referă la liste care conțin adrese IP sau nume de domenii considerate nesigure sau respectiv sigure. Aceste liste sunt utilizate pentru a filtra și controla traficul de e-mail și accesul la resurse online, în scopul de a preveni spam-ul și alte activități nedorite.

Un sistem de tip "blacklist" este o listă care conține adrese IP sau nume de domenii considerate nesigure sau asociate cu activități nedorite, precum trimiterea de spam sau găzduirea de conținut periculos. Un exemplu de astfel de listă este Domain Name System Blacklist (DNSBL).

DNSBL este un serviciu care permite serverelor de e-mail să verifice dacă adresa IP a unui server de e-mail este listată ca fiind asociată cu trimiterea de spam sau alte activități nedorite.

Pe de altă parte, o "whitelist" este o listă care conține adrese IP sau nume de domenii considerate sigure și de încredere. Aceste liste sunt utilizate pentru a permite accesul la resurse online sau pentru a primi e-mailuri de la anumite surse.

Whitelist-urile sunt adesea utilizate în combinație cu blacklist-urile pentru a asigura un control mai bun asupra traficului de e-mail și a accesului la resurse online.

Pentru a dezvolta și implementa o arhitectură pentru o platformă de monitorizare a domeniilor, care să stabilească gradul de reputație al acestora, se pot utiliza tehnici de depistare a domeniilor malițioase folosite în soluțiile Notos, Exposure și Kopis.

Având în vedere aspectele specifice de monitorizat, precum traficul și infrastructura DNS, precum și listele de blacklist și whitelist, se pot utiliza tehnologii și metode precum analiza datelor și algoritmi de învățare automată (ML) pentru clasificări și predicții.

3.3. Liste de tip blacklist

Există mai multe instrumente de verificare a listelor de tip blacklist de domenii disponibile pentru a verifica dacă un domeniu a fost inclus pe listă. Câteva dintre cele mai utilizate astfel de instrumente sunt:

3.3.1. Spamhaus

Este unul dintre principalii furnizori de blacklists pentru identificarea și blocarea spam-ului, a programelor malware și a altor activități malițioase. Spamhaus Block List (SBL) include o bază de date cuprinzătoare a surselor cunoscute de spam, în timp ce Exploits Block List (XBL) se concentrează pe identificarea adreselor IP ale mașinilor infectate care participă la activități de tip botnet (The Spamhaus Team, 2021).

Spamhaus oferă, de asemenea, alte liste, precum Policy Block List (PBL) pentru identificarea adreselor IP dinamice și Domain Block List (DBL) pentru blocarea domeniilor asociate cu spam sau malware.

Spamhaus DBL este o listă de nume de domenii cu reputație proastă. Aceasta este publicată în format DNSBL (Domain Name System Block List) de domenii. Aceste reputații ale domeniilor sunt calculate pe baza mai multor factori și sunt păstrate într-o bază de date care, la rândul ei, alimentează zona DBL.

Zona DBL poate fi interogată public, cu răspunsuri în timp real, la fel ca și alte zone DNSBL Spamhaus. Cei care utilizează un software de server de e-mail capabil să scaneze anteturile și corpurile mesajelor pentru URI-uri pot utiliza DBL pentru a identifica, clasifica sau respinge e-mailurile care conțin domenii incluse în lista DBL. Profesioniștii în domeniul securității și cercetătorii folosesc, de asemenea, reputația domeniului în activitatea lor.

DNSBL este o bază de date care este interogată în timp real de către serverele de poștă electronică în scopul de a obține o opinie cu privire la originea e-mailurilor primite. Rolul unei DNSBL, precum sistemul de consiliere SBL/XBL/PBL al Spamhaus, este de a oferi o opinie cu privire la faptul că o anumită adresă IP respectă politica proprie a Spamhaus de acceptare a e-mailurilor primite.

Baza de date de reputație este întreținută de o echipă de specialiști dedicați care utilizează diverse date din mai multe surse pentru a crea și menține un set mare de reguli care controlează un sistem automatizat care analizează în mod constant o mare parte din fluxul mondial de e-mail și domeniile din acesta.

Cele mai multe listări DBL se fac automat, deși, dacă este necesar, cercetătorii Spamhaus adaugă sau elimină listări manual. Datele DBL fac obiectul unui schimb cu alte sisteme Spamhaus, ceea ce poate duce la noi listări în DBL sau la includerea unor adrese IP în alte zone Spamhaus.

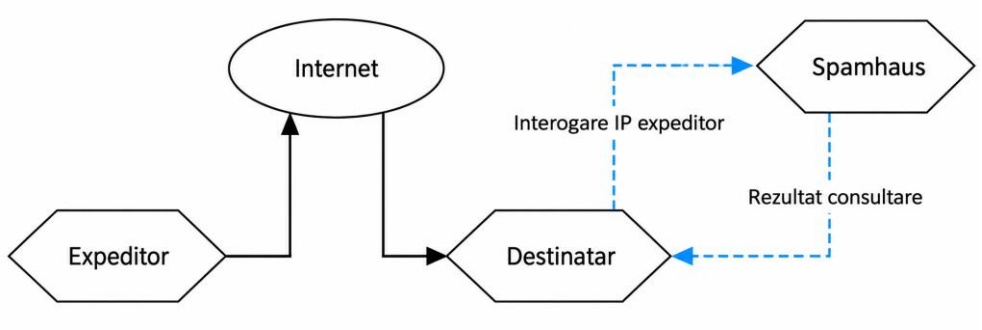


Figura 4. Consultarea unei surse de reputație în fluxul de e-mail
(The Spamhaus Team, 2021)

DBL funcționează atât ca o listă de blocare URI a domeniului, cât și ca o listă de blocare pe partea dreaptă (RHSBL). Este eficientă pentru filtrarea e-mailurilor în timpul sesiunii SMTP pentru toate verificările de antet - domeniile rDNS, HELO, MAIL FROM, From, Reply-To și Message-ID - precum și pentru URL-urile din mesaje. DBL este utilizat pe scară largă de multe părți, atât mari, cât și mici, pentru verificări care implică reputația domeniilor, în e-mail și în alte aplicații.

DBL este gestionată ca o listă și poate fi utilizată în siguranță de către sistemele de e-mail pentru a respinge e-mailurile care sunt marcate de aceasta. În plus, poate fi utilizată pentru etichetare, notare sau pliere. DBL include domenii care sunt utilizate în e-mailuri nesolicitate în masă, inclusiv phishing, fraudă sau trimiterea sau găzduirea de programe malware sau viruși, precum și alte domenii cu reputație proastă din cauza multor euristici.

DBL are un sistem de eliminare monitorizat, automatizat și cu autoservire. Listele DBL expiră, de asemenea, în mod automat după ce domeniile dispar din uzul comun sau pe măsură ce factorii de reputație se schimbă.

3.3.2. Surbl

The Spam URI Real-Time Blacklist (SURBL, 2026a) este concepută pentru a bloca domeniile și URL-urile regăsite în mesajele spam. Funcționează prin extragerea URL-urilor din conținutul e-mailurilor și compararea lor cu baza de date a domeniilor cunoscute ca fiind legate de spam. SURBL asigură detectarea în timp real și poate ajuta la prevenirea accesului utilizatorilor la site-uri web malițioase legate în e-mailurile spam.

SURBL este specializată în date de reputație furnizate în fluxuri aproape în timp real. Aceste date pot fi utilizate pentru a securiza fluxul de corespondență, comunicațiile mobile (SMS), accesul la Internet (navigare sigură, firewall-uri DNS) și multe alte activități. Cel mai cunoscut set de date este Multi, furnizat public. Acestea nu se limitează la operațiunile de poștă electronică. În prezent, SURBL oferă adrese criptografice, numere de telefon, o listă de surse de e-mail și fluxuri de domenii nou activate.

Multe dintre fluxuri sunt disponibile ca RPZ (Response Policy Zone). Seturile de date RPZ pot fi utilizate pentru a declanșa acțiuni în firewall-urile DNS, de exemplu, pentru a bloca accesul la site-uri periculoase (SURBL, 2026b; SURBL, 2026c).

3.3.3. Multi

Domeniile site-urilor web malițioase sau abuzive sunt enumerate în acest set de date. Indiferent de adresele IP ale expeditorului, acesta poate fi folosit pentru a filtra sau clasifica mesajele nesolicitate pe baza linkurilor din conținutul mesajului. Filtrarea bazată pe IP-uri cunoscute ale expeditorului rău intenționat este completată cel mai bine de aceasta.

Seturile de date SURBL s-au dovedit a fi o abordare extrem de eficientă pentru a identifica 95% din mesajele nesolicitate atunci când sunt combinate cu liste de expeditori. Multi are o variantă RPZ care este accesibilă privat.

3.3.4. Fresh

Fresh este o listă a domeniilor care au fost adăugate recent la delegările de fișiere de zonă TLD. Aceasta include o marcă de timp a momentului în care a fost detectată cea mai recentă modificare și, prin urmare, oferă o indicație a domeniilor delegate recent. Deoarece este mai probabil ca domeniile mai noi să fie abuzive, acest lucru poate fi folosit ca unul dintre mai mulți factori pentru a indica reputația domeniului.

3.3.5. HashBL

HashBL este o listă de hash-uri criptografice pentru diverse elemente legate de abuzuri pe Internet. Acest set de date este în continuă creștere, fiind adăugate noi categorii. În prezent sunt identificate următoarele:

- Furnizori de cloud public abuzivi
- Adrese de e-mail abuzive
- Liste complete de URI
- Linkuri de prescurtare abuzive
- Liste de adrese criptografice
- Liste de numere de telefon

3.3.6. Lista domeniilor bazate pe prescurtări

Lista domeniilor de prescurtare este o listă a serviciilor de prescurtare URI cele mai cunoscute, de la cele majore precum bit.ly, t.co, la multe altele. Acestea funcționează prin maparea unei adrese web lungi într-o bază de date și generarea unui identificator scurt, trimițând o comandă de redirecționare automată în browser ori de câte ori codul comprimat este accesat de un utilizator.

Principalul risc de securitate constă în mascarea totală a destinației reale, ceea ce împiedică utilizatorul să verifice structura domeniului și îl expune direct la atacuri de tip phishing sau la pagini web compromise. De asemenea, atacatorii pot folosi redirecționări dinamice pentru a schimba destinația finală după ce linkul a fost distribuit sau pot profita de reputația curată a serviciilor mari de prescurtare pentru a păcăli filtrele automate de securitate ale platformelor de mesagerie și e-mail. În plus, aceste servicii înregistrează automat date detaliate despre rețea, precum adresa IP, tipul de dispozitiv și locația geografică a fiecărei persoane care apasă pe link, oferind atacatorilor informații utile pentru personalizarea fraudelor cibernetice.

3.3.7. UriQ

URI Query (UriQ) este un API destinat verificării URI-urilor complete, ceea ce permite evaluarea unei adrese specifice, incluzând domeniul, calea către resursă și parametrii de interogare. Acesta este util în special pentru site-urile legitime care au fost compromise sau pe care sunt găzduite resurse abuzive, deoarece conținutul periculos poate fi limitat la anumite pagini sau secțiuni. În astfel de situații, includerea întregului domeniu sau a adresei IP în setul principal de date ar putea afecta și resursele legitime disponibile pe aceeași infrastructură. Prin verificarea la nivel de URI, UriQ permite o identificare mai precisă a resurselor vizate și susține aplicarea unor măsuri de filtrare selective, reducând riscul blocării nejustificate a întregului site.

3.3.8. Uribl

URI Blacklist (URIBL) este un serviciu cuprinzător de blacklists care vizează domeniile asociate cu spam, malware și alte activități rău intenționate. URIBL menține mai multe liste, inclusiv listele ABUSE, MULTI și RHS, fiecare dintre acestea având domenii de interes diferite. Lista ABUSE identifică domeniile asociate cu abuzuri, în timp ce lista MULTI detectează spam, malware și alte activități rău intenționate. Lista RHS se concentrează pe identificarea domeniilor care nu respectă standardele corespunzătoare de înregistrare a domeniilor.

Listele publice URIBL:

- black.uribl.com conține nume de domenii care aparțin și sunt utilizate de spammer-i, dar fără a se limita la acestea, cele care apar în URI-uri găsite în e-mailuri nesolicitate bulk și/sau comerciale (UBE/UCE). Această listă are ca obiectiv zero răspunsuri fals-pozitive. Această zonă se reconstruiește frecvent, pe măsură ce se adaugă noi date.
- grey.uribl.com conține domenii găsite în UBE/UCE. Poate include ESP-uri care permit clienților să își importe listele de destinatari și este posibil să nu aibă niciun control asupra metodelor de abonare. Această listă poate provoca rezultate fals pozitive, în funcție de definiția pe care o dați UBE/UCE. Această zonă se reconstruiește de mai multe ori pe zi, după cum este necesar.

- red.uribl.com conține domenii care apar în mod activ în fluxul de corespondență, nu sunt listate pe URIBL black și sunt fie monitorizate, fie foarte tinere (vârsta domeniului prin whois), fie folosesc caracteristici de confidențialitate whois pentru a-și proteja identitatea. Această listă este de natură automatizată.
- white.uribl.com conține nume de domenii legale pe care nu le dorim să apară pe alte liste URIBL. Această listă este destul de statică, cu doar câteva modificări pe zi. Această zonă se reconstruiește în funcție de necesități.
- multi.uribl.com verifică dacă un domeniu se află pe una dintre liste. Această zonă se reconstruiește dacă oricare dintre zonele de mai sus este reconstruită, cu excepția zonei albe.

3.3.9. Barracuda Reputation Block List (BRBL)

BRBL este o blacklist utilizată pe scară largă de către produsele de securitate Barracuda Networks (Barracuda Networks, 2026). Aceasta se concentrează pe identificarea adreselor IP asociate cu activități de spam. BRBL asigură blocarea în timp real a e-mailurilor nedorite prin verificarea reputației adresei IP expeditoare în baza sa de date

BRBL utilizează o implementare standard DNSBL (Domain Name System Block List) care poate fi utilizată pentru a reduce volumul de spam pe multe sisteme de e-mail populare, inclusiv Microsoft Exchange, IBM Lotus Domino, sendmail, Postfix și qmail, precum și de multe soluții antispam, precum Barracuda Spam & Virus Firewall.

Sistemele DNSBL enumeră adresele IP, adesea cele care au fost observate de operatorul listei ca fiind cele care trimit spam sau găzduiesc spammer-i. Prin adăugarea de intrări DNSBL în configurația unui server de e-mail, aceste servere pot fie să respingă încercările de conectare de la adresele IP listate, fie să folosească lista pentru a aplica politica de filtrare corespunzătoare.

DNSBL-urile sunt uneori denumite RBL-uri (Realtime Blackhole Lists) sau doar BL-uri (Block/Black lists). Este important de reținut că un DNSBL nu poate împiedica pe nimeni să trimită e-mailuri, împiedică doar livrarea la primitor, la instrucțiunile destinatarului. DNSBL-urile sunt instrumente strict defensive și nu pot provoca daune ofensive, precum atacuri denial-of-service (DDoS).

BRBL oferă o listă a adreselor IP care trimit spam. Sistemul Barracuda Reputation utilizează metode de colectare automată pentru a adăuga și șterge adrese IP din BRBL.

Sistemul automatizat de captare, colectare și clasificare a spam-ului adaugă automat adrese IP pe listă atunci când este detectat spam-ul. Atunci când se primește un e-mail, conexiunea este analizată automat pentru a determina dacă mașina care se conectează este fie un proxy deschis, fie un nod al unui botnet care generează spam. În oricare dintre aceste cazuri, adresa IP este adăugată imediat la lista de blocare a BRBL.

Cele mai multe adrese IP sunt listate ca urmare a trimiterii directe de spam sau viruși către detectoarele Sistemului de Reputație Barracuda. Sistemul Barracuda Reputation System detectează spam-ul prin utilizarea honeypots, adrese speciale create pentru a primi numai spam și care nu aparțin niciunui utilizator real și prin analiza activității protocolului spyware captiv. În plus, BRBL valorifică unele date derivate din Barracuda Blacklist (BBL) care este livrată firewall-urilor Barracuda Spam & Virus.

Utilizatorii care plasează mai multe computere în spatele unui sistem NAT gateway/firewall ar trebui să blocheze tot traficul de ieșire pe portul 25 de la toate computerele care nu au fost configurate și menținute explicit ca servere de e-mail.

Un singur computer infectat care trimite spam printr-o rețea care utilizează NAT poate duce la blocarea e-mailurilor din întreaga rețea locală (Barracuda Networks, 2026).

3.3.10. PhishTank

PhishTank este o blacklist condusă de o comunitate, special concepută pentru a detecta și bloca site-urile de phishing. Se bazează pe propunerile și verificarea utilizatorilor pentru a identifica și a pune pe lista neagră domeniile de phishing. PhishTank oferă un API care permite dezvoltatorilor și sistemelor de securitate să își integreze serviciile pentru o protecție proactivă împotriva atacurilor de phishing.

Acesta funcționează ca o platformă colaborativă unde utilizatorii pot trimite și verifica URL-urile sau site-urile web suspectate de phishing. PhishTank consolidează apoi aceste informații într-o bază de date cuprinzătoare, care este pusă la dispoziția publicului.

Funcționalitatea PhishTank implică mai multe etape. Utilizatorii pot înregistra la PhishTank URL-uri sau site-uri web suspecte de phishing pentru a fi analizate. Trimiterile pot fi făcute prin intermediul site-ului PhishTank sau prin intermediul API-ului său. Fiecare înregistrare include detalii despre site-ul suspectat de phishing, precum URL-ul și orice comentarii sau dovezi suplimentare.

Odată ce o înregistrare este făcută, aceasta trece printr-un proces de verificare. Comunitatea PhishTank, formată atât din voluntari, cât și din profesioniști în domeniul securității, analizează URL-urile trimise pentru a determina dacă acestea sunt într-adevăr site-uri de phishing.

Această abordare bazată pe comunitate contribuie la asigurarea unei game diverse de perspective și expertiză în identificarea tentativelor de phishing.

Membrii comunității pot vota cu privire la legitimitatea fiecărei sesizări, indicând dacă sunt de părere că URL-ul sau site-ul este sau nu o tentativă de phishing. Acest sistem de vot ajută la determinarea consensului dintre utilizatori și contribuie la scorul general de reputație al URL-urilor trimise.

PhishTank menține o bază de date cuprinzătoare cu URL-uri și site-uri web de phishing verificate. Această bază de date este actualizată în mod regulat și pusă la dispoziția publicului prin intermediul site-ului și al API. Utilizatorii pot interoga

baza de date pentru a verifica dacă un anumit URL este marcat ca fiind un site de phishing.

API-ul PhishTank permite integrarea cu diverse produse de securitate, browsere web și clienți de e-mail. Aceste integrări permit o protecție proactivă împotriva atacurilor de phishing prin compararea URL-urilor vizitate sau a e-mailurilor primite cu baza de date PhishTank. În cazul în care se găsește o potrivire, pot fi implementate avertismente sau blocaje adecvate pentru a împiedica utilizatorii să acceseze conținut de phishing.

PhishTank servește ca o resursă valoroasă în lupta împotriva atacurilor de tip phishing. Organizațiile și persoanele fizice pot utiliza baza de date și API-ul PhishTank pentru a-și îmbunătăți măsurile de securitate și pentru a proteja utilizatorii împotriva victimelor escrocheriilor de tip phishing.

3.3.11. Malwaredomains.com

Malwaredomains.com este o platformă dedicată furnizării de informații despre domeniile asociate distribuirii de programe malware, fiind cunoscută prin proiectul DNS-BH – Malware Domain Blacklist. Aceasta pune la dispoziție o listă de domenii identificate ca fiind utilizate pentru propagarea de software malițios, oferind o sursă de informații pentru identificarea și filtrarea destinațiilor periculoase de pe Internet.

Într-un sistem de reputație a numelor de domenii, o asemenea listă poate constitui o sursă externă de dovezi privind activitatea malițioasă. Prezența unui domeniu în listă poate contribui la evaluarea riscului, alături de caracteristicile tehnice și de informațiile provenite din alte surse. Absența sa nu demonstrează însă că domeniul este legitim, deoarece listele de blocare nu pot acoperi toate amenințările existente. De asemenea, utilizarea unor înregistrări istorice necesită verificarea actualității acestora, întrucât comportamentul și deținătorul unui domeniu se pot modifica în timp.

3.3.12. Fukushima Blacklist

Fukushima propune dezvoltarea unui sistem blacklist cu capacitatea de a analiza caracteristicile site-urilor web rău intenționate folosind informațiile despre domeniul lor, precum Sistemul autonom (AS), blocul adresei IP, adresa IP, domeniul și registrarul și propune o blacklist care combină blocurile de adrese IP și registrarii cu o reputație scăzută, care sunt frecvent utilizate de atacatori (Fukushima, Hori & Sakurai, 2011).

3.4. Liste de tip Whitelists

Aceste liste sunt de trei tipuri specifice unei aplicații, bazate pe reputație și bazate pe domenii.

3.4.1. Whitelists specifice unei aplicații

Listele de tip *whitelists*, denumite și liste de încredere sau liste de permisiuni, reprezintă un mecanism prin care anumite entități sunt aprobate explicit pentru accesarea unor resurse sau pentru realizarea unor interacțiuni cu un sistem informatic. În contextul securității numelor de domenii, acestea pot include domenii, subdomenii sau adrese web acceptate în conformitate cu politica de securitate a organizației. Includerea într-o astfel de listă exprimă o decizie de încredere într-un context determinat, fără a constitui o garanție permanentă privind absența comportamentului malițios.

Spre deosebire de listele de blocare, care identifică entități pentru care se aplică restricții, listele de încredere stabilesc entitățile cărora li se acordă anumite permisiuni. Într-un sistem cu acces restrictiv, acestea pot defini singurele destinații acceptate. În alte implementări, ele funcționează ca mecanisme de excepție, prin care anumite comunicări sunt permise sau sunt tratate diferit de regulile generale de filtrare. Efectul unei înregistrări depinde, prin urmare, de configurația sistemului și de controalele asupra cărora aceasta acționează.

Pentru analiza utilizării lor în evaluarea reputației domeniilor, pot fi diferențiate trei perspective: liste specifice unei aplicații, liste construite pe baza reputației și liste definite explicit la nivel de domeniu. Aceste categorii nu sunt reciproc exclusive, deoarece descriu dimensiuni diferite: contextul utilizării, criteriul acordării încrederii și nivelul de identificare a entității aprobate. Astfel, o listă utilizată de o aplicație de e-mail poate conține domenii selectate pe baza reputației și a relațiilor organizaționale.

3.4.2. Whitelists bazate pe reputație

Listele de încredere bazate pe reputație reunesc entități selectate în urma evaluării unor informații despre istoricul și comportamentul acestora. În această abordare, includerea într-o listă rezultă dintr-un proces de analiză, care poate lua în considerare stabilitatea utilizării domeniului, incidentele cunoscute, comportamentul comunicațiilor și concordanța informațiilor provenite din surse diferite.

Este necesară diferențierea între un serviciu de reputație și o listă de încredere. Un serviciu de reputație poate furniza scoruri sau categorii de risc, fără a publica o listă explicită de domenii aprobate. Transformarea acestor evaluări în permisiuni reprezintă o decizie suplimentară, stabilită prin politica organizației. Documentația Cisco Secure Email Gateway tratează separat evaluarea reputației domeniului expeditor și listele de excepții care pot determina omiterea acestei verificări pentru anumite domenii.

Construirea unei liste pe baza reputației necesită criterii explicite de acceptare. Absența unui domeniu din listele de blocare nu este suficientă pentru atribuirea unui statut de încredere, deoarece poate reflecta și lipsa observațiilor. În mod similar, vechimea unui domeniu sau utilizarea unui certificat digital valid poate contribui la evaluare, dar nu demonstrează, în mod independent, legitimitatea activității sale.

Decizia trebuie să țină seama de ansamblul dovezilor disponibile și de actualitatea acestora.

Reputația are un caracter dinamic. Un domeniu cu un istoric favorabil poate fi compromis, transferat unui alt deținător sau utilizat ulterior în scopuri diferite. În consecință, apartenența la o listă de încredere trebuie reevaluată periodic și atunci când apar informații noi relevante. Pentru trasabilitate, fiecare înregistrare poate fi însoțită de sursa informațiilor, motivul aprobării, data ultimei verificări și condițiile în care încrederea trebuie retrasă.

Organizațiile pot menține și liste interne ale domeniilor asociate furnizorilor, partenerilor sau instituțiilor cu care colaborează. În aceste situații, încrederea se bazează atât pe observații tehnice, cât și pe verificarea relației organizaționale. Existența unei relații contractuale justifică necesitatea comunicării, însă nu elimină posibilitatea compromiterii infrastructurii partenerului. Prin urmare, aprobarea accesului trebuie însoțită de monitorizare și de posibilitatea revocării rapide a permisiunilor.

3.4.3. Whitelists bazate pe domenii

Listele de încredere bazate pe domenii identifică explicit numele pentru care se acordă anumite permisiuni. Spre deosebire de categoria anterioară, definită prin criteriul reputației, această categorie descrie nivelul la care este aplicată regula. Un domeniu poate fi inclus în urma unei evaluări tehnice, a unei verificări administrative sau a unei cerințe operaționale.

Un aspect esențial este delimitarea domeniului aprobat de subdomeniile sale. O regulă aplicată exclusiv unui nume de gazdă are un efect mai restrâns decât una care include toate subdomeniile. De exemplu, aprobarea unei aplicații găzduite pe un anumit subdomeniu nu justifică automat acordarea acelorași permisiuni tuturor serviciilor administrate sub domeniul principal. Această distincție este relevantă mai ales atunci când diferite secțiuni ale infrastructurii sunt gestionate de entități distincte sau permit publicarea de conținut de către utilizatori.

În sistemele de filtrare a conținutului, listele de domenii pot permite accesul la resurse educaționale, administrative sau profesionale, conform politicii organizației. Încrederea are aici și o dimensiune funcțională: domeniul este aprobat deoarece oferă resurse necesare activității. Această aprobare nu trebuie confundată cu o evaluare completă a securității tuturor paginilor disponibile.

În cazul resurselor web, nivelul de domeniu poate fi insuficient de precis. Un site legitim poate conține o pagină compromisă, în timp ce restul conținutului rămâne neafectat. Într-o asemenea situație, o permisiune generală pentru întregul domeniu poate diminua eficacitatea filtrării. Acolo unde sistemul permite, regulile pot fi restrânse la anumite nume de gazdă sau adrese URI, pentru a reflecta mai fidel resursele aprobate.

Gestionarea listelor presupune și definirea modului de tratare a conflictelor. Un domeniu aprobat anterior poate apărea ulterior într-o sursă de informații despre amenințări. Politica sistemului trebuie să stabilească dacă permisiunea este

suspendată, dacă se solicită verificarea unui administrator sau dacă sunt aplicate controale suplimentare. Decizia și justificarea acesteia trebuie înregistrate pentru a permite auditarea modificărilor.

Eficacitatea listelor de încredere depinde de precizia criteriilor de includere, de limitarea permisiunilor acordate și de actualizarea înregistrărilor. O listă prea restrictivă poate întrerupe comunicații legitime, în timp ce una prea permisivă poate crea excepții exploatabile. Administrarea sa trebuie să includă responsabilități clare pentru aprobare, revizuire și eliminare, precum și păstrarea istoricului deciziilor.

Într-un sistem de reputație a numelor de domenii, apartenența la o listă de încredere poate fi utilizată ca dovadă favorabilă, analizată împreună cu indicatorii tehnici, semnalările de abuz și informațiile furnizate de operatori.

Combinarea listelor de încredere cu listele de blocare necesită reguli explicite privind prioritatea dovezilor și actualitatea acestora. O aprobare istorică nu ar trebui să anuleze automat o semnalare recentă și verificată de compromitere, iar retragerea încrederii trebuie să poată fi realizată atunci când apar dovezi relevante.

3.5. Monitorizarea inteligentă a domeniilor de Internet

Monitorizarea inteligentă a domeniilor Internet reprezintă un proces de supraveghere și evaluare a domeniilor web pentru a identifica potențiale amenințări, probleme de securitate sau comportamente nefavorabile. Această monitorizare se bazează pe tehnologii avansate precum analiza automată a conținutului, algoritmi de învățare automată și inteligență artificială pentru a identifica și raporta informații relevante despre domeniile web.

Platformele de monitorizare inteligentă pot analiza diferite aspecte ale domeniilor Internet, precum reputația, securitatea, autenticitatea și respectarea standardelor și reglementărilor. Acestea colectează și analizează informații din diverse surse, inclusiv baze de date publice, blacklists, rapoarte de securitate și feedback-ul utilizatorilor, pentru a evalua starea domeniilor web.

Principalele beneficii ale monitorizării inteligente a domeniilor de Internet includ:

- Identificarea și prevenirea amenințărilor. Prin analiza automată a conținutului și a comportamentului domeniilor web, platforma poate detecta site-uri web cu conținut malițios, phishing, malware sau alte amenințări de securitate. Astfel, utilizatorii pot fi avertizați în timp util și pot lua măsuri pentru a se proteja împotriva acestor amenințări.
- Verificarea autenticității domeniilor. Monitorizarea inteligentă poate verifica informațiile de înregistrare ale domeniilor și poate identifica site-uri web care încearcă să se prezinte sub o identitate falsă sau să încalce drepturile de proprietate intelectuală. Aceasta ajută la prevenirea fraudei online și asigură că utilizatorii interacționează cu domenii legitime.
- Evaluarea reputației domeniilor. Platforma poate analiza istoricul domeniilor web și feedback-ul utilizatorilor pentru a evalua reputația

acestora. Astfel, utilizatorii pot avea o perspectivă mai clară asupra calității și încrederii unui domeniu înainte de a interacționa cu acesta.

- Monitorizarea conformității. Prin evaluarea respectării standardelor și reglementărilor, platforma poate identifica domenii care încalcă legile privind protecția datelor, drepturile de autor sau alte reglementări relevante. Acest lucru ajută la menținerea unui mediu online sigur și etic.

Starea actuală a monitorizării inteligente a domeniilor Internet reflectă progrese semnificative în utilizarea tehnologiilor avansate și a metodelor de analiză pentru a identifica și evalua domeniile web.

Tehnologiile de analiză automată a conținutului, precum analiza semantică, procesarea limbajului natural și recunoașterea imaginilor, au avansat considerabil. Aceste tehnici permit identificarea și clasificarea automată a conținutului de pe site-urile web, facilitând detectarea conținutului rău intenționat, spamului sau altor tipuri de activități nedorite.

Algoritmii de învățare automată și inteligența artificială sunt folosiți pentru a antrena modele și algoritmi care pot identifica și clasifica domeniile web în funcție de diferiți factori, precum securitatea, autenticitatea sau reputația. Acești algoritmi pot învăța din datele de antrenare și pot oferi rezultate din ce în ce mai precise în evaluarea domeniilor.

Tehnologiile blockchain sunt utilizate pentru a asigura verificarea autenticității domeniilor web. Aceste tehnologii permit înregistrarea și urmărirea tranzacțiilor și schimbului de proprietăți ale domeniilor, reducând riscul de falsificare și sprijinind verificarea autenticității unui domeniu.

Monitorizarea inteligentă a domeniilor Internet implică adesea colaborarea între diferite entități, precum furnizorii de servicii de securitate, organizații non-guvernamentale și comunități de utilizatori. Această colaborare permite partajarea informațiilor și expertizei pentru a identifica și aborda problemele de securitate și reputație ale domeniilor web.

Este important de menționat că evoluția tehnologică continuă să aducă îmbunătățiri în domeniul monitorizării inteligente a domeniilor Internet. Abordările inovatoare, precum utilizarea învățării profunde, tehnologiile blockchain și analiza social media, pot aduce contribuții semnificative în domeniu.

Stabilirea reputației unui domeniu Internet se referă la evaluarea și atribuirea unei valori sau a unei încrederi unui domeniu web în funcție de calitatea, integritatea și performanța sa. Este un proces prin care se colectează și se analizează informații relevante despre domeniu pentru a determina modul în care este perceput și evaluat de către utilizatori și comunitatea online.

Stabilirea reputației unui domeniu implică mai mulți factori, inclusiv:

1. Primul pas în stabilirea reputației unui domeniu îl reprezintă colectarea datelor relevante despre acesta. Aceste date pot include informații despre proprietarul domeniului, istoricul domeniului, date de înregistrare, IP-uri asociate, conținutul paginilor și altele.
2. Analiza datelor pentru a identifica caracteristicile cheie ale domeniului și pentru a evalua performanța sa în diferite domenii relevante, precum

securitatea, autenticitatea și conținutul. Această analiză poate fi realizată prin utilizarea de tehnologii de analiză automată, algoritmi de învățare automată sau prin intervenția experților.

3. Monitorizarea activității domeniului este importantă pentru a detecta orice schimbări semnificative în comportamentul sau în activitatea acestuia. Aceasta poate fi realizată prin monitorizarea traficului de pe site-ul web, detectarea de atacuri cibernetice sau de spam, analizarea feedback-ului utilizatorilor sau prin alte metode relevante.
4. Securitatea, întrucât un domeniu cu o reputație bună este asociat cu un nivel ridicat de securitate. Acesta ar trebui să fie protejat împotriva amenințărilor cibernetice, precum hacking-ul sau phishing-ul și să ofere o experiență sigură pentru utilizatori.
5. Autenticitate deoarece utilizatorii au încredere în domeniile care sunt legitime și care respectă regulile și reglementările relevante. Înregistrarea corectă a domeniului și furnizarea informațiilor corespunzătoare despre proprietarul acestuia contribuie la creșterea încrederii în reputația sa.
6. Feedback-ul utilizatorilor poate juca un rol important în stabilirea reputației unui domeniu. Opiniile și experiențele utilizatorilor cu privire la domeniu, exprimate prin recenzii, comentarii sau rating-uri, pot influența percepția și reputația sa.
7. Performanță și disponibilitate, întrucât utilizatorii se așteaptă la un timp de încărcare rapid, la un site web bine funcțional și la o experiență fără probleme în interacțiunea cu domeniul.
8. Algoritmi de evaluare și scoruri pe baza datelor colectate și a analizelor realizate pentru a atribui un scor sau o clasificare domeniului în funcție de nivelul său de reputație. Acești algoritmi pot fi antrenați să identifice modele și tendințe relevante și să ofere o evaluare obiectivă a reputației.
9. Atribuirea unei valori de reputație. Pe baza analizei datelor și a monitorizării activității domeniului, se poate atribui acestuia o valoare de reputație. Aceasta poate fi o valoare numerică sau o valoare calitativă, precum "bun", "risc mediu" sau "riscant". Această valoare poate fi utilizată pentru a ghida utilizatorii în luarea deciziilor privind interacțiunea cu domeniul.

În general, stabilirea reputației unui domeniu Internet poate fi un proces complex și continuu, care necesită o combinație de tehnologii de analiză automată, monitorizare a activității și evaluări efectuate de către operatori.

3.6. Acoperirea surselor și limitele vizibilității

O sursă de informații despre reputație observă doar o parte a activității relevante. Această parte depinde de infrastructura de colectare, de participanți, de tipurile de incidente urmărite și de regulile de publicare. Lipsa unei semnalări poate însemna absența unui incident cunoscut, dar poate reflecta și lipsa vizibilității.

În evaluare trebuie delimitate domeniile observate de sursă, domeniile pentru care există un rezultat și domeniile pentru care nu poate fi formulată o concluzie.

Acoperirea nu se reduce la numărul de înregistrări. O colecție voluminoasă poate conține observații repetate despre un segment restrâns, în timp ce o colecție mai mică poate adăuga informație despre categorii anterior absente. Într-o comparație metodologică sunt utile dimensiunea temporală, tipurile de servicii, granulația indicatorilor și proporția cazurilor care pot fi verificate. Aceste caracteristici se descriu înaintea agregării, pentru a evita echivalarea volumului cu reprezentativitatea.

