

SIEM vendor selection 101

HackInBo Business Edition

Bologna, venerdì 27 maggio 2022

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

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?



Dr. Anton Chuvakin ✓
@anton_chuvakin



The mere fact that YOU use your [#SIEM](#) only as a log aggregator does NOT mean that SIEM = log aggregation.... [#random](#)

1:50 AM · Jul 12, 2017 from Fremont, CA



14



Reply



Copy link

DRIVER DI SCELTA

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



STORAGE / Data aggregation

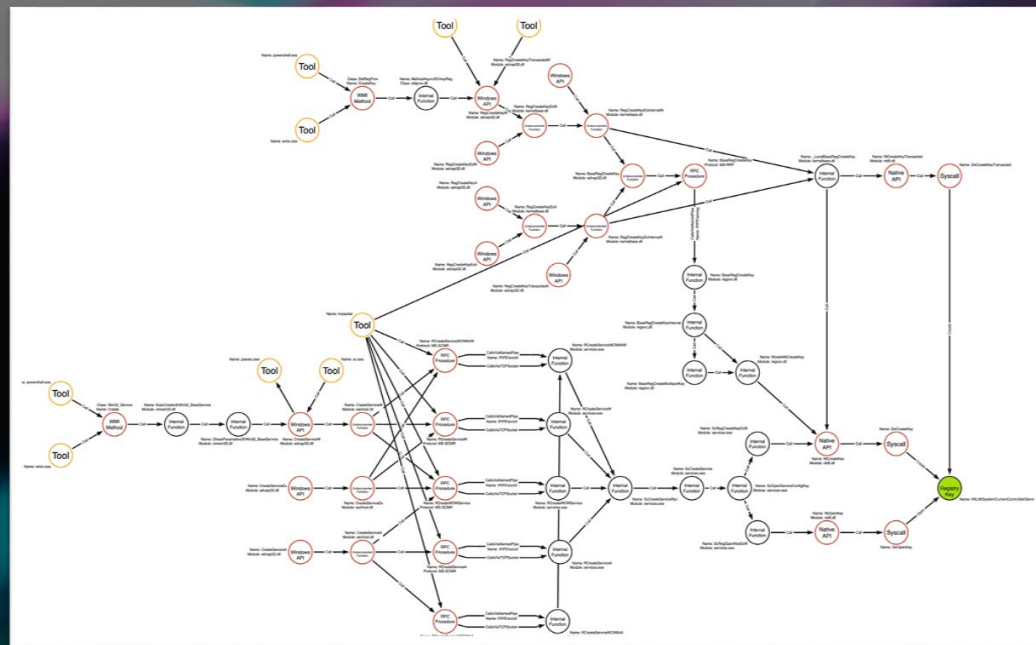
- Dove vengono archiviati I log? Viene prevista la compressione dei dati e la criptazione?
- Il SIEM utilizza un ambiente Cloud o On Premise?
- Posso personalizzare la log retention dei dati acquisiti nel SIEM?
- Sorgenti log supportate
- Metodo per acquisire il dato semplice e scalabile
- Un SIEM deve 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*

