IDS-RS — Sistem de Detectie a Intruziunilor in Reteaua Interna

Propunere de implementare pentru conducere

1. DE CE AVEM NEVOIE DE ACEST PROIECT

Contextul nostru

Reteaua noastra este una **restransa si securizata**. Nu vorbim despre atacuri venite din internet — perimetrul extern este protejat. Amenintarea reala vine **din interior**.

Imaginati-va cladirea noastra. Avem gard, avem poarta cu bariera, avem legitimatii. Nimeni din afara nu intra. Dar ce se intampla **inauntru**?

Daca un angajat conecteaza un laptop personal infectat la reteaua interna, acel laptop incepe sa "se uite" in jur — verifica ce calculatoare exista, ce servicii ruleaza, ce porturi sunt deschise. Sau un utilizator curios care instaleaza un tool de scanare "sa vada ce gaseste". Sau un cont compromis prin phishing care devine un punct de plecare pentru miscari laterale in retea.

Firewall-ul intern vede fiecare tentativa. Dar nimeni nu se uita.

Ce se intampla astazi

Firewall-ul genereaza mii de log-uri pe ora. Fiecare conexiune blocata este inregistrata — dar aceste log-uri stau in fisiere pe care **nimeni nu le citeste in timp real**. Este ca si cum ai avea camere de supraveghere in toata cladirea, dar niciun ecran nu este monitorizat.

Intrebarea nu este daca cineva va incerca ceva in reteaua interna. Intrebarea este: **vom sti cand se intampla?**

- Un laptop infectat care scaneaza reteaua poate fi activ **zile intregi** fara sa fie observat
- Un utilizator care testeaza limite poate escalada privilegii inainte sa intervina cineva

- Fara vizibilitate in timp real, echipa IT reactioneaza **dupa fapt**, nu in momentul in care se intampla

De ce conteaza

Conform rapoartelor internationale de securitate cibernetica:

- **60% din incidentele de securitate** au origine interna — angajati, contractori, echipamente compromise
- **Timpul mediu de detectie** a unei miscari laterale in retea este de **204 zile**
- **83% din compromiterile reussite** au fost precedate de o faza de **scanare a retelei** care ar fi putut fi detectata

Intr-o retea restransa ca a noastra, avantajul este ca **stim exact cine este inauntru**. Dezavantajul este ca, fara monitorizare, presupunem ca toti cei din interior sunt de incredere — si asta este cea mai periculoasa presupunere in securitate.

---

2. SOLUTIA: IDS-RS

Ce este IDS-RS

IDS-RS este un **Sistem de Detectie a Intruziunilor** dezvoltat intern, care monitorizeaza in timp real log-urile firewall-ului intern si detecteaza automat comportamente suspecte din reteaua noastra.

Cum functioneaza — pe intelesul tuturor

Ganditi-va la IDS-RS ca la un **dispecer inteligent pentru camerele de supraveghere**:

Firewall-ul raporteaza fiecare conexiune blocata individual — nu stie ca 50 de blocari de la aceeasi sursa inseamna o scanare.

IDS-RS coreleaza aceste evenimente si vede **tiparul**: "Statia 192.168.10.45 a incercat 50 de servicii diferite in 10 secunde — aceasta nu este activitate normala."

Echipa IT primeste instant o alerta cu IP-ul sursa, ce a incercat si comenzi gata de executat pentru investigare si izolare.

---

3. CE PUTEM DETECTA

Trei tipuri de comportament suspect

Scanare Rapida (Fast Scan): O statie care testeaza zeci de servicii in cateva secunde. Comportament tipic pentru un malware care "se uita in jur" imediat dupa infectare. Echivalentul cuiva care alearga pe hol si trage de fiecare usa.

Scanare Lenta (Slow Scan): O statie care testeaza cate un serviciu la cateva minute — incercand sa fie discreta. IDS-RS monitorizeaza pe perioade extinse si detecteaza si acest tipar. Echivalentul cuiva care verifica o usa pe zi, stiind ca o verificare rapida ar fi observata.