Sursele prezentate în acest capitol au scopuri diferite, de la analiza pasivă a DNS până la publicarea unor liste de indicatori (Antonakakis et al., 2010; Antonakakis et al., 2011; Barracuda Networks, 2026; Bilge et al., 2011; Fukushima, Hori & Sakurai, 2011). Combinarea lor trebuie să conserve această diferență. O listă orientată spre un tip de abuz nu poate fi tratată drept registru exhaustiv al tuturor amenințărilor. O sursă bazată pe sesizări nu descrie în mod necesar aceeași populație ca o sursă de telemetrie. Compararea rezultatelor necesită o definiție comună a obiectului și a intervalului observat.

În proiectarea colectării se poate întocmi o fișă pentru fiecare sursă: scop declarat, tip de indicator, periodicitate, informație temporală, condiții de acces și limite cunoscute. Fișa nu înlocuiește verificarea calității, ci face ipotezele vizibile. Dacă furnizorul schimbă schema sau modul de publicare, modificarea trebuie consemnată. O variație a numărului de semnalări poate proveni din această schimbare și nu trebuie interpretată imediat ca variație a activității malițioase.

3.7. Independența dovezilor și concordanța aparentă

Prezența unui domeniu în mai multe surse poate crește interesul analitic, dar nu demonstrează existența mai multor observații independente. Sursele pot redistribui același indicator sau pot utiliza un furnizor comun. În acest caz, numărarea surselor produce o impresie exagerată de confirmare. Trebuie distinse numărul publicațiilor, numărul observațiilor originare și numărul mecanismelor de verificare. Numai aceste distincții permit aprecierea contribuției reale a fiecărei informații.

Când proveniența este disponibilă, observațiile pot fi grupate după sursa inițială și evenimentul descris. Dacă proveniența nu este cunoscută, dependența nu trebuie exclusă prin presupunere. Raportul poate preciza că există concordanță între publicații, fără a o numi confirmare independentă. Această formulare păstrează valoarea practică a concordanței și evită atribuirea unei certitudini care nu a fost demonstrată.

Dezacordul trebuie analizat cu aceeași atenție. Două surse pot descrie momente diferite, servicii distincte sau niveluri diferite ale numelui. Un domeniu și o gazdă de sub acesta nu reprezintă aceeași unitate de observație. O listare activă și o înregistrare istorică nu exprimă aceeași stare. Înaintea aplicării unei reguli de

prioritate între surse, operatorul trebuie să verifice dacă afirmațiile sunt într-adevăr contradictorii.

Pentru agregare, o regulă transparentă este preferabilă unei ponderări a cărei semnificație nu poate fi explicată. Regula poate cere existența unei dovezi directe, poate separa observațiile recente de cele istorice sau poate trimite cazurile contradictorii spre verificare. În toate variantele, rezultatul trebuie să păstreze legătura cu observațiile componente. Această abordare dezvoltă cerințele de trasabilitate și validare umană din materialele operaționale, fără a atribui fiecărei surse o autoritate universală.

3.8. Evaluarea utilității unei surse în timp

Utilitatea unei surse se apreciază în raport cu o sarcină. Pentru identificarea timpurie contează momentul în care informația devine disponibilă, iar pentru verificarea retrospectivă contează și persistența istoricului. O sursă poate fi utilă într-unul dintre aceste scopuri și limitată în celălalt. Evaluarea trebuie să declare dacă urmărește descoperirea unor cazuri noi, confirmarea unor alerte sau documentarea evoluției unui incident.

Un indicator de interes este contribuția suplimentară a sursei la cazurile deja cunoscute. Aceasta poate fi examinată prin compararea unei proceduri cu și fără sursa respectivă, păstrând celelalte condiții. Nu este suficientă măsurarea numărului de indicatori noi: contează dacă aceștia sunt relevanți, verificabili și disponibili la momentul util. O analiză de acest tip trebuie să evite folosirea aceleiași surse atât pentru definirea etichetelor de referință, cât și pentru demonstrarea propriei eficiențe.

Continuitatea accesului face parte din utilitate. Întreruperile, întârzierile sau modificările formatului pot afecta interpretarea scorurilor. Sistemul trebuie să distingă un rezultat negativ autentic de eșecul interogării. În caz contrar, dispariția temporară a unei surse poate produce artificial o ameliorare a reputației. Monitorizarea colectării și a disponibilității surselor, discutată în documentele de monitorizare, trebuie corelată cu monitorizarea rezultatelor analitice.

Retragerea unei surse din flux nu ar trebui să șteargă proveniența observațiilor deja utilizate. Pentru reproducerea unei evaluări istorice rămân necesare versiunea informației, data accesului și regulile de transformare. În același timp, utilizarea curentă trebuie să indice că sursa nu mai este actualizată. Separarea arhivei de fluxul activ permite păstrarea valorii documentare fără prezentarea unor informații vechi drept confirmări recente. Această separare devine esențială când se compară evoluția scorurilor pe perioade îndelungate.

4. Date și indicatori pentru reputația numelor de domenii

4.1. Unitatea de observație și domeniul

Un nume de domeniu poate desemna un domeniu sau un subdomeniu al acestuia. Pentru o analiză reproductibilă sunt necesare două câmpuri distincte: numele complet observat și domeniul asociat. Dacă sursa furnizează un URL, se păstrează și resursa originală, deoarece incidentul poate fi limitat la o cale, la o aplicație sau la un serviciu.

Normalizarea nu trebuie să elimine dovezi. Transformarea unui nume complet într-un domeniu de bază este utilă pentru grupare, însă pierde informație dacă înlocuiește definitiv observația inițială. Înregistrarea trebuie să permită reconstruirea formei originale, a regulii de normalizare și a rezultatului acesteia. O eroare de identificare poate extinde nejustificat o clasificare asupra unor servicii fără legătură cu incidentul.

Identificarea domeniului nu se reduce întotdeauna la selectarea ultimelor două etichete. Regula trebuie să țină seama de structura spațiului de nume și să fie verificată pe exemple relevante. Pentru caractere internaționalizate se păstrează reprezentările necesare afișării și procesării, iar egalitatea identificatorilor se stabilește după o convenție documentată.

În colectarea TLS, ținta conexiunii este gazda observată. În datele de registru, obiectul este domeniul. Îmbinarea acestor surse trebuie să conserve diferența: mai multe gazde pot partaja atribute administrative, dar pot prezenta certificate și servicii distincte. Copierea atributelor părintelui nu transformă subdomeniile în observații statistice independente.

4.2. Populația de interes și mecanismul de selecție

Un corpus experimental este un eșantion construit prin reguli de includere și excludere. El poate urmări nume active, domenii recent înregistrate, domenii semnalate sau un portofoliu administrat. Aceste populații răspund unor întrebări diferite. Rezultatele obținute pentru una dintre ele nu trebuie prezentate ca descriere exhaustivă a întregului spațiu de nume analizat.

Selectarea exemplelor benigne din clasamente de popularitate favorizează domenii vizibile și stabile. Selectarea exemplelor pozitive din liste de blocare favorizează cazuri deja observate de furnizori. Un clasificator poate învăța diferențele dintre aceste mecanisme de selecție, chiar dacă obiectivul declarat este detectarea abuzului. Documentarea sursei fiecărui exemplu permite examinarea acestei posibilități.

Distribuția claselor se stabilește prin colectare și nu reprezintă automat prevalența operațională. Echilibrarea poate facilita anumite comparații experimentale, dar modifică interpretarea preciziei și a probabilităților. Raportul trebuie să separe proporția exemplelor pozitive din corpus de frecvența abuzului în populația în care va fi folosit sistemul.

Excluderea numelor fără răspuns poate modifica selectiv populația. Domeniile deja retrase, erorile temporare și serviciile care limitează interogările pot fi afectate diferit. O regulă corectă pentru un studiu despre domenii înregistrate poate fi nepotrivită pentru un studiu al indicatorilor istorici. Alegerea se justifică prin obiectiv și se documentează înaintea evaluării.

4.3. Eticheta de referință și dezacordul dintre surse

Eticheta este rezultatul unei proceduri. Dacă provine dintr-o listă, ea exprimă apartenența la acea sursă în condițiile și la momentul importului. Termenii benign și malițios pot fi convenții utile pentru învățare, dar nu trebuie să ascundă incertitudinea, vechimea sau granulația dovezilor.

Un domeniu prezent simultan într-o listă de popularitate și într-o listă de blocare necesită o regulă explicită. Variantele includ excluderea din experiment, păstrarea unei stări de conflict sau validarea manuală. Prioritatea acordată automat unei surse este o decizie metodologică, nu o rezolvare demonstrată a contradicției. Reguli diferite trebuie evaluate separat.

Lipsa unei listări negative nu este o confirmare benignă. Un corpus trebuie să precizeze cum au fost selectate exemplele negative și ce verificări au fost realizate. Într-un registru de cazuri, o etichetă confirmată poate include evaluatorul, data, dovezile și termenul de reevaluare. Într-un set de învățare, aceste metadate ajută la filtrarea observațiilor necorespunzătoare.

Etichetele și caracteristicile trebuie aliniate temporal. Dacă un domeniu este listat la un moment și interogat mult mai târziu, indisponibilitatea observată poate descrie retragerea sa, nu semnele care ar fi permis detectarea înaintea incidentului. Un model astfel antrenat poate identifica efectele remedierii mai bine decât debutul abuzului.

4.4. Datele administrative

Vârsta domeniului exprimă o durată calculată față de momentul observației. Pentru a fi comparabilă, trebuie cunoscute câmpul sursă și tratamentul reînregistrărilor. O vechime mare nu exclude compromiterea, iar o vechime mică nu dovedește intenția malițioasă. Interpretarea aparține unei combinații de indicii.

Timpul rămas până la expirare descrie un aspect al ciclului administrativ. Reînnoirea, transferul și întârzierile de actualizare pot modifica valoarea fără schimbarea utilizării domeniului. Datele imposibile, valorile negative și diferențele de fus orar trebuie verificate înaintea calculului caracteristicilor.

Identificatorul registrarului reprezintă o categorie. Codificarea numerică nu îi conferă o ordine naturală și nu justifică interpretarea unui cod mai mare ca risc mai ridicat. O asociere statistică poate reflecta portofoliul, perioada ori sursele de etichetare. Ea nu demonstrează răspunderea registrarului pentru comportamentul unui anumit domeniu.

Starea administrativă și accesibilitatea serviciului sunt noțiuni distincte. Un domeniu înregistrat poate să nu publice un site web; un eșec al interogării nu dovedește disponibilitatea pentru înregistrare. Colectorul trebuie să separe răspunsul semantic al serviciului de erorile de transport și de restricțiile de acces.

4.5. Observațiile DNS și TLS

Observațiile DNS trebuie însoțite de tipul interogării, resolverul utilizat și momentul colectării. NXDOMAIN, SERVFAIL și REFUSED au semnificații diferite. Un răspuns din cache poate fi valid în limitele sale temporale, dar nu trebuie confundat cu o verificare autoritativă realizată la același moment.

DNSSEC permite validarea criptografică a datelor DNS în condițiile unui lanț de încredere verificabil. Prezența unui indicator de delegare nu echivalează cu verificarea completă a tuturor răspunsurilor. Indicatorul tehnic nu certifică legitimitatea conținutului, iar absența sa nu este suficientă pentru o clasificare malițioasă.

Metadatele TLS includ emitentul, intervalul de valabilitate și proprietățile conexiunii observate. Versiunea protocolului este negociată între client și server; ea nu este un atribut intrinsec al certificatului. Rezultatul depinde și de configurația colectorului, de gazda interogată și de condițiile rețelei.

Prezența unui certificat valid susține o anumită verificare tehnică a conexiunii. Ea nu garantează că un serviciu este benign. Similar, un certificat cu valabilitate scurtă sau emis de o autoritate gratuită nu justifică singur o concluzie negativă. Interpretarea cere corelare cu observații despre activitate și istoric.

O eroare de negociere, un certificat absent și un certificat care nu a putut fi interpretat sunt stări distincte. Dacă implementarea le reduce la aceeași valoare, această pierdere trebuie documentată. În exploatare, păstrarea cauzei permite reevaluarea și evită transformarea unui incident al colectorului într-o suspiciune asupra domeniului.

4.6. Valori lipsă și codificare

Datele lipsă pot avea cauze informative: un serviciu nu există, un domeniu a fost retras sau o sursă este indisponibilă. Modelul poate utiliza această structură, dar utilitatea sa trebuie verificată în condiții diferite de colectare. O corelație puternică într-un corpus nu garantează stabilitatea semnalului după schimbarea surselor.

Schema distinge valoarea observată, indicatorul de disponibilitate și cauza absenței. O valoare numerică rezervată poate fi folosită în implementare, dar nu

trebuie confundată cu o măsurătoare reală. Transformările se învață în interiorul partițiilor de antrenare și se aplică identic datelor de evaluare.

Codificarea categorială trebuie să trateze explicit categoriile necunoscute. Emitenții noi și registrarii care nu apar în antrenare nu trebuie să schimbe ordinea coloanelor. Modelul se păstrează împreună cu schema de preprocesare, astfel încât inferența să reproducă aceleași transformări.

4.7. Calitatea colectării și reproducibilitatea

Colectarea la scară necesită limite de concurență, termene de așteptare și repetări controlate. Scopul este obținerea unor observații interpretabile, nu maximizarea necondiționată a numărului de cereri. Repetările trebuie să păstreze diferența dintre prima observație și rezultatul ulterior.

Un raport de colectare consemnează numărul intrărilor inițiale, duplicatele, excluderile, erorile și observațiile finale. Numărul domeniilor distincte se raportează separat de numărul rândurilor. Acest control permite identificarea diferențelor dintre corpusuri înaintea comparării algoritmilor.

Reproductibilitatea presupune versiunea surselor, amprenta fișierelor, regulile de normalizare, configurația colectoarelor și momentul execuției. Dacă datele nu pot fi distribuite, se poate documenta schema și procedura de acces. Disponibilitatea unei descrieri nu trebuie confundată cu disponibilitatea efectivă a corpusului sau cu reexecutarea experimentului.

4.8. Organizarea temporală a observațiilor

Pentru analiza reputației, o bază de date trebuie să permită reconstruirea informației disponibile la un moment determinat. O înregistrare care păstrează numai ultima valoare este suficientă pentru unele interogări curente, dar limitează analiza retrospectivă. Când o valoare se modifică, trebuie cunoscut dacă schimbarea a fost observată în infrastructură, comunicată de o sursă sau introdusă prin corectarea unei erori. Aceste situații au semnificații diferite pentru evaluare.

O schemă temporală poate separa momentul observației, momentul colectării și momentul validării. La acestea se poate adăuga intervalul pentru care sursa declară că informația este valabilă. Nu toate sursele oferă toate aceste elemente; lipsa lor se consemnează explicit. Estimarea unei date necunoscute nu trebuie prezentată ca observație. Când se folosesc intervale aproximative, precizia temporală devine o proprietate a înregistrării și trebuie păstrată în rapoarte.

Îmbinarea datelor urmărește informația accesibilă înaintea momentului de referință. Pentru o evaluare realizată la o anumită dată, folosirea unei observații ulterioare poate schimba nejustificat problema într-una retrospectivă. Regula se aplică și transformărilor aparent neutre, precum calcularea frecvenței unui emitent sau completarea unui câmp dintr-un export ulterior. Un control util este verificarea automată a ordinii temporale dintre predicție, caracteristici și eticheta folosită pentru evaluare.

Ca exemplu metodologic, o listare publicată după detectarea unui incident nu poate fi utilizată pentru a demonstra anticiparea acelui incident. Ea poate susține confirmarea retrospectivă, dacă aceasta este întrebarea studiului. Distincția nu diminuează valoarea datelor, ci delimitează concluzia permisă. Principiile de validare și audit pot fi aplicate prin păstrarea unor instantanee identificabile și prin documentarea regulilor de selecție temporală.

4.9. Relațiile dintre observații și independența eșantionului

Rândurile unui tabel nu reprezintă automat exemple independente. Mai multe subdomenii pot aparține aceluiași domeniu, mai multe interogări pot descrie același serviciu, iar mai multe domenii pot utiliza infrastructură comună. Aceste relații pot fi informative, dar pot produce și o evaluare prea optimistă dacă exemple foarte apropiate apar simultan în antrenare și testare. Înaintea construirii partițiilor este necesară identificarea relațiilor care pot transfera informație între rânduri.

Alegerea grupului de separare depinde de întrebarea cercetării. Separarea după domeniu examinează generalizarea către alte domenii, în timp ce separarea temporală examinează comportamentul pe observații ulterioare. Separarea după infrastructură poate formula o cerință mai restrictivă, dar poate elimina și relații legitime pentru utilizarea vizată. Nu există o singură partiționare care să răspundă tuturor întrebărilor. Raportul trebuie să precizeze scenariul reprezentat de fiecare protocol.

Într-o schemă de date, relațiile se pot păstra separat de atributele obiectului. O adresă observată, un server de nume sau un certificat constituie entități cu care domeniul are o relație la un anumit moment. Relația trebuie să includă intervalul și sursa observației. În acest mod se evită transformarea unei asocieri istorice într-o caracteristică permanentă și se pot verifica mai ușor grupurile folosite la validare.

Un control practic urmărește suprapunerea identificatorilor între partiții și numărul de observații pe grup. Un grup foarte mare poate domina rezultatul chiar dacă numărul total de rânduri este ridicat. Raportarea atât a rândurilor, cât și a grupurilor distincte face această situație vizibilă. Analiza relațională descrisă de sistemele de reputație bazate pe infrastructură (Antonakakis et al., 2010; Antonakakis et al., 2011; Mishsky, Gal-Oz & Gudes, 2015) trebuie astfel însoțită de o analiză a dependenței statistice introduse prin aceste relații.

4.10. Dicționarul de date și controlul transformărilor

Un dicționar de date descrie semnificația câmpurilor înainte ca acestea să fie utilizate de algoritm. Pentru fiecare atribut sunt utile definiția, tipul, unitatea de măsură, sursa, regulile de validare și tratamentul valorilor absente. O denumire precum vârstă sau stare este insuficientă fără precizarea obiectului și a momentului de calcul. Ambiguitățile mici din schemă pot produce diferențe importante între două implementări aparent identice.

Transformările trebuie să fie verificabile. Dacă o dată calendaristică devine o durată, se documentează momentul de referință și regula de rotunjire. Dacă o categorie devine un cod, se păstrează corespondența și comportamentul pentru valori noi. Dacă mai multe observații sunt agregate, se precizează fereastra temporală și funcția utilizată. Versiunea transformării este parte a experimentului, deoarece schimbarea ei poate modifica distribuția datelor fără schimbarea surselor originale.

Datele brute și datele prelucrate au roluri complementare. Primele permit verificarea interpretării și repetarea transformărilor, iar celelalte permit utilizarea coerentă de către model. Păstrarea datelor brute nu înseamnă colectare fără limite; se reține elementele necesare scopului documentat. Când anumite informații nu pot fi păstrate, se consemnează limitarea și efectul asupra posibilității de reproducere. O amprentă de fișier confirmă identitatea unei versiuni, dar nu înlocuiește conținutul necesar reexecutării.

Controlul transformărilor poate include verificarea domeniului valorilor, a consistenței între câmpuri și a variațiilor neașteptate. Totuși, o valoare rară nu trebuie eliminată automat doar pentru că este rară. Ea poate reprezenta o eroare sau un caz relevant. Decizia de corectare, excludere ori păstrare trebuie să fie motivată și numărată în raportul de pregătire. Această disciplină dezvoltă cerințele de calitate și trasabilitate ale colectării prezentate în materialele tehnice.

4.11. Construirea unui corpus fără circularitate

Un corpus de evaluare trebuie să permită o comparație între predicție și o referință a cărei proveniență este cunoscută. Circularitatea apare când eticheta este derivată din același semnal pe care modelul îl folosește pentru a o reproduce, iar rezultatul este prezentat ca detectare independentă. Reproducerea unei reguli de listare poate fi o sarcină legitimă, dar nu trebuie confundată cu demonstrarea capacității de a identifica toate formele de abuz.

Pentru fiecare familie de caracteristici se verifică relația cu mecanismul de etichetare. Apartenența la o listă care definește clasa pozitivă nu poate fi tratată ca o dovadă independentă a performanței. Alte atribute pot transmite indirect aceeași informație, de exemplu prin stări apărute după intervenția asupra domeniului. Analiza trebuie să urmărească atât scurgerile explicite de informație, cât și relațiile temporale care fac rezultatul mai ușor decât problema operațională declarată.

Un registru al excluderilor ajută la înțelegerea corpusului final. Acesta poate consemna duplicate, conflicte între surse, identificatori nevalizi și observații fără informația minimă necesară. Categoriile de excludere trebuie să fie aplicate consecvent. Dacă o regulă afectează preponderent o clasă, efectul asupra populației evaluate trebuie discutat. Curățarea datelor nu este o etapă neutră, deoarece modifică tipurile de cazuri asupra cărora se formulează concluziile.

Pentru evaluări ulterioare, procedura de constituire trebuie să poată fi repetată fără schimbări ascunse. Se păstrează configurația, versiunile surselor, ordinea operațiilor și numărul observațiilor la fiecare etapă. O modificare justificată produce o nouă versiune a corpusului. Compararea acesteia cu versiunea precedentă trebuie

să distingă efectul noilor date de efectul algoritmului. Astfel, un progres aparent nu este atribuit automat modelului atunci când problema evaluată s-a schimbat.

Înaintea utilizării corpusului se întocmește o fișă de caracterizare. Aceasta reunește întrebarea cercetării, populația vizată, intervalul observațiilor, definiția claselor și sursele utilizate. Se indică separat numărul înregistrărilor, numărul numelor distincte și numărul domeniilor. Fișa descrie mecanismul de selecție și principalele categorii excluse, astfel încât cititorul să poată aprecia distanța dintre eșantion și populația pentru care sunt formulate concluziile.

Fișa trebuie să distingă proprietățile măsurate de ipotezele de lucru. Apartenența la o sursă poate fi verificată într-un instantaneu, în timp ce caracterul benign presupus al unui exemplu poate depinde de o convenție de selecție. Această diferență se păstrează și atunci când implementarea utilizează o etichetă binară. Simplificarea necesară algoritmului nu trebuie să elimine explicația metodologică a etichetei.

Controlul de predare către etapa de modelare verifică dacă există identificatori stabili, reguli de grupare, marcaje temporale și o versiune completă a transformărilor. Se consemnează limitările care nu au putut fi rezolvate și se indică efectul lor posibil asupra evaluării. În acest fel, capitolul următor pornește de la o problemă definită și de la date caracterizate, iar alegerea algoritmului poate fi discutată în raport cu aceste condiții.

5. Algoritmi și validarea evaluărilor de reputație

5.1. Problema de clasificare și semnificația scorului

Clasificarea supervizată presupune o matrice de caracteristici și o etichetă pentru fiecare observație. În reputația domeniilor, eticheta poate reprezenta listarea într-o sursă, confirmarea unui incident sau o decizie operațională. Aceste obiective nu sunt echivalente. Definiția țintei trebuie să însoțească rezultatele, deoarece determină ce a fost efectiv învățat și măsurat.

Scorul produs de un model poate ordona observațiile după compatibilitatea cu clasa pozitivă. Interpretarea lui ca probabilitate cere verificarea calibrării pe populația relevantă. Transformarea într-un procent și afișarea într-o interfață nu conferă singure această semnificație.

Separarea dintre scor și acțiune permite utilizări diferențiate. Un prag poate selecta cazuri pentru investigație, iar altă regulă poate stabili condițiile unei măsuri operaționale. Alegerea depinde de costul erorilor, de resursele umane și de calitatea dovezilor. Optimizarea unei metrici statistice nu înlocuiește această decizie.

Un experiment de reputație trebuie să înceapă cu întrebarea la care se dorește un răspuns. Detectarea domeniilor deja semnalate, identificarea timpurie a unor cazuri noi și prioritizarea investigațiilor sunt obiective diferite. Ele pot utiliza aceleași instrumente statistice, dar cer alte date, alte momente de referință și alte criterii de succes. Un rezultat devine dificil de interpretat atunci când obiectivul se schimbă pe parcurs, fără ca protocolul să fie adaptat și declarat.

Întrebarea poate fi transformată într-un protocol prin definirea populației, a unității de predicție și a orizontului temporal. Se precizează ce informații sunt disponibile modelului și când este observată eticheta de referință. Urmează alegerea unui model de comparație și a metricilor relevante pentru utilizare. Criteriul principal se stabilește înaintea examinării rezultatelor finale; altfel, selectarea metricii favorabile poate ascunde un compromis nefavorabil în alte dimensiuni.

Modelele Random Forest și XGBoost, prezentate în sursele de specialitate (Breiman, 2001; Chen & Guestrin, 2016), constituie metode de învățare, nu protocoale complete de evaluare. Folosirea unui algoritm consacrat nu rezolvă selecția eșantionului, dependența dintre observații sau semnificația etichetelor. Compararea trebuie să includă aceleași partiții și aceleași informații disponibile. Când bugetele de ajustare diferă, această diferență trebuie raportată, deoarece rezultatul poate reflecta și efortul de optimizare.

Un protocol clar separă analiza exploratorie de confirmarea finală. Explorarea poate sugera caracteristici și ipoteze, dar verificarea acestora necesită date care nu au orientat deja alegerile. Dacă resursele nu permit o evaluare complet independentă,

limitarea se declară. Valoarea științifică rezultă și din precizia delimitării concluziilor, nu doar din mărimea unui indicator. În acest sens, descrierea experimentului trebuie să permită cititorului să identifice exact ce a fost testat și ce rămâne deschis.

5.2. Modele de referință și comparații

Un model simplu oferă un reper pentru utilitatea complexității suplimentare. O regulă pe un singur atribut sau o regresie logistică poate arăta că mare parte din separare provine dintr-un indicator dominant. Dacă un model complex aduce un câștig redus, costurile întreținerii și interpretării sale trebuie examinate explicit.

Comparația utilizează aceleași observații, etichete și partiții. Preprocesarea, tratarea valorilor lipsă și selecția pragului trebuie controlate, deoarece diferențele dintre ele pot explica aparenta superioritate a unui algoritm. Protocolul de selecție a hiperparametrilor se documentează înaintea examinării rezultatului final.

Random Forest și XGBoost sunt doi dintre cei mai utilizați algoritmi de învățare automată supravegheată, datorită capacității lor de a obține performanțe ridicate într-o varietate largă de probleme, de la clasificare binară și multi-clasă până la regresie. Deși ambele metode folosesc arbori de decizie ca elemente de bază, diferențele dintre ele sunt fundamentale, în special în ceea ce privește arhitectura de ansamblu, modul de învățare, strategia de combinare a predicțiilor și sensibilitatea la hiperparametri.

Random Forest este o metodă de tip bagging („bootstrap aggregating”), care construiește un ansamblu de arbori de decizie independenți. Fiecare arbore este antrenat pe un subset diferit al datelor de antrenament, generat prin eșantionare aleatorie cu înlocuire. În plus, la fiecare nod din arbore, selecția variabilelor candidate pentru divizare este restricționată la un subset aleatoriu al caracteristicilor disponibile.

Această combinație în selecția datelor și a variabilelor face ca arborii individuali să fie diverși, reducând corelațiile dintre ei și, implicit, variabilitatea modelului final. După antrenare, predicția finală este obținută prin agregarea predicțiilor individuale, astfel încât în cazul clasificării, se utilizează votul majoritar, iar în cazul regresiei, media aritmetică.

Random Forest este cunoscut pentru capacitatea sa de a gestiona seturi de date cu multe caracteristici, inclusiv caracteristici redundante sau irelevante, datorită mecanismului intern de selecție aleatorie. De asemenea, este tolerant la date zgomotoase și oferă măsuri de importanță a caracteristicilor, care sunt utile pentru interpretabilitate.

Cu toate acestea, Random Forest poate deveni ineficient atunci când vine vorba de detalii subtile în date, întrucât abordarea paralelă limitează capacitatea de învățare iterativă sau corectivă.

XGBoost, prescurtare pentru eXtreme Gradient Boosting, aparține familiei boosting-ului, care adoptă o abordare complet diferită. În loc să construiască arbori

în paralel și independent, boosting-ul construiește arborii secvențial, fiecare nou arbore fiind antrenat pentru a corecta erorile comise de modelul anterior.

XGBoost aplică o metodă de optimizare a unei funcții obiectiv, care combină o funcție de pierdere (de exemplu eroare logaritmică, eroare pătratică medie etc.) cu un termen de regularizare, menit să penalizeze modelele prea complexe. Prin această abordare, XGBoost învață în mod aditiv, adăugând arbori care contribuie treptat la reducerea pierderii globale. Spre deosebire de metodele clasice de boosting, XGBoost integrează optimizări semnificative la nivel de implementare precum suport pentru paralelizare în construirea arborilor, gestionarea inteligentă a valorilor lipsă, reducerea complexității prin „pruning" și regularizare.

Un alt avantaj major al XGBoost este precizia sa în sarcini dificile, în special în seturi de date etichetate cu dezechilibre mari sau cu relații non-liniare complexe. Cu toate acestea, eficiența modelului depinde considerabil de selecția atentă a hiperparametrilor, precum rata de învățare (learning rate), numărul de arbori (estimatori), adâncimea maximă a fiecărui arbore, subsampling-ul datelor sau caracteristicilor și regulile de regularizare.

Antrenarea unui model XGBoost poate necesita o etapă de validare atentă și ajustări iterative, dar rezultatele sunt adesea remarcabile în ceea ce privește scorurile de precizie, recall, F1 sau AUC.

Alegerea dintre Random Forest și XGBoost depinde de structura datelor, metoda de validare și resursele disponibile pentru reglarea hiperparametrilor. Superioritatea unui algoritm trebuie demonstrată prin comparații realizate pe aceleași partiții și cu același protocol de evaluare.

Random Forest combină arbori antrenați pe eșantioane și subseturi de caracteristici, în timp ce XGBoost adaugă succesiv arbori pentru reducerea erorii funcției obiectiv. Diferența metodologică motivează evaluarea comparativă, fără a justifica o ierarhie universală a performanței.

5.3. Criterii de acceptanță și trasabilitate

Criteriile de acceptanță trebuie definite înainte de rularea testelor pentru a evita selectarea retrospectivă a unor praguri favorabile. Pentru metricile ML, baseline-ul îl reprezintă performanța raportată anterior, însă validarea curentă trebuie să urmărească reproducerea rezultatelor și identificarea variației. Pentru serviciile web, pragurile de latență trebuie stabilite separat pentru inferența pură și pentru evaluarea completă, deoarece interogările WHOIS, DNS și TLS introduc timpi externi care nu sunt controlați de model.

Trasabilitatea se realizează printr-o matrice Cerință–Test–Rezultat–Acțiune. În cazul unui test eșuat, raportul trebuie să indice dacă problema este blocantă, dacă există un mecanism de fallback și dacă problema afectează scorul de reputație sau doar disponibilitatea unei informații auxiliare. Această clasificare simplifică prioritizarea remedierilor.

Tabelul 2. Trasabilitate

ID	Cerință	Test	Criteriu
VAL-01	Modelul discriminează cele două clase	set de test rezervat	metricile rămân apropiate de baseline și nu apar regresii majore
INT-01	Colectarea externă nu blochează serviciul	timeout DNS/TLS	răspuns controlat și logare
FUN-01	Utilizatorul poate analiza un domeniu	flux end-to-end	rezultat afișat fără eroare
SEC-01	Inputul este validat	input invalid/malițios	cererea este respinsă fără executarea necontrolată
PERF-01	Inferența pură este rapidă	benchmark concurent	latență stabilă și error rate redus

5.4. Caracteristicile utilizate și preprocesarea

Validarea unui corpus începe cu verificarea compoziției, a surselor și a unității de observație. Distribuția claselor se raportează explicit, împreună cu regulile de tratare a conflictelor. Corpusurile folosite efectiv în această carte și rezultatele lor sunt prezentate în Capitolul 11; nu sunt utilizate seturile experimentale din predări.

În etapa de validare, setul trebuie verificat pentru duplicate, domenii inactive, suprapuneri între surse și intrări care corespund aceluiași domeniu. O atenție specială trebuie acordată contaminării între train și test. Dacă același domeniu sau entități strâns legate apar în ambele subseturi, performanța poate fi supraestimată. În plus, sursele de blacklist pot conține domenii legitime compromise, ceea ce înseamnă că eticheta „malițios” descrie un status la un moment de timp, nu neapărat intenția inițială de înregistrare.

Pentru reproductibilitate se recomandă ca validarea curentă să păstreze un snapshot al datelor și un identificator al sursei. Orice reîmprospătare a listelor externe trebuie tratată ca o versiune nouă a setului de date, deoarece modificarea compoziției poate schimba distribuția caracteristicilor și poate afecta interpretarea scorurilor.

O atenție suplimentară trebuie acordată dimensiunii temporale a etichetelor. Statutul unui domeniu se poate modifica: un domeniu legitim poate fi compromis, iar un domeniu care a găzduit conținut malițios poate fi ulterior dezactivat sau transferat. Din acest motiv, eticheta și caracteristicile tehnice ar trebui asociate aceluiași interval temporal. Colectarea caracteristicilor mult după momentul în care domeniul a fost introdus într-o blacklist poate altera relația dintre date și etichetă și poate conduce la concluzii prea optimiste despre performanța modelului.

Validarea setului de date trebuie să păstreze și trasabilitatea sursei. Pentru fiecare intrare este util să se cunoască originea etichetei, momentul importului și regulile de normalizare aplicate. Această informație permite investigarea eventualelor conflicte între surse și măsurarea dependenței modelului de anumite liste. În cazul în care o aceeași familie de domenii apare în mai multe surse, gruparea

înainte de împărțirea train/test reduce riscul ca exemple aproape identice să ajungă în ambele seturi.

Tabelul 3. Verificarea setului de date

Verificarea setului de date	Motivație	Rezultat așteptat
Duplicare	evitarea ponderării artificiale	0 duplicate după normalizare
Suprapunere whitelist/blacklist	evitarea conflictelor de etichetă	conflictele identificate și rezolvate prin regula documentată
Domenii inactive	reducerea zgomotului	intrările nevalide excluse sau marcate
Grupare domeniu	reducerea leakage-ului	entitățile înrudite nu sunt împărțite necontrolat
Snapshot temporal	reproductibilitate	data colectării și sursa sunt păstrate

Schema de caracteristici stabilește câmpurile utilizate de model și transformările acestora. Datele de registru, TLS și eventualele observații DNS trebuie diferențiate de metadatele păstrate numai pentru audit. În studiul de caz sunt folosite cele zece caracteristici specificate în tabelul dedicat; nu se presupune adăugarea altor predictori.

Validarea preprocesării trebuie să confirme că valorile booleene, categorice și numerice sunt transformate identic în timpul antrenării și al inferenței. Câmpurile lipsă trebuie tratate determinist și trebuie verificat dacă un eșec de colectare este interpretat de model ca „absența caracteristicii” sau ca „valoare necunoscută”. Diferența este importantă: un certificat absent și un certificat care nu a putut fi citit din cauza unui timeout nu reprezintă același fenomen operațional.

Regulă de validare: schema de caracteristici trebuie versionată împreună cu modelul. La încărcarea modelului, serviciul trebuie să verifice ordinea și numele coloanelor înainte de inferență.

5.5. Protocolul de evaluare

Protocolul trebuie fixat înaintea comparației. Când observațiile partajează un domeniu, partițiile se formează pe grupuri. Stratificarea păstrează proporțiile claselor, dar nu rezolvă singură dependența dintre nume. Orice validare temporală trebuie să documenteze momentele colectării și etichetării.

Setul de test trebuie menținut separat de procesul de tuning. Alegerea pragului de clasificare, calibrarea și selecția hiperparametrilor trebuie efectuate numai pe datele de antrenare și validare. După înghețarea configurației, setul rezervat este utilizat o singură dată pentru evaluarea finală. Pentru o versiune ulterioară a modelului, același set poate funcționa ca benchmark de regresie, dar este recomandată și o validare temporală pe date mai noi.

Reproductibilitatea presupune păstrarea seed-ului, a versiunilor bibliotecilor, a hiperparametrilor și a listei exacte de coloane folosite la antrenare. Un rezultat care nu poate fi reprodus pe aceeași intrare are valoare redusă pentru validare. În mod ideal, execuția trebuie să genereze automat un fișier cu parametrii experimentului și metricile obținute, împreună cu identificatorul modelului salvat.

În plus față de împărțirea stratificată, pentru o etapă ulterioară este recomandată o validare grupată sau temporală.