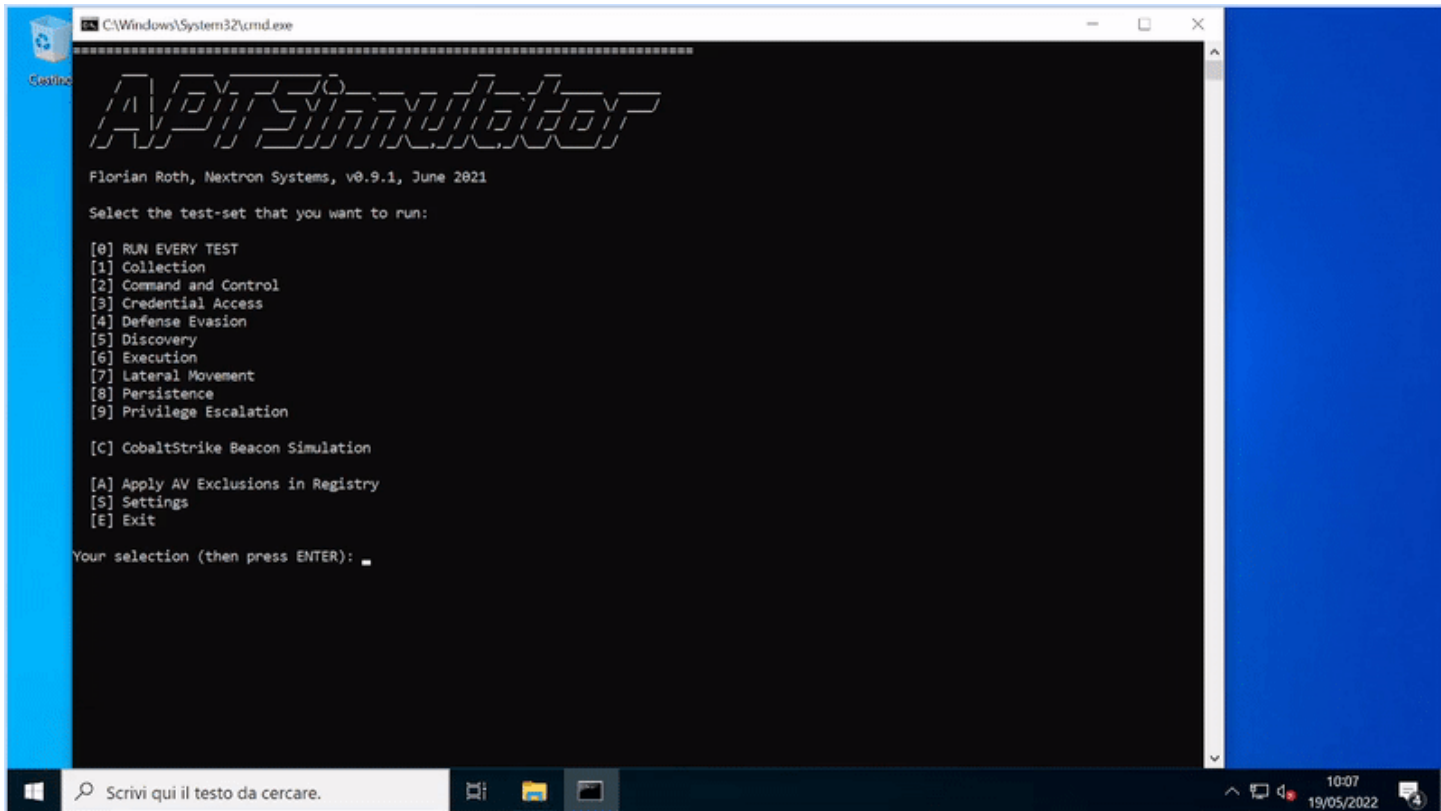
real-TIME MONITORING and alerting

- 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

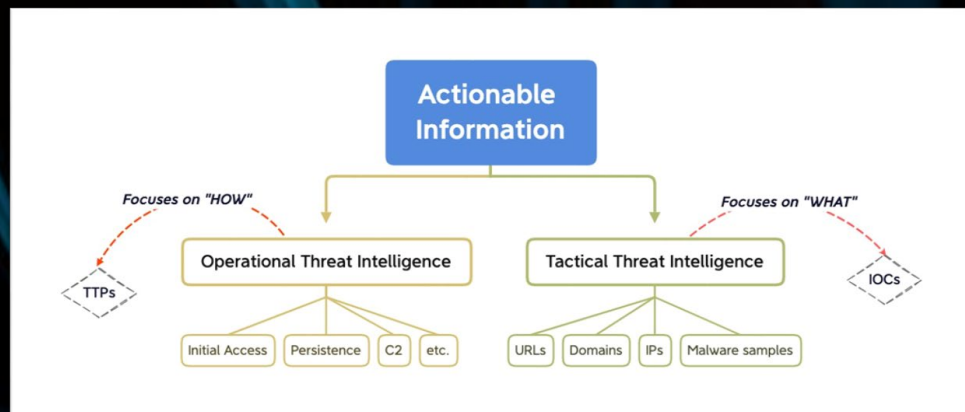


APT SIMULATOR extended

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)
Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/4)	Communication Through Removable Media
External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/4)	Boot or Logon Autostart Execution (0/4)	Build Image on Host	Credentials from Password Stores (0/4)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts (0/4)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)
Phishing (0/2)	Inter-Process Communication (0/3)	Browser Extensions	Browser Extensions (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/4)	Browser Session Hijacking	Dynamic Resolution (0/3)
Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)
Supply Chain Compromise (0/2)	Scheduled Task/Job	Create Account	Domain Policy Modification (0/2)	Direct Volume Access	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels
Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Escape to Host	Domain Policy Modification (0/2)	Modify Authentication Process (0/5)	Container and Resource Discovery	Use Alternate Authentication Material (0/4)	Data from Configuration Repository (0/2)	Ingress Tool Transfer
Valid Accounts	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Debugger Evasion	Taint Shared Content	Data from Information Repositories (0/3)	Multi-Stage Channels
	System Services (0/2)	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Use Alternate Authentication Material (0/4)	Data from Local System	Non-Application Layer Protocol
	User Execution (0/4)	Hijack Execution Flow (0/4)	Hijack Execution Flow (0/4)	File and Directory Permissions Modification (0/4)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port
	Windows Management Instrumentation	Implant Internal Image	Process Injection (0/12)	Hide Artifacts (0/10)	OS Credential Dumping	Group Policy Discovery		Data from Network Shared Drive	Protocol Tunneling
		Modify Authentication Process (0/5)	Scheduled Task/Job (0/4)	Hijack Execution Flow (0/4)	Steal Application Access Token	Network Service Discovery		Data from Removable Media	Proxy (0/4)
		Office Application Startup (0/5)	Valid Accounts (0/4)	Impair Defenses (0/9)	Steal or Forge Kerberos Tickets	Network Share Discovery		Data Staged (0/2)	Remote Access Software
		Pre-OS Boot (0/5)		Indicator Removal on Host (0/4)	Steal Web Session Cookie	Network Sniffing		Email Collection (0/3)	Traffic Signaling (0/1)
		Scheduled Task/Job (0/4)		Indirect Command Execution	Unsecured Credentials (0/4)	OS Credential Dumping		Input Capture (0/4)	Web Service (0/3)
		Server Software Component (0/5)		Masquerading		Steal Application Access Token		Screen Capture	
		Traffic Signaling (0/1)		Modify Authentication Process (0/5)		Permission Groups Discovery		Video Capture	
				Modify Cloud Compute Infrastructure (0/4)		Process Discovery			
				Modify Registry		Query Registry			
						Remote System Discovery			

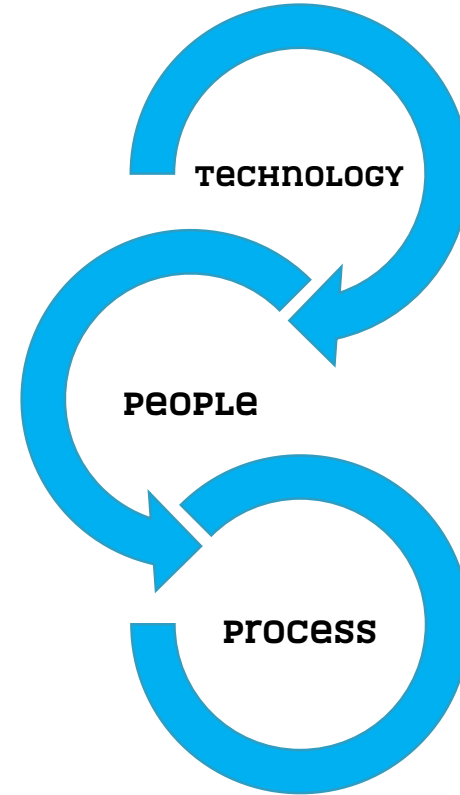
THreat INTELLIGENCE

- 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