Scanare cu Acces (Accept Scan): Identifica cazurile in care cineva descopera servicii care **raspund** — nu doar cele blocate. Cel mai periculos tip, deoarece persoana gaseste efectiv puncte de acces functionale in retea.

Vizibilitate pe multiple canale

Canal	Ce primiti
SIEM	Alerte in platforma centralizata, corelate cu alte evenimente
Email	Notificare detaliata cu comenzi de reactie gata de executat

---

4. BENEFICII

Control intern complet

- **Stim in secunde** cand o statie din retea incepe sa se comporte suspect
- **Fiecare tentativa de scanare** este inregistrata si alertata — nimic nu trece neobservat
- **Comenzi de reactie gata pregatite** — echipa nu pierde timp cautand ce sa execute

Operare simpla

- **Un singur fisier de configurare** — fara cunostinte de programare
- **Configurarea se modifica fara oprire** — ajustari in timp real
- **Sistemul se intretine singur** — curatare automata, fara interventie manuala

Avantaje pentru organizatie

- **Dezvoltat intern** — control complet, fara licente, fara dependenta de furnizor extern
- **Compatibil cu infrastructura existenta** — functioneaza cu firewall-urile si SIEM-ul pe care le avem deja
- **Implementare graduala** — fara impact asupra serviciilor in productie

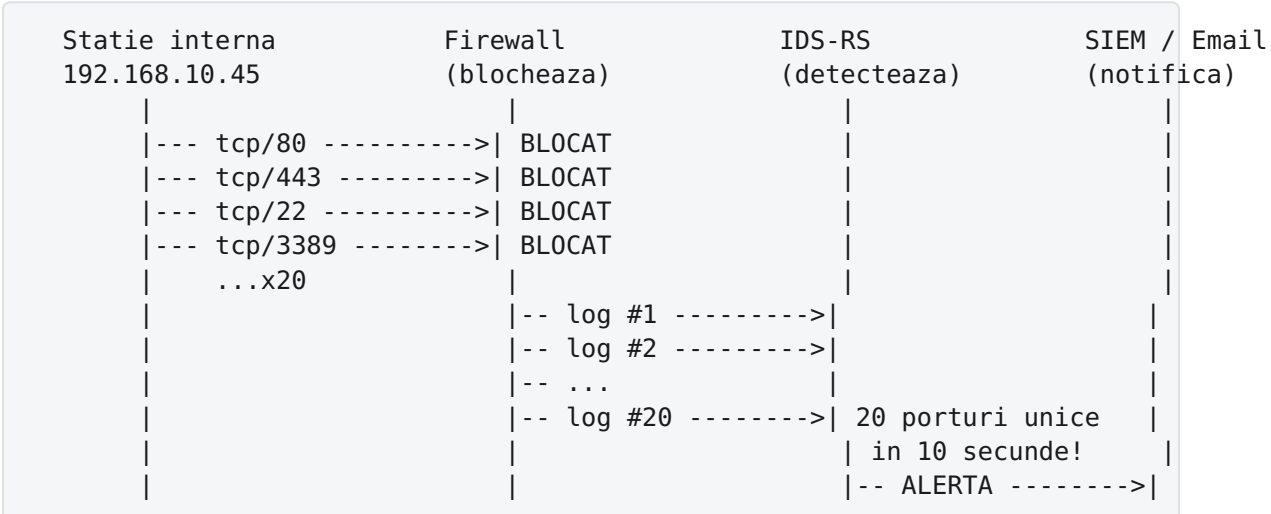
---

5. CE VEDETI CONCRET

Arhitectura sistemului

Calatoria unui eveniment — de la activitate suspecta la alerta

O statie infectata din retea bate la 20 de servicii diferite. Firewall-ul blocheaza fiecare tentativa si trimite un log. IDS-RS le coreleaza:



Cum arata alerta in SIEM (ArcSight)

Echipa vede direct in consola SIEM un eveniment clar, cu toate detaliile:

```
+-----------------+-----------------+-----------------+------+----------+---------------
| Time            | Source Address  | Target Address  | Cnt  | Priority | Message
+-----------------+-----------------+-----------------+------+----------+---------------
| Feb 26 14:30:00 | 192.168.10.45  | 10.0.0.1        |  20  | High     | Fast Scan detect
|                 |                 |                 |      |          | in 10s | ports:
+-----------------+-----------------+-----------------+------+----------+---------------
```

