SCUOLA NORMALE SUPERIORE

Cybersecurity e Universita'

Federico Calzolari
Chief Information Security Officer
Scuola Normale Superiore

#OSW2021

RETE ITALIANA OPEN SOURCE

UNIVERSITA' E [IN]SICUREZZA

RIOS RETE ITALIANA OPEN SOURCE

USE CASE "TIPICO"

Device noti, ma soprattutto ignoti

- 100K device differenti / anno collegati alla rete di ateneo
- device controllati: pc del personale amministrativo, server centrali (~500)

=> il rapporto tra i due numeri: 5 per MILLE

Obblighi di compliance normativa per il comparto IT:

- GDPR
- Misure minime di sicurezza ICT per PA

Tra questi obblighi:

- controllo di postura di tutti i device collegati (AntiVirus, IDS, IPS on board)
- white list di tutte le app consentite (Google + Apple Store: 5M)

COSA GIRA NELLA TUA RETE

RIOS RETE ITALIANA OPEN SOURCE

A QUESTO PUNTO...
tanto vale sapere cosa gira nella tua rete.

Problema tipico di una Universita':

- elevatissima biodiversita': da studenti che vivono nei collegi a ricercatori nelle piu' diverse aree e discipline
- sistemi behavioral analysis based incapaci di adeguarsi a tale biodiversita': troppi falsi positivi

Soluzione: LogOs

- monitoraggio e raccolta log da varie fonti (server critici)
- inventario dei dispositivi connessi alla rete
- analisi real time
- sistema: ElasticSearch (DB + Search Engine), Kibana (Dashboard), Wazuh (threat detection, integrity monitoring, incident response and compliance)

ANALISI DATI E SVILUPPI FUTURI

RETE ITALIANA OPEN SOURCE

A COSA POSSONO SERVIRE I DATI RACCOLTI?

Attraverso i log raccolti e' possibile effettuare analisi su diversi target e su diverse scale temporali:

- andamenti macroscopici nel tempo (es: volume degli attacchi ricevuti)
- particolarità di singoli eventi (es: ricostruzione di un singolo attacco e del suo intorno)

SVILUPPI FUTURI

Realizzazione di un IDS Intrusion Detection System:

- deep packet inspection
- dashboard real time su potenziali anomalie o attacchi in corso

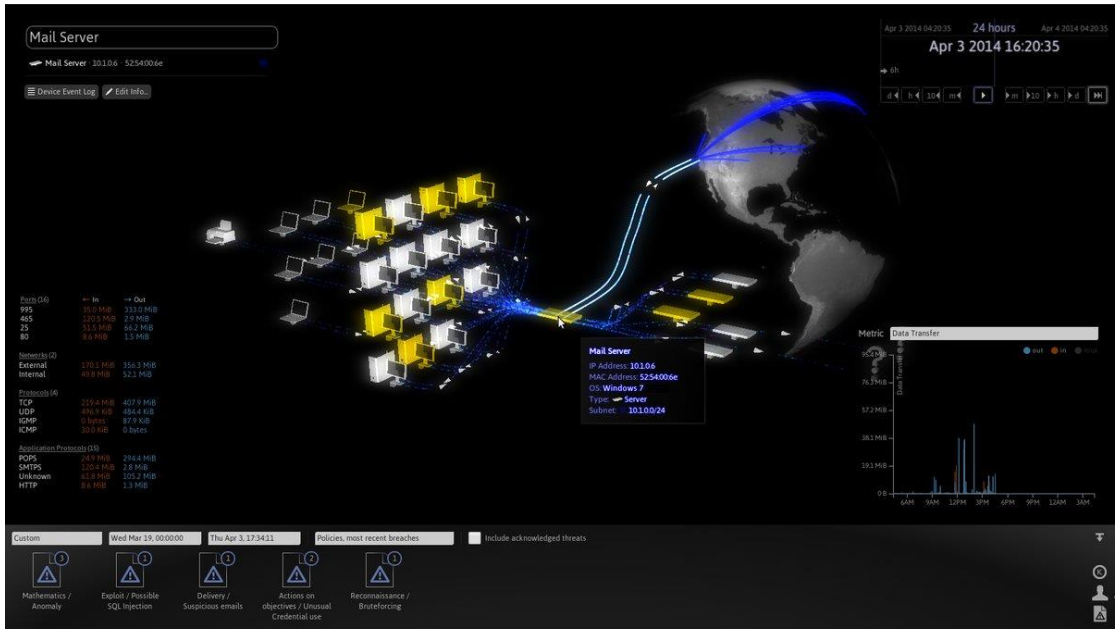
OSW2021 OPENSOURCEWEEK

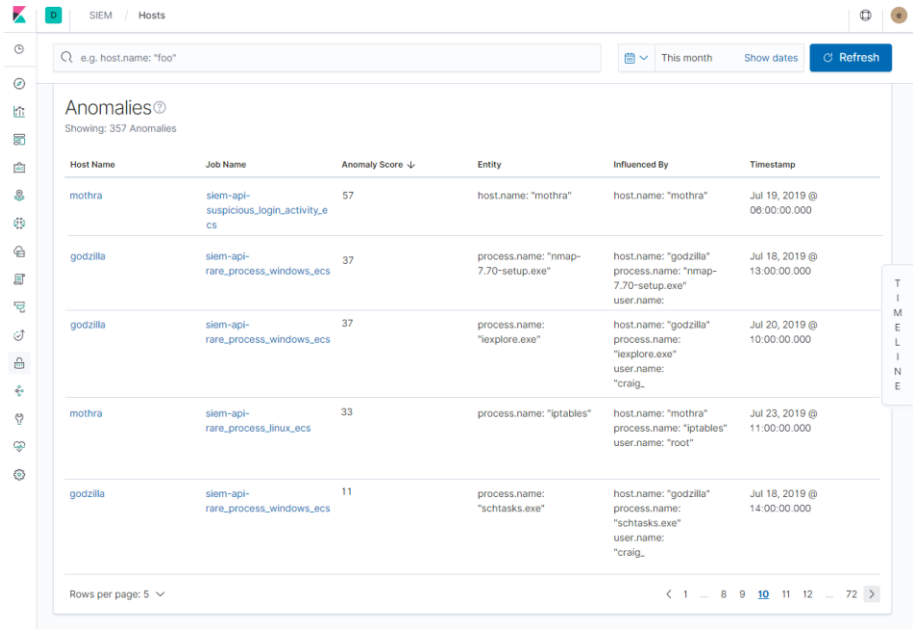
SEMPLIFICAZIONE

RETE ITALIANA OPEN SOURCE

IL PROBLEMA DELLE DASHBOARD

Esistono strumenti “fighissimi” ma altrettanto cari che propongono delle dashboard fantascientifiche, per la comprensione delle quali occorre pero’ un intero corso di laurea dedicato.





OSW2021 OPENSOURCEWEEK

SEMPLIFICAZIONE bis

IL MIO SOGNO?

Una dashboard “iper”semplificata:

- luce verde: puoi andare a letto tranquillo
- luce rossa: a dormire ci si pensera' un'altra volta

Motivazioni:

- scarsita’ di tempo/personale da dedicare all’analisi dei dati relativi alla sicurezza informatica

Perche’ un sistema open ElasticSearch based?

- modularita' ed elasticita' del sistema
- possibilita’ di realizzare dashboard ben calibrate per le esigenze del singolo utente

Federico Calzolari
SCUOLA NORMALE SUPERIORE