Security Information and Event Management System

Proiect TPI

UNSTB

ETTI

2024– 2025

III RST

Andronie Vasile Laurentiu

Maravela Viorel

Anul

1.Introducere

Security Information and Event Management (prescurtat SIEM), reprezinta un sistem de aparare a companiilor impotriva atacurilor cibernetice.

Un astfel de manager combina functionalitatea de gestiune a informatiilor de securitate precum si a evenimentelor, oferind astfel capacitatea companii sa se apere atat in mod reactiv cat si proactiv.

Printre altele un SIEM ofera transparenta traficului prin retea, alerteaza asupra posibilelor amenintari, raspunde in mod activ la evenimente suspicioase sau malitioase.

2. Analiza Pietei

Cel mai cunoscut si utilizat SIEM este SPLUNK, care apartine de Cisco.

Printre altele Splunk ofera:

- Analiza si vizualizarea datelor de tip log
- Functionalitati avansate de cautare, alertate si creare de dashboarduri
- Monitorizare de performanta, securitate si conformitate

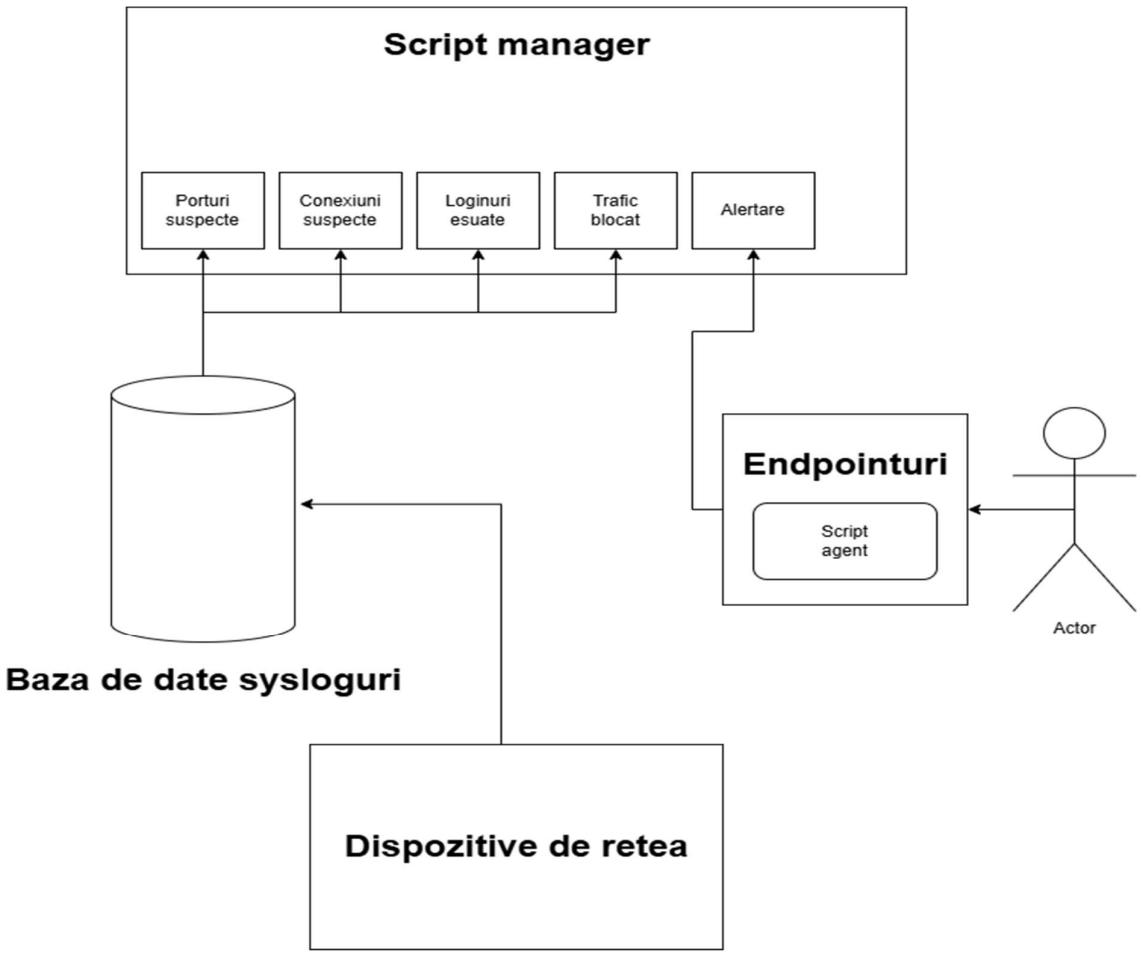
O alta unealta disponibila de piata este Wazuh, care este mai orientat pe dispositive endpoint.

Acesta ofera:

- Detectie de amenintari si monitorizare integritate fisiere
- Management al vulnerabilitatilor si raspuns la incidente
- Capacitate de functionare impreuna cu alte platforme

3.Proiectare

Schema bloc (prototip)



1. **Script manager**

Este un script care va rula pe un server. Va indeplini majoritatea functionalitatilor ale SIEM-ului de alertare si/sau prevenire a amenintarilor precum, inchidere de porturi, alertate de conexiuni suspecte, alertare si/sau blocare incercari de brute-force, alertare si/sau prevenire port scan.

2. **Script agent**

Este un script care va rula pe dispozitive de tip endpoint. Acesta va trimite alerte scriptului manager care va anunta utilizatorii retele de posibile amenintari. In general, dar nu limitat la, va indeplini 3 functii:

verificare loginuri esuate local, verificare loginuri remote, verificare posibila infectie malware. Acest script va avea si capacitatea proactiva de a termina (kill) procesele suspecte. Este compatibil cu Linux (Debian) si Windows.

3. **Baza de date sysloguri**

Dispozitivele de retea pot trimite evenimente ce se petrec la nivelul lor

prin protocolul syslog. Baza de date va pastra aceste jurnale de loguri astfel incat managerul sa le poata prelucra riguros, analizand si evenimente anterioare pentru corelatie intre aceste loguri si o mai buna luare de decizie.