Campuri disponibile pentru investigare: - **Source Address** — statia care scaneaza (cine) - **Target Address** — ce tinta a fost scanata (unde) - **Cnt** — cate porturi unice au fost testate (cat de agresiv) - **ScannedPorts** — lista completa a porturilor (ce a cautat)

Cum arata email-ul de alerta

Echipa IT primeste un email structurat, cu tot ce trebuie sa stie si sa faca:

```
============================================================
    ALERTA DE SECURITATE -- IDS-RS
============================================================

  Tip scanare:    Fast Scan
  Severitate:     RIDICATA

------------------------------------------------------------
  DETALII EVENIMENT
------------------------------------------------------------

  IP sursa:             192.168.10.45
  IP destinatie:        10.0.0.1
  Porturi scanate:      20
  Timestamp:            2026-02-26 14:30:00

  Porturi:              21, 22, 23, 25, 53, 80, 110, 143,
                        443, 993, 995, 3389, 8080, ...

------------------------------------------------------------
  COMENZI UTILE (quick check)
------------------------------------------------------------

  # Log-uri firewall pentru acest IP (ultima ora):
  log show -s 192.168.10.45 -t "last 1 hour"

  # Conexiuni active de la acest IP:
  fw tab -t connections -s | grep 192.168.10.45

  # Blocare temporara (SAM):
  fw sam -t 3600 -I src 192.168.10.45

============================================================

      ____  ____  ____  ____
     / ___|| ___|| __ )|___ \
     \___ \|___ \|  _ \  __) |
      ___) |___) | |_) |/ __/
     |____/|____/|____/|_____|

  Generat automat de S5B2
============================================================
```

Inginerul de garda vede instant: **cine** scaneaza, **ce** a scanat, si are comenzi **gata de executat** — copy/paste direct in firewall.

Scenarii de conectare

IDS-RS se adapteaza la infrastructura existenta, fara schimbari majore:

Scenariul A — Firewall direct catre IDS-RS:

```
  Checkpoint/FortiGate         IDS-RS
  Firewall intern     -------->  UDP :5555
                      syslog     parser = "gaia" / "fortigate"
```

Scenariul B — Prin platforma ArcSight (SIEM deja existent):

```
  Firewall       ArcSight            IDS-RS
  intern  -----> SmartConnector ---->  UDP :5555
         syslog (normalizeaza         parser = "cef"
                 la format CEF)
```

In ambele cazuri, conectarea inseamna o singura regula de forwarding pe firewall sau pe ArcSight — fara modificari ale politicilor de securitate.

Structura proiectului

```
ids-rs/
├── config.toml             # Configurare (un singur fisier, totul aici)
├── src/
│   ├── main.rs             # Orchestrare: receptie, procesare, alerte
│   ├── config.rs           # Citire si validare configurare
│   ├── detector.rs         # Motor detectie: Fast / Slow / Accept Scan
│   ├── alerter.rs          # Trimitere alerte: SIEM (UDP) + Email (SMTP)
│   ├── display.rs          # Afisare in terminal (dashboard live)
│   └── parser/
│       ├── mod.rs          # Interfata comuna pentru parseri
│       ├── gaia.rs         # Parser Checkpoint Gaia
│       ├── cef.rs          # Parser CEF / ArcSight
│       └── fortigate.rs    # Parser Fortinet FortiGate
└── tester/
    ├── tester.py           # Simulator trafic pentru testare
    └── sample_*.log        # Log-uri de test pre-generate
```

---

6. OBIECTIVE DE IMPLEMENTARE

Implementarea se desfasoara in **8 obiective**:

OBIECTIVUL 1 — Motor de detectie scanari

> *Livram: detectie automata Fast Scan + Slow Scan cu praguri configurabile*

Sistemul primeste log-urile de la firewall si identifica in timp real statiile care scaneaza reteaua interna — atat scanari agresive (secunde), cat si discrete (minute).

