SIEM VENDOR SELECTION 101

HackInBo Business Edition

Bologna, venerdì 27 maggio 2022

axitea
SECURITY EVOLUTION

WHOAMI

- Computer Science @Politecnico di Milano
- Mi occupo di automatizzare e migliorare i processi del SOC oltre che di supporto nella risposta agli incidenti.
- Responsabile servizi gestiti @SOC Axitea

murd00ck

axitea
SECURITY EVOLUTION

CONTESTO

- *“A modern SIEM should be viewed as a central nervous system, capturing data and generating information that security teams can use as intelligence to detect potentially malicious activity before any damage is realized, providing a safety net that can catch potential threats that might slip through traditional defenses.”*

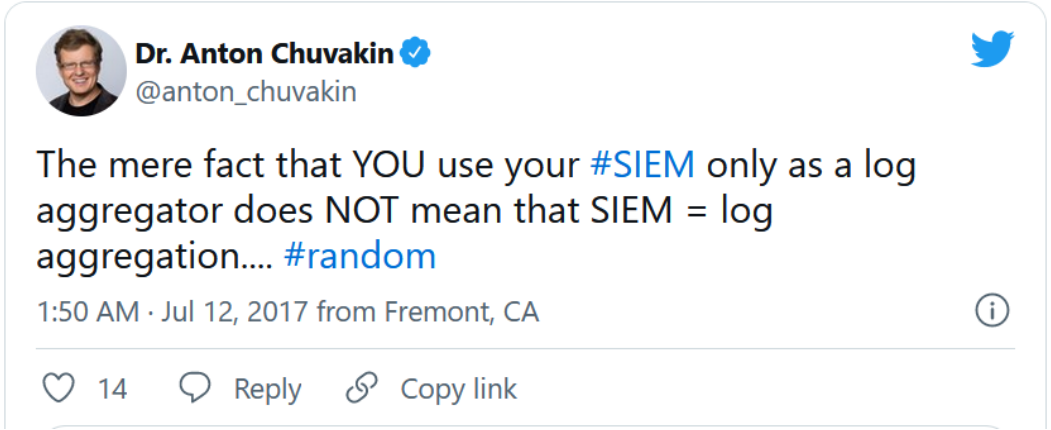
- L'importanza di una soluzione SIEM per le aziende di oggi è amplificata dalla crescente complessità degli attacchi e dall'uso di servizi cloud che non fanno altro che aumentare la superficie della vulnerabilità.

- L'83% dei team di sicurezza coinvolti indica che il proprio team non riesce a rispettare la regola 1-10-60 a causa dell'elevato volume di eventi.*

**Fonte: Cloud SIEM Buyers Guide*

Driver strategici

- Qual è il livello di organizzazione del tuo team se oggi dovesse accadere una compromissione interna?
- Hai skill interne per scrivere log query, investigare allarmi, fare attività di incident response e tuning del SIEM?
- Hai processi scalabili e testati per il rilevamento di minacce e l'investigazione?
- Che cosa mi aspetto di ottenere integrando un SIEM nell'infrastruttura?

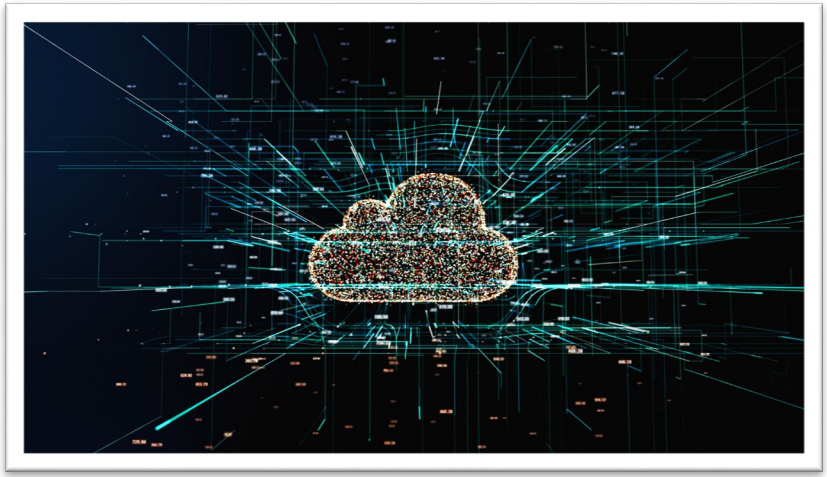


Driver di scelta

Per valutare una tecnologia SIEM abbiamo delineato 4 macro categorie di analisi

Storage / Data aggregation

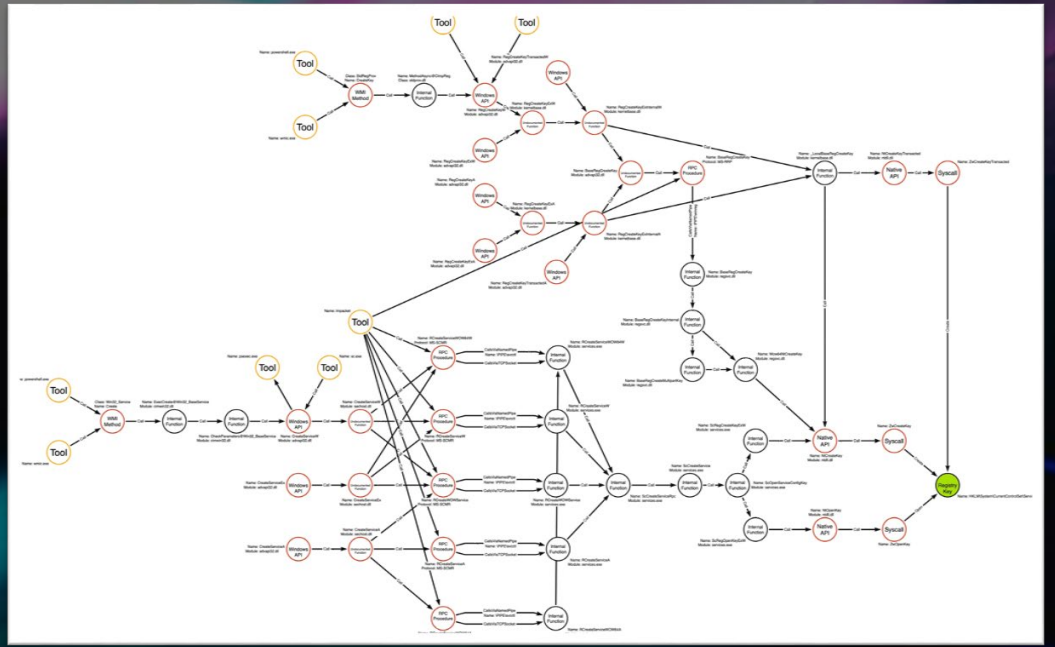
- Dove vengono archiviati I log? Viene prevista la compressione dei dati e la criptazione?
- Il SIEM utilizza un ambiente Cloud o On Premise?
- Posso personalizzare la log retention dei dati acquisiti nel SIEM?
- Sorgenti log supportate
- Metodo per acquisire il dato semplice e scalabile
- Un SIEM deve riuscire a dividere i silos delle diverse nomenclature di log riuscendo a **normalizzare** e **correlare** diverse fonti.



