SIEM – Security Information and Event Management sustavi

Branko Mažar
Služba za sigurnost usluga
CARNet

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sadržaj

- Uvod ili što je SIEM?
- Analiza log zapisa
- Osnove rada SIEM sustava
- Arhitektura SIEM sustava
- Dimenzioniranje SIEM sustava
- SIEM sustavi na tržištu

Uvod

- SIEM – sustavi za upravljanje sigurnosnim događajima na temelju prikupljanja, analize i prikaza informacija prisutnih u log zapisima
- SIEM = SIM + SEM
- SIM – Security Information Management
  - Analiza log zapisa u stvarnom vremenu
- SEM – Security Event Management
  - Pohrana i forenzička analiza log zapisa

Analiza log zapisa

- Aplikacije, računalna i mrežna oprema generiraju velike količine log zapisa
- Log zapisi sadrže informacije o radu sustava, greškama, korisničkim aktivnostima
- Velike količina informacija u log zapisima zahtijeva automatiziranu analizu
- Analiza u stvarnom vremenu -> pravovremena detekcija anomalija u radu informacijskog sustava

Osnove rada SIEM sustava

- Analiza log zapisa primjenom regularnih izraza
- Agregacija – prikupljanje i grupiranje
- Korelacija – analiza u stvarnom vremenu
- Praćenje i obavještavanje u stvarnom vremenu
- Prikaz rezultata analize log zapisa
- Pohrana log zapisa i forenzička analiza

Regularni izrazi

- Regularni izrazi su temelj rada SIEM sustava
- Primjenom regularnih izraza detektiraju se specifični uzorci u log zapisima
  - Predefinirani regularni izrazi – detekcija poznatih sigurnosnih anomalija
  - Lokalno definirani regularni izrazi – detekcija sigurnosnih anomalija specifičnih za pojedine aplikacije i uređaje

Agregacija i korelacija

- Agregacija – prikupljanje i grupiranje log zapisa
  - Logovi operacijskog sustava, web poslužitelja, baze podataka, vatrozida, IDS-a, mrežne opreme …
- Korelacija – praćenje i analiza log zapisa
  - Analiza pojedine skupine log zapisa
  - Analiza i međusobna usporedba različitih skupina log zapisa
  - Detekcija i prioritetiziranje anomalija

Agregacija i korelacija – Primjer 1

Više neuspješnih pokušaja autentikacije na servis SSH – prioritet 5:

```
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
```

Agregacija i korelacija – Primjer 2

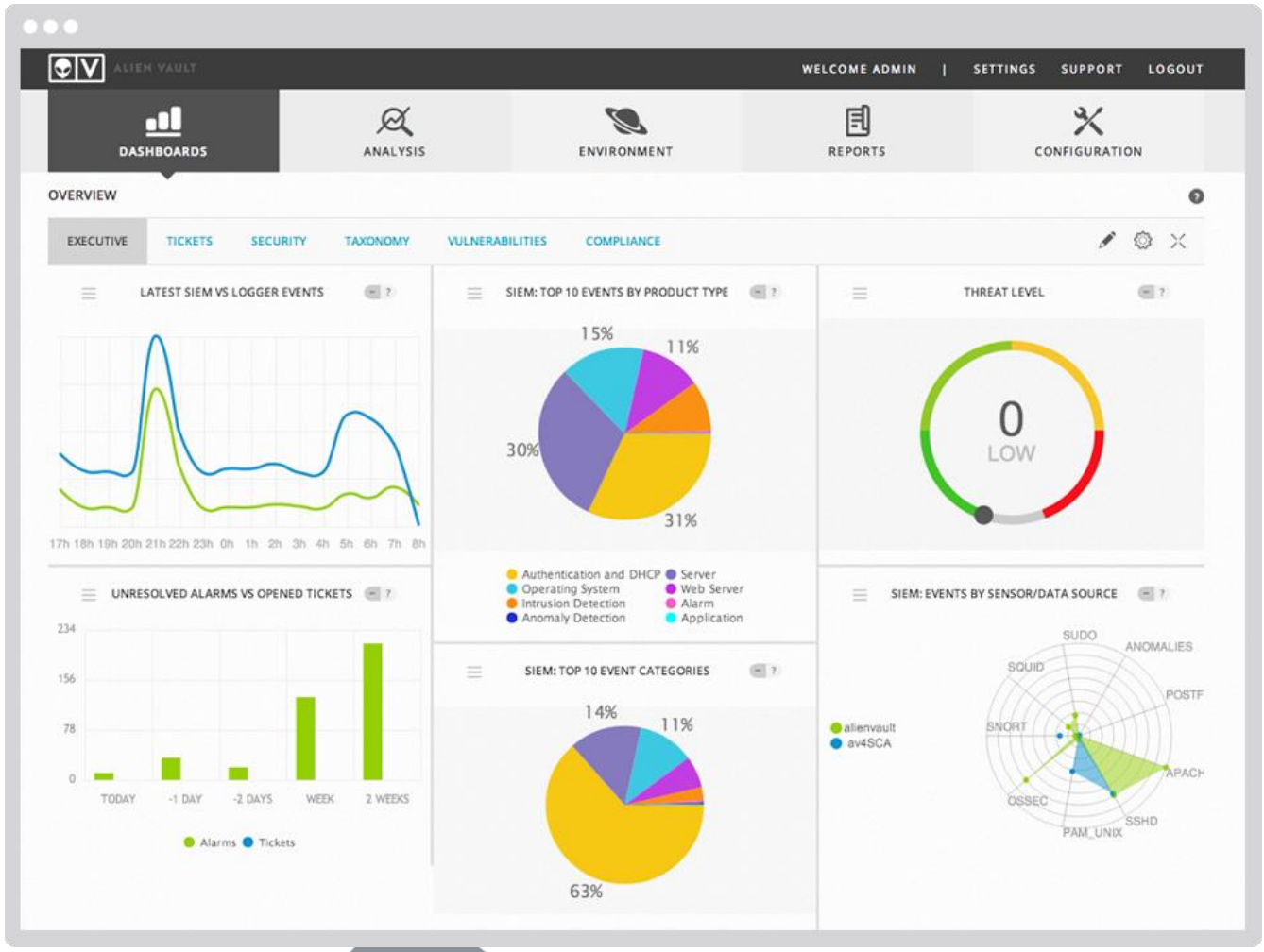
Uspješna autentikacija na servis SSH nakon više neuspješnih pokušaja spajanja – prioritet 10:

```
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Failed password for root from 192.168.5.2 ssh2
Nov 10 22:13:12 server sshd: Connection from 192.168.5.5
Nov 10 22:13:12 server sshd: Accepted password for root from 192.168.5.2 ssh2
```