OBIECTIVUL 2 — Integrare cu platforma SIEM

> *Livram: alerte automate in ArcSight, corelabile cu alte evenimente*

Alertele ajung in SIEM in format standard CEF, cu IP sursa, IP tinta, lista porturilor si severitate. Protejate impotriva manipularii prin sanitizare anti-injection.

OBIECTIVUL 3 — Notificari email cu comenzi de reactie

> *Livram: email structurat cu detalii + comenzi copy-paste pentru investigare*

Echipa primeste email-uri clare cu tot ce trebuie sa stie si sa faca: IP-ul sursa, ce a scanat, si comenzi gata de executat pentru verificare log-uri, conexiuni active si blocare temporara.

OBIECTIVUL 4 — Suport multi-vendor firewall

> *Livram: compatibilitate cu Checkpoint Gaia, CEF (standard) si Fortinet FortiGate*

Sistemul intelege log-urile de la trei tipuri majore de firewall. Arhitectura modulara permite adaugarea altor producatori in viitor fara a modifica restul sistemului.

OBIECTIVUL 5 — Detectie avansata si auto-protectie

> *Livram: detectie Accept Scan + rate limiting + gestionare inteligenta memorie*

Detectia este extinsa cu identificarea porturilor care raspund (Accept Scan). Sistemul se protejeaza singur impotriva supraincarcarii si gestioneaza memoria automat, fara interventie.

OBIECTIVUL 6 — Securizare si protectie anti-abuz

> *Livram: sanitizare anti-injection CEF, rate limiting UDP, limite memorie per IP*

Sistemul se protejeaza singur: sanitizarea datelor previne manipularea alertelor din SIEM, rate limiting-ul protejeaza procesarea impotriva flood-ului de log-uri, iar memoria este limitata per IP cu evictie automata a datelor vechi — fara risc de suprasaturare.

OBIECTIVUL 7 — Validare configuratie si testare

> *Livram: validare automata cu 16+ reguli, suite de teste unitare, tester de simulare*

Configuratia este verificata automat la pornire — toate erorile sunt raportate dintr-o singura rulare. Proiectul include teste unitare pentru fiecare componenta si un tester Python care simuleaza trafic de scanare pentru verificarea detectiei in conditii controlate.

OBIECTIVUL 8 — Operare autonoma si monitorizare live

> *Livram: dashboard live, hot reload configuratie, mentenanta automata*

Sistemul ruleaza 24/7 fara interventie: curatare automata a datelor expirate, reincarcarea configuratiei fara oprire, statistici in timp real si validare automata a configuratiei la pornire.

---

7. SUMAR

```
FARA IDS-RS                          CU IDS-RS
==================                   ==================

O statie interna scaneaza            O statie interna scaneaza
reteaua                              reteaua
     |                                    |
     v                                    v
Firewall-ul blocheaza                Firewall-ul blocheaza
(log pierdut in mii                  IDS-RS vede tiparul
 de alte log-uri)                    in SECUNDE
     |                                    |
     v                                    v
Nimeni nu observa                    Alerta instantanee:
ore / zile / niciodata               Email + SIEM
     |                                    |
     v                                    v
Statia compromisa                    Echipa izoleaza statia
continua sa opereze                  in MINUTE
     |                                    |
     v                                    v
MISCARE LATERALA                     INCIDENT NEUTRALIZAT
NEDETECTATA                          INAINTE DE ESCALADARE
```

IDS-RS ne da controlul asupra a ceea ce se intampla in reteaua noastra. Nu inlocuieste firewall-ul — il face vizibil.

---

8. CERERE DE AVIZARE

Solicitam aprobarea pentru implementarea sistemului IDS-RS in infrastructura interna, conform celor 8 obiective prezentate.

Ce livram: - Sistem complet functional, testat si documentat - Fara costuri de licenta — solutie dezvoltata intern - Implementare graduala, fara impact asupra serviciilor existente - Compatibilitate cu infrastructura actuala de firewall si SIEM

Ce avem nevoie: - Acces la log-urile firewall-ului intern prin port UDP dedicat - Un server (fizic sau virtual) pentru rularea IDS-RS - Coordonare cu echipa de retea pentru configurarea initiala