Validarea grupată urmărește ca domenii apropiate sau provenite din aceeași entitate logică să nu fie separate artificial între train și test, iar validarea temporală simulează mai bine utilizarea operațională.

5.6. Strategia de testare

Strategia de testare este organizată pe principiul separării responsabilităților. Testele funcționale verifică dacă un flux produce rezultatul așteptat din perspectiva utilizatorului; testele de integrare verifică schimbul de date dintre componente; testele de robustețe verifică degradarea controlată atunci când una dintre surse nu răspunde; testele de performanță măsoară timpii și capacitatea de procesare; iar validarea ML analizează separat calitatea clasificatorului. Această separare previne interpretarea unei metrici bune a modelului ca dovadă suficientă pentru funcționarea corectă a întregii platforme.

Pentru componenta ML, unitatea de evaluare este domeniul împreună cu setul său de caracteristici și eticheta de referință. Pentru serviciile de colectare, unitatea de evaluare este tranzacția de rețea sau răspunsul API. Pentru interfață, unitatea de evaluare este scenariul de utilizare, de exemplu autentificarea, căutarea unui domeniu, consultarea unui scor sau generarea unui raport. Rezultatele trebuie păstrate într-un jurnal de test care conține data, versiunea aplicației, versiunea modelului, setul de date și statusul scenariului.

Testarea trebuie să poată fi repetată după orice modificare relevantă. Din acest motiv, scenariile critice sunt formulate independent de detaliile vizuale ale interfeței. Un redesign al paginii panoul de sinteză nu trebuie să invalideze testul care verifică existența și consistența metricilor, iar schimbarea unei biblioteci de rețea nu trebuie să modifice contractul funcțional al colectării WHOIS/DNS/TLS.

Prioritizarea scenariilor se face în funcție de impact și probabilitate. Fluxurile de autentificare, evaluarea unui domeniu, încărcarea datelor de reputație și comunicarea dintre aplicația web și componenta ML sunt considerate critice, deoarece defectarea lor poate împiedica utilizarea platformei sau poate genera rezultate înșelătoare. Funcțiile auxiliare, precum elementele de prezentare sau anumite filtre neesențiale, pot fi tratate cu o prioritate inferioară, fără a elimina însă testarea lor.

Pentru fiecare defect identificat se recomandă înregistrarea severității, a pașilor de reproducere, a rezultatului așteptat, a rezultatului observat și a versiunii în care remedierea a fost verificată. În acest mod, procesul de testare devine un ciclu controlat: identificare, remediere, retestare și închidere. Reexecutarea testelor de

regresie după modificări este obligatorie pentru funcțiile critice, astfel încât o corecție locală să nu introducă efecte secundare în alte module.

Tabelul 4. Testarea sistemului

Categorie	**Scop**	**Exemple de criterii**
Validare ML	Confirmarea capacității de generalizare	Accuracy, Precision, Recall, F1, AUROC, AUPRC, stabilitate între folduri
Funcțional	Verificarea fluxurilor utilizatorului	autentificare, căutare, detalii domeniu, raportare
Integrare	Verificarea schimbului de date	Registry API → Flask → model → interfață
Robustețe	Comportament în caz de eroare	timeout (timp de așteptare), răspuns incomplet, lipsă TLS, DNS failure
Performanță	Capacitate și latență	requests/s (solicitări), mediană, p95, p99, rata de erori
Securitate	Reducerea suprafeței de atac	validare input, control acces, CSRF/XSS

Mediul de testare trebuie să separe aplicația, stocarea, colectoarele și serviciul de evaluare. Versiunile și configurațiile se consemnează pentru fiecare componentă. Interfețele registrului, DNS și TLS trebuie testate atât cu răspunsuri nominale, cât și cu erori și date incomplete.

Verificarea datelor de registru trebuie să distingă răspunsul administrativ de erorile de transport. Se testează separat răspunsurile nominale, expirarea timpului de așteptare, conexiunea refuzată și limitarea ratei. Niciun eșec de comunicare nu se transformă automat într-un verdict asupra domeniului.

Datele obținute prin API-ul registrului, de exemplu vechimea, data de expirare, DNSSEC și identificatorul registrarului trebuie validate înainte de a fi transmise modelului. O valoare lipsă sau imposibilă trebuie logată, iar serviciul trebuie să decidă explicit dacă evaluarea continuă cu un set parțial de caracteristici sau este amânată.

Tabelul 5. Testarea DAS

ID	**Scenariu**	**Rezultat așteptat**
DAS-01	domeniu înregistrat	status interpretat corect; domeniul este păstrat
DAS-02	domeniu disponibil	status interpretat corect; domeniul nu este tratat ca activ
DAS-03	timeout	eroare controlată; retry conform politicii; fără etichetare falsă
DAS-04	răspuns necunoscut	log + status necunoscut
REG-01	câmpuri lipsă din API	validare schemă și fallback explicit

Testarea DNS urmărește separat răspunsurile autoritative, rezoluția și stările de eroare. NXDOMAIN, SERVFAIL și REFUSED nu sunt echivalente. Lipsa unei înregistrări MX nu înseamnă imposibilitatea rezoluției numelui.

Tabelul 6. Testarea DNS

ID	Intrare / condiție	Așteptare
DNS-01	rezoluție normală	NS/MX și status colectate
DNS-02	NXDOMAIN	status explicit, fără excepție necontrolată
DNS-03	SERVFAIL	marcat ca eroare operațională/retry
DNS-04	REFUSED	marcat separat; logat
DNS-05	timeout	evaluarea nu blochează întregul request

Colectorul SSL/TLS trebuie verificat cu certificate valide, expirate, lipsă, handshake eșuat și host inaccesibil. Implementarea analizei descrise în studiul de caz colectează emitentul, data emiterii, perioada de valabilitate și versiunea TLS. În cazul în care handshake-ul nu poate fi realizat, componentele lipsă sunt returnate controlat, iar mecanismul poate încerca o conectare pe portul 80 pentru obținerea adresei IP. Testarea trebuie să confirme că această ramură de fallback nu produce blocaje și că motivul absenței TLS este păstrat în loguri.

Tabelul 7. Testarea TLS

ID	Scenariu	Rezultat
TLS-01	certificat valid	issuer, valid_from, validity și tls_version completate
TLS-02	certificat expirat	status detectat fără întreruperea procesării
TLS-03	fără TLS	has_ssl=false și valori lipsă controlate
TLS-04	handshake timeout	timeout respectat + log + fallback
TLS-05	host inaccesibil	eroare izolată; request-ul nu blochează worker-ul

Testarea trebuie să urmărească faptul că o excepție într-o rutină nu anulează necontrolat toate celelalte rezultate și că există limite pentru numărul de conexiuni simultane. Pentru loturi mari, batching-ul și semafoarele asincrone previn epuizarea descriptorilor de fișiere și reduc riscul de blocare din partea surselor externe. În raportul final de rulare trebuie înregistrate separat latențele surselor, pentru a diferenția timpul modelului de timpul I/O.

Comportamentul sub încărcare trebuie evaluat și în prezența unor dependențe lente. Un număr mare de conexiuni simultane către servicii externe poate consuma descriptorii disponibili, poate produce timeout-uri în cascadă și poate afecta cererile care altfel ar fi răspuns rapid.

Limitarea concurenței, folosirea semafoarelor asincrone și stabilirea unor timeout-uri separate pentru fiecare sursă sunt măsuri potrivite pentru a menține platforma într-o stare controlată.

Pentru serviciile care impun limitări de acces, este preferabilă o strategie de retry cu backoff, combinată cu cache pe termen scurt. Retry-ul imediat și repetat poate amplifica o indisponibilitate temporară. În schimb, degradarea controlată permite returnarea unui rezultat parțial, marcat explicit ca atare, iar reevaluarea completă poate fi programată ulterior.

Testele funcționale trebuie să reproducă fluxurile utilizatorilor și să verifice atât comportamentul normal, cât și mesajele de eroare. Capturile prototipului prezentate în documentația interfeței definesc contextul testării; verificarea unei versiuni necesită dovezi produse de versiunea respectivă.

Testele trebuie să confirme respingerea credențialelor greșite, redirecționarea utilizatorului neautentificat, expirarea sesiunii și protejarea rutelor care afișează date operaționale. În plus, trebuie verificat ca mesajele de eroare să nu dezvăluie informații sensibile despre existența conturilor sau detalii interne ale aplicației.

Performanța serviciului trebuie măsurată în condiții explicite de încărcare. Inferența pe caracteristici deja disponibile și evaluarea completă cu interogări externe sunt operații diferite. Timpii uneia nu pot fi prezentați ca timpi ai celeilalte.

Benchmark-ul pentru validarea operațională trebuie să măsoare minimum trei scenarii: inferență pură cu caracteristici deja disponibile; evaluare completă cu surse externe; evaluare completă în condiții de degradare controlată a unei surse. Pentru fiecare scenariu se înregistrează requests/sec, median latency, error rate, CPU și RAM. Rezultatele trebuie asociate cu numărul de request-uri concurente și cu durata testului.

Pentru a evita concluziile bazate pe o singură rulare, testele de performanță trebuie repetate în condiții comparabile și trebuie raportate distribuții, nu doar medii. Mediana descrie comportamentul obișnuit, iar percentilele p95 și p99 evidențiază cererile lente care pot afecta experiența operatorului.

În același timp, error rate-ul trebuie analizat împreună cu latența, deoarece un throughput aparent bun nu este relevant dacă o parte importantă a cererilor eșuează.

Un scenariu realist de încărcare poate combina căutări interactive cu evaluări batch. Cererile interactive ar trebui prioritizate pentru a păstra un timp de răspuns predictibil, în timp ce evaluările masive pot fi procesate în fundal. Monitorizarea CPU, a memoriei, a conexiunilor la baza de date și a timpului petrecut în dependențe externe permite identificarea resursei care limitează scalarea.

Caching-ul este potrivit pentru date cu volatilitate redusă sau pentru răspunsuri externe costisitoare, însă TTL-ul trebuie ales astfel încât platforma să nu prezinte date prea vechi ca fiind actuale.

Pentru DNS și certificate, cache-ul poate reduce latența și încărcarea surselor, dar actualizarea trebuie să țină cont de modificările operaționale. În cazul scorului ML, cache-ul trebuie invalidat atunci când se schimbă versiunea modelului sau setul de caracteristici.

Tabelul 8. Analiza performanței modelului

Scenariu	Concurență	Metrici de înregistrat	Status
Inferență pură	1 / 10 / 50 / 100	RPS, mediană, error rate	de confirmat prin benchmark
Evaluare completă	1 / 10 / 25 / 50	latențe surse + end-to-end	de confirmat
Sursă externă lentă	10 / 25	timeout, retry, error rate	de confirmat
Procesare batch	loturi 100 / 1000	timp total, CPU, RAM	de confirmat

Robustețea platformei este evaluată prin injectarea unor erori controlate. Dacă Registry API, DAS, DNS sau TLS nu răspund, serviciul trebuie să diferențieze lipsa datelor de un rezultat negativ. Evaluarea poate continua cu caracteristici parțiale doar dacă modelul și contractul de inferență permit acest lucru și dacă utilizatorul este informat că scorul are informații incomplete. În cazul în care lipsesc caracteristici obligatorii, evaluarea trebuie marcată ca nereușită, nu convertită într-un scor aparent valid.

Testarea robustă include și injectarea deliberată a unor condiții de defect: răspunsuri lente, conexiuni refuzate, payload-uri incomplete și indisponibilitatea temporară a unei componente. Scopul nu este doar verificarea faptului că excepția este capturată, ci și confirmarea că utilizatorul primește un mesaj coerent, că eroarea este înregistrată și că sistemul poate reveni la funcționarea normală fără intervenții disproporționate.

Pentru dependențele externe este utilă definirea unei matrice de fallback. De exemplu, indisponibilitatea TLS poate permite continuarea evaluării cu caracteristicile disponibile, în timp ce lipsa completă a datelor de registru poate impune marcarea rezultatului ca incomplet. Regula de fallback trebuie să fie explicită și aceeași în toate componentele, astfel încât interfața să nu prezinte un scor cu aparență de certitudine atunci când datele esențiale lipsesc.

Tabelul 9. Scenarii de testare

Scenariu	Comportament corect	Risc evitat
Registry API indisponibil	timeout + mesaj controlat + log	scor bazat pe date invalide
DNS timeout	retry limitat / fallback	blocarea worker-ului
TLS handshake failure	valori lipsă explicite	excepție necontrolată
răspuns JSON incomplet	validare schemă	KeyError / mapare greșită
model indisponibil	healthcheck failed / 503	predicție cu artefact corupt

Inputul de tip domeniu trebuie validat înainte de orice interogare externă. Se verifică lungimea, structura etichetelor, caracterele permise, IDN/punycode și eliminarea schemelor sau căilor atunci când endpoint-ul așteaptă doar FQDN. Cererile care conțin caractere de control, secvențe pentru injection sau URL-uri complete trebuie respinse sau normalizate explicit. Această măsură reduce atât

erorile funcționale, cât și riscul de SSRF sau utilizare necontrolată a serviciului ca proxy de rețea.

La nivelul API-ului se recomandă rate limiting, autentificare pentru endpoint-urile interne și jurnalizarea cererilor. Log-urile nu trebuie să conțină parole, token-uri sau date WHOIS sensibile care nu sunt necesare pentru diagnostic.

Fiecare predicție importantă trebuie să poată fi asociată cu versiunea modelului, schema de caracteristici și timestamp-ul evaluării. Pentru exploatare se recomandă versionarea modelului și rollback (revenire) pentru a permite revenirea în cazul unei regresii. În etapa de validare se verifică faptul că artefactul anterior rămâne disponibil și că schimbarea modelului nu necesită modificări manuale necontrolate ale datelor din baza de date.

Analiza limitărilor metodologice consolidează un set de îmbunătățiri care pot fi implementate incremental. Acestea nu schimbă obiectivul principal al platformei, ci reduc ambiguitatea scorului, cresc observabilitatea și fac sistemul mai rezilient la variația surselor externe.

Fiecare îmbunătățire trebuie verificată printr-un criteriu înainte/după. Pentru optimizările de performanță se compară latența și rata de erori; pentru robustețe se repetă scenariul care a produs defectul; pentru modificările ML se compară metricile pe același set de validare. Această disciplină evită declararea unei modificări drept îmbunătățire doar pentru că implementarea a fost schimbată.

În cazul modificărilor care afectează modelul sau preprocesarea, versiunea anterioară trebuie păstrată suficient timp pentru comparație și rollback. O nouă versiune poate fi promovată numai după ce trece criteriile stabilite și după ce rezultatele sunt documentate. Într-un mediu operațional, posibilitatea de revenire rapidă este importantă deoarece unele probleme devin vizibile abia pe fluxul real de date.

Tabelul 10. Riscuri și mecanisme de remediere

Problemă / risc	**Îmbunătățire propusă**	**Efect așteptat**
latență dominată de I/O	asyncio + timeout + batching	reducerea timpului blocant și izolarea surselor lente
interogări repetate	cache cu TTL controlat	reducerea încărcării și a latenței
scor prezentat ca probabilitate absolută	calibrare / etichetare „scor model”	interpretare corectă
regresie după actualizare	model versioning + rollback	revenire rapidă și auditabilă
concept drift	monitorizare distribuții + re-antrenare periodică	menținerea performanței în timp
lipsă trasabilitate	logging structurat + correlation ID	diagnostic și audit
posibil leakage	group/temporal split	estimare mai realistă a generalizării
rezultate fals pozitive	threshold tuning și review uman	reducerea alertelor inutile

Îmbunătățirile de performanță trebuie evaluate înainte și după modificare. De exemplu, introducerea cache-ului nu este considerată reușită doar pentru că reduce numărul de request-uri externe; trebuie măsurat și riscul de date stale. Similar, creșterea timeout-ului poate reduce erorile, dar poate produce acumularea request-urilor.

Îmbunătățirile ML trebuie tratate ca versiuni noi, nu ca simple modificări de configurare. Orice schimbare a setului de caracteristici, a codificării, a hiperparametrilor sau a pragului necesită rerularea suitei de validare și compararea cu baseline-ul. O versiune nouă este promovată doar dacă nu introduce regresii relevante și dacă diferențele sunt documentate.

5.7. Rezultatele finale ale validării și criteriile de acceptare

Acceptarea operațională presupune completarea matricei de verificare cu rezultate obținute pe versiunea evaluată. Existența prototipului și a rezultatelor experimentale nu înlocuiește dovada funcționării integrate în mediul de exploatare.

Decizia de acceptare trebuie să distingă între neconformități blocante și observații care pot fi tratate ulterior. O eroare care împiedică evaluarea unui domeniu sau produce rezultate eronate fără avertizare este blocantă. În schimb, o problemă minoră de prezentare poate fi consemnată ca îmbunătățire ulterioară dacă nu afectează funcția principală. Această clasificare clarifică starea platformei la momentul predării și reduce ambiguitatea în interpretarea rezultatelor.

Pentru închiderea etapei se recomandă o revizuire comună a matricei de teste, a incidentelor rămase deschise și a limitărilor cunoscute. Raportul final trebuie să reflecte starea reală a sistemului: funcțiile validate, condițiile în care rezultatele sunt fiabile și situațiile în care operatorul trebuie să aplice verificări suplimentare.

Tabelul 11. Validare și criterii de acceptare

Categorie	Baseline disponibil	Validare curentă	Criteriu de acceptare
ML – set test	De stabilit pe corpusul și protocolul evaluării curente	de rerulat	fără regresie semnificativă față de baseline
ML – AUROC/AUPRC	De stabilit pe corpusul și protocolul evaluării curente	de rerulat	valori stabile și raportate cu aceeași metodă
Inferență mocked	sute RPS; mediană <1 ms	de rerulat	stabilitate fără erori
WHOIS/DAS	flux documentat	de testat	erori diferențiate de statusurile semantice
DNS/TLS	colectare asincronă documentată	de testat	timeout/fallback controlat
UI	module prototip disponibile	de testat	fluxurile critice trec testele
Securitate	CSRF/XSS menționate în arhitectură	de verificat	niciun defect critic deschis

5.8. Erori și incertitudine

Analiza erorilor este mai importantă operațional decât o singură valoare de acuratețe. Un *rezultat fals pozitiv* poate conduce la prioritizarea inutilă a unui domeniu legitim, la generarea unei alerte sau la consumarea timpului unui analist. Cauzele probabile includ domenii foarte noi, certificate recent emise, lipsa DNSSEC, date incomplete sau corelații statistice legate de registrar. Aceste semnale nu reprezintă dovezi de abuz și trebuie interpretate în context.

Un *rezultat fals negativ* este mai critic: un domeniu malițios poate avea certificat valid, DNSSEC, un registrar cunoscut și o vechime semnificativă. În plus, compromiterea unui domeniu legitim schimbă comportamentul fără a modifica neapărat caracteristicile istorice. Din acest motiv, validarea trebuie să includă scenarii adversariale și exemple de domenii compromise, iar sistemul trebuie să combine scorul ML cu semnale operaționale și cu evoluția temporală.

Costurile celor două tipuri de eroare nu sunt egale și trebuie corelate cu utilizarea platformei. Pentru un modul de prioritizare, un număr limitat de rezultate fals pozitive poate fi tolerabil dacă acestea sunt revizuite de un operator, în timp ce un rezultat fals negativ poate lăsa neobservat un domeniu cu risc real. Pragul de decizie trebuie deci ales în raport cu obiectivul operațional, nu exclusiv pentru maximizarea acurateții globale.

Analiza calitativă a erorilor trebuie să urmărească tipare recurente. Dacă majoritatea rezultatelor fals pozitive apar la domenii foarte noi sau fără TLS, problema poate indica o dependență excesivă de aceste caracteristici. Dacă rezultatele fals negative sunt concentrate pe domenii vechi compromise, este necesară completarea semnalelor cu indicatori dinamici. O astfel de analiză oferă informații mai utile pentru îmbunătățirea platformei decât simpla raportare a unui procent agregat.

Tabelul 12. Analiza calitativă a erorilor

Tip eroare	Exemplu de cauză	Acțiune de validare
Rezultat fals pozitiv	domeniu nou și certificat recent	verificare manuală + analiza istoricului și a surselor externe
Rezultat fals pozitiv	lipsă DNSSEC	nu se tratează ca dovadă singulară
Rezultat fals negativ	domeniu vechi compromis	analiză Istoricul reputației și semnale post-compromitere
Rezultat fals negativ	atacator imită infrastructură benignă	test adversarial și extinderea caracteristicilor

Matricea de confuzie descrie relația dintre clasa de referință și decizia modelului. Sensibilitatea urmărește proporția cazurilor pozitive identificate, în timp ce precizia urmărește proporția cazurilor confirmate dintre cele semnalate. Rata falselor pozitive se raportează la exemplele negative. Aceste mărimi au numitori

diferiți; interpretarea lor ca procente interschimbabile poate conduce la estimări greșite ale volumului de verificare necesar.

Un exemplu numeric ipotetic clarifică diferența. Se consideră 10.000 de domenii, dintre care 100 pozitive conform referinței și un model cu sensibilitate de 80% și rată a falselor pozitive de 1%. Modelul identifică 80 de cazuri pozitive și semnalează greșit 99 dintre cele 9.900 negative. Rezultă 179 de alerte, dintre care aproximativ 44,7% sunt pozitive conform referinței. Aceste numere sunt exclusiv un calcul didactic, nu un corpus suplimentar și nu un rezultat experimental al cărții.

Dacă aceeași sensibilitate și aceeași rată a falselor pozitive s-ar menține într-o populație cu altă prevalență, precizia s-ar modifica. Menținerea acestor rate este însă o ipoteză, nu o proprietate garantată a transferului. Distribuția atributelor și dificultatea cazurilor pot fi diferite. De aceea, un calcul bazat pe prevalență trebuie prezentat ca scenariu condiționat și completat prin validare pe populația efectivă de utilizare.

Pentru operator, consecința practică este că un procent aparent mic de erori poate produce un volum mare de alerte neconfirmate. Evaluarea trebuie să includă capacitatea de verificare și timpul necesar unui caz, fără a transforma aceste constrângeri în justificări pentru ignorarea sistematică a unor categorii. Alegerea pragului devine o decizie documentată asupra compromisului dintre identificare și încărcarea procesului. Analiza falselor pozitive și negative din metodologia de validare trebuie astfel conectată cu fluxul operațional.

O valoare punctuală rezumă rezultatul obținut pe un anumit eșantion. Ea nu arată singură cât de sensibil este rezultatul la alegerea observațiilor sau la variațiile procedurii de învățare. Raportarea trebuie să precizeze sursa incertitudinii examinate: variația între partiții, variația între inițializări sau variația determinată de eșantionare. Aceste componente nu sunt echivalente și nu pot fi reunite într-un interval fără explicarea metodei.

Când observațiile sunt grupate, estimarea incertitudinii trebuie să respecte unitatea relevantă de independență. Repetarea selecției unor rânduri foarte asemănătoare poate sugera o stabilitate excesivă. O procedură care reselectează grupuri răspunde unei alte ipoteze și trebuie descrisă ca atare. Alegerea metodei de estimare este legată de modul în care se dorește generalizarea rezultatului: către alte observații ale acelorași domenii sau către domenii diferite.

Comparația dintre modele este mai informativă când urmărește aceleași cazuri. Două scoruri medii apropiate pot ascunde tipuri de erori foarte diferite. Este utilă examinarea cazurilor asupra cărora metodele sunt de acord și a celor asupra cărora diferă, precum și distribuția diferențelor între subgrupuri relevante. Un avantaj numeric mic nu justifică automat înlocuirea modelului dacă implică degradări în categorii importante sau cerințe operaționale disproporționate.

Rezultatul unei comparații trebuie formulat la nivelul demonstrat de date. Superioritatea pe un corpus, într-un protocol determinat, nu înseamnă superioritate universală. Dacă diferența este instabilă, concluzia poate fi că metodele au performanțe apropiate în condițiile examinate. Costul colectării, posibilitatea de explicare și ușurința revalidării pot deveni atunci criterii suplimentare, declarate

separat de performanța predictivă. O alegere justificată integrează aceste criterii fără a le transforma retrospectiv în dovezi statistice.

5.9. Interpretare și calibrare

Pentru interpretare la nivel de caz, este recomandată utilizarea SHAP sau a unei metode echivalente care explică contribuția caracteristicilor la o predicție individuală. În interfață, explicația trebuie prezentată ca suport pentru analist și nu ca demonstrație cauzală. De exemplu, faptul că emitentul certificatului influențează scorul nu înseamnă că emitentul este responsabil de activitatea domeniului.

În evaluarea statistică, probabilitățile produse de modelele de gradient boosting nu trebuie interpretate ca măsură absolută a riscului fără calibrare. În consecință, procentele afișate în interfață trebuie denumite „scor de model" sau calibrate înainte de a fi prezentate ca probabilitate. Pentru calibrare se pot utiliza Platt scaling sau isotonic regression pe un set de calibrare separat, urmate de verificarea Brier score și a curbei de calibrare.

În procesul de calibrare se recomandă compararea probabilității prezise cu frecvența observată a clasei pozitive pe intervale de scor. Dacă, de exemplu, domeniile plasate în zona 0,8–0,9 sunt malițioase într-o proporție semnificativ diferită, scorul nu trebuie prezentat ca probabilitate directă. Până la realizarea unei calibrări validate, interfața poate utiliza termenii de scor al modelului sau de nivel de reputație, evitând formulări care sugerează o probabilitate statistică exactă.

Explicațiile SHAP trebuie interpretate tot în context. Ele indică modul în care caracteristicile influențează predicția unui model antrenat pe un anumit set de date, nu demonstrează o relație cauzală. Pentru un operator, utilitatea lor constă în identificarea rapidă a semnalelor care au contribuit la clasificare și în orientarea verificărilor manuale către datele relevante.

Un scor poate ordona corect exemplele fără să exprime o probabilitate bine calibrată. Pentru interpretarea probabilistică trebuie examinată corespondența dintre valorile scorului și frecvențele observate ale clasei de referință. Evaluarea se realizează pe date care nu au fost folosite pentru ajustarea aceleiași calibrări. În plus, corespondența depinde de populație și de modul de etichetare; o calibrare verificată într-un experiment nu poate fi transferată automat într-un alt context.

Calibrarea nu elimină limitele referinței. Dacă etichetele descriu apartenența la o listă, probabilitatea estimată privește acea definiție operațională. Nu devine, prin schimbarea formei de prezentare, probabilitatea tuturor comportamentelor malițioase posibile. Interfața și raportul trebuie să precizeze sensul scorului. Afișarea unui procent cu multe zecimale nu adaugă informație atunci când incertitudinea datelor este ridicată.

O politică de decizie poate include abținerea. Aceasta înseamnă trimiterea către verificare suplimentară a cazurilor pentru care dovezile sunt insuficiente sau pentru care condițiile de aplicare a modelului nu sunt îndeplinite. Abținerea nu trebuie confundată cu o etichetă benignă și nici folosită pentru eliminarea cazurilor dificile din raportarea performanței. Se raportează proporția cazurilor acoperite și

rezultatele obținute pe acestea, alături de caracteristicile cazurilor rămase fără decizie automată.

Criteriile de abținere pot privi lipsa unor surse esențiale, categorii necunoscute sau contradicții nerezolvate. Un scor situat aproape de un prag poate justifica verificarea, dar apropierea de prag nu este singura formă de incertitudine. Un model poate produce un scor extrem pe un exemplu care diferă de datele de antrenare. Combinarea controlului calității datelor cu verificarea umană dezvoltă principiile de interpretare responsabilă din materialele de bune practici.

Analiza prin ablație examinează rezultatul obținut după eliminarea controlată a unei caracteristici sau a unei familii de caracteristici. Scopul este identificarea contribuției informației respective în condițiile protocolului. O asemenea analiză trebuie să păstreze comparabilitatea partițiilor și a metricilor. Dacă eliminarea unei surse schimbă și numărul de exemple evaluate, diferența poate proveni din modificarea populației, nu numai din informația eliminată.

Corelația dintre caracteristici complică interpretarea. Eliminarea unui atribut poate avea efect redus deoarece alte atribute transmit informație asemănătoare. Efectul redus nu demonstrează inutilitatea absolută a atributului. Invers, o scădere mare poate indica dependența modelului de o sursă care nu va fi disponibilă în toate condițiile de utilizare. Concluzia trebuie să privească relația dintre informație, model și protocol, fără a transforma rezultatul într-o ierarhie universală a indicatorilor.

Ablația poate fi organizată pe familii cu semnificație operațională: date administrative, observații de infrastructură sau rezultate ale unor surse externe. Această organizare permite discutarea costului și a robusteții. Dacă două configurații au rezultate apropiate, configurația cu mai puține dependențe poate prezenta avantaje practice, dar alegerea necesită și verificarea tipurilor de erori. O medie apropiată poate ascunde pierderea unui semnal important într-o categorie restrânsă.

Rezultatele ablației se raportează împreună cu configurația de referință, regulile de ajustare și numărul observațiilor. O explicație a modelului bazată pe importanța atributelor nu înlocuiește acest experiment, deoarece răspunde unei întrebări diferite. Analiza comparativă trebuie să arate ce se întâmplă când informația lipsește efectiv. În acest mod, testarea componentei de învățare automată poate susține decizii arhitecturale privind colectarea și funcționarea cu date parțiale.

Rezultatul agregat poate fi dominat de categoriile cele mai numeroase. Pentru a înțelege comportamentul modelului, evaluarea poate examina separat grupuri definite înaintea analizei: domenii cu date complete, domenii cu anumite observații lipsă sau domenii observate în perioade diferite. Definirea grupurilor trebuie să aibă o justificare metodologică. Selectarea ulterioară numai a grupurilor cu rezultate favorabile produce o imagine incompletă a performanței.

Pentru fiecare subgrup se raportează dimensiunea și distribuția claselor. O metrică obținută pe foarte puține cazuri nu permite aceeași precizie a concluziei ca una obținută pe un grup mai mare. Absența erorilor într-un grup mic nu demonstrează absența riscului. Dacă nu există suficiente exemple dintr-o clasă, anumite comparații nu sunt informative și trebuie prezentate ca limitări, fără înlocuirea lor prin valori care sugerează certitudine.

Analiza pe subgrupuri poate arăta unde este necesară colectare suplimentară sau o politică de abținere. Nu rezultă automat că fiecare grup necesită un model separat. Separarea modelelor poate reduce volumul datelor disponibile pentru fiecare și poate complica validarea. Mai întâi se examinează cauza diferenței: calitatea etichetelor, accesibilitatea surselor, distribuția atributelor sau dificultatea intrinsecă a sarcinii.

Raportarea trebuie să păstreze legătura dintre concluzia generală și aceste rezultate. Dacă un model funcționează satisfăcător numai în condițiile existenței unor surse, condiția devine parte a domeniului său de utilizare. Dacă unele categorii sunt insuficient reprezentate, transferul către ele rămâne o ipoteză. O astfel de delimitare transformă evaluarea dintr-o simplă comparație de scoruri într-o descriere verificabilă a situațiilor în care metoda poate sprijini decizia.

5.10. Reproductibilitate și limite

Generalizarea necesită controlul suprapunerilor, validare pe grupuri și verificări pe perioade sau surse distincte. O metrică favorabilă pe un corpus nu înlocuiește evaluarea în populația operațională.

Atunci când setul de date este construit din liste de referință și liste de blocare, diferențele dintre semnificațiile și ferestrele temporale ale surselor trebuie documentate. În viitor, etichetele pot fi îmbogățite cu timestamp, sursă și nivel de încredere. Această abordare ar permite separarea unui domeniu înregistrat malițios de un domeniu legitim compromis și ar îmbunătăți analiza evoluției temporale a reputației.

Pentru robustețea statistică sunt recomandate intervale de încredere bootstrap, testul McNemar (McNemar, 1947) pentru predicții pereche și testul DeLong pentru comparația AUROC. Pentru interpretarea operațională sunt recomandate calibrarea, decision-curve analysis și evaluarea pragurilor în funcție de costul rezultatului fals pozitiv și fals negativ.

În exploatare, distribuțiile caracteristicilor și claselor trebuie monitorizate pentru concept drift. Pentru exploatare se recomandă reantrenare lunară sau trimestrială în funcție de dinamica amenințărilor, împreună cu model versioning și rollback. Frecvența efectivă trebuie determinată pe baza drift-ului observat, nu doar pe un calendar fix.

Validarea externă trebuie realizată pe date care nu au contribuit la definirea etichetelor și, pe cât posibil, pe o perioadă ulterioară celei de antrenare. Rezultatele foarte ridicate raportate intern sunt utile ca baseline, dar generalizarea reală se confirmă numai atunci când modelul își păstrează performanța în fața unor surse, campanii și tipare noi.

Un experiment reutilizabil trebuie descris astfel încât cititorul să poată identifica intrările, operațiile și rezultatele. Documentarea include scopul, versiunea corpusului, criteriile de selecție, partițiile, transformările, configurația modelelor și metricile. Se precizează ce elemente pot fi distribuite și ce elemente rămân

inaccesibile. Disponibilitatea codului nu compensează lipsa datelor, după cum disponibilitatea datelor nu compensează lipsa regulilor de prelucrare.

Rezultatele trebuie asociate unei configurații identificabile. O modificare a pragului, a preprocesării sau a criteriului de excludere produce un rezultat nou, chiar dacă algoritmul păstrează aceeași denumire. Jurnalul experimentelor permite urmărirea acestor diferențe și reduce riscul de a reuni într-un singur tabel valori obținute în condiții incompatibile. Numărul execuțiilor exploratorii și criteriul de selectare a configurației finale trebuie descrise suficient pentru interpretarea comparației.

În final, raportul separă rezultatele observate de recomandările pentru utilizare. Primele sunt limitate de corpus și protocol; recomandările includ și considerente operaționale care trebuie declarate. O secțiune dedicată limitărilor arată ce nu a fost verificat, ce date lipsesc și ce experiment ar putea clarifica întrebările rămase. Această structură susține continuitatea cercetării și evită prezentarea unei configurații experimentale drept soluție definitiv validată pentru orice populație de domenii.

6. Analiza operațională a reputației

6.1. De la semnal la investigație

Un semnal poate proveni dintr-o listă externă, dintr-o abatere de comportament, dintr-o sesizare sau dintr-un model. Primul pas este identificarea obiectului și a contextului temporal. Operatorul stabilește dacă observația privește domeniul, o gazdă, o adresă IP sau un URL. Această distincție determină atât verificările ulterioare, cât și domeniul de aplicare al concluziei.

Scorul contribuie la prioritizare, dar nu reprezintă singur o constatare. Operatorul verifică sursele, actualitatea și motivele clasificării, apoi formulează explicații alternative. Un rezultat negativ poate reflecta un incident real, o configurație incompletă, o sursă indisponibilă sau o etichetă veche. Investigația trebuie să permită diferențierea acestor situații.

Triajul ține seama de severitatea posibilă, credibilitatea dovezilor și impactul asupra utilizatorilor. Un semnal slab, dar asociat unui serviciu sensibil, poate justifica o verificare rapidă. Urgența nu justifică însă omiterea motivului deciziei. Evidența trebuie să indice ce este cunoscut, ce este presupus și ce rămâne de verificat.

Profilul reunește date administrative, observații DNS, atribute TLS, istoric și semnale externe. Fiecare categorie trebuie să indice sursa și momentul. Un profil complet vizual poate conține date de vârste diferite; interfața trebuie să evite impresia că toate au fost colectate simultan.

Identificatorul normalizat trebuie să rămână vizibil alături de forma observată când diferența este relevantă. Scorul este însoțit de scala sa, sens, prag și versiune. Starea validării umane se afișează separat de clasa automată, astfel încât operatorul să poată identifica o concluzie încă neconfirmată.

Istoricul explică schimbările, dar nu stabilește singur cauza lor. O scădere poate rezulta din observații noi, schimbarea modelului sau indisponibilitatea unei surse. Compararea valorilor cere verificarea continuității metodei și a acoperirii datelor. În lipsa acestei verificări, graficul poate sugera un incident care nu a fost demonstrat.

Lipsa istoricului este o condiție de analiză, nu o dovadă de abuz. Un domeniu nou poate avea servicii încă neconfigurate, certificate recent emise și o prezență redusă în sursele externe. Aceste observații trebuie corelate cu scopul aparent al serviciului și cu indicatori independenți.