Praćenje, obavještavanje i prikaz rezultata

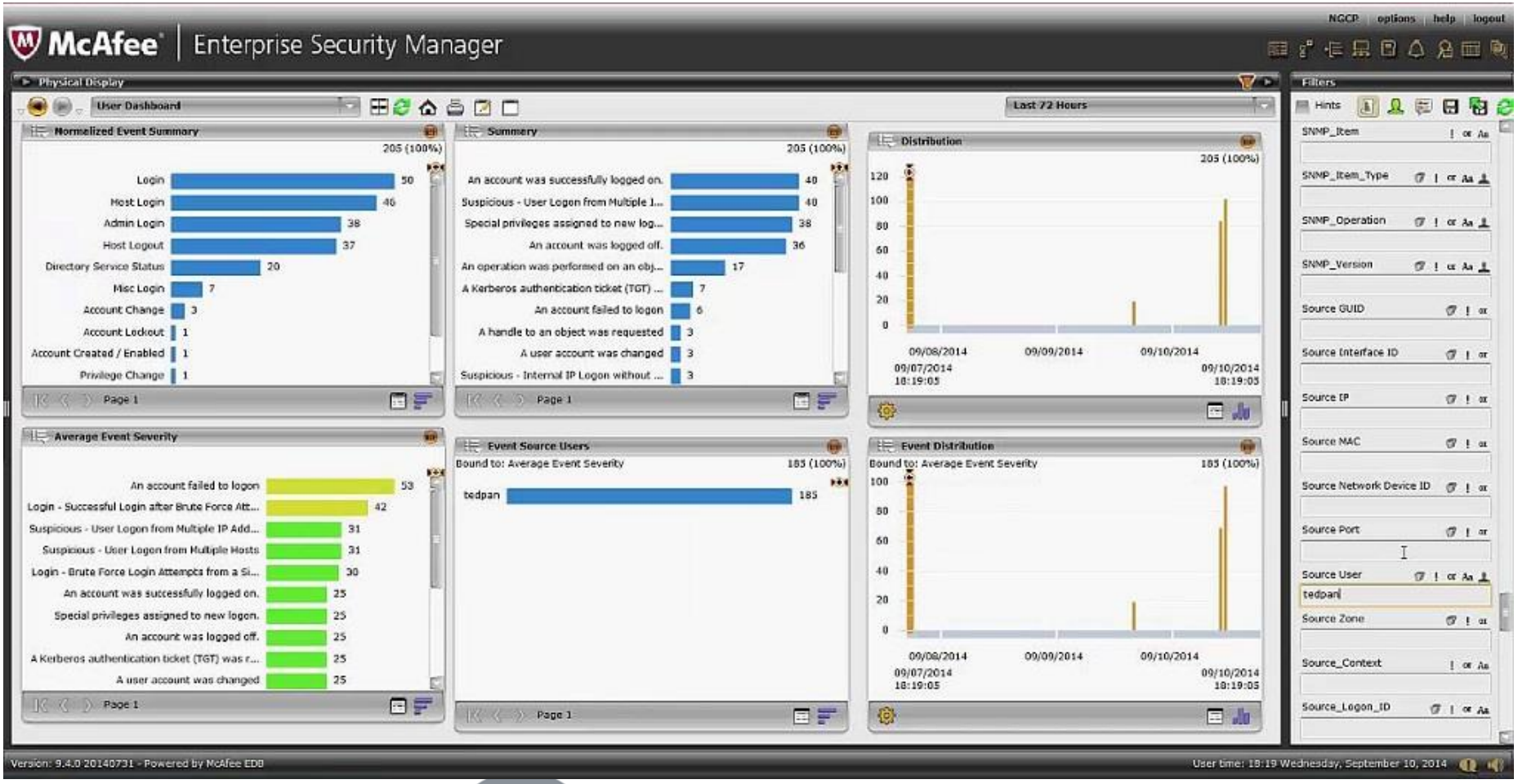
- Agregacija i korelacija se izvršavaju kontinuirano
  - Novi log zapisi se analiziraju trenutno
- Obavještavanje administratora u stvarnom vremenu:
  - Najčešće putem e-maila i SMS poruka
- Pregledan prikaz rezultata agregacije i korelacije:
  - Web sučelje