There is no cloud
it's just someone else's computer

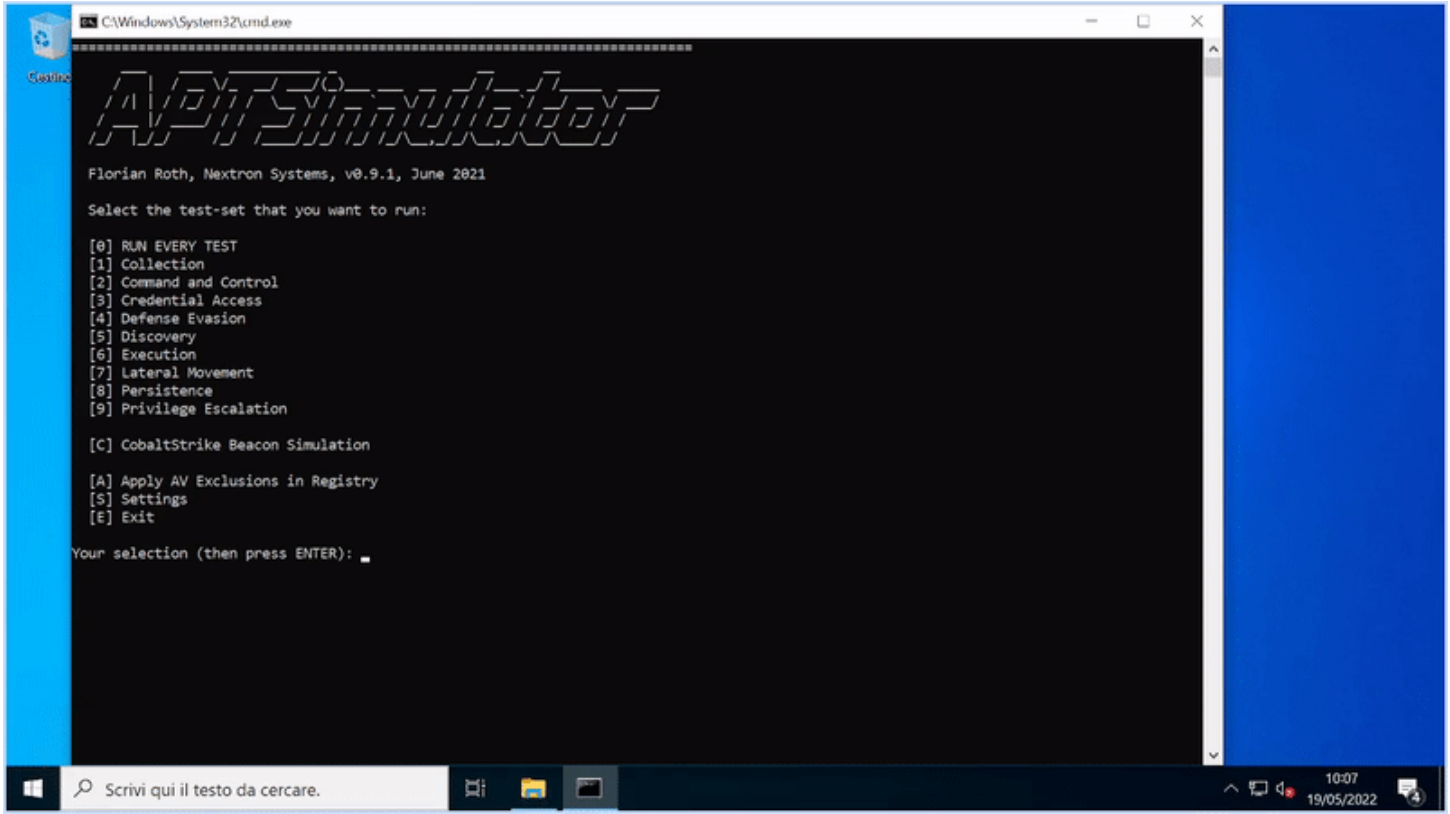
Real-time Monitoring and Alerting

- Automatizzare il triage degli allarmi generati
- Anomaly detection
- Regole di correlazione aggiornate dal Vendor
- Facilità nella creazione di nuovi casi d'uso
- APT Simulator



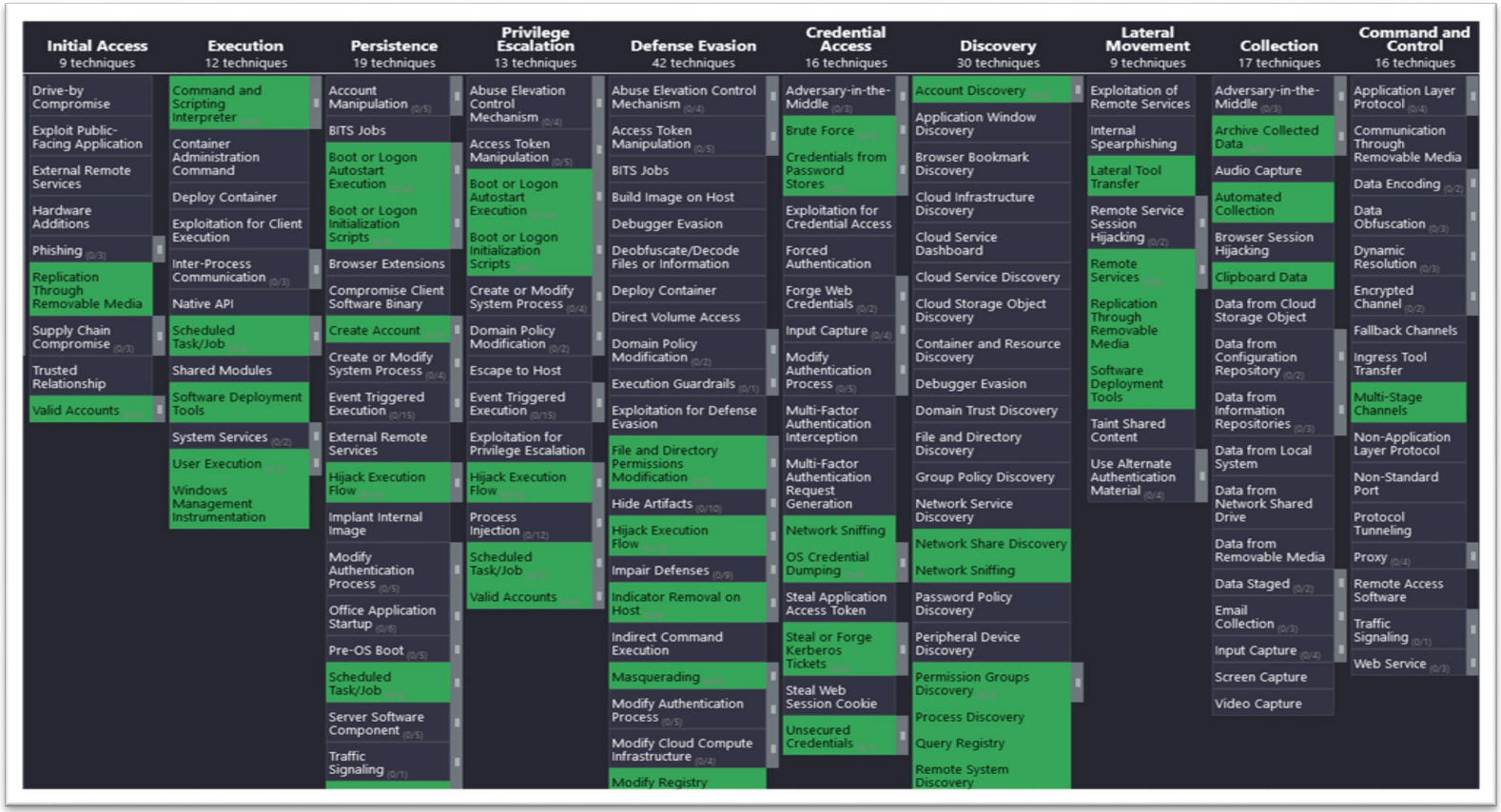
Fonte: Jared Atkinson

APT SIMULATOR EXTENDED



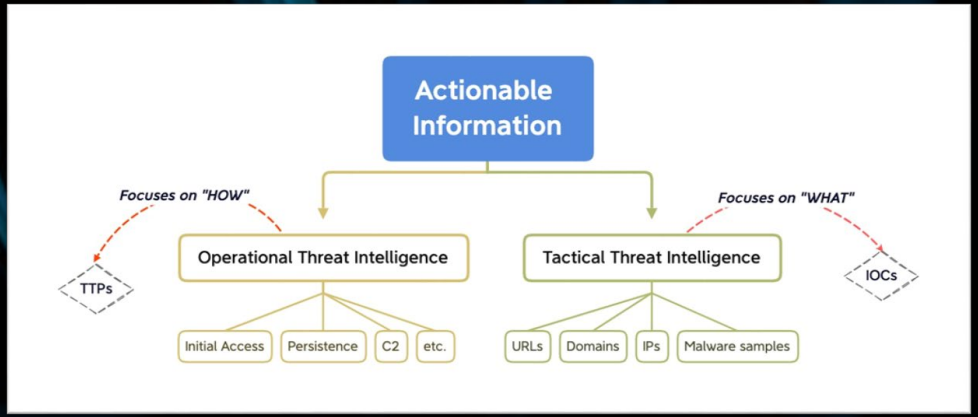
https://github.com/murd00ck/APTSimulatorExtended

APT SIMULATOR EXTENDED



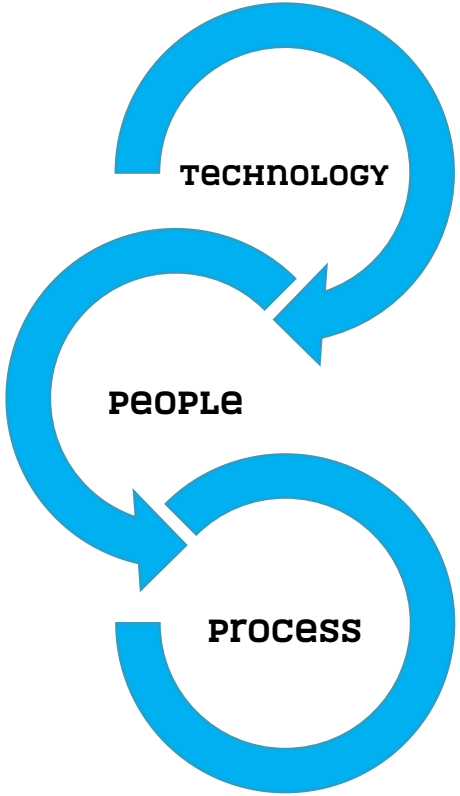
Threat Intelligence

- Supporto per l'acquisizione di feed di IOCs
- Enrichment degli allarmi attraverso il contesto fornito dalla Threat Intelligence
- Tipologie di TI:
  1. servizi di intelligence sulle minacce che forniscono informazioni aggiornate su tattiche, tecniche e procedure di attacco, oltre a un contesto aggiuntivo per vari tipi di incidenti e attività.
  2. criticità degli asset, l'utilizzo, la connettività, la proprietà e, infine, il ruolo, la responsabilità dell'utente.



PPT IMPACT

- Processi scalabili per aggiungere nuove sorgenti log
- Processo di condivisione dei requisiti di logging con team di sviluppo interni
- Risorsa da dedicare per deployment, tuning della piattaforma, ricerca dei log e aggiornamento casi d'uso



grazie

Axitea S.p.A
Via Gallarate 156
20151 Milano (MI)
Tel +39 02 3003131
www.axitea.com

https://github.com/murd00ck/edr101

https://github.com/murd00ck/siem101

axitea
SECURITY EVOLUTION