Verificarea urmărește coerența identității, starea delegării, accesibilitatea serviciilor și eventualele semnale confirmate. Dacă informațiile sunt insuficiente, cazul poate fi păstrat pentru reevaluare. Termenul de revizuire se stabilește în raport cu dinamica datelor și cu impactul potențial, fără a transforma monitorizarea într-o etichetă definitivă.

Reputația istorică favorabilă nu exclude un incident recent. Modificările de conținut, redirecționările sau schimbările de infrastructură pot orienta investigația, dar trebuie comparate cu activitățile autorizate. O actualizare legitimă poate produce aceleași diferențe tehnice ca o modificare neautorizată.

Analiza caută dovezi localizabile și reproduce observațiile în condiții controlate. Dacă incidentul privește o resursă sau un subdomeniu, extinderea concluziei asupra întregului domeniu necesită justificare. Remedierea trebuie urmărită prin reevaluare, cu păstrarea istoricului și retragerea clasificării atunci când dovezile nu o mai susțin.

Adresele IP, serverele de nume și certificatele pot lega observații, însă infrastructura partajată limitează interpretarea. O relație tehnică nu demonstrează identitate de operator sau intenție comună. Corelarea produce ipoteze care trebuie confruntate cu date independente și cu perioada de utilizare a infrastructurii.

La nivel de portofoliu, comparația necesită aceeași unitate de numărare și aceeași fereastră temporală. Un număr mai mare de alerte poate rezulta dintr-un portofoliu mai mare sau dintr-o acoperire mai bună a surselor. Indicatorii trebuie normalizați și însoțiți de limitele colectării înaintea concluziilor comparative.

Raportul consemnează întrebarea investigată, obiectul, observațiile, metoda și concluzia. Faptele colectate se separă de interpretări și de recomandări. Sunt păstrate contradicțiile relevante, datele lipsă și criteriul pentru o eventuală reevaluare.

Închiderea unui caz poate însemna confirmare, infirmare, remediere sau insuficiența dovezilor. Aceste stări au semnificații diferite și trebuie păstrate în evidență. Procedura din capitolul 9 descrie câmpurile și controalele necesare, astfel încât rezultatul să poată fi verificat și, dacă este cazul, corectat ulterior.

6.2. Construirea cronologiei unui caz

Analiza operațională poate începe cu ordonarea observațiilor într-o cronologie. Aceasta trebuie să distingă evenimentele confirmate, momentele raportate de surse și momentele verificărilor proprii. Scopul nu este construirea unei narațiuni fără goluri, ci identificarea succesiunii susținute de date. Intervalele necunoscute se păstrează ca atare.

O cronologie prea precisă, construită prin completarea implicită a informațiilor lipsă, poate orienta greșit concluzia.

Pentru fiecare eveniment se consemnează obiectul, sursa și relevanța pentru ipoteza investigată. Modificarea unui server de nume poate preceda un incident, dar simpla ordine temporală nu demonstrează o relație cauzală. Schimbarea poate avea o explicație administrativă legitimă. Operatorul trebuie să examineze dacă există observații suplimentare care susțin legătura și dacă aceeași explicație este compatibilă cu întregul set de dovezi.

Cronologia ajută și la identificarea efectelor intervenției. Un domeniu poate deveni inaccesibil după semnalare sau după aplicarea unei măsuri. Dacă indisponibilitatea este tratată drept semnal preexistent, analiza poate atribui modelului o capacitate de anticipare pe care nu a demonstrat-o. Raportul trebuie să

separe starea observată înaintea incidentului, starea din timpul investigației și starea constatată după remediere.

Într-un dosar operațional, cronologia poate fi completată incremental, cu păstrarea autorului fiecărei modificări. Corectarea unei date nu trebuie să elimine explicația corecției, mai ales dacă aceasta schimbă interpretarea cazului. Rezultatul este o evaluare care poate fi revizuită de alt operator fără a depinde de memoria celui care a realizat prima analiză.

6.3. Ipoteze alternative și verificări discriminatorii

Un semnal de reputație poate admite mai multe explicații. O variație rapidă a adreselor poate fi asociată unei infrastructuri abuzive, dar poate apărea și în servicii distribuite legitime. Un nume recent înregistrat poate aparține unei activități noi obișnuite. Analiza trebuie să formuleze ipoteze alternative plauzibile și să identifice observațiile care le-ar diferenția. Enumerarea lor nu este un exercițiu formal, ci un control împotriva confirmării premature a primei suspiciuni.

O verificare discriminatorie este utilă atunci când rezultatul ei poate modifica aprecierea ipotezelor. Repetarea aceleiași interogări fără schimbarea condițiilor poate confirma persistența observației, dar nu adaugă neapărat informație despre cauză. În schimb, verificarea granulației indicatorului, a perioadei sau a serviciului afectat poate clarifica dacă semnalul privește întregul domeniu. Alegerea următorului pas trebuie motivată prin întrebarea pe care acesta o poate rezolva.

Operatorul trebuie să distingă observația de interpretare în notele cazului. Afirmația că o sursă a listat domeniul descrie un fapt verificabil despre acea sursă. Afirmația că domeniul a fost creat pentru abuz este o interpretare mai puternică, ce necesită alte dovezi. Păstrarea separată a acestor niveluri permite reevaluarea concluziei chiar dacă observațiile inițiale rămân corecte.

Închiderea unei investigații poate avea loc și cu un rezultat neconcludent. Lipsa dovezilor suficiente nu trebuie convertită automat în confirmare benignă, iar imposibilitatea infirmării unei suspiciuni nu o transformă în fapt. Un rezultat neconcludent poate specifica verificările realizate, limitele întâlnite și condițiile unei reevaluări. Această formulare este compatibilă cu principiile de proporționalitate și decizie umană din ghidurile sursă și susține utilizarea responsabilă a scorurilor.

6.4. Infrastructura partajată și limitele propagării reputației

Relațiile de infrastructură permit identificarea unor grupuri de interes, dar nu justifică transferul automat al reputației. Mai multe domenii pot utiliza aceeași adresă, același furnizor sau același serviciu de distribuție fără să aibă același titular ori aceeași activitate. Asocierea tehnică este o observație despre conectivitate sau administrare, nu o dovadă suficientă de coordonare. Analiza trebuie să precizeze ce relație a fost constatată și de ce este relevantă.

O relație devine mai informativă dacă este examinată în timp și în context. Partajarea unei resurse la un anumit moment diferă de utilizarea succesivă a aceleiași

resurse de către entități fără legătură. Frecvența, durata și exclusivitatea asocierii pot orienta investigația, însă nu înlocuiesc verificarea comportamentului. Modelele de reputație bazate pe relații, discutate în literatura inclusă (Antonakakis et al., 2010; Antonakakis et al., 2011; Mishsky, Gal-Oz & Gudes, 2015), trebuie interpretate împreună cu aceste limite.

Pentru grupuri mari de infrastructură, raportul ar trebui să evite concluziile colective bazate pe un singur caz. Este utilă separarea indicatorilor comuni de dovezile specifice fiecărui domeniu. Dacă un grup este folosit pentru prioritizare, acest lucru se declară; dacă este folosit pentru clasificare, trebuie prezentată justificarea suplimentară. Efectele asupra entităților neimplicate constituie un criteriu de evaluare a regulii de propagare.

La nivel operațional, o hartă relațională servește mai întâi generării de ipoteze. Ea poate sugera domenii care necesită verificare, fără a le atribui din start verdictul unui vecin. Decizia finală trebuie să păstreze lanțul de argumentare și să permită identificarea contribuției relaționale. Dacă o asociere dispare sau este corectată, sistemul trebuie să poată revizui concluziile dependente de ea. Astfel se evită persistența unei reputații derivate dintr-o legătură care nu mai este susținută.

6.5. Reevaluarea după schimbarea condițiilor

Reevaluarea poate fi declanșată de o observație nouă, de expirarea unei perioade de valabilitate sau de modificarea condițiilor în care a fost produs scorul. Schimbarea unei surse, a modelului ori a regulilor de normalizare poate afecta comparabilitatea cu evaluarea precedentă. Operatorul trebuie să distingă o schimbare a domeniului de o schimbare a instrumentului de măsurare. Altfel, diferența dintre două scoruri poate fi interpretată incorect drept ameliorare sau agravare.

O reevaluare documentată păstrează versiunea anterioară și arată ce informație nouă a intervenit. Nu este suficientă înlocuirea verdictului. Trebuie precizat dacă noua concluzie rezultă din remediere confirmată, din corectarea unei erori sau din insuficiența dovezilor curente. Aceste motive au consecințe diferite pentru raportare și pentru utilizarea cazului ca exemplu de antrenare.

În absența unei observații directe recente, eliminarea unei listări externe nu demonstrează automat rezolvarea incidentului. Ea reprezintă o schimbare a stării publicate de acea sursă. În mod simetric, persistența unei listări poate reflecta o politică de retenție și nu o activitate confirmată la data curentă. Reevaluarea trebuie să consulte, în măsura posibilului, atât istoricul sursei, cât și dovezile relevante pentru serviciul afectat.

Rezultatul se comunică printr-o stare actuală și o explicație a tranziției. Pentru analiză longitudinală, această explicație permite separarea recuperării reale de fluctuațiile colectării. Pentru instruirea operatorilor, cazurile reevaluate arată de ce o decizie corectă la un moment poate necesita ulterior modificare. Monitorizarea continuă capătă astfel un rol metodologic: menține legătura dintre evaluare și condițiile efective în care aceasta rămâne aplicabilă.

7. Interpretarea responsabilă și bunele practici

7.1. Scopul și domeniul de aplicare

Politica de utilizare stabilește regulile de interpretare și responsabilitățile utilizatorilor unui sistem de reputație. Ea completează validarea tehnică prin criterii de decizie proporțională, verificabilă și documentată.

Politica se adresează operatorilor care consultă dashboard-ul și rezultatele de reputație, analiștilor care investighează alertele, administratorilor tehnici care mențin platforma, personalului care gestionează modelul ML și, acolo unde procesele organizaționale o prevăd, registrarilor sau partenerilor implicați în remedierea incidentelor. Principiile sunt aplicabile atât analizei individuale a unui domeniu, cât și monitorizării unui portofoliu.

Un sistem de reputație trebuie utilizat ca sistem de suport decizional. Scorul, categoria de risc și explicațiile oferite de model sunt semnale care prioritizează investigația; ele nu constituie automat o constatare juridică, o dovadă de abuz sau o justificare suficientă pentru o acțiune ireversibilă. Atunci când impactul unei decizii este ridicat, rezultatul automat trebuie validat de un operator uman și corelat cu date suplimentare.

Aplicarea politicii presupune separarea rolurilor de observare, analiză și aprobare. Un utilizator care consultă un scor poate iniția o verificare, însă o măsură cu impact ridicat trebuie documentată și, după caz, confirmată de rolul responsabil. Politica urmărește astfel să reducă atât reacțiile insuficiente la semnale reale, cât și intervențiile excesive generate de interpretarea izolată a unui indicator.

Documentul trebuie utilizat împreună cu manualul tehnic și cu procedurile interne ale organizației. Politica descrie principiile și comportamentul așteptat, nu înlocuiește controalele tehnice, regulile juridice sau responsabilitățile operaționale deja stabilite. Atunci când există diferențe între o recomandare generală și o procedură formală aplicabilă unui incident, procedura formală are prioritate.

Principiu central: sistemul oferă indicatori de reputație și risc. Un scor mare nu demonstrează automat că un domeniu este malițios, iar un scor mic nu garantează că domeniul este sigur.

7.2. Contextul amenințărilor asociate domeniilor

Domeniile Internet sunt utilizate ca infrastructură pentru servicii legitime, dar pot fi folosite și pentru phishing, distribuire de malware, comandă și control, fraudă, redirect-uri, typosquatting sau campanii de scurtă durată. Unele domenii sunt înregistrate direct în scop abuziv; altele sunt domenii legitime care devin periculoase

după compromitere. Această diferență este importantă pentru interpretarea reputației și pentru alegerea răspunsului.

Sistemele de reputație încearcă să reducă timpul dintre apariția semnalelor și investigația umană. Evaluarea poate corela atribute de registru, vechimea domeniului, DNSSEC, caracteristici SSL/TLS, informații DNS și surse de reputație. Niciunul dintre aceste semnale nu este suficient izolat. De exemplu, un certificat TLS valid confirmă criptarea conexiunii și identitatea tehnică certificată, dar nu garantează că activitatea găzduită este benignă. Similar, lipsa DNSSEC nu transformă automat un domeniu legitim într-un domeniu malițios.

Amenințările se modifică în timp. Un atacator poate folosi certificate legitime, registrari cunoscuți, domenii vechi sau infrastructură care imită comportamentul benign. Din acest motiv, instruirea și conștientizarea utilizatorului trebuie să includă nu doar citirea scorului curent, ci și consultarea istoricului, a explicațiilor și a semnalelor complementare.

Riscul trebuie privit pe întreg ciclul de viață al domeniului. Un domeniu poate fi nou și legitim, poate funcționa o perioadă fără incidente și poate fi ulterior compromis. Invers, o infrastructură folosită într-o campanie malițioasă poate dispărea sau poate fi transferată. Din acest motiv, conștientizarea nu se limitează la identificarea domeniilor noi, ci include observarea schimbărilor care apar după stabilirea unei reputații inițiale.

Operatorii trebuie să evite asocierea automată dintre un singur atribut și o amenințare. Certificatul, registrarul, vârsta, DNSSEC sau prezența într-o listă externă au valoare atunci când sunt corelate. Un proces de analiză bun combină semnale tehnice, informații temporale și context operațional și păstrează explicit posibilitatea ca datele să fie incomplete sau depășite.

Tabelul 13. Amenințări asociate domeniilor

Tip amenințare	Exemplu	Ce urmărește operatorul
Phishing	domeniu asemănător unui brand	vârstă, nume, certificat, blacklist, redirect-uri
Malware / C2	domeniu folosit pentru distribuție sau comandă	IoC, DNS, reputație, infrastructură
Domeniu nou abuziv	campanie de scurtă durată	domain age, NS, TLS, surse externe
Domeniu legitim compromis	site existent alterat	scădere scor, schimbări DNS/conținut, redirect-uri
Fast-flux / rotație	infrastructură schimbată rapid	evoluția DNS și tipare temporale

7.3.Principiile de utilizare a sistemului de reputație

Scorul exprimă rezultatul unui model bazat pe caracteristicile observate. Nu reprezintă o certitudine și trebuie interpretat împreună cu contextul. Orice măsură cu impact ridicat trebuie precedată de o verificare manuală a indicatorilor și a surselor.

Lipsa unui răspuns DNS/TLS din cauza unei erori tehnice nu trebuie confundată cu lipsa efectivă a serviciului sau cu un indicator malițios. Analiza trebuie să poată fi reconstituită: domeniu, dată, scor, versiune model, indicatori, decizie și persoana care a validat.

Nivelul de intervenție trebuie să corespundă severității și calității dovezilor. Un rezultat vechi trebuie reevaluat înaintea unei decizii, deoarece reputația și infrastructura se pot schimba.

În cazurile neclare se recomandă principiul confirmării prin surse independente. Un scor ridicat trebuie verificat prin cel puțin un indicator tehnic sau o sursă externă relevantă înainte de escaladare, atunci când situația permite. Această regulă nu înseamnă amânarea reacției la un incident evident, ci reducerea deciziilor bazate pe o singură observație care se poate dovedi eronată.

În mod similar, absența unei confirmări externe nu anulează automat alerta. Unele amenințări noi nu sunt încă prezente în feed-uri publice. Operatorul trebuie să păstreze un echilibru între confirmare și actualitate, folosind istoricul domeniului și modificările recente pentru a decide dacă este necesară monitorizarea, investigația sau escaladarea.

Vârsta domeniului și istoricul

Vârsta redusă poate crește suspiciunea deoarece multe campanii abuzive folosesc infrastructură recent creată, dar numeroase servicii legitime sunt, în mod natural, noi. Operatorul trebuie să coreleze *domain_age* cu celelalte caracteristici. Un domeniu nou cu certificat valid, date de registrar, coerente și fără semnale externe negative, poate necesita doar monitorizare, în timp ce un domeniu nou care apare simultan în mai multe surse de reputație necesită investigație prioritară.

Vechimea mare nu garantează siguranța. Domeniile legitime pot fi compromise, transferate sau reutilizate. De aceea, istoricul reputației și modificările recente sunt importante pentru detectarea situațiilor în care profilul tehnic se schimbă brusc.

Certificatul SSL/TLS

Prezența unui certificat SSL/TLS arată că serviciul poate stabili o conexiune criptată și oferă informații despre emitent, perioada de valabilitate și versiunea protocolului. Un atacator poate obține însă certificate valide, inclusiv prin servicii automatizate.

Prin urmare, *has_ssl* și *ssl_certificate_issuer* trebuie interpretate precum caracteristici ale modelului, nu ca verdict de legitimitate. Un certificat expirat sau o versiune TLS veche poate indica o problemă de mentenanță, dar nu dovedește intenție malițioasă.

DNSSEC și informațiile DNS

DNSSEC oferă protecție criptografică pentru autenticitatea răspunsurilor DNS, însă adoptarea sa nu este universală. Absența DNSSEC este un semnal de postură tehnică, nu o dovadă de abuz. În schimb, statusuri precum NXDOMAIN,

SERVFAIL sau REFUSED trebuie citite în contextul momentului evaluării. SERVFAIL poate reflecta o problemă temporară, iar REFUSED poate rezulta din politica serverului.

Înregistrările NS și MX ajută la înțelegerea infrastructurii. Schimbările bruște ale nameserverelor sau mutarea către o infrastructură neobișnuită pot justifica o investigație, mai ales dacă sunt însoțite de o scădere a reputației.

Totuși, schimbările legitime de hosting sau registrar pot produce același tip de semnal.

Registrar și datele de registru

Identificatorul registrarului este una dintre caracteristicile utilizate de model. Utilizatorul trebuie să evite concluzia că un registrar este „rău” doar pentru că unele domenii din portofoliul său au scoruri ridicate.

Corelațiile statistice pot reflecta volum, segment de clienți sau factori temporali. Datele registrarului sunt utile pentru escaladare și pentru context, dar decizia trebuie luată la nivelul domeniului și al dovezilor disponibile.

Blacklist și threat intelligence

Apariția într-o blacklist este un semnal puternic, dar sursele pot avea scopuri, frecvențe de actualizare și criterii diferite. Un domeniu poate rămâne listat după remediere sau poate apărea după compromiterea temporară a unui site legitim. Operatorul trebuie să noteze sursa, timestamp-ul și tipul indicatorului și, acolo unde este posibil, să verifice dacă listarea este încă activă.

Scorul unui domeniu se interpretează în raport cu definiția țintei și cu datele pe care a fost evaluat modelul. În studiul de caz, clasa pozitivă este definită prin apartenența la liste de blocare. O valoare ridicată a scorului pentru această clasă exprimă compatibilitatea caracteristicilor cu exemplele pozitive din corpus. Semnificația probabilistică și transferul către populația operațională necesită verificări distincte.

Categoria de prioritizare rezultă dintr-o regulă documentată, asociată versiunii modelului și condițiilor de colectare. Cazurile cu date insuficiente se marchează explicit. Confirmarea compromiterii se realizează prin analizarea dovezilor pentru serviciul și perioada investigate.

7.4. Nivelurile de risc și acțiunile recomandate

Nivelurile de risc trebuie să simplifice prioritizarea fără a ascunde incertitudinea. Pragurile exacte pot fi ajustate după calibrarea modelului și evaluarea costului erorilor.

Politica recomandă patru niveluri operaționale, utilizate ca punct de pornire pentru investigație.

Tabelul 14. Nivelurile de risc și acțiunile recomandate

Nivel	Interpretare	Acțiune recomandată
Trusted	risc redus conform semnalelor disponibile	monitorizare normală; revalidare la schimbări relevante
Watch	semnale neconcludente sau date incomplete	verificare suplimentară și urmărirea evoluției
High Risk	mai multe semnale negative / surse concordante	investigație prioritară; colectare dovezi; posibilă escaladare
Compromised / Critical	dovezi de compromitere sau incident activ	escaladare imediată și proces formal de răspuns

Un domeniu poate trece dintr-o categorie în alta pe măsură ce apar date noi. Operatorul nu trebuie să păstreze automat o etichetă istorică dacă informațiile actuale o contrazic. În același timp, schimbările bruște trebuie explicate și documentate, în special atunci când generează acțiuni operaționale.

Nivelul de risc trebuie separat conceptual de încrederea în date. Un caz poate avea severitate potențială ridicată, dar dovezi incomplete, situație în care acțiunea potrivită este investigația rapidă, nu declararea imediată a unui verdict. În schimb, mai multe surse concordante pot justifica escaladarea chiar dacă scorul numeric se află aproape de pragul dintre două categorii.

Pragurile operaționale trebuie revizuite periodic. Dacă numărul de alerte depășește capacitatea de analiză sau dacă prea multe alerte sunt închise ca rezultate fals pozitive, pragul și regulile de prioritizare trebuie reevaluate împreună cu echipa tehnică. Scopul nu este reducerea artificială a alertelor, ci menținerea unui volum care poate fi verificat fără a pierde cazurile cu risc real.

7.5. Procedura de investigare a unui domeniu

Investigația standard începe cu verificarea rezultatului curent și continuă cu elementele care pot confirma sau contrazice scorul. Ordinea de mai jos limitează bias-ul de confirmare: analistul nu caută doar dovezi care susțin categoria modelului, ci verifică activ și explicații alternative.

La finalul verificării, operatorul trebuie să consemneze concluzia și baza ei. O decizie minimă include domeniul, momentul analizei, categoria atribuită de sistem, indicatorii relevanți, sursele suplimentare consultate și acțiunea aleasă. Această evidență permite revizuirea ulterioară a cazului și este utilă pentru identificarea erorilor sistematice de interpretare.

Dacă datele sunt contradictorii, cazul nu trebuie forțat într-o concluzie definitivă. Poate fi încadrat temporar în monitorizare, cu o reevaluare după un interval stabilit. Această opțiune este importantă pentru domeniile nou create, pentru incidente aflate la început și pentru situațiile în care serviciile externe nu sunt disponibile la momentul verificării.

7.6. Instruire prin conștientizare pentru domeniile nou înregistrate

Domeniile nou înregistrate merită atenție deoarece au istoric redus și pot fi utilizate în campanii rapide. În același timp, caracteristica „nou" este comună tuturor proiectelor legitime recent lansate. Operatorul trebuie să verifice combinația de semnale: vârsta, nameserverele, certificatul, DNSSEC, registrarul și sursele de reputație. Lipsa unei componente nu este suficientă pentru clasificarea definitivă.

Operatorii trebuie să fie conștienți că această categorie generează natural rezultate fals pozitive. Numeroase proiecte, magazine, campanii sau servicii legitime folosesc domenii recent înregistrate și certificate emise în aceeași perioadă. În consecință, vârsta redusă trebuie să crească nivelul de atenție, dar să nu declanșeze singură o măsură restrictivă.

O investigație mai solidă corelează vârsta cu nameserverele, registrarul, existența serviciilor web și mail, informațiile TLS, apariția în feed-uri externe și eventualele asemănări lexicale cu entități cunoscute. Dacă semnalele sunt puține sau contradictorii, monitorizarea pe termen scurt poate furniza informații mai relevante decât o clasificare definitivă la prima evaluare.

În modulul dedicat domeniilor noi, recomandarea operațională este ca utilizatorul să urmărească motivele scorului și să diferențieze problemele de configurare de indicatorii de abuz. Dacă un domeniu nu apare în blacklist și nu există alte dovezi negative, o categorie Watch poate fi mai potrivită decât o escaladare imediată, în funcție de pragurile organizației.

Un domeniu legitim poate deveni periculos după compromiterea contului, infrastructurii sau aplicației web. În acest caz, caracteristicile istorice – vechime mare, registrar cunoscut, certificat valid – pot rămâne pozitive. Detectarea necesită monitorizarea schimbărilor: scădere bruscă de reputație, DNS modificat, redirect-uri, artefacte malware, content hash drift sau alte IoC. Aceste semnale trebuie corelate temporal pentru a evita atribuirea eronată a unei modificări legitime.

Pentru un domeniu cu reputație istorică bună, schimbarea este adesea mai relevantă decât valoarea absolută a unui indicator. Modificarea nameserverelor, emiterea neașteptată a unui certificat, apariția unor redirect-uri sau scăderea accelerată a scorului pot indica un eveniment care merită analizat chiar dacă domeniul nu a ajuns încă într-o categorie critică.

Instruirea trebuie să sublinieze că reputația pozitivă anterioară nu constituie o excepție permanentă. Domeniile legitime sunt ținte valoroase tocmai pentru că beneficiază de încredere. Pentru cazurile confirmate, după remediere este necesară o reevaluare pentru a verifica revenirea infrastructurii la o stare normală și pentru a evita închiderea prematură a incidentului.

Înainte de escaladare, analistul trebuie să verifice dacă semnalul este actual și reproductibil. De exemplu, un redirect poate fi produs de o campanie legitimă, geo-targeting sau o configurare temporară. Un indicator de malware confirmat de mai multe surse are o greutate mai mare decât o schimbare unică de conținut.

7.7. Analiza evoluției reputației

Evoluția temporală a reputației oferă context temporal și reduce dependența de o singură evaluare. Utilizatorul trebuie să urmărească direcția și amplitudinea modificărilor, nu doar valoarea absolută. Un scor stabil în timp oferă mai multă încredere decât un scor obținut pentru prima dată; o scădere bruscă necesită verificarea evenimentelor tehnice produse în aceeași perioadă.

Trendul nu trebuie extrapolat automat. O revenire rapidă poate indica remedierea unui incident, o eroare temporară de colectare sau o schimbare a datelor externe. Pentru cazurile importante se păstrează timestamp-urile și explicațiile fiecărei modificări relevante.

7.8. Roluri și responsabilități

Separarea rolurilor reduce riscul ca aceeași persoană să genereze, interpreteze și aprobe o acțiune critică fără control suplimentar. Pentru incidente cu severitate ridicată, politica recomandă minimum o validare de către un al doilea rol înaintea unei măsuri ireversibile, cu excepția situațiilor urgente definite de procedurile organizației.

Tabelul 15. Roluri și responsabilități

Rol	Responsabilități principale	Nu trebuie să facă
Operator	consultă alertele, verifică indicatorii, deschide cazuri	să considere scorul verdict automat
Analist	investighează, corelează surse, documentează și escaladează	să elimine dovezi contradictorii
Administrator platformă	acces, disponibilitate, loguri, backup, configurație	să modifice modelul fără versionare
Responsabil ML	monitorizare drift, validare, re-antrenare, rollback	să promoveze un model fără benchmark
Registrar / partener	investighează sesizările și sprijină remedierea	să interpreteze o alertă nevalidată ca sancțiune automată

Separarea responsabilităților reduce riscul ca aceeași persoană să genereze, interpreteze și închidă fără verificare o alertă cu impact major. Pentru incidente importante, analistul documentează concluzia, iar rolul responsabil validează acțiunea sau escaladarea. Administratorul tehnic menține platforma și datele operaționale, dar nu modifică retroactiv rezultatul unei investigații fără o justificare consemnată.

În perioadele în care un rol nu este disponibil, trebuie să existe un înlocuitor desemnat. Conștientizarea include și cunoașterea traseului de escaladare: cine poate fi contactat, în ce interval și ce informații trebuie transmise. O alertă corect identificată, dar trimisă fără context sau către persoana nepotrivită, poate întârzia reacția la fel de mult ca lipsa detecției.

7.9. Protecția datelor și utilizarea responsabilă

Platforma poate procesa date tehnice despre domenii, infrastructură, registrari și evenimente de evaluare. Accesul trebuie acordat pe principiul necesității de a cunoaște și al celui mai mic privilegiu. Logurile trebuie să conțină informațiile necesare pentru audit, dar nu trebuie să dubleze nejustificat date sensibile din sursele WHOIS sau token-uri de autentificare.

Perioada de păstrare trebuie stabilită în raport cu scopul. Logurile necesare auditului pot avea o durată diferită de cache-ul pentru interogări DNS sau de fișierele temporare generate în timpul unei evaluări. Păstrarea nediferențiată a tuturor datelor crește suprafața de risc și complică aplicarea principiului minimizării.

Exporturile și capturile folosite în instruire trebuie verificate înainte de distribuire. Dacă includ date operaționale, identificatori sau informații care nu sunt necesare scopului didactic, acestea trebuie eliminate sau anonimizate. Materialele de conștientizare trebuie să prezinte scenarii suficient de realiste pentru învățare fără a expune inutil date interne.

Datele cu caracter personal, atunci când apar în surse de registru, trebuie gestionate conform scopului legitim al proiectului și principiilor GDPR: minimizare, limitarea scopului, integritate, confidențialitate și perioade de păstrare justificate. Pentru analize statistice și dezvoltarea modelului se recomandă pseudonimizarea sau eliminarea câmpurilor care nu sunt necesare clasificării.

Exporturile și rapoartele trebuie să includă numai informațiile necesare destinatarului. Partajarea externă a unui caz trebuie să evite expunerea unor date care nu contribuie la investigație. Accesul la istoricul evaluărilor și la logurile administrative trebuie jurnalizat pentru a permite investigarea utilizării necorespunzătoare.

7.10. Managementul incidentelor și escaladarea

Un scor fără explicație poate conduce la automatizare excesivă. Interfața ar trebui să prezinte, acolo unde este posibil, factorii relevanți: vechimea domeniului, caracteristicile TLS, statusul DNS, blacklist-urile și evoluția reputației. Explicațiile SHAP pot fi folosite pentru a arăta ce caracteristici au împins predicția într-o direcție, însă nu trebuie descrise ca relații cauzale.

O explicație utilă trebuie să diferențieze faptul observat de interpretarea sa. De exemplu, „certificat emis recent” este un fapt tehnic, în timp ce „certificatul indică un domeniu malițios” este o concluzie care necesită context. Materialele de

instruire trebuie să păstreze această separare pentru a preveni transformarea corelațiilor modelului în reguli cauzale rigide.

Atunci când explicațiile automate sunt disponibile, operatorul le folosește ca punct de pornire pentru verificare, nu ca justificare finală. O decizie documentată trebuie să includă și surse verificabile: date de registru, rezultate DNS/TLS, feed-uri de reputație sau observații privind evoluția domeniului.

În comunicarea internă se preferă formulări precum „modelul a atribuit un scor ridicat deoarece semnalele X, Y și Z au contribuit la predicție" în locul formulării „domeniul este malițios deoarece nu are DNSSEC". Această diferență de limbaj reduce riscul ca un semnal statistic să fie transformat într-o regulă absolută.

Escaladarea se bazează pe activitatea observată, impactul potențial și urgența cazului. O suspiciune cu impact ridicat poate fi transmisă rapid pentru analiză, cu păstrarea explicită a incertitudinii.

Confirmarea unui incident se consemnează separat de recomandarea sau executarea unei măsuri. Pentru fiecare acțiune se înregistrează obiectul, justificarea, persoana care aprobă, executantul și rezultatul.

La reevaluare se actualizează aprecierea curentă și se păstrează versiunea anterioară. O modificare a scorului poate proveni din date noi, din schimbarea metodei sau dintr-o eroare de colectare. Trecerea la verdictul remediat se justifică prin verificări adecvate incidentului, iar rectificarea unei clasificări eronate se înregistrează cu motiv și responsabil. Produsele în care a fost folosită versiunea anterioară se identifică pentru corectare, după caz.

7.11. Programul de conștientizare și instruire

Conștientizarea nu trebuie redusă la citirea unui manual o singură dată. Utilizatorii care operează sistemul trebuie să primească o instruire inițială și actualizări atunci când se schimbă modelul, interfața sau procedurile. Pentru rolurile operaționale este utilă o sesiune practică bazată pe cazuri: domeniu benign nou, domeniu High Risk, domeniu legitim compromis și indisponibilitatea unei surse externe.

Pentru operatori, instruirea trebuie să insiste pe navigarea în platformă, interpretarea scorurilor și recunoașterea datelor incomplete. Pentru analiști se adaugă investigația multi-sursă, documentarea deciziilor și evaluarea contradicțiilor dintre indicatori.

Administratorii au nevoie de instruire privind logurile, controlul accesului, starea serviciilor și procedurile de escaladare tehnică.

O sesiune eficientă combină prezentarea cu exerciții. După explicarea principiilor, utilizatorul trebuie să analizeze câteva scenarii și să justifice acțiunea aleasă. Evaluarea nu trebuie să urmărească memorarea unor praguri, ci capacitatea de a explica de ce un caz necesită monitorizare, investigație sau escaladare.

Tabelul 16. Program de instruire

Activitate	Frecvență recomandată	Conținut
Integrare	la acordarea accesului	navigare, scoruri, niveluri de risc, escaladare
Revizuirea politicilor	anual sau la schimbări majore	erori frecvente de interpretare și politici actualizate
Exercițiu	trimestrial/semestrial	investigație pe scenarii simulate
Actualizarea modelului	la promovarea unei versiuni noi	schimbări în caracteristici, praguri și limitări
Evaluarea incidentului	după incident relevant	lecții învățate și actualizarea procedurilor

Scenariul A - Domeniu recent înregistrat

Un domeniu înregistrat de 12 zile are certificat TLS valid, nu are un indicator DNSSEC disponibil și nu apare în sursele negative consultate. Sistemul îl trimite la verificare suplimentară. Operatorul verifică actualitatea și starea colectării și explică de ce aceste observații sunt insuficiente pentru confirmarea abuzului. Stabilește verificările următoare și termenul reevaluării.

Răspuns așteptat: Vârsta redusă, certificatul și absența unei listări sunt observații contextuale. Verdictul poate rămâne neconcludent; nu se impune o concluzie benignă sau malițioasă numai pentru încheierea exercițiului.

Scenariul B - Modificarea bruscă a evaluării

Un domeniu urmărit curent este trecut în investigație prioritară. Sunt observate schimbări DNS și redirecționări. Analistul verifică dacă s-au modificat modelul, sursele sau serviciile și compară observațiile în timp. Examinează atât ipoteza compromiterii, cât și explicații precum o migrare sau o actualizare autorizată.

Răspuns așteptat: Creșterea scorului justifică verificarea. Confirmarea compromiterii necesită dovezi privind caracterul neautorizat sau malițios al activității, obiectul afectat și perioada.

Scenariul C - Listare contradictorie

Un nume apare într-o sursă negativă, în timp ce celelalte observații sunt obișnuite. Operatorul verifică sursa originară, data listării, categoria și resursa afectată. Stabilește dacă listarea privește aceeași gazdă și aceeași perioadă și documentează eventualele contradicții.

Răspuns așteptat: Numărul listelor nu substituie verificarea proveniență. Verdictul se justifică prin relevanța dovezilor; dezacordurile nerezolvate rămân explicite.

Scenariul D - Colectare incompletă

Conexiunea TLS expiră, iar rezoluția DNS este lentă. Operatorul consemnează erorile și verifică starea colectorului. Evaluarea continuă numai dacă metoda admite datele parțiale și rezultatul este marcat corespunzător; în caz contrar se amână și se programează o nouă încercare.

Răspuns așteptat: Timeout-ul nu este convertit într-o dovadă că serviciul nu are TLS sau că domeniul este malițios.

Eficiența programului de conștientizare poate fi urmărită prin indicatori simpli: procentul utilizatorilor instruiți, scorul la evaluările de instruire, timpul mediu de reacție la alerte, proporția cazurilor documentate complet, rata rezultatelor fals pozitive confirmată și timpul până la escaladare pentru cazurile critice. KPI-urile nu trebuie utilizate pentru a stimula închiderea rapidă în detrimentul calității investigației.

KPI-urile nu trebuie folosite izolat. Un timp de reacție foarte mic poate ascunde decizii superficiale, iar un număr mare de incidente închise nu indică automat eficiență. Este utilă corelarea timpului de reacție cu rata de confirmare, numărul de reanalizări și calitatea documentării. Obiectivul este un proces rapid atunci când dovezile sunt clare și suficient de riguros atunci când informațiile sunt contradictorii.

Revizuirea periodică a politicii trebuie să includă feedback din utilizare. Întrebările frecvente, greșelile recurente și situațiile care produc interpretări diferite între operatori indică zone unde documentația trebuie clarificată. Politica rămâne astfel un document operațional, actualizat pe baza modului în care platforma este folosită în practică.

Politica se revizuiește cel puțin anual și ori de câte ori apar schimbări semnificative în model, sursele de date, rolurile, legislația sau procedurile de răspuns. După un incident important, lecțiile învățate trebuie comparate cu regulile existente și integrate în versiunea următoare. Fiecare versiune a politicii trebuie păstrată pentru audit.

Tabelul 17. Etape de verificare pentru un domeniu

Moment	**Checklist**
La analizarea unui domeniu	Confirmare domeniu și date; verificare scor și categorie; consultare indicatori; verificare surse externe; consultare istoric; documentare concluzie.
Înainte de escaladare	Există minimum o dovadă independentă? Datele sunt actuale? S-a exclus o eroare de colectare? Impactul acțiunii este proporțional?
După remediere	Re-rulare evaluare; verificare dacă indicatorii s-au schimbat; notare rezultat; închidere caz doar după confirmare.
După update de model	Verificare versiune; consultare schimbări; rularea scenariilor de regresie; confirmarea că interpretarea scorurilor nu s-a schimbat neanunțat.

Instruirea se recomandă în format practic, pe fluxuri, nu exclusiv prin prezentarea meniurilor. O sesiune completă poate fi împărțită în trei module: orientare și interpretare, investigații ghidate și scenarii de incident. Utilizatorii trebuie să execute efectiv un lookup, o verificare de domeniu nou și o investigație de compromitere.

Tabelul 18. Etapele instruirii utilizatorilor

Modul	Durată orientativă	Conținut
Introducere	30 min	roluri, navigare, niveluri de risc
Analiză domeniu	60 min	lookup, indicatori, Momentum
Domenii noi	30 min	new domain check și interpretare
Compromiteri	45 min	anomalii, escaladare
Raportare	30 min	Raportare și audit
Exercițiu final	45 min	scenariu complet și justificarea deciziei

Trainerul trebuie să insiste asupra limitărilor: lipsa DNSSEC nu înseamnă automat rău intenționat, un certificat valid nu dovedește legitimitate, iar scorul modelului nu este un verdict. Scopul instruirii este obținerea unei decizii explicabile și reproductibile.

Evaluarea utilizatorilor trebuie să combine întrebări de înțelegere cu exerciții practice. Criteriul principal nu este memorarea meniurilor, ci capacitatea de a interpreta corect un caz și de a decide când este necesară escaladarea.

Tabelul 19. Evaluarea utilizatorilor

Competență	Exemplu de probă	Criteriu
Navigare	localizarea modulelor	fără asistență
Căutare	analiza unui domeniu	identifică scor, last scan și indicatori
Interpretare	caz cu semnale contradictorii	nu trage concluzie dintr-un singur semnal
Escaladare	caz High Risk/Compromised	alege fluxul corect
Raportare	rezumat investigație	include dovezi și limitări

Utilizatorii care nu îndeplinesc criteriile pentru cazurile critice trebuie să repete partea practică înainte de a primi responsabilități de escaladare. Rezultatele instruirii se păstrează conform politicilor interne aplicabile.

Utilizarea responsabilă a unui sistem de reputație presupune combinarea automatizării cu validarea umană. Modelul poate prioritiza eficient domenii și poate corela caracteristici care ar fi dificil de analizat manual la scară, dar decizia operațională trebuie să țină cont de calitatea datelor, de context și de evoluția în timp.

Politica de conștientizare standardizează interpretarea indicatorilor, nivelurile de risc, responsabilitățile și fluxul de escaladare. Aplicarea sa reduce atât riscul de rezultate fals pozitive tratate excesiv, cât și riscul ca un domeniu aparent legitim să fie ignorat după compromitere.

Documentul trebuie utilizat împreună cu raportul de validare și actualizat pe măsură ce platforma și modelul evoluează.

7.12. Protecția datelor și audit

Administratorul trebuie să mențină separarea mediilor, controlul configurației și trasabilitatea release-urilor. Modificările de infrastructură se execută controlat și se păstrează o cale de rollback. Bunele practici pentru administratori includ:

- monitorizarea latenței și erorilor;
- rotația și retenția controlată a logurilor;
- backup periodic și testarea restaurării;
- actualizarea componentelor și remedierea vulnerabilităților;
- principiul privilegii minime pentru conturi și servicii;
- smoke tests după implementare;
- versionarea separată a aplicației și a modelului ML.

Backup-ul fără test de restaurare nu este suficient. Periodic, o restaurare trebuie verificată într-un mediu controlat pentru a confirma că fișierele și baza de date pot fi recuperate în mod coerent.

Securitatea unui sistem de reputație trebuie abordată prin defense in depth. Autentificarea limitează accesul, validarea inputului reduce riscul de injecție, iar rate limiting-ul protejează endpoint-urile costisitoare. Dependențele trebuie actualizate, iar accesul administrativ trebuie auditat.

Tabelul 20. Bune practici pentru protecția datelor

Control	Bună practică
Autentificare	conturi individuale, politici interne de parolă/MFA dacă este disponibil
Autorizare	least privilege
Input	validare FQDN, lungime și caractere permise
Web	CSRF/XSS protections și escaping
API	rate limit, timeout, autentificare
Secrete	variabile/secret store, niciodată în cod
Audit	log pentru acțiuni administrative și release-uri

Datele WHOIS și logurile pot conține informații care necesită protecție. Buna practică este minimizarea: se păstrează doar datele necesare scopului operațional, se limitează accesul și se stabilește o perioadă de retenție. Exporturile trebuie controlate, iar rapoartele nu trebuie să conțină date personale fără justificare.

Auditul trebuie să fie suficient pentru a demonstra cine a executat o acțiune administrativă și când, fără a transforma logurile într-o copie completă a datelor de lucru.

Pentru investigații, request_id și timestamp-ul sunt preferabile copieri repetate ale conținutului sensibil.

Bune practici includ:
- separarea logurilor tehnice de audit trail;
- controlul accesului la loguri;
- retention policy documentată;
- anonimizare sau pseudonimizare unde este posibil;
- revizuirea exporturilor și a rapoartelor înainte de distribuție.

Modelul trebuie gestionat ca un artefact versionat. Antrenarea, validarea și promovarea sunt etape separate. Preprocesarea, inclusiv maparea booleenelor, codificarea categoriilor și alinierea caracteristicilor, trebuie să fie identică între train și inference. Ideal, transformările sunt incluse într-un pipeline salvat și testat.

Pentru validare se recomandă separarea temporală și/sau pe grupuri atunci când există riscul ca domenii înrudite să ajungă în train și test.

Tabelul 21. Auditul modelului

Etapă	**Control minim**
Antrenare	snapshot date, seed, cod și configurație versionate
Validare	set separat, metrici multiple, error analysis
Promovare	comparare cu model curent și smoke test
Producție	model_version și feature_schema în log
Monitorizare	drift, missing values, feedback
Rollback	artefact anterior disponibil și testat

8. Utilizare, instruire și monitorizare continuă

8.1. Scop, public și condiții de utilizare

Instruirea urmărește formarea unui mod reproductibil de lucru pentru operatori, analiști și administratori. Competențele esențiale sunt identificarea corectă a obiectului, verificarea datelor, interpretarea scorurilor și consemnarea deciziei. Aceste principii sunt independente de interfața utilizată.

Sistemul de reputație este un sistem de suport decizional. Rezultatul unei evaluări trebuie corelat cu indicatorii tehnici disponibili, cu istoricul domeniului și cu sursele externe. În special, un scor ridicat de risc nu reprezintă singur dovada unei activități malițioase, iar un scor favorabil nu reprezintă o garanție absolută de siguranță.

Materialele de instruire trebuie să utilizeze scenarii documentate și date adecvate scopului didactic. Denumirile modulelor se adaptează instrumentului folosit, iar exercițiile urmăresc funcțiile de analiză și calitatea deciziilor, fără a depinde de o anumită organizare vizuală.

Tabelul 22. Roluri și responsabilități

Rol	Utilizare principală	Responsabilitate
Operator	lookup (căutare), dashboard (tablou de bord), verificări curente	analizează și documentează cazurile
Analist	investigații și corelare semnale	validează și escaladează
Administrator	configurare, acces, operare	menține disponibilitatea și auditul
Responsabil ML	versiuni model și revalidare	controlează calitatea modelului

Accesul la funcțiile principale este rezervat utilizatorilor autentificați. Utilizatorul introduce credențialele în pagina de login, iar după autentificare primește acces la modulele permise rolului său. La terminarea sesiunii se utilizează funcția de logout, în special pe stații partajate sau în contexte operaționale în care accesul neautorizat ar putea expune informații despre investigații.

Fiecare cont trebuie să primească numai drepturile necesare sarcinilor curente. Un operator nu trebuie să dețină implicit permisiuni administrative, iar acțiunile cu impact asupra configurației sau modelului trebuie separate de activitățile obișnuite de consultare.

Se pot defini regulile de sesiune precum:

- nu se partajează conturile între utilizatori;
- sesiunile se închid după finalizarea activității;

- erorile de autentificare repetate se raportează administratorului;
- permisiunile necorespunzătoare se tratează ca problemă de acces, nu se ocolesc prin utilizarea altui cont.

8.2. Fluxuri standard de lucru

Lookup obișnuit

panoul de sinteză → registrul de domenii → lookup → verificare scor și last scan → analiză indicatori → consultare Momentum → concluzie și notă operațională.

Domeniu nou

New domain check → verificare vârstă/înregistrare → DNS/SSL/TLS → blacklist → corelare semnale → Watch sau investigație, după caz.

Domeniu legitim cu schimbare bruscă

Compromise Watch → comparare istoric → verificare DNS/TLS și semnale suplimentare → clasificare incident → escaladare → revalidare după remediere.

Generare raport

Finalizarea analizei → raportarea → generare → verificare conținut → distribuire către destinatarii autorizați.

Situațiile frecvente și troubleshooting pot include:

Tabelul 23. Situații ce necesită analiză

Simptom	**Cauză posibilă**	**Ce face utilizatorul**
lookup nu se finalizează	sursă externă lentă / serviciu indisponibil	reîncearcă o dată, apoi raportează cu timestamp
WHOIS lipsă	timeout/rate limit	nu presupune că domeniul este liber; verifică statusul
DNS SERVFAIL	problemă de rezoluție	notează răspunsul și verifică ulterior
SSL lipsă	domeniu fără TLS sau handshake eșuat	distinge între proprietate și eroare de colectare
scor neașteptat	date noi / caracteristică lipsă / model	verifică indicatorii și istoricul
raport blocat	worker/job failure	verifică status, apoi solicită suport

La raportarea unei probleme, utilizatorul furnizează minim: modulul, domeniul dacă este relevant, ora aproximativă, acțiunea executată și mesajul de

eroare. Nu se transmit parole și nu se copiază date personale care nu sunt necesare depanării.

8.3. Obiectivele monitorizării în exploatare

Trecerea de la prototip la exploatare necesită monitorizarea întregului lanț: colectarea caracteristicilor, accesul la surse, evaluarea, persistența și raportarea. Disponibilitatea paginii web nu demonstrează funcționarea corectă a surselor sau actualitatea predicțiilor. Planul de monitorizare trebuie să lege fiecare indicator de un responsabil și de o acțiune verificabilă.

Arhitectura de referință rămâne cea documentată anterior: aplicația principală este construită în Django și utilizează PostgreSQL, serviciile sunt containerizate, iar componenta de reputație bazată pe machine learning este expusă printr-un serviciu Flask. Pentru caracterizarea domeniilor sunt utilizate date de registru, WHOIS/DAS, DNS și SSL/TLS. Monitorizarea trebuie, prin urmare, să permită localizarea rapidă a unei degradări la nivelul oricăreia dintre aceste dependențe.

Obiectivele acestei secțiuni sunt definirea criteriilor post-lansare, stabilirea indicatorilor care trebuie urmăriți, descrierea alertării și a procesului de remediere, monitorizarea calității modelului ML și furnizarea unui set de proceduri repetabile pentru operarea platformei. Accentul este pus pe trasabilitate: fiecare incident, schimbare de versiune și abatere de la pragurile stabilite trebuie să poată fi urmărite ulterior.

Tabelul 24. Criteriile post-lansare

Obiectiv	**Ce se urmărește**	**Rezultat așteptat**
Disponibilitate	starea serviciilor web, API și bază de date	detectarea rapidă a indisponibilității
Performanță	latență, throughput, timpi dependențe externe	identificarea bottleneck-urilor
Calitate ML	distribuția scorurilor, erori, drift	menținerea utilității modelului
Trasabilitate	loguri, versiuni, utilizator, domeniu	audit și reproducerea incidentelor
Continuitate	retry, fallback, rollback	degradare controlată în caz de eroare

8.4. Lansarea în producție, controlul release-ului și monitorizare

Lansarea în producție trebuie tratată ca un proces controlat, nu ca o simplă copiere a prototipului pe un server accesibil utilizatorilor. Build-ul candidat este verificat înainte de promovare, configurația este separată de cod iar componentele care conțin secrete sau date de conectare sunt furnizate prin mecanisme dedicate de configurare. Versiunile aplicației și ale modelului ML trebuie să poată fi identificate independent.

După promovarea release-ului se execută un set scurt de smoke tests. Se verifică răspunsul paginii de autentificare, accesul unui utilizator autorizat, citirea datelor din bază, evaluarea unui domeniu de test, încărcarea dashboard-ului și funcționarea unui flux de raportare. Pentru componenta ML se verifică atât încărcarea modelului, cât și alinierea exactă a caracteristicilor la structura salvată în timpul antrenării.

Tabelul 25. Monitorizarea aplicației

Control	Moment	Criteriu
Health check aplicație	post-deploy	răspuns fără eroare și dependențe principale disponibile
Migrare DB	pre/post	schema compatibilă cu versiunea aplicației
Model ML	post	model încărcat și predicție executată
Lookup domeniu	post	date afișate fără blocarea fluxului
Rollback	pre	procedură și artefact anterior disponibile

Strategia de monitorizare este organizată pe patru straturi: experiența utilizatorului, serviciile aplicației, dependențele externe și calitatea modelului ML. Separarea acestor straturi este importantă deoarece un scor care nu poate fi generat la timp poate avea cauze foarte diferite: o problemă a aplicației, o interogare externă lentă, indisponibilitatea bazei de date sau o eroare de preprocesare.

Pentru fiecare componentă se definesc indicatori de nivel de serviciu (SLI) și obiective interne (SLO). Pragurile trebuie stabilite pe baza măsurătorilor reale din mediul final. În această documentație sunt definite tipurile de indicatori și relația lor cu acțiunile operaționale, nu valori fictive de producție.

Tabelul 26. Indicatori de nivel de serviciu

Domeniu	SLI recomandat	Acțiune la degradare
Aplicație web	availability, p95 latency, 5xx rate	investigare serviciu/container și dependențe
API ML	inference success rate, p95 inference	verificare model, alinierea caracteristicilor, resurse
PostgreSQL	connection errors, query latency	pool, indexuri, blocaje, capacitate
Surse externe	timeout/error rate pe sursă	retry, circuit breaker, fallback
Job-uri	durată, backlog, failed jobs	reprocesare și dimensionare workers

Alertele trebuie clasificate după impact: informativ, warning, high și critical. O eroare izolată la o interogare SSL nu este echivalentă cu indisponibilitatea generală a serviciului. Severitatea este determinată de amploare, durată și efectul asupra funcțiilor critice.

Monitorizarea aplicației trebuie să permită corelarea metricilor cu logurile. Pentru traficul web se urmăresc rata de cereri, timpii de răspuns, codurile HTTP și excepțiile. Pentru runtime se urmăresc CPU, memorie, spațiu pe disc și restarturile containerelor. În cazul bazei de date sunt relevante conexiunile, interogările lente, blocajele și creșterea volumului de date.

Măsurarea exclusivă a mediei poate ascunde degradările resimțite de utilizatori.

Tabelul 27. Monitorizarea traficului web, runtime și a bazei de date

Metrică	Semnificație	Interpretare
5xx rate	erori server	creșterea indică defecte de aplicație sau dependențe
CPU/RAM	presiune pe runtime	corelată cu concurența și job-urile
DB query time	performanța persistenței	poate indica indexuri sau lock-uri

Monitorizarea unui sistem ML nu se oprește la disponibilitatea endpoint-ului de inferență. Modelul poate continua să răspundă tehnic, dar să devină mai puțin util dacă distribuția datelor se schimbă. Din acest motiv, trebuie urmărite atât metricile operaționale, cât și caracteristicile intrărilor și distribuția scorurilor produse.

Se recomandă agregarea periodică a proporției de domenii încadrate în categoriile operaționale și a distribuțiilor pentru caracteristici cheie precum domain_age, registrar_id, has_dnssec, has_ssl și datele TLS. Modificările bruște pot semnala fie o schimbare reală în populația de domenii, fie o problemă de colectare/preprocesare.

Concept drift și data drift trebuie tratate separat. Data drift indică schimbarea distribuției datelor de intrare, în timp ce concept drift presupune schimbarea relației dintre semnale și eticheta reală. Confirmarea celui de-al doilea necesită etichete ulterioare sau investigații manuale. Un semnal de drift nu trebuie să declanșeze automat reantrenarea fără validare.

Fiecare predicție relevantă pentru audit trebuie asociată unei versiuni de model și unei versiuni de schemă a caracteristicilor. O versiune nouă se promovează doar după validare pe set separat și după compararea cu modelul curent. Rollback-ul trebuie să poată fi realizat fără reconstruirea întregii aplicații.

Tabelul 28. Elemente monitorizate, riscuri și recomandări

Element monitorizat	Semnal de risc	Răspuns recomandat
Distribuția scorurilor	schimbare abruptă față de valorile de bază	verificare surse
Valori lipsă	creștere susținută	verificare WHOIS/DNS/TLS
Fals pozitive confirmate	tendință ascendentă	prag/calibrare/reantrenare
Versiunea modelului	diferențe neașteptate între versiuni	rollback și analiză comparativă
Importanța caracteristicilor	dominare nouă neexplicată	analiză de bias/leakage

Un sistem de reputație poate depinde de servicii care nu sunt controlate integral de aplicație. Din acest motiv, orice raport de monitorizare trebuie să distingă între eroarea internă și degradarea unei surse externe. În special, WHOIS/DAS, DNS și negocierea SSL/TLS pot avea timpi de răspuns variabili sau pot aplica limite de rată.

Pentru WHOIS/DAS se urmăresc disponibilitatea, timpul de conectare, timpul total de răspuns și tipurile de status returnate. Mecanismul de colectare documentat anterior include o limitare tocmai pentru a evita blocarea. Orice creștere a timeout-urilor trebuie separată de situațiile în care domeniul este pur și simplu disponibil sau nu este disponibil.

Monitorizarea DNS trebuie să facă diferența între NXDOMAIN, SERVFAIL, REFUSED și timeout. Aceste rezultate au semnificații diferite și nu trebuie agregate sub o singură etichetă de eroare. Pentru domeniile active se pot verifica suplimentar schimbările NS, MX și prezența DNSSEC.

Pentru SSL/TLS se monitorizează succesul handshake-ului, expirarea certificatelor, versiunea TLS și fallback-ul către portul 80 atunci când handshake-ul nu poate fi realizat. Lipsa informației TLS trebuie înregistrată separat de clasificarea reputațională pentru a evita confundarea unei probleme de colectare cu o proprietate a domeniului.

Tabelul 29. Metrici DNS, SSL/TLS și de registru

Sursă	Metrici	Fallback / reacție
WHOIS/DAS	latență, timeout, limitarea ratei	reîncercare controlată, cache
DNS	NXDOMAIN/SERVFAIL/REFUSED/timeout	reîncercare limitată, rezolver alternativ dacă este permis
SSL/TLS	Succes la stabilirea conexiunii, analiza certificatului	fallback HTTP pentru informații minime
API registru	disponibilitate, cod de răspuns, latență	cache pentru date stabile, alertare

Pe lângă serviciile tehnice, trebuie monitorizate și fluxurile pe care le utilizează efectiv operatorii. Un health check care răspunde cu HTTP 200 nu demonstrează că panoul de sinteză afișează date coerente sau că registrul de domenii poate finaliza o analiză de domeniu. De aceea sunt recomandate teste sintetice periodice pentru fluxurile critice.

Tabelul 30. Monitorizarea fluxurilor utilizate de operatori

Modul	Flux monitorizat	Semnal de defect
Sinteză operațională	încărcare sumar și navigare	metrici lipsă sau blocare dashboard
Registru de domenii	lookup și afișare reputație	lookup eșuat / date incoerente
Istoricul reputației	generare istoric	grafice fără date sau ordine temporală eronată

Modul	Flux monitorizat	Semnal de defect
Domenii noi	evaluare domeniu recent	surse necorelate / timeouts
Compromiteri	scan și semnale de anomalie	job incomplet / semnale absente
Portofolii	afișare profil registrar	date lipsă / mapping invalid
Raportare	generare și acces raport	job blocat sau fișier indisponibil

Raportarea periodică trebuie să combine indicatorii tehnici cu indicatorii funcționali și ML. O singură valoare de uptime nu este suficientă pentru a descrie calitatea serviciului. Se recomandă raportarea pe intervale stabile – zilnic pentru incidente și disponibilitate, săptămânal pentru tendințe operaționale și lunar pentru performanța modelului și capacitate.

Valorile de mai jos reprezintă câmpuri de raportare ce trebuie completate din sistemul de monitorizare. Tabelul reprezintă un model de raportare care se completează cu măsurători din exploatare. Baseline-ul inițial poate folosi rezultatele de performanță documentate în fazele anterioare doar ca referință pentru componenta ML, nu ca dovadă de uptime în producție.

Tabelul 31. Model de raportare

Indicator	Valoare perioadă	Tendință	Acțiune/observații
Uptime aplicație	[de completat]	[de completat]	
p95 lookup domeniu	[de completat]	[de completat]	
Rată 5xx	[de completat]	[de completat]	
Disponibilitate WHOIS/DAS	[de completat]	[de completat]	
Rată succes inferență ML	[de completat]	[de completat]	
Job-uri raport eșuate	[de completat]	[de completat]	
Alerte drift	[de completat]	[de completat]	

Un raport final de perioadă trebuie să includă maximum câteva concluzii acționabile: ce s-a degradat, ce s-a îmbunătățit, ce incidente au necesitat intervenție și ce schimbări sunt propuse pentru următoarea perioadă. Astfel se evită acumularea de metrici fără valoare operațională.

Monitorizarea are valoare doar dacă rezultatele sunt transformate în acțiuni. Pentru un sistem de reputație, optimizarea trebuie orientată în primul rând către dependențele I/O și către eliminarea operațiilor repetitive. Caching-ul cu TTL controlat este potrivit pentru informații relativ stabile iar operațiile independente pot fi executate asincron. Timeout-urile trebuie definite per sursă pentru a preveni blocarea întregului request.

La nivelul bazei de date, creșterea volumului de evaluări impune verificarea indexurilor pe câmpurile utilizate în filtrare și ordonare. La nivelul modelului, îmbunătățirea continuă înseamnă validarea periodică a performanței, calibrarea scorurilor atunci când acestea sunt prezentate utilizatorului drept nivel de încredere și menținerea unui proces de versionare și rollback.

Tabelul 32. Monitorizare și măsuri de remediere

Problemă observabilă	Măsură	Efect urmărit
request-uri externe lente	timeout + async + cache	latență mai previzibilă
query-uri repetate	indexuri + cache	încărcare DB redusă
job-uri în backlog	workers și batching	timp de procesare redus
scoruri instabile	monitorizare drift + revalidare	calitate ML menținută
release defect	canary/smoke + rollback	impact limitat

Monitorizarea unui sistem de reputație trebuie să distingă schimbarea fenomenului observat de schimbarea capacității de observare. Dacă o sursă răspunde mai rar, distribuția atributelor poate varia fără ca domeniile să se fi modificat. Dacă se schimbă populația interogată, proporția alertelor poate varia fără o degradare a modelului. Un tablou de monitorizare trebuie să permită examinarea acestor explicații înainte de formularea unei concluzii despre performanță.

Pentru fiecare perioadă se pot compara numărul solicitărilor, proporția rezultatelor utilizabile, cauzele erorilor și compoziția populației analizate. O modificare a ratei de alerte se interpretează împreună cu aceste elemente. De exemplu, creșterea interogărilor pentru domenii deja semnalate poate crește proporția scorurilor ridicate fără să indice o schimbare generală a amenințărilor. Monitorizarea trebuie să păstreze contextul selecției, inclusiv canalul prin care cazurile au intrat în sistem.

Detectarea unei schimbări distribuționale constituie un semnal pentru analiză, nu o demonstrație că modelul a devenit inutil. În absența unor etichete recente, nu poate fi măsurată direct performanța predictivă pe perioada respectivă. Se poate verifica funcționarea colectării și se pot examina exemple, dar raportul trebuie să distingă aceste verificări de validarea statistică. Această delimitare împiedică prezentarea stabilității infrastructurii drept dovadă a stabilității preciziei.

Documentația de monitorizare oferă cadrul operațional pentru consemnarea incidentelor și a schimbărilor. Dezvoltarea metodologică propusă aici leagă fiecare alertă de monitorizare de o ipoteză verificabilă: indisponibilitate a sursei, modificare a schemei, schimbare a populației sau degradare confirmată prin etichete. Alegerea intervenției se face după această analiză. Reantrenarea nu trebuie să înlocuiască repararea colectării și nici să ascundă o schimbare nedeclarată a obiectivului.

O versiune nouă poate fi examinată pe același flux de observații ca versiunea curentă, fără ca rezultatele sale să determine imediat acțiunile. Această comparație permite identificarea diferențelor de scor și a cazurilor afectate de schimbare. Ea nu demonstrează singură o îmbunătățire, deoarece acordul cu versiunea precedentă nu reprezintă o referință a adevărului. Cazurile divergente trebuie analizate în raport cu dovezile disponibile și cu obiectivul utilizării.

Compararea trebuie să păstreze aceeași definiție a intrării. Dacă noua versiune utilizează alte surse sau alte transformări, diferența observată nu poate fi atribuită exclusiv modelului. Se documentează separat schimbările de date, de algoritm și de politică. Atunci când este posibil, examinarea lor succesivă clarifică contribuția

fiecărei modificări. Dacă schimbările sunt inseparabile, raportul le descrie ca o modificare comună a sistemului.

Criteriile de adoptare pot include calitatea predicțiilor, proporția cazurilor fără rezultat, timpul de răspuns și posibilitatea explicării. Criteriile trebuie stabilite înainte de comparare și interpretate împreună. O reducere a timpului de procesare nu compensează automat o degradare inacceptabilă a rezultatelor, după cum o diferență predictivă mică nu justifică orice cost operațional. Decizia consemnează compromisurile acceptate și condițiile în care acestea vor fi reevaluate.

Revenirea la versiunea precedentă trebuie să includă compatibilitatea datelor și a transformărilor, nu doar înlocuirea unui fișier de model. Un model anterior poate necesita o schemă care nu mai este produsă de colectorul actual. Procedurile de versionare trebuie astfel aplicate întregului lanț. Înregistrarea versiunii folosite pentru fiecare evaluare permite ulterior explicarea diferențelor și reconstituirea rezultatelor relevante.

Tabelul 33. Matrice de monitorizare

Componentă	Control	Frecvență	Severitate
Web	/login disponibil	5 min	High
Web	rata HTTP 5xx	5 min	High
API ML	sănătate/inferență	5 min	Critical
DB	conexiuni eșuate	5 min	Critical
DB	latența interogării	15 min	Warning
WHOIS/DAS	Rata de timeout	15 min	Warning
DNS	SERVFAIL/timeout	15 min	Warning
TLS	eșec al negocierii conexiunii	30 min	Warning
Workers	sarcini eșuate	10 min	High
Reports	backlog	30 min	Warning
ML	distribuția scorurilor	zilnic	Warning
ML	rata caracteristicilor lipsă	zilnic	High
ML	drift	săptămânal	High
Storage	spațiu liber	15 min	High
Audit	acțiuni administrative	continuu	Informativ

Checklist operațional

Checklist zilnic

- verificarea alertelor critical/high neînchise;
- verificarea ratei de erori și a latenței p95/p99;
- verificarea job-urilor eșuate sau blocate;
- verificarea disponibilității WHOIS/DAS, DNS și TLS;
- verificarea spațiului pe disc și a restarturilor containerelor.

Checklist săptămânal

- analiza tendințelor de latență și volum;
- revizuirea incidentelor și a cauzelor recurente;
- verificarea distribuției scorurilor ML și a missing values;
- revizuirea modificărilor de configurație și a audit trail-ului.

Checklist după release

- smoke tests pentru autentificare, lookup, inferență și raportare;
- compararea metricilor cu baseline-ul anterior;
- confirmarea versiunii de model și a schemei de caracteristici;
- confirmarea procedurii de rollback și păstrarea artefactului anterior.

8.5. Logging și trasabilitate

Logarea trebuie structurată astfel încât un incident să poată fi urmărit de la acțiunea utilizatorului până la dependența care a produs eroarea. Pentru cererile de analiză se recomandă un identificator de corelare transmis între aplicația web, serviciul ML și job-urile asincrone. Acest identificator permite reunirea evenimentelor fără a stoca mai multe date personale decât este necesar.

Pentru predicții, logul operațional ar trebui să păstreze versiunea modelului, timestamp-ul, starea colectării caracteristicilor și rezultatul, evitând includerea nejustificată a datelor sensibile. Pentru accesul administrativ se păstrează un audit trail separat, care consemnează schimbări de configurație, promovări de model și operațiuni de rollback.

Tabelul 34. Logging și trasabilitate

Eveniment	Câmpuri minime	Scop
Request analiză	timestamp, request_id, endpoint, status	corelare și depanare
Inferență ML	model_version, feature_schema, rezultat	reproductibilitate
Eroare externă	sursă, timeout/status, request_id	separarea dependențelor
Acțiune admin	utilizator, acțiune, moment	audit
Deployment	release id, model id, rezultat smoke test	trasabilitate release

8.6. Managementul incidentelor și scenarii operaționale

Scenariile următoare sunt propuse pentru testarea procesului operațional. Ele nu sunt prezentate ca incidente reale. Pentru fiecare caz se urmăresc detectarea, clasificarea severității, limitarea impactului, remedierea și verificarea finală.

Tabelul 35. Managementul incidentelor

Scenariu	Impact posibil	Răspuns
WHOIS indisponibil	caracteristici incomplete, latență	fallback, marcare date lipsă, alertă dacă persistă
Creștere 5xx	indisponibilitate parțială	corelare loguri
Bază de date lentă	dashboard și căutare lentă	query analysis, indexuri, conexiuni
ML endpoint indisponibil	fără scor nou	restart controlat / rollback model-serviciu
Drift al scorurilor	clasificări potențial degradate	analiză distribuții și revalidare model
Job raport blocat	rapoarte indisponibile	reprocesare și verificare worker

Fluxul de escaladare recomandat este: detecție → validare inițială → clasificare severitate → alocare responsabil → limitare impact → remediere → revalidare → închidere. Închiderea unui incident trebuie să includă o cauză probabilă sau confirmată și, pentru incidentele semnificative, o măsură preventivă.

8.7. Optimizare și îmbunătățire continuă

Cazurile analizate de operatori pot îmbunătăți datele de referință, dar selecția lor trebuie înțeleasă. Dacă sunt verificate numai alertele cu scor ridicat, colecția rezultată nu descrie toate domeniile procesate. Ea oferă informație despre partea selectată de model.

Folosirea acestei colecții pentru evaluarea generală poate ascunde erorile din zona scorurilor mici și poate consolida preferințele modelului inițial.

Un program de verificare poate include atât cazuri prioritizate, cât și un eșantion din celelalte categorii. Cele două componente au scopuri diferite: intervenția rapidă și evaluarea procesului. Dimensiunea lor depinde de resurse, însă mecanismul de selecție trebuie înregistrat. În analiza rezultatelor, cazurile selectate prin reguli diferite nu se reunesc ca și cum ar proveni dintr-o selecție uniformă. Proveniența etichetei include astfel și motivul pentru care cazul a fost verificat.

Evaluatorul trebuie să poată separa dovezile de predicția pe care o verifică. Dacă verdictul final reproduce scorul fără examinarea unor informații suplimentare, eticheta nu reprezintă o confirmare independentă. În activitatea curentă, ascunderea scorului nu este întotdeauna oportună, dar pentru anumite exerciții de control poate permite examinarea influenței sale asupra judecății. Condițiile evaluării se consemnează pentru a interpreta corect acordul dintre om și model.

Integrarea cazurilor în antrenare se face după verificarea calității și a versiunii etichetelor. Corecțiile ulterioare trebuie să poată fi urmărite până la corpusurile care le-au utilizat.

Recomandările privind instruirea, auditul și ciclul de viață al modelelor susțin această organizare. Îmbunătățirea continuă devine astfel un proces de acumulare controlată a dovezilor, nu o simplă reciclare a predicțiilor anterioare ca etichete definitive.

Exploatarea unui sistem distribuit de reputație necesită observarea aplicației, bazelor de date, serviciului de evaluare și surselor externe. Disponibilitatea și performanța se urmăresc împreună cu acoperirea datelor, erorile confirmate și versiunile. În condiții de degradare, rezultatul trebuie să indice limitele datelor folosite.

În exploatare, succesul trebuie evaluat prin stabilitatea fluxurilor critice și prin capacitatea echipei de a detecta și remedia rapid abaterile. Caching-ul, procesarea asincronă, timeout-urile, logging-ul structurat și rollback-ul sunt mecanisme complementare. Pentru componenta ML, versionarea, revalidarea și observarea drift-ului sunt obligatorii pentru a evita situația în care un serviciu disponibil tehnic produce rezultate din ce în ce mai puțin relevante.

Cadrul prezentat în acest capitol susține operarea controlată a platformei. Valorile reale de producție vor completa matricea de monitorizare pe măsură ce sunt colectate, fără a modifica principiile de măsurare și responsabilitățile definite aici.

9. Procedura de înregistrare și validare a informațiilor despre domenii malițioase

Evaluarea automată devine utilă operațional atunci când fiecare observație este asociată unui domeniu, unei surse, unui moment și unei decizii verificabile. Procedura propusă definește un circuit independent de platformă pentru înregistrarea și actualizarea informațiilor despre domenii suspecte sau confirmate ca malițioase. Ea poate fi implementată într-un registru de cazuri sau într-o aplicație de management al incidentelor. Câmpurile reprezintă cerințe de evidență, nu funcționalități presupuse ale unui produs.

Înregistrarea unui caz nu produce automat blocarea domeniului, notificarea unor terți sau introducerea într-o listă distribuită public. Aceste acțiuni au propriile roluri de aprobare și trebuie documentate separat. Scopul procedurii este transformarea unei semnalări într-un ansamblu de observații și concluzii care poate fi revizuit, corectat și urmărit în timp.

9.1. Scopul și unitatea de evidență

Unitatea principală de evidență este cazul de investigație, identificat printr-un cod unic. Un caz poate conține mai multe observații asupra aceluiași domeniu și poate fi legat de alte cazuri ale aceleiași campanii. Domeniul , numele complet al gazdei și adresa URL se păstrează distinct, deoarece activitatea malițioasă poate afecta numai un subdomeniu sau o resursă. Extinderea concluziei la întregul domeniu necesită justificare explicită.

Procedura se aplică semnalărilor introduse manual, alertelor automate și importurilor din surse externe. În cazul importului în lot, validările de structură pot fi automatizate, dar proveniența fiecărei observații trebuie păstrată. Un lot nu reprezintă o singură dovadă uniformă: intrările sale pot avea date de observare, categorii și niveluri de încredere diferite.

O evidență completă separă datele brute de interpretări. Răspunsul DNS, rezultatul unei interogări și captura unui comportament observat sunt date; concluzia că infrastructura deservește phishing este o interpretare fundamentată. Operatorul nu modifică observația inițială pentru a o face să corespundă verdictului. O corecție produce o versiune nouă și păstrează justificarea schimbării.

9.2. Rolurile și responsabilitățile

Operatorul de introducere preia semnalarea, verifică identitatea obiectului analizat, caută cazurile existente și completează câmpurile obligatorii. El poate marca înregistrarea ca incompletă sau poate solicita informații suplimentare. În lipsa

atribuțiilor de validare, operatorul nu schimbă singur starea în malițios confirmat și nu aplică măsuri asupra infrastructurii externe.

Analistul examinează dovezile, verifică actualitatea și independența surselor, stabilește întinderea afectării și formulează verdictul motivat. Pentru deciziile cu impact ridicat se desemnează un responsabil de aprobare distinct, potrivit organizării interne. Administratorul asigură funcționarea registrului, drepturile de acces, integritatea jurnalului și recuperarea evidențelor. Responsabilul componentei ML gestionează utilizarea ulterioară a etichetelor validate.

Separarea rolurilor poate fi adaptată dimensiunii echipei, dar identitatea persoanei care a introdus datele trebuie să rămână distinctă de identitatea persoanei care a aprobat măsura. În echipele mici, excepțiile de la verificarea independentă se consemnează și se revizuiesc ulterior. O aprobare se raportează la versiunea exactă a dovezilor și a concluziei, nu la un caz aflat încă în modificare.

9.3. Inițierea și verificarea semnalării cazului

La primire, operatorul atribuie identificatorul cazului și înregistrează momentul preluării. Se păstrează canalul de intrare, identificatorul sesizării sau al alertei și o descriere fidelă a motivului semnalării. Momentul introducerii în registru nu înlocuiește momentul observării activității. Dacă acesta din urmă este necunoscut, se marchează explicit necunoscut, fără a copia automat data curentă.

Operatorul verifică dacă domeniul poate fi identificat fără ambiguitate. Dacă informația este o adresă URL, se separă schema, gazda, portul și calea. Textul primit se păstrează ca intrare originală iar forma normalizată este stocată separat. Caracterele de control și intrările neconforme se resping înainte de orice interogare. Domeniile internaționalizate se păstrează atât în forma Unicode, cât și în reprezentarea ASCII compatibilă cu identificarea tehnică.

Înainte de crearea unei înregistrări noi se caută domeniul și indicatorii asociați în registru. Dacă există un caz deschis pentru aceeași activitate și aceeași perioadă, observația nouă se atașează acestuia. Dacă activitatea este diferită ori reapare după remediere, se creează un caz distinct, legat de cel anterior.

Duplicatele nu se șterg fără urmă; se marchează relația de consolidare și identificatorul cazului principal.

Se înregistrează numele complet observat și domeniul determinat printr-o regulă documentată. Eliminarea automată a tuturor subdomeniilor poate distruge informația despre o compromitere localizată.

De asemenea, simpla păstrare a ultimelor două etichete nu este o regulă universală pentru toate sufixele publice. Operatorul verifică rezultatul normalizării înainte de asocierea cu un domeniu existent.

Adresele IP asociate sunt observații temporale, nu identificatori permanenți ai domeniului. În medii de găzduire partajată, o adresă poate deservi domenii fără legătură între ele. Un caz nu transferă automat verdictul către toate numele rezolvate la aceeași adresă. Pentru fiecare asociere se păstrează momentul, tipul de înregistrare și sursa rezoluției.

Dacă semnalarea privește un URL, acesta se păstrează în evidența restricționată în forma necesară reproducerii observației. În rapoartele distribuite oamenilor se poate utiliza o reprezentare neactivabilă, precum hxxps și [.] în locul separatorului de domeniu. Forma destinată afișării nu trebuie introdusă accidental în câmpul tehnic utilizat de colectoare.

9.4. Colectarea și conservarea dovezilor

Operatorul atașează sau referențiază dovezile disponibile: alertă inițială, rezultat al unei surse de reputație, răspuns DNS, metadate TLS, captură de ecran, jurnal ori raport de analiză autorizată. Pentru fiecare obiect se înregistrează sursa, momentul colectării, metoda și identificatorul de stocare. Fișierele primesc o amprentă criptografică, de exemplu SHA-256, împreună cu algoritmul utilizat; amprenta permite verificarea integrității, dar nu dovedește adevărul conținutului.

Conținutul potențial malițios se examinează într-un mediu aprobat pentru analiză. Operatorul nu deschide resurse suspecte în sesiunea obișnuită autentificată și nu execută fișierele primite pentru a verifica manual o semnalare. Dovezile care nu necesită acces activ se colectează prioritar. Accesul activ, atunci când este necesar, trebuie să respecte competențele echipei și procedurile de investigație aplicabile.

Datele originale se conservă separat de versiunile redactate pentru partajare. Dacă o captură conține informații nerelevante despre persoane, versiunea distribuită se minimizează iar relația cu originalul rămâne înregistrată. Jurnalul trebuie să arate cine a adăugat, consultat, exportat sau înlocuit un obiect probator și motivul operației.

Pentru o listare externă se notează atât momentul interogării, cât și momentul observării publicat de sursă, dacă există. Două servicii care redistribuie același flux nu constituie automat două confirmări independente. Atunci când proveniența comună este cunoscută, operatorul marchează dependența. Când nu poate fi stabilită, independența rămâne necunoscută.

Fiecare indicator primește un tip, o valoare, un moment de observare și o sursă. Pentru DNS se păstrează tipul interogării, rezultatul, codul de răspuns și resolverul sau colectorul.

Pentru TLS se păstrează gazda, portul, momentul conexiunii, rezultatul verificării și, dacă sunt disponibile, emitentul, perioada de valabilitate și amprenta certificatului. Starea validării DNSSEC se distinge de simpla existență a unor înregistrări asociate.

Un câmp poate fi prezent, absent verificat, necunoscut, necolectat sau afectat de eroare. Valorile trebuie codificate explicit. De exemplu, expirarea unei interogări nu demonstrează inexistența certificatului. Se păstrează codul erorii și momentul ultimei încercări, astfel încât lipsa unei informații să poată fi remediată fără schimbarea nejustificată a verdictului.

Evaluarea automată se salvează ca instantaneu: valoare numerică, scală, sensul scorului, clasă prezisă, prag, versiunea modelului și schema caracteristicilor.

Dacă versiunea nu este disponibilă, se marchează necunoscută și se solicită completarea din jurnal. O valoare fără definiția scalei nu este suficientă pentru comparație. Numele instrumentului se înregistrează ca proveniență a evaluării.

9.5. Verificarea înregistrării înainte de validare

Înainte de trimiterea către analist, operatorul verifică identitatea domeniului, proveniența, marcajele temporale, existența dovezilor și completarea valorilor necunoscute.

Registrul trebuie să prevină salvarea unui verdict confirmat fără justificare și fără identificarea persoanei responsabile. Pentru un caz încă incomplet, salvarea este permisă numai cu starea corespunzătoare și cu descrierea informațiilor lipsă.

Analistul verifică dacă dovezile privesc același obiect și aceeași perioadă. El examinează posibilitatea unei găzduiri partajate, a unei listări istorice, a unei redirecționări legitime sau a unei schimbări de proprietar. Dacă observația privește doar o cale URL sau un subdomeniu, întinderea concluziei se precizează înaintea oricărei recomandări de măsură.

Validarea fixează o versiune a cazului și a setului de dovezi. Orice modificare ulterioară a verdictului, sferei de afectare sau justificării necesită o nouă revizie. Actualizările auxiliare, precum adăugarea unei observații de monitorizare, nu trebuie să rescrie aprobarea existentă. Istoricul arată clar ce a fost cunoscut la momentul fiecărei decizii.

9.6. Escaladarea și consemnarea măsurilor

Escaladarea este determinată de activitatea observată, impact, actualitate și competența echipei. Cazurile cu dovezi de activitate malițioasă în curs sunt transmise rolului desemnat, împreună cu un rezumat, indicatorii, dovezile, limitele analizei și acțiunea solicitată.

Înregistrarea momentului escaladării și a destinatarului permite urmărirea răspunsului.

O măsură se consemnează ca obiect separat: tipul, domeniul de aplicare, motivul, persoana care o aprobă, persoana care o execută, momentul și rezultatul. Se diferențiază recomandarea de acțiunea efectiv realizată.

Trimiterea unei notificări nu demonstrează remedierea iar solicitarea suspendării nu echivalează cu suspendarea domeniului.

Pentru o măsură temporară se stabilește un moment de reevaluare și un responsabil. Termenele de răspuns se definesc prin procedura organizației, în funcție de severitate și programul de operare; nu se deduc din scorul modelului. Dacă un caz depășește termenul, se păstrează motivul și escaladarea suplimentară, evitând închiderea automată fără analiză.

9.7. Reevaluarea, remedierea și retragerea clasificării

Reevaluarea se inițiază la primirea unor dovezi noi, la expirarea termenului stabilit, la raportarea remedierii sau la contestarea clasificării. Operatorul colectează observații actuale și le compară cu cele care au susținut verdictul inițial.

Un verdict poate fi corectat dacă dovezile inițiale au fost atribuite greșit sau interpretate eronat. Corecția păstrează valoarea anterioară, noua valoare, motivul, autorul și aprobarea. Dacă informația a fost transmisă către alte sisteme sau persoane, se înregistrează destinatarii care trebuie informați despre corecție și rezultatul comunicării.

Închiderea include concluzia finală, starea activității, măsurile realizate și condițiile de redeschidere. Pentru un domeniu remediat se păstrează distincția dintre istoricul malițios și evaluarea curentă. Dacă investigația nu a obținut suficiente informații, cazul poate fi închis ca neconcludent, cu motivul și criteriile care ar justifica reluarea.

Înregistrările operaționale pot contribui la îmbunătățirea seturilor de date numai după o etapă de control al calității. Exportul include eticheta validată, intervalul temporal, sursele și nivelul de încredere. Cazurile neconcludente nu se transformă automat în exemple benigne iar cazurile duplicate nu trebuie multiplicate artificial prin importuri repetate.

Un model nu trebuie reantrenat folosind propria predicție drept etichetă confirmată fără validare independentă. Altfel se creează un circuit prin care erorile modelului sunt reproduse în setul de antrenare. Operatorii și analiștii documentează dovezile care susțin eticheta, astfel încât procesul de învățare să poată distinge confirmarea umană de simpla preluare a scorului.

La pregătirea experimentelor, domeniile din aceeași campanie sau entitate se grupează atunci când există informații suficiente. Partiționarea temporală și păstrarea unui set extern ajută la evaluarea generalizării. Versiunea exportului, regulile de filtrare și momentul extragerii se conservă împreună cu modelul rezultat.

Se consideră o semnalare fictivă pentru *autentificare.exemplu.invalid*, asociată unei pagini care imită un serviciu. Sufixul invalid este utilizat exclusiv pentru exemplificare iar cazul nu desemnează o infrastructură reală. Operatorul păstrează gazda observată și adresa resursei, deschide cazul DEMO 001 și consemnează proveniența și momentul semnalării. Verdictul inițial este neconcludent, nu malițios confirmat.

Dacă există numai o captură furnizată de un terț, aceasta este înregistrată cu proveniența sa iar absența verificării directe rămâne explicită. Analistul verifică legătura dintre captură, domeniu și moment. Dacă datele nu permit confirmarea, solicită completări și stabilește reevaluarea. Dacă se obțin dovezi concordante ale colectării frauduloase a credențialelor, analistul poate confirma categoria phishing și poate propune escaladarea, indicând precis resursa afectată.

Înainte de închidere se verifică condițiile ca identitatea domeniului să fie corectă, faptul că dovezile pot fi localizate, momentele sunt interpretabile, scorul are sens și versiune documentate sau lipsa este explicită, verdictul are justificare,

măsurile sunt separate de recomandări, responsabilul și reevaluarea sunt stabilite. O înregistrare care îndeplinește aceste condiții poate susține o decizie verificabilă și o corecție ulterioară fără pierderea istoricului.

9.8. Informațiile înregistrate de operator

Câmpurile obligatorii la inițiere permit salvarea unui caz incomplet. Câmpurile condiționale devin obligatorii atunci când observația sau acțiunea există. Câmpurile de validare sunt necesare înaintea confirmării verdictului. Necunoscut și neaplicabil sunt valori explicite, însoțite de motiv acolo unde este relevant.

Tabelul 36. Informațiile înregistrate de operator

Nr.	Câmp	Cerință	Date și reguli
1	Identificator caz	Obligatoriu	Cod unic imuabil; legături către cazuri duplicate sau conexe.
2	Operator și momentul introducerii	Obligatoriu	Identitate autentificată; dată și oră în UTC; fusul sursei se păstrează separat.
3	Intrare originală și domeniu normalizat	Obligatoriu	Text primit, FQDN, domeniu ; Unicode și ASCII pentru IDN; regula de normalizare.
4	URL și întinderea afectării	Condițional	Resursa exactă, gazdă, port, cale; domeniu întreg sau subdomeniu; justificarea sferei.
5	Proveniența semnalării	Obligatoriu	Canal, sursă, identificator extern și momentul primirii.
6	Prima și ultima observare	Obligatoriu	Date distincte de data introducerii; „necunoscut” dacă sursa nu oferă momentul.
7	Motivul semnalării	Obligatoriu	Descriere factuală a comportamentului reclamat și a contextului.
8	Categoria activității	La validare	Phishing, malware, comandă și control, fraudă, redirecționare; alte categorii motivate.
9	Originea abuzului	La validare	Înregistrare pentru abuz, domeniu legitim compromis sau origine necunoscută.
10	Stare și verdict	Obligatoriu	Starea procesului separată de verdict; valorile controlate și istoricul tranzițiilor.
11	Încredere, severitate și prioritate	La validare	Trei atribute distincte, fiecare cu justificarea atribuirii.
12	Dovezi și integritate	La validare	Identificator obiect, sursă, moment, metodă, locație restricționată și amprentă cu algoritm.
13	Date DNS	Condițional	Tip întrebare, valori, cod răspuns, TTL, colector, moment; DNSSEC validat distinct de prezență.
14	Date de registru	Condițional	Registrar, date relevante de înregistrare și expirare, sursa și momentul; fără date personale inutile.
15	Date TLS	Condițional	Gazdă și port, rezultat, emitent, valabilitate, versiune, amprentă, moment și erori.

Nr.	Câmp	Cerință	Date și reguli
16	Surse de reputație	Condițional	Denumire, referință a listării, categoria, data sursei, data consultării și relațiile de dependență.
17	Rezultat al evaluării automate	Condițional	Instrument, scor brut, scală, sens, clasă, prag, moment, versiunea modelului și schema caracteristicilor.
18	Calitatea colectării	Obligatoriu	Prezent, absent verificat, necunoscut, necolectat sau eroare; motiv și ultimă încercare.
19	Justificarea verdictului	La validare	Dovezile decisive, contradicțiile, limitele și motivul concluziei.
20	Validare și aprobare	La validare	Analist, aprobator dacă este necesar, moment și versiunea cazului aprobat.
21	Escaladare și acțiuni	Condițional	Destinatar, solicitare, aprobare, executant, moment, întindere și rezultat efectiv.
22	Reevaluare și închidere	La validare	Responsabil, termen sau declanșator, concluzie, dovada remedierii și criteriu de redeschidere.
23	Acces, retenție și partajare	Obligatoriu	Nivel de acces, politică de păstrare, destinatari autorizați și evidența exporturilor.
24	Istoric și corecții	Automat	Autor, moment, valoare anterioară și nouă, motiv; fără suprascrierea istoricului.
25	Eligibilitate pentru ML	Condițional	Etichetă validată, interval temporal, proveniență, versiune export și excluderile aplicate.

Circuitul de lucru este: primirea semnalării, identificarea obiectului, verificarea duplicatelor, colectarea dovezilor, completarea indicatorilor, analiza, validarea, escaladarea dacă este necesară, reevaluarea și închiderea. Calitatea evidenței se măsoară prin completitudine, trasabilitate și posibilitatea corectării. Numărul de cazuri introduse nu este suficient pentru a evalua eficiența operatorilor: contează și timpul până la validare, proporția cazurilor returnate pentru completări, actualitatea dovezilor și corecțiile justificate.

Procedura transpune în evidența cazului principiile de trasabilitate, control uman și actualitate din politica de utilizare și din ghidul de bune practici.

Procedura de înregistrare produce informații comparabile numai dacă operatorii aplică aceleași definiții. O categorie precum suspect poate avea sensuri diferite pentru evaluatori diferiți: lipsa unor date, existența unei semnalări sau confirmarea parțială a unui comportament. Dicționarul stărilor trebuie să precizeze dovezile minime, condițiile de utilizare și relația cu verdictul final. Definițiile trebuie însoțite de exemple și de situații în care categoria nu se aplică.

Pentru verificarea consistenței se poate selecta un eșantion de cazuri evaluat independent de doi operatori. Independența presupune că al doilea evaluator nu pornește de la verdictul primului, atunci când obiectivul este măsurarea acordului. Se compară atât rezultatul, cât și motivele. Două verdicte identice pot proveni din interpretări incompatibile iar două verdicte diferite pot reflecta accesul la informații colectate în momente diferite.

Dezacordurile se clasifică înainte de a fi rezolvate: identificare diferită a obiectului, interpretare diferită a dovezilor, informație temporală incompletă sau aplicare neuniformă a criteriilor. Rezolvarea trebuie să consemneze motivul și eventualele clarificări aduse procedurii. Scopul nu este obținerea artificială a unui acord perfect, ci reducerea variației care provine din ambiguități evitabile. Cazurile dificil de decis pot rămâne marcate ca incerte.

Rezultatele acestui control pot alimenta instruirea periodică și revizuirea formularelor, în continuarea recomandărilor din documentele de utilizare și bune practici. Dacă un câmp generează frecvent interpretări diferite, se examinează definiția sa, nu doar atenția operatorilor. Dacă o categorie este prea largă, poate fi necesară separarea ei. Modificarea produce o versiune nouă a procedurii iar înregistrările anterioare rămân asociate versiunii sub care au fost evaluate.

O înregistrare validată poate necesita corectare. Identificatorul poate fi incomplet, momentul poate fi interpretat greșit sau o sursă poate retrage o afirmație. Procedura de rectificare trebuie să permită corectarea fără pierderea trasabilității. Se păstrează valoarea anterioară, valoarea corectată, motivul, autorul și momentul modificării. Când rectificarea privește numai forma, acest lucru se distinge de schimbarea unei concluzii analitice.

Efectele unei corecții pot depăși cazul inițial. Înregistrarea poate fi inclusă într-un raport, într-un export de indicatori sau într-un corpus de învățare. De aceea, evidența trebuie să permită identificarea produselor care au utilizat versiunea greșită. Nu toate produsele pot fi retrase sau recalculate imediat; limita se consemnează, împreună cu acțiunea întreprinsă. Rectificarea în baza principală nu garantează actualizarea tuturor copiilor.

Pentru datele folosite la învățare, corecția produce o problemă de versiune. Un model deja antrenat nu este modificat prin simpla schimbare a etichetei din registru. Trebuie evaluat dacă este necesară reconstruirea corpusului și reantrenarea, în raport cu amploarea erorii și utilizarea modelului. Înregistrarea versiunilor permite explicarea diferențelor dintre rezultatele obținute înainte și după corecție, fără a ascunde existența erorii inițiale.

Controlul final al rectificării verifică atât conținutul, cât și propagarea sa. Operatorul confirmă că identificatorul corect este asociat dovezilor potrivite, că verdictul a fost reevaluat și că destinatarii interni relevanți pot identifica versiunea actuală. Principiile de audit, control al accesului și monitorizare susțin acest circuit. Prin aplicarea lui, procedura devine un mecanism de menținere a calității informației pe durata utilizării, nu numai un formular de introducere inițială.

10. Arhitectură pentru sisteme de evaluare a reputației

10.1. Rolul registrului și relațiile dintre participanți

Un registru de domenii administrează înregistrările din spațiul de nume pentru care este responsabil și susține funcționarea delegărilor corespunzătoare. Pentru analiza reputației, registrul reprezintă o sursă administrativă distinctă de furnizorul de găzduire, operatorul DNS și titularul domeniului. Identificarea sursei și a relației cu figurile reproduse sau adaptate ilustrează această perspectivă organizațională. Relațiile dintre roluri oferă un cadru de analiză aplicabil unor spații de nume diferite.

Funcțiile relevante pentru integrarea informațiilor despre domenii includ:

- Înregistrarea numelor și menținerea evidenței lor administrative, potrivit regulilor spațiului de nume.
- Gestionarea delegărilor și publicarea datelor necesare funcționării zonei TLD.
- Aplicarea procedurilor referitoare la solicitări, corectarea informațiilor și soluționarea situațiilor contestate, în limitele atribuțiilor fiecărui participant.
- Transferul numelor de domenii de la un Registrar la altul
- Trade-ul numelor de domenii de la un deținător la alt deținător
- Actualizarea informațiilor referitoare la titularul unui nume de domeniu.
- Protejarea operațiunilor administrative și urmărirea modificărilor relevante pentru securitate. Evenimentele de schimbare trebuie corelate cu istoricul tehnic, fără a presupune că orice transfer sau actualizare indică un abuz.
- Colaborarea cu registrari, titulari și echipe de răspuns pentru clarificarea observațiilor și coordonarea remediilor. Canalele și responsabilitățile se stabilesc înaintea incidentelor.
- Controlul accesului la informații și limitarea utilizării lor la scopul analizei, cu păstrarea unei evidențe a consultărilor și modificărilor.

Reputația se construiește din corelarea acestor date administrative cu observații tehnice și comportamentale. Nici registrul și nici o singură sursă externă nu oferă implicit o imagine completă asupra tuturor utilizărilor unui domeniu.

Delegările domeniilor de nivel superior sunt documentate în baza de date a zonei rădăcină publicată de IANA (IANA, 2026). Aceasta permite identificarea informațiilor de delegare, dar nu constituie o evaluare a reputației numelor înregistrate sub un TLD.

Administrarea unui TLD și administrarea unei zone DNS sunt niveluri distincte. Zonele pot fi delegate către operatori autoritativi iar delimitarea

responsabilităților este relevantă pentru interpretarea observațiilor și pentru localizarea unei schimbări tehnice (Stăicuț, 1995).

Registrantul este persoana sau organizația titulară a dreptului de utilizare a unui nume de domeniu, în condițiile aplicabile înregistrării. Registrarul intermediază operațiunile în relația cu registrul. Într-o investigație, identificarea registrarului nu trebuie confundată cu identificarea persoanei care controlează conținutul sau infrastructura.

Registrarii sunt companii, parteneri cu registrul, care în unele cazuri oferă și alte servicii, precum găzduire web și servicii de e-mail. Registrul propagă modificările în baza de date a zonei (zona de scriere), iar ulterior este folosit pentru a popula serverele DNS și serverul whois.

Numele de domenii sunt în general înregistrate pentru un număr de ani, în funcție de regulile registrului și taxele plătite. La sfârșitul perioadei de înregistrare a unui nume de domeniu, deținătorul poate solicita reînnoirea acestuia, sau poate deveni disponibil pentru înregistrarea altcuiva. Un domeniu poate fi transferat de la un Registrant la altul la cerere.

Modelul Registry–Registrar–Registrant separă evidența centrală, intermedierea operațiunilor și utilizarea numelui. Registrarul desemnat gestionează operațiunile autorizate pentru un domeniu, iar schimbarea acestuia urmează un proces controlat. Sistemul de reputație trebuie să păstreze istoricul schimbărilor, deoarece o relație administrativă actuală nu descrie neapărat situația de la momentul incidentului.

Figura 5 ilustrează relațiile dintre registru, registrari și titularii numelor de domenii. Titularul deține dreptul de utilizare a numelui de domeniu, în condițiile contractuale aplicabile. Registrarul intermediază operațiunile de înregistrare și administrare. În funcție de rol și de drepturile acordate, operațiunile includ actualizarea datelor, reînnoirea, transferul, modificarea serverelor de nume și gestionarea înregistrărilor DNSSEC.

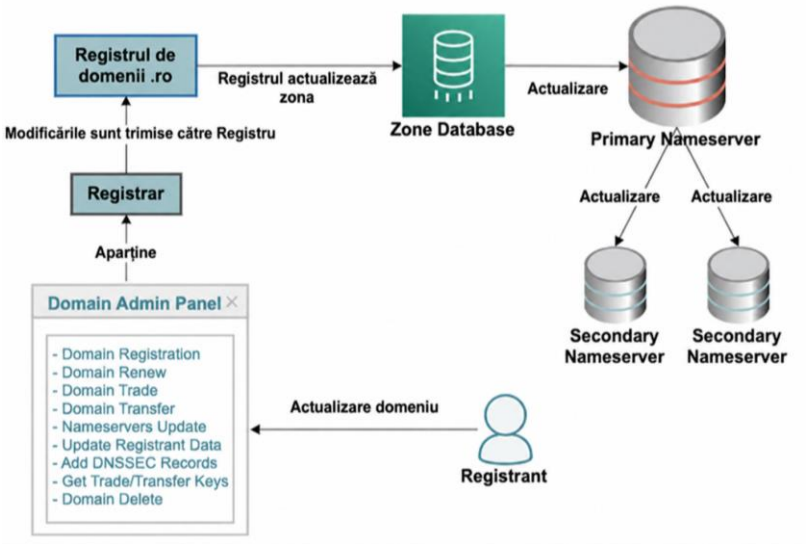


Figura 5. Arhitectura business a registrului de domenii .ro

În exemplul ilustrat, portalul registrarului comunică printr-o interfață cu serviciile registrului. Principiul general este separarea solicitării, autorizării, înregistrării, modificării și publicării datelor. Evenimentele rezultate pot alimenta analiza reputației dacă sunt disponibile și utilizate în scopul autorizat.

10.2. Cerințe la nivel business pentru un sistem de reputație a domeniilor

Un sistem de reputație de domeniu pentru un registru de domenii este necesar să îndeplinească anumite cerințe pentru a fi eficient. Cerințele cheie sunt:

- Colectarea datelor cu acuratețe. Sistemul trebuie să poată colecta cu acuratețe date despre numele de domenii, inclusiv data de înregistrare a acestora, adresele IP asociate cu acestea și orice date istorice legate de utilizarea lor.
- Monitorizare în timp real. Frecvența monitorizării se stabilește în funcție de dinamica amenințării și de timpul acceptabil până la detectare. Analiza periodică și analiza declanșată de evenimente pot fi combinate; o cerință de actualizare rapidă trebuie exprimată prin latențe măsurabile.
- Algoritmi de învățare automată. Evaluarea poate utiliza reguli, agregarea indicatorilor, modele statistice sau combinații ale acestora. Învățarea automată este o opțiune care trebuie justificată prin date și rezultate comparative; ea nu este o condiție obligatorie pentru existența unui sistem de reputație.
- Filtrare colaborativă. Analiza relațională poate identifica infrastructură partajată și tipare comune. Relația dintre două domenii justifică o verificare suplimentară, dar nu demonstrează singură existența aceluiași titular sau a aceleiași intenții.
- Integrarea informațiilor despre amenințări. Sistemul va integra fluxuri de informații despre amenințări pentru a oferi un context suplimentar pentru comportamentul numelui de domeniu.
- Interfață ușor de utilizat. Sistemul va avea o interfață ușor de utilizat, care să permită registrarilor de domenii și agențiilor de aplicare a legii să acceseze și să interpreteze cu ușurință datele.
- Protecția confidențialității. Sistemul va proteja confidențialitatea solicitanților care înregistrează domeniile, oferind în același timp date suficiente pentru analiză.
- Răspuns în timp util. Sistemul va oferi răspunsuri în timp util registrarilor de domenii și agențiilor de aplicare a legii atunci când sunt detectate activități suspecte, astfel încât să poată fi luate măsuri adecvate pentru a preveni abuzul.
- Scalabilitate. Sistemul va putea gestiona volume mari de date și va fi scalabil pentru a găzdui un număr tot mai mare de nume de domenii și utilizatori.

- Securitate robustă. Sistemul va încorpora măsuri de securitate puternice pentru a proteja împotriva accesului neautorizat și a încălcării datelor (Holland, 2019).

10.2.1. O arhitectură generică pentru un sistem de reputație a domeniilor

În general, arhitectura pentru reputația numelui de domeniu implică un sistem complex de colectare a datelor, analiză și bucle de feedback pentru a identifica și preveni spam-ul, phishingul și alte activități rău intenționate asociate cu un anumit nume de domeniu.

Unele dintre caracteristicile cheie ale sistemului propus includ monitorizarea continuă a traficului DNS pentru a detecta orice domeniu nou care ar putea fi asociat cu o activitate rău intenționată, algoritmi de învățare automată pentru a analiza datele și a identifica domeniile potențial compromise, utilizează o varietate de surse de informații despre amenințări pentru a fi actualizat cu privire la cele mai recente amenințări și programe malware și va oferi rapoarte personalizabile care pot fi adaptate pentru a răspunde nevoilor specifice ale diferitelor registre de domenii sau Registrari.

Prin utilizarea arhitecturii generice propuse, Registrele de domenii, Registrarii și alte organizații pot personaliza și implementa o soluție dedicată nevoilor lor specifice.

Arhitectura separă colectarea observațiilor, calculul caracteristicilor, evaluarea și prezentarea rezultatului. Regulile euristice și modelele învățate pot prelucra aceleași date, cu păstrarea versiunilor și a limitelor fiecărei metode. Compararea rezultatelor lor trebuie să utilizeze cazuri de referință validate independent, evitând validarea circulară.

Inițial, domeniile sunt normalizate și verificate pentru a evita interogări redundante. Rezultatele existente pot fi reutilizate numai în limita unei perioade de valabilitate documentate. Listele de referință benignă pot influența prioritatea, dar nu exclud permanent un domeniu din analiză: domeniile legitime pot fi compromise. Colectoarele preiau date de registru, observații DNS, informații TLS și semnale externe. Pentru fiecare sursă se înregistrează momentul, starea interogării și eventualele erori. Datele rezultate sunt introduse într-o coadă de procesare împreună cu identificatorul obiectului.

Procesele de lucru preiau sarcini din coadă și aplică reguli sau transformări versionate. Rezultatul poate fi un scor, o clasă și un set de explicații. Dacă se utilizează scala 0–100, sensul ei trebuie declarat explicit; această convenție de prezentare nu conferă automat scorului semnificația unei probabilități calibrate.

Coada de rezultate permite stocarea și utilizarea asincronă a evaluărilor. Predicțiile și rezultatele euristice nu devin automat etichete corecte pentru reantrenare. Datele de învățare trebuie să includă un proces separat de validare a etichetelor, iar testarea să folosească observații care nu au influențat dezvoltarea modelului. Diagrama din Figura 5 descrie procesarea operațională; fluxul de antrenare necesită aceste controale suplimentare.

Interfața de analiză prezintă rezultatul împreună cu momentul evaluării, sursele, istoricul și explicațiile disponibile. Operatorul trebuie să poată distinge un scor recent calculat pe date vechi de o evaluare bazată pe observații recent colectate. Această distincție este independentă de tehnologia de implementare.

Soluția de monitorizare automată a reputației domeniilor reprezintă un instrument puternic pentru monitorizarea reputației domeniilor, care poate fi folosit de Registrari, proprietari de site-uri web și profesioniști în securitate pentru a identifica potențialele amenințări și pentru a lua măsurile adecvate pentru a-și proteja activele online.

Timpul până la actualizarea reputației depinde de frecvența colectării, durata procesării și disponibilitatea surselor. Aceste întârzieri trebuie măsurate și afișate atunci când afectează interpretarea rezultatului.

Figura 6 prezintă un flux generic de colectare și procesare, adaptat din arhitectura studiului de caz. Instrumentele indicate sunt exemple; selectarea lor depinde de tipul observației și de controalele de acces și execuție.

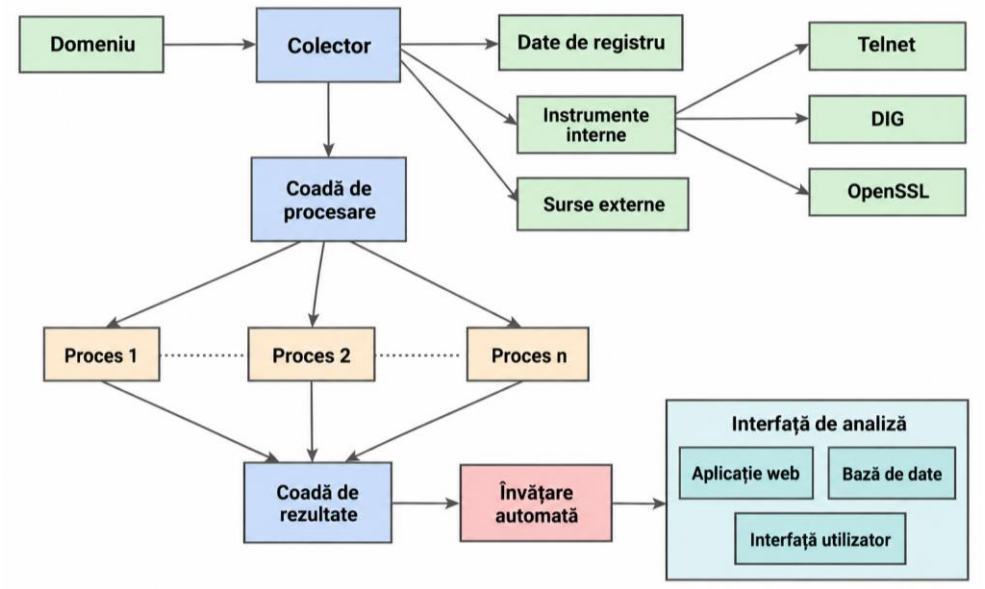


Figura 6. Flux generic de colectare și evaluare

10.3. Metodologia de selecție a framework-ului arhitectural

Selectarea unui cadru arhitectural pornește de la complexitatea organizațională, numărul integrărilor și cerințele de guvernanță. Metoda de mai jos compară criterii utile pentru orice sistem de reputație: interoperabilitate, sustenabilitate, scalabilitate și trasabilitate. Scopul nu este impunerea unui cadru unic, ci justificarea relației dintre nevoile organizației și artefactele folosite pentru descrierea soluției.

10.4. Metodologia de cercetare

Analiza cadrului arhitectural urmărește compararea unor metode de descriere a proceselor, datelor și tehnologiilor. Criteriile trebuie aplicate în contextul organizației, cu precizarea compromisurilor și a resurselor disponibile. Studiul de caz utilizează TOGAF; alte implementări pot adopta o descriere mai restrânsă, dacă aceasta susține responsabilitățile și verificările necesare.

Definirea domeniului de aplicare asigură că framework-ul selectat se aliniază exact cu obiectivele specifice ale sistemului, previne ambiguitatea și asigură că cadrul este adaptat pentru a satisface nevoile și obiectivele unice ale organizației.

Evaluarea flexibilității domeniului de aplicare asigură că cadrul ales se poate scala și adapta pe măsură ce organizația evoluează. Acesta protejează împotriva limitărilor potențiale în abordarea cerințelor business emergente.

Performanța este esențială pentru susținerea proceselor business eficiente. Capacitatea framework-ului de a gestiona dimensiunea și cerințele de performanță ale sistemului influențează direct eficacitatea și receptivitatea operațiunilor.

Recunoașterea rolului critic al datelor reflectă înțelegerea contemporană că datele sunt piatra de temelie a întreprinderilor moderne. Capacitatea framework-ului de a aborda gestionarea datelor, calitatea și integrarea este vitală pentru menținerea unui ecosistem informațional robust și fiabil.

Recunoașterea importanței principiilor SOA este crucială pentru promovarea agilității organizaționale. Un framework care susține o abordare orientată spre servicii permite soluții modulare, reutilizabile și adaptabile, aliniind IT-ul la nevoile afacerii.Accentul pe limbajele de modelare recunoaște necesitatea unei comunicări și a documentării clare. Un framework care acceptă limbaje și notații preferate de modelare facilitează colaborarea eficientă, asigurând că proiectele arhitecturale sunt comunicate clar în întreaga organizație.

Prioritizarea considerațiilor de securitate răspunde la peisajul tot mai mare a amenințărilor și la nevoia de a proteja informațiile sensibile. Un framework cu funcții de securitate robuste protejează împotriva amenințărilor cibernetice și asigură confidențialitatea, integritatea și disponibilitatea datelor. Asigurarea conformității cu standardele industriale și de reglementare garantează că organizația aderă la normele de securitate stabilite. Acest lucru este crucial pentru menținerea încrederii, îndeplinirea cerințelor legale și protejarea datelor sensibile.

Luarea în considerare a standardelor subliniază importanța aderării la standardele industriei și organizaționale. Un framework care se aliniază cu cele mai bune practici asigură coerența în dezvoltarea arhitecturii și promovează interoperabilitatea cu alte sisteme.Utilizarea unui framework care este considerat standard facilitează integrarea cu sistemele și tehnologiile existente, reducând problemele de compatibilitate și simplificând peisajul IT general.

Recunoașterea importanței arhitecturii business asigură că framework-ul selectat pune un accent puternic pe alinierea strategiilor IT cu obiectivele generale business. Acest criteriu este esențial pentru a genera valoare și pentru a se asigura că arhitectura susține direct obiectivele sistemului. Totodată, promovează o aliniere puternică între cerințele la nivel de business și sistemele, favorizând o abordare colaborativă care reduce decalajul dintre afaceri și părțile interesate din IT.

Pe lângă evaluarea performanței în general, este necesar a se lua în considerare capacitatea framework-ului de a defini și monitoriza indicatorii cheie de performanță specifici. Acest lucru permite măsurarea în termeni cuantificabili a rezultatelor.

Abordarea framework-ului cu privire la limbajele de modelare este un aspect extrem de important. Un framework care promovează utilizarea limbajelor de modelare și a notațiilor acceptate la scară largă asigură coerența și interoperabilitatea între artefactele arhitecturale.

Aceste criterii au fost selectate pentru a aborda aspectele cheie referitoare la arhitecturile enterprise, asigurându-se că framework-ul selectat nu este doar robust din punct de vedere tehnic, ci și se aliniază cu obiectivele sistemului propus, susține dezvoltarea eficientă a acestuia și îndeplinește standardele și cerințele de securitate contemporane.

10.5. Analiza comparativă a FEAF, TOGAF, UAF și Zachman Framework

Comparația FEAF, TOGAF, UAF și Zachman urmărește diferențele de scop și de reprezentare a arhitecturii. Alegerea unui cadru trebuie legată de nevoile organizației care operează evaluarea reputației, de actorii implicați și de nivelul de formalizare necesar.

Tabelul 37 oferă o prezentare generală în ceea ce privește domeniul de aplicare, particularitățile și considerațiile legate de performanță, date, SOA, limbaje de modelare, securitate și standarde. De asemenea, evidențiază abordările respective ale limbajelor de modelare. În general, alegerea framework-ului depinde de nevoile și contextul organizațional specific. În scopul acestei cercetări, toate aceste 4 framework-uri sunt comparate în tabelul următor, cu scopul de a selecta cel mai potrivit pentru descrierea arhitecturii sistemului de reputație a numelor de domeniu.

Tabelul 37. Analiză comparativă a modelelor arhitecturale identificate

Caracteristică	**FEAF**	**TOGAF**	**UAF**	**Zachman**
Domeniu de aplicare și aplicabilitate	Agenții guvernamentale federale din SUA	Diverse industrii și organizații la nivel global	Sisteme și întreprinderi complexe	Diverse industrii și organizații
Particularități	Cinci modele sau componente de referință: Componenta Performanță, compone-nta Business, Componenta de servicii, Componenta Tehnică, Conponenta de Date	Trei componente arhitecturale: Arhitectura Business, Arhitectura de date și aplicații, Arhitectura tehnologică	Patru componente arhitecturale: Arhitectura Business, Arhitectura Sistemelor de informații, Arhitectura tehnologică și Arhitectura operațională	Include o taxonomie pentru descrierile arhitecturale

Caracteristică	FEAF	TOGAF	UAF	Zachman
Alinierea cu standarde	Nu este un standard	Nu este un standard	Folosit ca standard	Nu este un standard
Accent pe arhitectura business	Accent puternic pe arhitectura business	Adresează arhitectura business;	Promovează integrarea între domenii	Oferă un sistem de clasificare
Performanță și Metrici	Model de referință pentru performanță și metrici (PRM) pentru măsurare	Ia în considerare performanța la nivel business	Subliniază trasabilitatea și ciclul de viață	Nu încorporează în mod explicit valori
Limbajul de modelare	Folosește adesea UML, BPMN și alte notații standard	Oferă îndrumări privind modelarea arhitecturii	Asociat cu instrumentele de modelare SysML și UML	Nu prescrie un anumit limbaj
Managementul datelor	Model de referință pentru date bazat pe standard de date (DRM)	Îndrumări extinse privind date și informații	Oferă o abordare integrată pentru date	Nu oferă îndrumări specifice privind datele
Arhitectura orientată către servicii (SOA)	Model de referință pentru componentele de tip servicii (SRM)	Adresează SOA într-un context arhitectural mai larg	Include diverse componente arhitecturale pentru descrierea serviciilor	Nu este axat pe tehnologie
Securitate și confidențialitate	Profil de securitate și confidențialitate (SPP) pentru cerințe	Acoperă securitatea într-o manieră generalizată	Acceptă documente clare și cuprinzătoare	Nu abordează în mod specific securitatea

În studiul de caz a fost ales TOGAF pentru organizarea descrierii arhitecturale (Priyadharshini, 2013; The Open Group, 2022). Această alegere ilustrează o metodă de lucru; nu demonstrează superioritatea universală a cadrului și nu condiționează corectitudinea unui sistem de reputație de utilizarea sa.

TOGAF oferă o abordare structurată și cuprinzătoare pentru dezvoltarea arhitecturii întreprinderii, făcându-l ideal pentru ecosisteme complexe pentru scorul reputației numelor de domenii. Acesta pune accent pe alinierea arhitecturii cu obiectivele strategice ale unei organizații sau sistem, asigurându-se că aplicația sau ecosistemul susține obiectivele globale la nivel business, faza de arhitectură business a TOGAF facilitând această aliniere.

Un cadru arhitectural poate susține alinierea proceselor și documentarea schimbărilor. Beneficiile depind de aplicarea sa efectivă și de verificarea implementării; utilizarea cadrului nu garantează automat securitatea, eficiența economică sau calitatea predicțiilor.

TOGAF suportă integrarea diverselor surse de date, precum datele registrului de domeniu, înregistrările DNS și serviciile de date web, asigurând fluxuri de date sigure și bine definite. De asemenea, promovează interoperabilitatea, facilitând integrarea ecosistemului cu sisteme externe și aderarea la standardele industriei, ceea ce este crucial în contextul reputației domeniului.

10.6. Descrierea Arhitecturii Sistemului de Reputație Nume de Domenii utilizând TOGAF

Standardul TOGAF oferă o abordare formală de modelare pentru a evidenția stakeholder-i (părțile interesate), anumite aspecte cheie și vizualizări. Vizualizările sunt artefactele principale într-o descriere a arhitecturii, deoarece sunt reprezentări ale arhitecturii generale care sunt semnificative pentru una sau mai multe părți interesate. Diferiți stakeholderi cu roluri diferite în sistem vor avea preocupări diferite.

Ciclul ADM cuprinde faza preliminară și fazele A–H, cu managementul cerințelor ca proces transversal. Pentru un sistem de reputație, descrierea urmărește părțile interesate, procesele, datele, aplicațiile, infrastructura și guvernanța. Organizația centrală poate fi un registru, un furnizor de servicii sau o echipă de securitate.

10.7. Vizualizarea Stakeholder-ilor (Stakeholders Architecture View)

Punctul de vedere al părților interesate (Stakeholders Viewpoint) face parte din arhitectura business definită în cadrul TOGAF. Este folosit pentru a identifica și documenta părțile interesate de sistem, preocupările și punctele lor de vedere.

Diagrama următoare exemplifică părțile interesate într-o implementare pentru un registru de domenii:

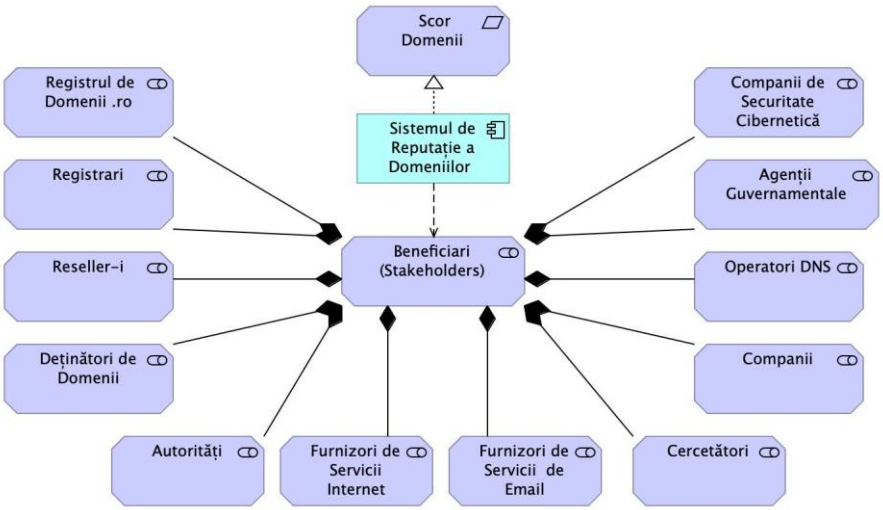


Figura 7. Părțile interesate ale Sistemului de Reputație a Domeniilor (Stakeholders View)

Un instrument care determină scorul reputației unui domeniu pentru un registru ccTLD de nume de domenii este o componentă critică pentru gestionarea spațiului de nume de domenii și pentru asigurarea securității și integrității generale a registrului. Diferiți beneficiari sunt implicați sau influențați de un astfel de instrument în moduri diferite:

Operatorul registrului poate utiliza evaluările pentru prioritizarea verificărilor și pentru informarea participanților relevanți. Competențele administrative, responsabilitățile de validare și condițiile notificării trebuie definite separat de calculul scorului.

Registrarii de domenii sunt companii sau entități care vând nume de domenii unor persoane fizice sau juridice. Sistemul de reputație îi ajută prin monitorizarea reputației domeniilor pe care aceștia le administrează, deoarece domeniile cu o reputație proastă le pot afecta gradul de încredere al vizitatorilor sau afacerea.

Reseller-i de domenii sunt companii care cumpără nume de domenii de la registrari și le vând persoanelor fizice sau juridice. Aceștia beneficiază de implementarea sistemului într-un mod similar cu registrarii.

Registranții sunt titularii numelor de domenii și pot fi afectați de erorile evaluării. Mecanismele de clarificare și corectare a informațiilor fac parte din proiectarea sistemului.

Organizațiile cu atribuții de investigare pot utiliza rezultatele pentru orientarea analizei. Un scor nu înlocuiește dovezile necesare unei constatări și nu stabilește singur identitatea autorului unui abuz.

Furnizorii de servicii de Internet (ISP) folosesc instrumente de reputație a domeniului pentru a filtra sau bloca e-mailurile și traficul provenite de la domeniile cu reputație negativă. Acest lucru ajută la reducerea spamului, a phishing-ului și a distribuirii de programe malware (RiskAnalytics, 2026).

Furnizorii de servicii de e-mail (ESP) folosesc scorul reputației domeniilor pentru a determina legitimitatea expeditorilor de e-mail și pentru a reduce riscul ca utilizatorii lor să primească e-mailuri de tip spam sau phishing.

Cercetătorii care studiază amenințările online, atacurile cibernetice și abuzul numelor de domenii se bazează pe instrumente de reputație pentru a analiza tendințele și amenințările din spațiul Internet.

Companiile de securitate care furnizează servicii de securitate, precum informații despre amenințări, software de securitate și firewall-uri, pot folosi datele despre reputația domeniului pentru a-și îmbunătăți ofertele de securitate.

Operatorii infrastructurii și serviciilor DNS se pot baza pe datele despre reputație pentru a menține integritatea DNS.

Agențiile guvernamentale și organizațiile de standardizare, precum ICANN (Internet Corporation for Assigned Names and Numbers) sunt implicate în stabilirea politicilor și standardelor legate de reputația și securitatea numelor de domenii.

Companiile de securitate cibernetică care oferă soluții de securitate cibernetică încorporează adesea date despre reputația domeniilor în mecanismele lor de detectare și prevenire a amenințărilor.

Principala cerință îndeplinită de Sistemul de Reputație a Domeniilor este Scorul domeniului. Cei mai mulți factori interesați descriși mai sus sunt implicați sau beneficiază de sistem. Următoarea figură dezvoltată în ArchiMate (Beauvoir și Sarrodie, 2026; The Open Group, 2013), bazându-se pe standardul TOGAF EA, ilustrează stakeholder-i sistemului.

Beneficiarii Sistemului de Reputație a Domeniilor joacă roluri diferite iar interesele lor se pot intersecta uneori, astfel încât echilibrarea nevoilor și preocupărilor acestor părți interesate este esențială pentru menținerea unui registru de nume de domenii sigur și de încredere.

10.8. Arhitectura la nivel Business (Business Architecture View)

Arhitectura Business descrisă utilizând TOGAF EA pentru un sistem de reputație de domeniu, ilustrată în figura următoare, evidențiază componentele business ale sistemului și relațiile dintre ele. În cazul de utilizare actual, sistemul constă din mai multe componente business, inclusiv surse de date interne și externe, achiziție de date, preprocesare, procesare, stocare, calcularea scorului de reputație al domeniului (scoring) și o componentă de stocare a datelor în care informațiile privind scorul domeniului sunt preluate, stocate și afișate.

Sursele administrative descriu înregistrarea și modificările unui domeniu. Sursele interne pot include observații validate de analiști, incidente și feedback documentat. Sursele externe pot furniza înregistrări DNS, metadate TLS și indicatori de amenințare. Aceste categorii trebuie păstrate distinct, împreună cu proveniența și momentul fiecărei observații, pentru a evita confuzia dintre semnal automat și concluzie confirmată.

Funcția de achiziție a datelor este responsabilă cu colectarea datelor din diverse surse, atât interne, cât și externe. Această funcție include mecanisme pentru preluarea datelor, asimilarea datelor și transformarea datelor.

Preprocesarea implică curățarea, normalizarea și validarea datelor primite pentru a asigura calitatea și consistența acestora și implică deduplicarea datelor, îmbogățirea datelor și standardizarea formatului.

Componenta Procesare îndeplinește sarcinile de bază pentru evaluarea reputației. Utilizează algoritmi, modele și euristici pentru a analiza datele și a calcula scorurile reputației domeniului. Această funcție implică evaluarea datelor pentru a identifica anomalii, amenințări, schimbarea frecventă a deținătorului și alți indicatori ai comportamentului domeniului.

Funcția de stocare se referă la baze de date și soluții de stocare a datelor pentru a menține înregistrări istorice ale domeniilor, atributelor acestora și valorile scorului reputației.

Funcția business Scorul Domeniului se bazează pe un set de algoritmi și reguli de învățare automată pentru determinarea scorului de reputație pentru fiecare domeniu, luând în considerare diferiți factori, precum comportamentul domeniului, istoricul și datele colectate din sursele de date interne și externe.

Depozitul de date (Data Warehouse) servește ca un depozit pentru rezultatele scorului și alte date despre domenii. Stochează date istorice, tendințe și rezultate agregate. Instrumentele de business intelligence și sistemele de raportare pot accesa Data Warehouse pentru a oferi informații părților interesate.

Obiectivul acestei arhitecturi business, ilustrată în figura următoare, este de a oferi o înțelegere la nivel înalt a modului în care sistemul de reputație a domeniului funcționează în contextul business mai larg, permițând părților interesate să vizualizeze fluxul de date, procese și relații care contribuie la evaluarea și managementul reputației domeniilor.

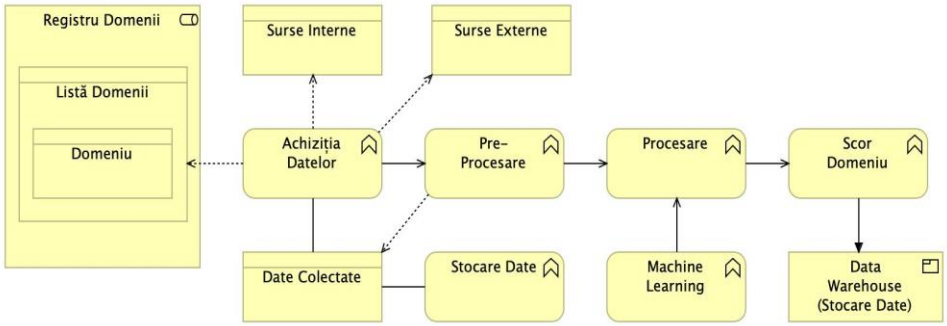


Figura 8. Arhitectura Business (Business Architecture View)

10.9. Arhitectura Sistemelor Informaționale și Datelor (Information Systems and Data Architecture View)

Arhitectura Sistemelor Informaționale și Datelor, ilustrată în continuare, se concentrează pe proiectarea arhitecturii aplicației și demonstrează modul în care Arhitectura Business este realizată prin intermediul Sistemelor Informaționale (Tepandi et al., 2019).

Arhitectura Sistemelor Informaționale pentru un Sistem de Reputație a Numelor de Domenii oferă o imagine de ansamblu la nivel înalt a componentelor sistemului, proceselor și interacțiunilor acestora. Permite vizualizarea funcțiilor sistemului, componentelor și fluxurilor de date între diferite componente.

Componenta Collect and Pre-Process este responsabilă pentru achiziționarea de date despre numele de domenii din baza de date a registrului, surse interne și externe, utilizând un mecanism de tip crawler care colectează informații legate de domeniu, precum detalii de înregistrare, înregistrări DNS, date istorice, informații și tranzacții din lista neagră. La următorul pas, preprocesează datele colectate pentru consistență și calitate.

Componenta de stocare păstrează datele achiziționate de Componenta de colectare și preprocesare și menține un depozit de informații legate de domenii, care include atât date istorice, cât și cu date obținute în timp real.

Componenta de procesare este responsabilă pentru analiza și procesarea datelor colectate și efectuează diverse sarcini de evaluare a reputației pentru a evalua informațiile legate de domeniu și pentru a determina scorul reputației. Utilizează algoritmi și reguli definite pentru a evalua reputația domeniului, pentru a identifica amenințările și pentru a evalua datele despre domeniu.

Componenta de învățare automată execută inferența pe caracteristici validate și poate fi actualizată printr-un proces separat de reantrenare. Versiunea nouă este evaluată înainte de activare, iar posibilitatea revenirii la versiunea anterioară trebuie păstrată.

Componenta de raportare generează și ilustrează informații rezultate în urma procesării datelor și evaluării reputației. Furnizează vizualizări, rapoarte și notificări părților interesate. Agregă și ilustrează datele despre reputația domeniului, generează rapoarte despre tendințele de comportament ale domeniului și trimite alerte părților interesate relevante atunci când este necesar.

Componenta Panou de Administrare oferă o interfață de utilizator pentru administratorii de sistem și operatori. Are diverse funcții, inclusiv gestionarea datelor, configurarea sistemului și raportarea. Permite utilizatorilor să configureze sursele de date, să gestioneze setările de crawling, să configureze mecanisme de alertă, să integreze Componenta de raportare și să se bazeze pe rezultatul componentelor anterioare.

Administrarea include controlul accesului, configurarea surselor, urmărirea erorilor și gestionarea versiunilor. Modificările modelului și ale pragurilor se înregistrează, astfel încât evaluările istorice să rămână interpretabile.

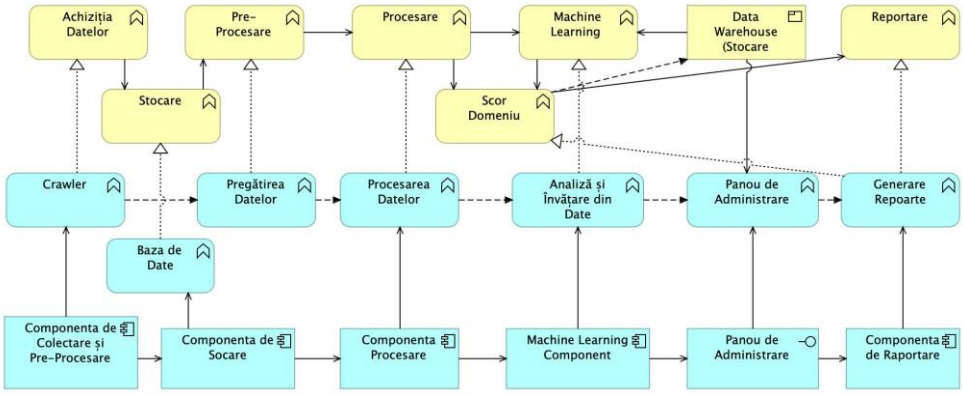


Figura 9. Arhitectura Sistemelor Informaționale și de Date
(Information Systems and Data Architecture View)

Descrierea Arhitecturii Sistemului Informațional furnizează o descriere a sistemului de reputație a numelor de domenii, evidențiind funcțiile și componentele Sistemului Informațional, interacțiunile și procesele implicate. Astfel, le permite beneficiarilor și arhitecților să vizualizeze arhitectura sistemului și modul în care componentele sale interacționează pentru a atinge obiectivele sistemului.

10.10. Arhitectura Tehnologică (Technology Architecture View)

Arhitectura tehnologică de mai jos ilustrează opțiunile analizate în studiul de caz. Limbajele, bazele de date și bibliotecile sunt exemple de implementare a funcțiilor descrise, nu cerințe universale. Selecția concretă trebuie justificată prin volum, latență, competențele echipei și posibilitatea întreținerii.

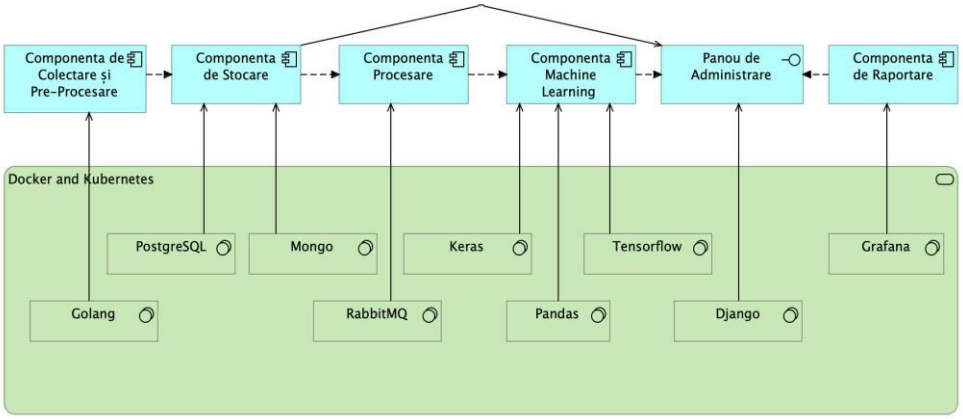


Figura 10. Arhitectura Tehnologică (Technology Architecture View)

Componenta de colectare și preprocesare (dezvoltată în Golang). Această componentă este responsabilă pentru colectarea datelor despre domenii din diverse surse. Golang, cunoscut și sub numele de Go, este un limbaj compilat tip static, cunoscut pentru eficiența sa, suportul concurenței și ecosistemul puternic de biblioteci. Este potrivit pentru dezvoltarea crawlerelor web și a instrumentelor de achiziție de date datorită caracteristicilor sale de performanță.

Componenta de stocare (MongoDB și PostgreSQL) servește ca repository (spațiu de stocare) atât pentru datele brute, cât și pentru cele preprocesate. Utilizează o combinație de tehnologii de baze de date:

PostgreSQL este utilizat ca sistem de gestionare a bazei de date pentru panoul de analiză. Este o bază de date relațională puternică și open-source, cunoscută pentru integritatea și fiabilitatea datelor. PostgreSQL stochează toate datele relevante, inclusiv informații despre reputația domeniului, conturile de utilizator și setările de configurare.

PostgreSQL nu este utilizat pentru stocarea datelor brute, nestructurate din crawler. Pentru aceasta va fi utilizată o bază de date MongoDB. Structura flexibilă bazată pe documente a MongoDB este ideală pentru a găzdui diferite tipuri de date și structuri care pot fi întâlnite în urma utilizării crawler-ului. Este potrivită pentru manipularea unor volume mari de date semi-structurate sau asemănătoare JSON.

Componenta Procesare prelucrează și analizează datele. Utilizează RabbitMQ, un broker de mesaje care permite comunicarea eficientă între diferite componente ale sistemului. Este un instrument de încredere pentru gestionarea sarcinilor de procesare a datelor și distribuirea volumului de lucru.

Componenta Machine Learning folosește diverse biblioteci de învățare automată și analiză a datelor. Keras este un framework deep-learning open-source care oferă abstracții la nivel înalt pentru construirea și antrenarea modelelor de învățare automată, inclusiv rețele neuronale. Pandas este o bibliotecă de gestionare și analiză a datelor care utilizează structuri și funcții de date pentru lucrul cu date structurate. TensorFlow este un framework open-source de învățare automată dezvoltat de Google. Este folosit pentru construirea și formarea modelelor de învățare automată, inclusiv modele deep-learning. Este cunoscut pentru flexibilitatea și suportul pentru rețelele neuronale.

Componenta Panou de administrare (Django și Node.js) oferă o interfață ușor de utilizat pentru administratorii de sistem și utilizatori. Include Componenta de raportare și Componenta de interacțiune cu utilizatorul. Componenta de raportare asigură funcționalitatea de monitorizare în timp real, deoarece afișează actualizări privind reputația domeniului, permițând utilizatorilor să răspundă rapid la schimbări și potențiale amenințări. Interacțiunea cu utilizatorul permite utilizatorilor să interacționeze cu datele. Un exemplu este verificarea reputației domeniului și luarea de decizii informate pe baza informațiilor prezentate.

Tehnologiile au fost selectate după o analiză preliminară, astfel încât să susțină implementarea sistemului și pentru a se potrivi cerințelor și funcțiilor specifice fiecărei componente a sistemului. Combinația acestor tehnologii asigură colectarea, procesarea, stocarea, învățarea automată și interacțiunea utilizatorului, creând un sistem robust și cuprinzător pentru determinarea reputației numelor de domenii.

O implementare web poate separa serviciile de interogare, persistența și prezentarea. În exemplul tehnologic analizat, Django susține logica aplicației; alegerea sa nu influențează direct validitatea statistică a reputației. Aceasta depinde de date, etichete și metoda de evaluare.

Backend-ul panoului de analiză este construit folosind framework-ul Django. Django este un cadru de dezvoltare web de nivel înalt pentru Python cunoscut pentru eficiența și siguranța pe care o oferă. Este folosit pentru executarea sarcinilor pe server, gestionarea bazelor de date și procesarea datelor.

Pentru a facilita comunicarea între frontend și backend, Django Rest Framework este utilizat pentru a crea interfața programabilă RESTful API. Această interfață permite interacțiunea între frontend și baza de date, accesând reputația domeniilor într-o manieră structurată.

Interfața cu utilizatorul este dezvoltată folosind Next.js cu ReactJS. Next.js este un framework React popular, care simplifică crearea aplicațiilor React. ReactJS este o bibliotecă JavaScript folosită în crearea interfețelor de aplicație. Împreună, realizează o interfață inteligentă și interactivă pentru a accesa și vizualiza datele domeniilor.

Componenta Crawler, colectează date din diverse surse, inclusiv datele registrului, unelte interne și externe. Structura flexibilă bazată pe documente a MongoDB este ideală pentru acomodarea diverselor tipuri de date și structuri care pot fi întâlnite în timpul web crawling-ului. Este potrivită pentru manipularea unor volume mari de date semi-structurate sau de tip JSON.

Django procesează cererile utilizatorilor, recuperează date din PostgreSQL și returnează scorurile de reputație a domeniilor pe baza criteriilor și surselor descrise anterior.

Datele prelucrate despre reputația domeniilor sunt prezentate utilizatorului într-un format interactiv și ușor de folosit prin intermediul interfeței cu utilizatorul. Utilizatorii vor avea la dispoziție istoricul domeniilor, scorurile de reputație, vechimea, statusul SSL și/sau alte informații relevante.

Raportarea permite selectarea unui domeniu, portofoliu sau interval temporal și păstrează criteriile selecției. Rapoartele trebuie să includă sursele, limitele acoperirii, versiunile și starea validării concluziilor, pentru a putea fi interpretate și în afara interfeței.

Selecția unor tehnologii specifice, inclusiv TensorFlow, RabbitMQ și Django pentru implementarea unui sistem de reputație a numelor de domeniu, poate fi justificată pe baza caracteristicilor, capacităților și adecvării lor pentru cerințele sistemului. Acestea includ baze de date și soluții de stocare a datelor pentru a asigura persistența și recuperarea datelor, precum și backup-ul și arhivarea datelor.

Descrierea Arhitecturii Tehnologice oferă o imagine de ansamblu cuprinzătoare a tehnologiilor utilizate de fiecare componentă din cadrul Sistemului de reputație a numelor de domeniu. Totodată, furnizează o descriere detaliată a stivei tehnologice, permițând comunicarea eficientă și alinierea arhitecturii tehnologice cu obiectivele și cerințele organizației.

10.11. Managementul Schimbărilor Arhitecturale (Architecture Change Management)

Scopul acestei etape este gestionarea și monitorizarea schimbărilor arhitecturale pe termen lung.

Activitățile includ:

- Monitorizarea arhitecturii pentru a detecta nevoile de schimbare.
- Gestionarea cererilor de schimbare și evaluarea impactului acestora.
- Actualizarea arhitecturii pentru a reflecta schimbările agreate.
- Modificările sunt efectuate astfel încât arhitectura să rămână relevantă și aliniată cu obiectivele organizației.

O schimbare a unui sistem de reputație pornește de la o nevoie documentată și se evaluează asupra arhitecturii, datelor și deciziilor dependente. Implementarea urmează verificării compatibilității, iar activarea trebuie să permită urmărirea efectelor și revenirea controlată.

10.12. Contractele informaționale dintre componente

O arhitectură de reputație trebuie să definească sensul informației schimbate între componente. Un colector nu transmite doar o valoare, ci și obiectul observat, momentul, sursa și starea operației. Un modul de evaluare nu transmite doar un scor, ci și versiunea modelului și condițiile de aplicare. Fără aceste elemente,

componentele pot funcționa tehnic, dar pot interpreta diferit același rezultat. Contractul informațional stabilește ce înseamnă fiecare mesaj și ce nu poate fi dedus din el.

Pentru o observație DNS, contractul poate distinge răspunsul obținut de eșecul colectării. Pentru o observație administrativă, poate distinge absența unui câmp de absența înregistrării. Pentru predicție, poate separa rezultatul disponibil de cazul în care datele nu satisfac cerințele minime. Aceste stări trebuie să rămână distincte până la interfața operatorului. Reducerea lor la o valoare implicită poate simplifica implementarea, dar transferă ambiguitatea către decizie.

Contractele includ și reguli de evoluție. Introducerea unui câmp nou, schimbarea unei unități sau modificarea unei categorii poate afecta preprocesarea și interpretarea. Consumatorii informației trebuie să poată identifica versiunea primită și să trateze explicit variantele necunoscute. Acceptarea silențioasă a unei scheme incompatibile este deosebit de problematică atunci când produce scoruri aparent valide. Verificarea compatibilității reprezintă, prin urmare, o condiție a validității analitice.

Perspectivele arhitecturale permit legarea acestor contracte de cerințe și responsabilități. O cerință de trasabilitate trebuie să apară atât în modelul datelor, cât și în fluxul aplicației și în mecanismul de audit. Diagrama oferă orientarea generală, iar contractul precizează obligațiile la fiecare interfață. Consistența dintre aceste niveluri face posibilă verificarea arhitecturii prin scenarii concrete, fără a depinde de o implementare particulară.

10.13. Reconstituirea unei evaluări și gestionarea dependențelor

Reconstituirea unei evaluări presupune identificarea observațiilor și a transformărilor care au produs-o. Păstrarea scorului final și a numelui algoritmului este insuficientă. Sunt necesare versiunea modelului, schema caracteristicilor, configurația preprocesării și referințele către datele utilizate. Când o sursă se actualizează continuu, interogarea ei ulterioară poate furniza alt rezultat. Arhitectura trebuie să prevadă o formă de conservare a informației relevante pentru evaluarea istorică.

Se poate distinge reproducerea exactă de reanalizarea pe date actuale. Prima urmărește obținerea aceluiași rezultat în condițiile inițiale, în timp ce a doua urmărește o concluzie valabilă în condițiile curente. Ambele sunt utile, dar răspund unor întrebări diferite. Interfața și raportul trebuie să indice ce operație a fost efectuată. Un scor recalculat astăzi nu trebuie prezentat drept reproducere a unei evaluări realizate anterior.

Dependențele pot fi reprezentate prin legături între observație, setul de caracteristici, model, evaluare și decizie. Dacă o observație este corectată, aceste legături permit identificarea rezultatelor care pot necesita revizuire. Dacă un model este retras, evaluările istorice nu dispar, dar pot fi marcate cu contextul retragerii. Separarea evaluării de decizie permite și păstrarea motivului pentru care un operator a ales o acțiune diferită de sugestia automată.

Cerința trebuie aplicată proporțional cu scopul și cu informațiile care pot fi păstrate. Nu este necesară duplicarea necontrolată a tuturor datelor pentru a obține trasabilitate. Este însă necesar să se declare ce poate fi reconstituit și ce limitări rămân.

10.14. Prioritizarea cerințelor prin scenarii de utilizare

Cerințele arhitecturale devin mai clare când sunt examinate prin scenarii. Un operator care verifică un singur domeniu are nevoie de răspuns explicabil și de acces la dovezi. O analiză periodică a unui portofoliu necesită procesare repetabilă și comparabilitate temporală. O reevaluare a unui incident necesită acces la istoricul modificărilor. Aceste utilizări pot partaja componente, dar nu au aceleași priorități de performanță, disponibilitate și păstrare a datelor.

Pentru fiecare scenariu se definește rezultatul așteptat și modul în care sistemul se comportă când o dependență nu este disponibilă. Un răspuns parțial poate fi acceptabil dacă este marcat clar și nu permite o decizie care cere date complete. În alte situații, operația trebuie amânată. Arhitectura trebuie să permită exprimarea acestei diferențe, în loc să aplice aceeași regulă tuturor utilizărilor. Degradarea controlată este o proprietate a serviciului oferit, nu doar a infrastructurii.

Prioritizarea include costul colectării și al verificării umane. O caracteristică suplimentară poate îmbunătăți evaluarea, dar poate crește dependența de o sursă lentă sau dificil de întreținut. Beneficiul trebuie examinat printr-un protocol comparabil și pus în relație cu cerințele scenariului. Decizia de includere nu se bazează exclusiv pe disponibilitatea tehnică a atributului. Se documentează contribuția așteptată și condițiile în care aceasta va fi reevaluată.

În cadrul TOGAF prezentat în acest capitol (The Open Group, 2013), legătura dintre cerințe, componente și schimbări poate fi urmărită prin aceste scenarii. O modificare a modelului sau a sursei trebuie examinată asupra utilizărilor afectate, nu numai asupra componentei schimbate. Această disciplină păstrează arhitectura orientată către evaluarea reputației și responsabilitatea deciziei. Studiul de caz din capitolul următor ilustrează o aplicare particulară, ale cărei rezultate trebuie citite în limitele datelor și protocolului său.

11. Studiu de caz. Domeniile .ro

11.1. Obiectivul și delimitarea studiului

Aplicația dezvoltată pentru stabilirea reputației domeniilor .ro reprezintă contextul aplicativ al studiului iar întrebarea examinată este în ce măsură atributele de înregistrare și metadatele TLS permit ordonarea și clasificarea numelor .ro potrivit etichetelor provenite din liste de reputație.

Aplicația facilitează utilizarea rezultatului, însă existența ei nu constituie o validare a modelului. Unitatea principală a analizei este observația etichetată, asociată unui nume și unui domeniu.

Sunt utilizate două colecții: corpusul principal din septembrie 2026, cu 11.286 de nume și colecția anterioară, cu 5.053 de domenii. Colecțiile diferă prin selecție, proporția claselor, tratarea numelor fără date de registru și prezența subdomeniilor. Din acest motiv, comparația dintre ele este un control al consistenței, nu o măsurare izolată a efectului creșterii volumului de date.

Clasa pozitivă este definită prin apartenența la liste de blocare. Rezultatele caracterizează predicția acestei etichete în corpusurile analizate; nu reprezintă o demonstrație că fiecare nume pozitiv este malițios la momentul lecturii. Acest nivel de precizie terminologică este necesar pentru interpretarea măsurătorilor și pentru utilizarea lor într-un proces de investigație (Rotună, Dumitrache & Sandu 2022; Rotună et al., 2023; Rotună, Sacală & Alexandru, 2025).

11.2. Compoziția celor două corpusuri

Corpusul principal conține 7.196 de observații provenite din liste de referință și 4.090 din liste de blocare. Cele 11.286 de nume corespund unui număr de 9.406 domenii distincte și includ 2.555 de rânduri pentru subdomenii.

Numărul observațiilor nu trebuie confundat cu numărul entităților administrative independente.

Colecția anterioară cuprinde 5.053 de domenii, dintre care 2.547 provin din lista de referință și 2.506 din liste de blocare. Ea este aproape echilibrată prin construcție. În schimb, proporția clasei pozitive în corpusul din 2026 este de aproximativ 36,2%. Niciuna dintre proporții nu estimează automat prevalența abuzului în întregul spațiu .ro.

Diferența dintre 9.406 domenii distincte și 8.731 de rânduri care nu sunt subdomenii este relevantă: prima valoare include părinții identificați prin grupare iar a doua numără numai observațiile păstrate după eliminarea rândurilor de subdomeniu. Cele două numărători nu sunt interschimbabile.

Tabel 38. Comparația corpusurilor .ro

Caracteristică	Septembrie 2026	Colecția anterioară
Observații	11.286 nume; 9.406 domenii distincte; 2.555 subdomenii	5.053 domenii
Clasa de referință	7.196 (63,8%)	2.547 (50,4%)
Clasa pozitivă	4.090 (36,2%)	2.506 (49,6%)
Surse de referință	Tranco, Cisco Umbrella, Majestic	Tranco
Colectare administrativă	Serviciul REST al registrului	Verificare WHOIS / registru
Atribute	10; 21 coloane după codificare	10; 20 coloane după codificare
Certificat indisponibil	22,1%	20,2%
IP indisponibil	11,7%	9,2%
Rol	Evaluare principală	Control al consistenței între colecții

11.3. Sursele și regulile de constituire

Pentru corpusul principal, sursele de referință sunt Tranco, Cisco Umbrella și Majestic. Colecția anterioară utilizează Tranco și surse de blocare precum URLhaus, phishunt.io și dns-blacklists. Tranco este utilizat ca sursă de selecție a unor domenii populare, nu ca certificat de legitimitate.

În versiunea finală a colectării, normalizarea include conversia numelor internaționalizate, eliminarea duplicatelor și respingerea numelor care apar cu ambele etichete. Interfața REST a registrului este interogată pentru domeniul asociat fiecărui nume, inclusiv pentru structurile de nivel secundar. Conexiunea TLS pe portul 443 și rezoluția IP sunt realizate pentru numele complet observat. Colecția anterioară a fost restrânsă la domenii înregistrate, verificate prin serviciul de registru. Un statut administrativ de înregistrare nu dovedește că un site web este activ.

În versiunea finală, observațiile pentru care interogarea registrului nu reușește după repetări sunt păstrate cu atribute lipsă. Această schimbare de selecție contribuie la diferențele dintre corpusuri.

11.4. Caracteristicile utilizate de model

Ambele corpusuri folosesc zece atribute de înregistrare, structură a numelui și TLS. Eticheta is_blacklisted este ținta de învățare și nu face parte din cele zece caracteristici de intrare. Includerea ei ca predictor ar compromite sensul evaluării.

Vârsta și timpul până la expirare descriu ciclul administrativ. Identificatorul registrarului adaugă un context categorial. Indicatorul DNSSEC se referă la informația disponibilă despre delegare și trebuie interpretat potrivit metodei de colectare. Niciunul dintre aceste atribute nu constituie singur o probă a abuzului.

Tabel 39. Caracteristicile celor două corpusuri

Variabilă	Tip	Interpretare
domain_age	Numeric	Zile de la înregistrare la observație
expiration	Numeric	Zile până la expirarea domeniului
has_dnssec	Boolean	Indicator al delegării DNSSEC ce indică prezența DS/DNSKEY
registrar_id	Categorial	Identificatorul registrarului
has_ssl	Boolean	Certificat TLS observat
ssl_certificate_issuer	Categorial	Emitentul certificatului
ssl_certificate_valid_from	Numeric	Zile de la emiterea certificatului
ssl_certificate_validity	Numeric	Zile până la expirarea certificatului
tls_version	Categorial	Versiunea TLS negociată
domain_length	Numeric	Lungimea numelui analizat

Atributele TLS descriu disponibilitatea certificatului, emitentul, timpul de la emitere, valabilitatea rămasă și versiunea negociată. Lungimea numelui este calculată pe numele complet din corpusul principal, astfel încât poate reflecta prezența subdomeniilor. Această alegere trebuie păstrată în interpretarea importanței sale, fără a atribui automat semnalul unei proprietăți intrinseci a domeniului.

11.5. Disponibilitatea datelor și efectul retragerii domeniilor

În corpusul principal, datele de registru lipsesc pentru 4,8% dintre observații. Diferența dintre clase este mare: aproximativ 0,2% pentru numele din listele de referință și 13,0% pentru cele din listele de blocare. Lipsa certificatului privește 22,1% dintre observații, cu 11,2% și, respectiv, 41,2% pe clase.

Adresa IP nu este disponibilă pentru 11,7% din observațiile corpusului principal; 3,9% pentru clasa de referință și 25,3% pentru clasa pozitivă. Aceste diferențe pot oferi informație predictivă, însă pot reflecta și faptul că anumite nume au fost deja retrase sau dezactivate după listare. Modelul poate recunoaște consecințele unei intervenții, fără a demonstra aceeași putere înaintea incidentului.

În colecția anterioară, lipsa certificatului este raportată pentru 20,2% dintre domenii, iar lipsa adresei IP pentru 9,2%. Comparația cu corpusul principal trebuie să țină seama de filtrarea anterioară la domenii înregistrate și de absența rândurilor de subdomeniu. Diferența dintre valori nu poate fi atribuită exclusiv evoluției securității spațiului .ro.

În corpusul din 2026, 52,7% dintre observațiile pozitive sunt subdomenii, față de 5,6% dintre observațiile de referință. Numele care au același părinte partajează atributele registrului. Dacă sunt împărțite aleatoriu între antrenare și testare, evaluarea poate beneficia de informații despre aceeași entitate administrativă în ambele subseturi.

Gruparea după domeniul împiedică această suprapunere specifică. Ea nu elimină toate formele de dependență: domenii distincte pot aparține aceleiași campanii sau pot folosi infrastructură comună. Totuși, pentru structura corpusului principal, reprezintă un control necesar și mai apropiat de situația evaluării unui părinte nevăzut anterior.

Lungimea numelui poate codifica indirect apartenența la o infrastructură de găzduire prin subdomenii. Un rezultat predictiv bazat pe această structură nu trebuie interpretat ca dovadă că toate subdomeniile sunt riscante. Concluzia privește distribuția corpusului și trebuie verificată pe populații cu mecanisme de selecție diferite.

11.6. Algoritmul și fluxul experimental

Fluxul separă construirea corpusului, extragerea caracteristicilor, preprocesarea, antrenarea și evaluarea. XGBoost este algoritmul principal, comparat cu Random Forest și cu modele mai simple. Această comparație urmărește valoarea suplimentară a ansamblurilor de arbori asupra acelorași date, nu stabilirea unei ierarhii universale între algoritmi.

XGBoost construiește succesiv arbori care reduc funcția obiectiv, cu mecanisme de regularizare. Random Forest agregă arbori construiți pe eșantioane și subseturi de caracteristici. Ambele pot reprezenta relații neliniare, însă rezultatele depind de codificare, etichete și partiții. Un model mai complex nu remediază o definiție ambiguă a clasei pozitive.

Există două scheme de validare încrucișată pe cinci partiții: stratificată, în care numele sunt tratate ca observații independente, și stratificată cu grupare după domeniul. Pentru corpusul principal, estimarea grupată este cea reținută ca referință. Predicțiile obținute pe partițiile excluse de la antrenare sunt reunite, astfel încât fiecare nume este evaluat de un model care nu l-a folosit la antrenare.

Modelele de referință includ regresia logistică pe atribute standardizate și arbori de adâncime redusă. Pragul implicit este 0,5. Diferența dintre ansambluri este analizată prin testul exact McNemar asupra predicțiilor discordante. Intervalele de încredere pentru acurațețe sunt raportate prin 2.000 de reeșantionări bootstrap ale predicțiilor obținute în afara antrenării. În reproducerea rezultatului trebuie verificată configurația efectivă din scripturi. Confirmarea necesită artefactele experimentale originale.

11.7. Rezultatele corpusului de 11.286 de nume

În validarea grupată, XGBoost obține acuratețea 0,787, cu interval de încredere de 95% între 0,779 și 0,794, AUC 0,860 și scor Brier 0,143. La pragul 0,5, precizia pentru clasa pozitivă este 0,771 iar sensibilitatea 0,585. Rezultatul susține utilizarea pentru ordonare și triaj, însă lasă neidentificată o parte importantă a exemplelor pozitive din corpus.

Tabel 40. Rezultate pe 11.286 de nume .ro

Model	Acuratețe grupată [IC 95%]	AUC grupată	Brier grupat	Acuratețe stratif.	AUC stratif.
XGBoost	0,787 [0,779–0,794]	0,860	0,143	0,808 [0,801–0,815]	0,880
Random Forest	0,778 [0,771–0,786]	0,854	0,148	0,809	0,882
Regresie logistică	0,752	0,816	0,162	0,761	0,823

Random Forest obține acuratețea 0,778 și AUC 0,854. Diferența de acuratețe este sub un punct procentual. Au fost identificate 929 de predicții discordante: 511 corecte numai pentru XGBoost și 418 numai pentru Random Forest. Testul McNemar produce p = 0,003. Semnificația statistică nu trebuie confundată cu o diferență operațională mare; utilitatea se apreciază în raport cu volumul și costul cazurilor suplimentare identificate.

În validarea stratificată fără grupare, XGBoost ajunge la acuratețea 0,808 și AUC 0,880 iar Random Forest la 0,809 și 0,882. Diferența dintre ansambluri nu mai este semnificativă în comparația raportată, cu p = 0,95. Creșterea față de schema grupată arată cât de mult poate influența protocolul concluzia despre performanță.

Agregarea predicțiilor grupate la nivelul celor 9.406 de domenii distincte produce pentru modelul analizat acuratețea 0,791 și AUC 0,837. Acesta este un rezultat la alt nivel de agregare și nu trebuie amestecat cu metricile calculate pe cele 11.286 de nume. O împărțire grupată separată, de tip 80/20, oferă acuratețea 0,789 și AUC 0,860 pe 2.258 de observații de test, ca verificare suplimentară.

11.8. Rezultatele corpusului de 5.053 de domenii

Tabel 41. Rezultate pe 5.053 de domenii .ro

Model	Acuratețe	AUC
XGBoost	0,698 [0,686–0,711]	0,786
Random Forest	0,699	0,780
Regresie logistică	0,683	0,765

Pentru colecția anterioară, XGBoost obține acuratețea 0,698, cu intervalul 0,686–0,711 și AUC 0,786. Random Forest obține 0,699 și AUC 0,780 iar regresia logistică 0,683 și AUC 0,765. Comparația dintre ansambluri are p = 0,91; datele raportate nu susțin o diferență măsurabilă între ele.

Vârsta domeniului este dominantă în această colecție, iar un arbore cu o singură divizare pe vârstă ajunge la acuratețea 0,681. Această observație arată importanța modelelor simple de referință: o parte semnificativă a separării este disponibilă fără o combinație complexă de caracteristici.

Diferența de AUC dintre cele două colecții nu demonstrează că adăugarea de exemple a produs singură îmbunătățirea. Corpusul principal include nume fără înregistrare disponibilă și o proporție mare de subdomenii în clasa pozitivă. Compoziția, momentul și regulile de colectare se schimbă simultan. Concluzia prudentă este că atributele au un semnal util, dar variabil între populații.

11.9. Importanța atributelor și ablațiile

Sunt raportate, pe împărțirea grupată rezervată pentru analiză, o scădere medie a acurateței de 0,073 la permutarea lungimii numelui, 0,048 pentru vârsta domeniului și 0,045 pentru timpul de la emiterea certificatului. Urmează identificatorul registrarului și valabilitatea rămasă a certificatului, fiecare cu 0,034. Aceste valori exprimă dependența modelului de atribute în contextul corpusului, nu efecte cauzale asupra abuzului.

Tabel 42. Ablații și verificări pentru corpusul principal

Atribute sau schemă	Acuratețe	AUC	Brier
Toate atributele	0,787	0,860	0,143
Fără identificatorul registrarului	0,780	0,849	0,149
Numai atribute administrative	0,760	0,802	0,166
Numai atribute TLS	0,717	0,756	0,188
Fără vârsta domeniului	0,771	0,844	0,152
Numai vârsta domeniului	0,681	0,634	0,213
Fără indicatorii de disponibilitate	0,785	0,859	0,144
Fără lungimea numelui	0,742	0,806	-
Cu indicator explicit de subdomeniu	0,842	0,899	-
Numai rânduri fără subdomenii	0,837	0,835	0,119
Antrenare pe domenii de peste un an; test pe cohorta recentă	0,760	0,695	0,174

Atributele administrative folosite separat produc AUC 0,802 iar cele TLS AUC 0,756. Eliminarea vârstei conduce la AUC 0,844, în timp ce vârsta singură produce 0,634. Spre deosebire de corpusul anterior, niciun atribut unic nu explică întreaga separare din colecția principală.

Eliminarea indicatorilor expliciți de disponibilitate modifică foarte puțin rezultatul: AUC 0,859 față de 0,860. Aceasta nu dovedește că disponibilitatea este irelevantă, deoarece codurile pentru valori lipsă din celelalte câmpuri păstrează aceeași informație. O ablație trebuie interpretată în raport cu redundanța reprezentării, nu numai cu numele coloanei eliminate.

Eliminarea lungimii numelui reduce AUC la 0,806, iar adăugarea unui indicator explicit de subdomeniu o crește la 0,899. Acest câștig evidențiază influența

compoziției listelor. Un predictor foarte eficient într-un corpus poate exploata o diferență de selecție care nu se menține în populația operațională.

După eliminarea celor 2.555 de rânduri de subdomeniu rămân 8.731 de nume. Acuratețea crește la 0,837, dar AUC scade la 0,835, iar sensibilitatea la pragul 0,5 ajunge la 0,406. Creșterea acurateței coexistă cu reducerea capacității de recuperare a clasei pozitive, în contextul unei proporții pozitive de aproximativ 22%. Acest exemplu arată de ce acuratețea nu este suficientă.

11.10. Domeniile recent înregistrate și transferul temporal

Verificarea raportată antrenează modelul pe 9.927 de nume al căror domeniu are peste un an și îl evaluează pe 817 nume asociate unor domenii înregistrate în ultimul an. Rezultatul este AUC 0,695, acuratețe 0,760 și sensibilitate 0,384. Puterea de discriminare este mai redusă tocmai pentru populația recentă, importantă în screeningul preventiv.

Acesta este un control pe cohorte definite prin vechime. Nu este echivalent, prin el însuși, cu o validare prospectivă completă în care modelul este înghețat la o dată și evaluat pe evenimente colectate ulterior. Pentru o astfel de concluzie sunt necesare marcaje temporale ale caracteristicilor și etichetelor, precum și separarea cronologică efectivă.

Rezultatul justifică evaluarea unor date administrative și comportamentale suplimentare, dar nu permite atribuirea anticipată a unui câștig. Orice extindere trebuie comparată pe aceleași cohorte și trebuie să demonstreze că semnalul ar fi fost disponibil la momentul deciziei, nu numai după apariția listării.

11.11. Calibrarea și pragul de decizie

Pentru corpusul principal, probabilitățile XGBoost sunt descrise ca apropiate de frecvențele observate. Calibrarea izotonică realizată în interiorul validării nu îmbunătățește scorul Brier: 0,145 față de 0,143; pierderea logaritmică este 0,442 față de 0,437. În corpusul anterior, calibrarea reduce scorul Brier de la 0,192 la 0,185.

Rezultatele arată că verificarea calibrării trebuie repetată pentru fiecare populație. O procedură de corecție utilă într-o colecție nu aduce obligatoriu un beneficiu în alta. Calibrarea față de etichetele din liste nu înseamnă, de asemenea, calibrare față de toate incidentele reale, care pot fi incomplet observate.

Tabel 43. Efectul pragului asupra metricilor

Prag	Precizie	Sensibilitate	F1
0,30	0,633	0,788	0,702
0,50	0,771	0,585	0,665
0,70	0,887	0,432	0,581
0,85	0,941	0,303	0,458

Creșterea pragului ridică precizia și reduce sensibilitatea în rezultatele raportate. La 0,30, modelul recuperează aproximativ 78,8% dintre exemplele pozitive, cu precizia 0,633. La 0,85, precizia este 0,941, dar sensibilitatea scade la 0,303. Pragul trebuie ales în funcție de obiectiv: investigație largă, selecție restrânsă sau o altă acțiune documentată.

Tabel 44. Valori predictive la prevalențe ipotetice și prag fix 0,5

Prevalență	Valoare predictivă pozitivă	Valoare predictivă negativă
36 % (corpus)	0,771	0,793
10 %	0,397	0,951
5 %	0,238	0,976
1 %	0,056	0,995

Estimările pentru prevalențe diferite utilizează sensibilitatea 0,585 și specificitatea 0,901 raportate la pragul 0,5. Ele sunt calcule condiționate de menținerea acestor rate, nu măsurători ale prevalenței reale din .ro. La o prevalență ipotetică de 5%, valoarea predictivă pozitivă este aproximativ 0,238 iar la 1% aproximativ 0,056. Volumul verificărilor umane poate deveni astfel important chiar pentru un model cu AUC util.

11.12. Limite și implicații pentru utilizare

Principala limită este relația dintre eticheta bazată pe liste și fenomenul operațional urmărit. Sursele pot fi incomplete, întârziate sau concentrate asupra anumitor tipuri de abuz. Rezultatele nu estimează direct toate domeniile malițioase din spațiul .ro și nu justifică o acțiune ireversibilă doar pe baza scorului.

A doua limită este efectul disponibilității. Numele deja retrase sau serviciile deja dezactivate pot fi mai ușor de separat decât amenințările aflate la început. Utilitatea pentru detectare preventivă trebuie măsurată distinct de recunoașterea unor cazuri cunoscute și deja tratate.

A treia limită privește dependențele dintre observații și transformările datelor. Gruparea după domeniul reduce o formă de contaminare, dar nu controlează toate relațiile de infrastructură sau campanie. Intervalele de încredere și testele trebuie citite în condițiile protocolului raportat, inclusiv ale unității de reeșantionare.

12. Concluzii

12.1. Reputația ca evaluare contextuală

Numele de domeniu este un punct de legătură între procese administrative, servicii tehnice și activități observabile. Niciuna dintre aceste perspective nu descrie singură întregul comportament al unui domeniu. Evaluarea trebuie să precizeze obiectul, intervalul și dovezile, precum și nivelul până la care concluzia poate fi extinsă. Distincția dintre domeniu, subdomeniu și resursă web este fundamentală pentru evitarea unor atribuiri nejustificate.

Corelarea observațiilor externe cu datele administrative poate îmbunătăți evaluarea reputației, în măsura în care aceste date sunt disponibile, dar nu elimină incertitudinea. Un registru poate descrie starea înregistrării fără să observe toate serviciile sau toate incidentele. O listă externă poate semnala abuzul fără să descrie complet istoricul administrativ. Valoarea analizei rezultă din corelarea acestor perspective și din păstrarea limitelor fiecăreia.

Separarea reputației de riscul unei acțiuni permite utilizarea proporțională a rezultatelor. Același semnal poate justifica o verificare suplimentară și poate fi insuficient pentru o măsură cu impact ridicat. Un sistem util păstrează explicit stările de incertitudine, datele lipsă și dezacordurile dintre surse, în loc să le transforme artificial într-o concluzie categorică.

12.2. Calitatea datelor precedă alegerea algoritmului

Construirea corpusului determină ce relație poate învăța modelul. Popularitatea, listarea, retragerea și compromiterea sunt fenomene diferite, care se pot suprapune. O etichetă derivată din liste trebuie interpretată prin criteriul și momentul sursei. Evaluarea experimentală este mai convingătoare atunci când documentează această procedură și limitele ei, nu numai numărul observațiilor.

Normalizarea, deduplicarea și gruparea după domeniul sunt controale metodologice. Ele trebuie să păstreze datele originale și să evite atât multiplicarea artificială a exemplelor, cât și pierderea informației despre incidente limitate la subdomenii. Valorile lipsă trebuie legate de cauzele colectării, deoarece indisponibilitatea poate influența semnificativ modelul.

Validarea trebuie să urmărească independența informațională dintre dezvoltare și evaluare. Preprocesarea, alegerea caracteristicilor, pragurile și calibrarea trebuie controlate în interiorul protocolului. O împărțire convenabilă a rândurilor nu garantează separarea entităților, campaniilor sau perioadelor relevante.

12.3. Lecțiile și limitele studiului de caz

Studiul de caz utilizează două colecții de nume de domenii „.ro”. Prima include 11.286 de și a doua 5.053. Pe corpusul principal, validarea grupată produce pentru XGBoost AUC 0,860 și acuratețea 0,787. Pe colecția anterioară, valorile sunt 0,786 și 0,698. Aceste rezultate susțin existența unui semnal predictiv, cu limite care depind de selecție și de protocol.

Avantajul față de Random Forest este redus în corpusul principal și nu este demonstrat în colecția anterioară. Alegerea algoritmului trebuie, în consecință, justificată prin rezultate comparabile și prin cerințe de exploatare. Datele nu susțin proclamarea unei superiorități generale sau transferul automat al performanței asupra altor populații de domenii.

Disponibilitatea serviciilor și structura subdomeniilor explică o parte importantă a separării. Domeniile deja retrase sau neaccesibile pot furniza un semnal diferit de cel necesar prevenirii timpurii. Rezultatul mai modest pentru cohorta recent înregistrată arată necesitatea evaluării distincte a populațiilor de interes operațional.

12.4. Arhitectura și procedura ca suport pentru sisteme de reputație

Arhitectura trebuie să facă vizibile proveniența datelor, transformările și responsabilitățile. Perspectivele TOGAF prezentate în carte organizează procesele, informațiile și tehnologiile fără a transforma un cadru de modelare într-o garanție de calitate. Separarea colectării, evaluării și deciziei permite verificarea fiecărei componente și localizarea erorilor.

Procedura de evidență completează modelul statistic. Înregistrarea domeniului, a sursei, a momentului, a dovezilor și a evaluatorului permite urmărirea unei concluzii și corectarea sa. În absența acestei evidențe, chiar un scor calculat corect poate fi utilizat în afara contextului sau păstrat după expirarea relevanței sale.

Monitorizarea trebuie să urmărească atât disponibilitatea serviciului, cât și actualitatea datelor și evoluția erorilor. O aplicație care răspunde fără erori nu este neapărat un sistem care evaluează corect. Schimbările de surse, modele și praguri necesită versiuni, verificări și posibilitatea revenirii.

12.5. Direcții de cercetare și aplicare

O direcție prioritară este colectarea unor observații aliniate temporal cu incidentele și evaluarea prospectivă pe date ulterioare. Aceasta ar separa mai bine semnalele disponibile înaintea abuzului de efectele listării și retragerii. Cohortele recente, domeniile legitime compromise și serviciile cu date incomplete trebuie examinate distinct.

O a doua direcție este analiza contribuției surselor. Experimentele care elimină succesiv liste, familii de caracteristici și grupuri de infrastructură pot evidenția dependențe ascunse. Extinderea datelor administrative sau comportamentale trebuie evaluată prin același protocol, fără a presupune anticipat un beneficiu.

O a treia direcție privește evaluarea intervenției umane. Sunt necesare decizii documentate, criterii comune și măsurarea dezacordului între evaluatori. Etichetele validate operațional pot îmbunătăți analiza, dar trebuie protejate de circularitate: predicția modelului nu trebuie retransformată necritic în adevăr de antrenare.

Contribuția unei abordări academice și operaționale a reputației constă în legătura verificabilă dintre observație, estimare și acțiune. Această legătură permite folosirea utilă a algoritmilor, fără a ascunde limitele datelor, incertitudinea și responsabilitatea deciziei.

Mulțumiri

Această lucrare de cercetare a fost susținută printr-o finanțare din partea Autorității Naționale pentru Cercetare, în cadrul Programului Nucleu, cod proiect: PN 2338 02 01, titlul proiectului: „Arhitectura – platforma de monitorizare inteligentă a domeniilor Internet prin dezvoltarea unui sistem dinamic de stabilire a reputației (TLDRep)".

În ceea ce privește utilizarea instrumentelor de asistență la redactare, precizăm că s-a recurs la procesarea automată a textului pentru traducerea unor părți/expresii din carte, precum și pentru corectarea manuscrisului. În cadrul acestui proces, anumite fragmente au fost reformulate pentru a le îmbunătăți claritatea, concizia sau corectitudinea gramaticală, fără a modifica sensul sau conținutul informațional al acestora.

Bibliografie

Almashhadani, A.O., Kaiiali, M., Carlin, D. & Sezer, S. (2020) MaldomDetector: A system for detecting algorithmically generated domain names with machine learning. *Computers & Security*. 93, articolul 101787. https://doi.org/10.1016/j.cose.2020.101787.

Antonakakis, M., Perdisci, R., Dagon, D., Lee, W. & Feamster, N. (2010) Building a dynamic reputation system for DNS. În Proceedings of the 19th USENIX Security Symposium. *USENIX Association*, pp. 273–290. Disponibil la: https://www.usenix.org/legacy/events/sec10/tech/full_papers/ Antonakakis.pdf.

Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou II, N. & Dagon, D. (2011) Detecting malware domains at the upper DNS hierarchy. În Proceedings of the 20th USENIX Security Symposium. *USENIX Association*. Disponibil la: https://www.usenix.org/conference/usenix-security-11/detecting-malware-domains-upper-dns-hierarchy.

Arends, R., Austein, R., Larson, M., Massey, D. & Rose, S. (2005) *Protocol Modifications for the DNS Security Extensions*. RFC 4035. https://doi.org/10.17487/RFC4035.

Barracuda Networks (2026) *Barracuda Reputation and Email Categorization*. Documentația Email Gateway Defense, 28 iulie. Disponibil la: https://documentation.campus.barracuda.com/wiki/spaces/EGD/pages/2850900/Barracuda+Reputation+and+Email+Categorization [Accesat: 26 octombrie 2026].

Beauvoir, P. & Sarrodie, J.-B. (2026) *Archi: Open Source ArchiMate Modelling*. Disponibil la: https://www.archimatetool.com/ [Accesat: 26 octombrie 2026].

Bilge, L., Kirda, E., Kruegel, C. & Balduzzi, M. (2011) EXPOSURE: Finding malicious domains using passive DNS analysis. În Proceedings of the Network and Distributed System Security Symposium (NDSS 2011). *Internet Society*. Disponibil la: https://www.ndss-symposium.org/ndss2011/exposure-finding-malicious-domains-using-passive-dns-analysis/.

Breiman, L. (2001) Random forests. *Machine Learning.* 45, 5–32. https://doi.org/10.1023/A:1010933404324.

Caglayan, A., Toothaker, M., Drapeau, D., Burke, D. & Eaton, G. (2009) Real-time detection of fast flux service networks. În 2009 Cybersecurity Applications & Technology Conference for Homeland Security. *IEEE*. pp. 285–292. https://doi.org/10.1109/CATCH.2009.44.

Chen, T. & Guestrin, C. (2016) XGBoost: A scalable tree boosting system. În Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. *ACM*. pp. 785–794. https://doi.org/10.1145/2939672.2939785.

Damas, J. & Neves, F. (2008) *Preventing Use of Recursive Nameservers in Reflector Attacks*. RFC 5358. https://doi.org/10.17487/RFC5358.

DeLong, E.R., DeLong, D.M. & Clarke-Pearson, D.L. (1988) Comparing the areas under two or more correlated receiver operating characteristic curves: A nonparametric approach. *Biometrics*. 44(3), 837–845. https://doi.org/10.2307/2531595.

Fukushima, Y., Hori, Y. & Sakurai, K. (2011) Proactive blacklisting for malicious web sites by reputation evaluation based on domain and IP address registration. În 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. *IEEE*. pp. 352–361. https://doi.org/10.1109/TrustCom.2011.46.

Holland, B. (2019) TLD operator perspective on the changing cyber security landscape. *Centre for International Governance Innovation*, 9 aprilie. Disponibil la: https://www.cigionline.org/articles/tld-operator-perspective-changing-cyber-security-landscape/ [Accesat: 26 octombrie 2026].

Hubert, A. & van Mook, R. (2009) *Measures for Making DNS More Resilient against Forged Answers*. RFC 5452. https://doi.org/10.17487/RFC5452.

IANA (2026) *Top-Level Domains*. Disponibil la: https://www.iana.org/domains/root/db [Accesat: 26 octombrie 2026].

ICANN Security and Stability Advisory Committee (ICANN SSAC) (2010) *A Registrant's Guide to Protecting Domain Name Registration Accounts*. SAC044, 5 noiembrie. Disponibil la: https://www.icann.org/en/groups/ssac/documents/sac-044-en.pdf.

Internet Systems Consortium (2018) *Using the Response Rate Limiting Feature*. Actualizat la 17 septembrie. https://kb.isc.org/docs/aa-00994 [Accesat: 26 octombrie 2026].

Lombardo, P., Saeli, S., Bisio, F., Bernardi, D. & Massa, D. (2018) Fast flux service network detection via data mining on passive DNS traffic. *Lecture Notes in Computer Science*, 11060, 463–480. Cham: Springer. https://doi.org/10.1007/978-3-319-99136-8_25.

McNemar, Q. (1947) Note on the sampling error of the difference between correlated proportions or percentages. *Psychometrika*. 12(2), 153–157. https://doi.org/10.1007/BF02295996.

Mishsky, I., Gal-Oz, N. & Gudes, E. (2015) A topology based flow model for computing domain reputation. În Samarati, P. (ed.) Data and Applications Security and Privacy XXIX. DBSec 2015. *Lecture Notes in Computer Science*. 9149, 277–292. Springer. https://doi.org/10.1007/978-3-319-20810-7_20.

OWASP Foundation (2026) Test for Subdomain Takeover. În *Web Security Testing Guide*, versiunea 4.2, secțiunea 4.2.10, identificator WSTG-CONF-10. Disponibil la: documentația OWASP [Accesat: 26 octombrie 2026]. OWASP Web Security Testing Guide.

Priyadharshini (2013) *Top 10 Benefits of TOGAF® Certification in Enterprise Architecture*. Simplilearn. https://www.simplilearn.com/TOGAF-certification-benefits-article.

RiskAnalytics (2026) *Community Projects*. Disponibil la: https://riskanalytics.com/community/ (Accesat: 26 octombrie 2026).

Rose, S., Liu, C. & Gibson, R. (2026) Secure Domain Name System (DNS) Deployment Guide. *NIST Special Publication* 800-81, revizia 3. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-81r3.

Rotună, C.-I., Dumitrache, M. & Sandu, I.-E. (2022) Assessment of machine learning algorithms for automated monitoring. *Romanian Journal of Information Technology and Automatic Control*. 32(3), 73–84. https://doi.org/10.33436/v32i3y202206.

Rotună, C.I., Gheorghiță, A., Sandu, I., Dumitrache, M., Udroiu, M. & Smada, D. (2023) A generic architecture for building a domain name reputation system. *Studies in Informatics and Control*. 32(2), 39–49. https://doi.org/10.24846/v32i2y202304.

Rotună, C.I., Sacală, I.Ș. & Alexandru, A. (2025) Towards proactive domain name security: An adaptive system for .ro domains reputation analysis. *Future Internet*. 17(10), articolul 478. https://doi.org/10.3390/fi17100478.

Ruposky, T.J. (2022) The exponential rise of cybercrime. *University of Central Florida Department of Legal Studies Law Journal*. 5. Disponibil la: volumul publicat de University of Central Florida. ccie.ucf.edu

Scalzo, F. (2017) DNS-based threats: DNS reflection and amplification attacks. *Verisign Blog*, 13 decembrie. Disponibil la: https://blog.verisign.com/security/dns-based-threats-dns-reflection-amplification-attacks/ [Accesat: 26 octombrie 2026].

Stăicuț, E. (1995) Domain Name Systems, InterNIC and RIPE Procedures. În *Proceedings of the NATO Advanced Networking Workshop: The First CEENet Workshop on Networks Technology, Varșovia, Polonia, 15–24 septembrie*. CEENet.

SURBL (2026a) *Implementation Guidelines*. Disponibil la: https://www.surbl.org/guidelines [Accesat: 26 octombrie 2026].

SURBL (2026b) *Our Reputation Lists*. Disponibil la: https://www.surbl.org/lists [Accesat: 26 octombrie 2026].

SURBL (2026c) *SURBL: Intelligence and Reputation Services*. Disponibil la: https://www.surbl.org/ [Accesat: 26 octombrie 2026].

Tepandi, J., Grandry, E., Fieten, S., Rotuna, C., Sellitto, G.P., Zeginis, D., Draheim, D., Piho, G., Tambouris, E. & Tarabanis, K. (2019) Towards a cross-border reference architecture for the once-only principle in Europe: An enterprise modelling approach. The Practice of Enterprise Modeling. PoEM 2019. *Lecture Notes in Business Information Processing*. 369, 103–117. Springer, https://doi.org/10.1007/978-3-030-35151-9_7.

The Open Group (2013) *ArchiMate® 2.1 Specification*. Document C13L. The Open Group. Disponibil la: catalogul oficial al standardelor. www.opengroup.org.

The Open Group (2022) *The TOGAF® Standard, 10th Edition—Introduction and Core Concepts*. Document C220. The Open Group. Disponibil la: https://www.opengroup.org/library/c220.

The Spamhaus Team (2021) Best practice: DNSBLs and email filtering—how to get it right. *Spamhaus*, 27 ianuarie. Disponibil la: https://www.spamhaus.org/resource-hub/email-security/best-practice-dnsbls-and-email-filtering-how-to-get-it-right/ [Accesat: 26 octombrie 2026].

Udroiu, A.-M. & Vevera, A.-V. (2018) Using blockchain technology in designing cyber-security solutions. În Cîrciumaru, F. și Atanasiu, M. (eds.) *International Scientific Conference Strategies XXI: The Complex and Dynamic Nature of the Security Environment*, vol. 2. București: Editura Universității Naționale de Apărare „Carol I”, pp. 324–332.



Numărul numelor de domenii este în continuă creștere, iar incidentele de securitate cresc exponențial. Prin urmare, sunt necesare soluții automatizate pentru monitorizarea numelor de domenii și alertarea beneficiarilor. Determinarea nivelului de reputație al unui nume de domeniu sporește securitatea pentru persoane fizice, instituții publice și companii private, oferind utilizatorilor o imagine clară asupra gradului de încredere asociat unui domeniu.

Lucrarea de față prezintă arhitectura unei soluții de monitorizare automatizată, concepută pentru a stabili reputația fiecărui domeniu .ro, precum și a altor domenii. Obiectivul principal este consolidarea încrederii în utilizarea domeniilor .ro, prin reducerea activităților malițioase pe Internet, realizată prin monitorizare automatizată și atenuarea consecințelor.

Se acordă o importanță deosebită calității datelor, trasabilității proveniență acestora și gradului de actualitate a observațiilor. Metodele de învățare automată sunt discutate prin prisma validării, erorilor și interpretării scorurilor. Analiza operațională evidențiază importanța dovezilor verificabile și a deciziilor documentate. Lucrarea include o procedură pentru înregistrarea și validarea informațiilor despre domenii malițioase. Cartea se adresează cercetătorilor, specialiștilor în securitate și administratorilor de infrastructuri.

ISBN ONLINE 978-606-95858-9-4