Prikaz rezultata – AlienVault SIEM



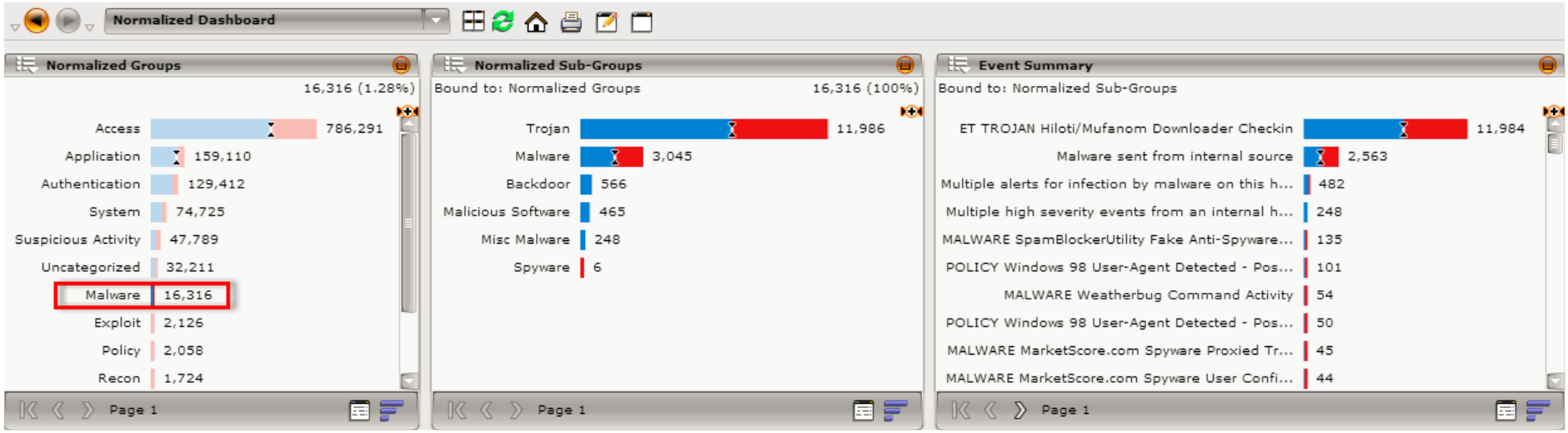
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Prikaz rezultata – McAfee ESM



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Prikaz rezultata – detekcija malicioznog koda



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Pohrana log zapisa i forenzička analiza

- Agregirani podaci se pohranjuju u baze podataka
  - Vanjske baze podataka (MySQL, PostgreSQL, MSSQL …)
  - „Proprietary” baze podataka – optimizirane za brzu analizu velike količine podataka
- Ugrađeni mehanizmi za povijesni pregled i analizu zapisa
- Izrada izvještaja

Arhitektura SIEM sustava

- SIEM sustavi se najčešće temelje na klijent-poslužitelj arhitekturi
- Poslužiteljski dio
  - Agregacija, korelacija, praćenje, obavještavanje, pohrana, forenzička analiza, izrada izvještaja
- Klijentski dio
  - Prikupljanje log zapisa i njihovo prosljeđivanje na poslužitelj
  - Syslog ili putem vlastitih protokola

Dimenzioniranje SIEM sustava

- Količina log zapisa se mjeri kao EPS – Events per Second
- Softverski SIEM sustavi
  - Količina log zapisa manja od 1000 EPS
- Hardverski SIEM sustavi
  - Količina log zapisa veća od 1000 EPS
  - Distribuirana arhitektura za sustave s više od 10 000 EPS

SIEM sustavi na tržištu

- Open source sustavi
  - AlienVault OSSIM
  - OSSEC
- Komercijalni sustavi
  - Splunk
  - HP ArcSight
  - McAfee ESM
  - IBM Security QRadar
  - AlienVault USSIM
  - …

Hvala na pažnji!

Branko Mažar

Branko.Mazar@CARNet.hr

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK