EDR 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

CONTESTO

All’anno 2020 le tecnologie EDR sono state adottate da 1/3 dei team di sicurezza

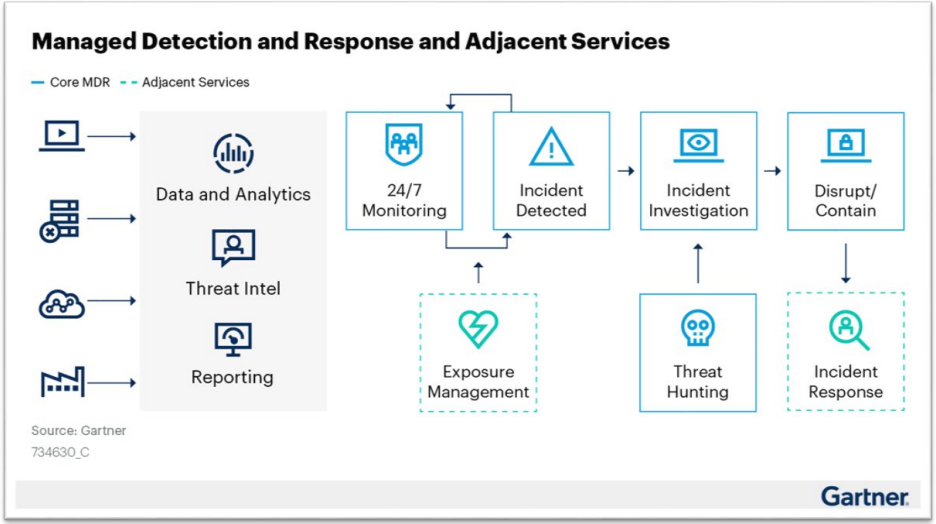
+35%

Nei prossimi 5 anni si prevede un raddoppio del numero di organizzazioni che utilizzeranno soluzioni EDR.

X2

Ruolo di un Managed Service Provider

- Alarm management 24/7 con funzione di triage, investigazione e risposta agli incidenti.
- Incident Management
- Ottimizza investimenti e scelte tecnologiche del Cliente
- Accesso immediato a risorse per esigenze di Threat Hunting
- Capacità di ricostruzione della Kill Chain Attack

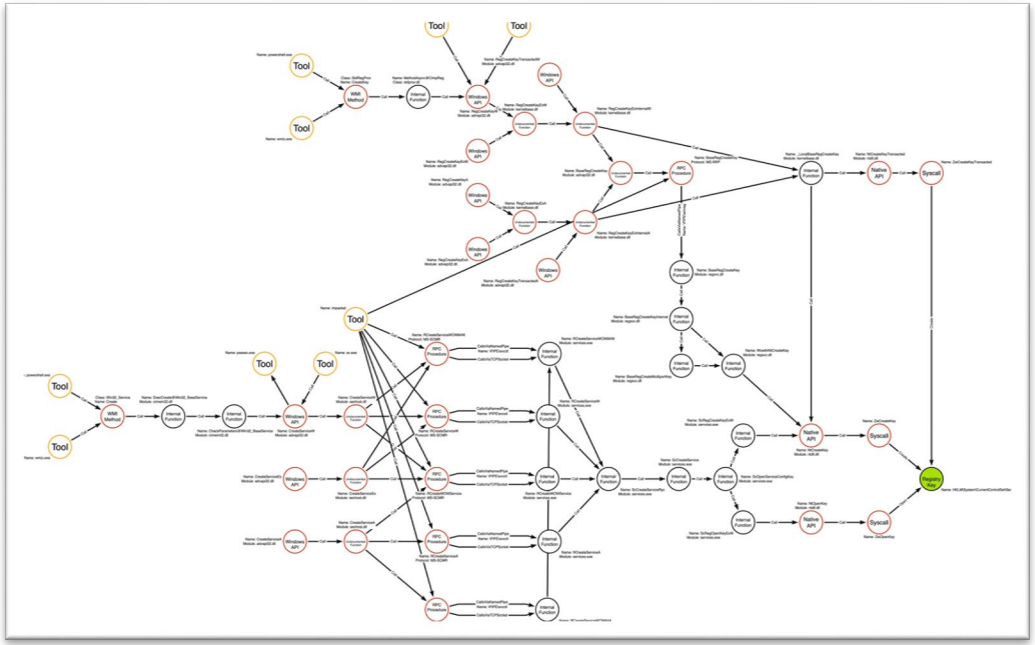


Driver di scelta

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

Prevention

- Prevenzione di malware conosciuti e di tipo zero-day
- Ransomware prevention
- Prevenzione di attacchi file-less
- Asset Management / Vulnerability Management

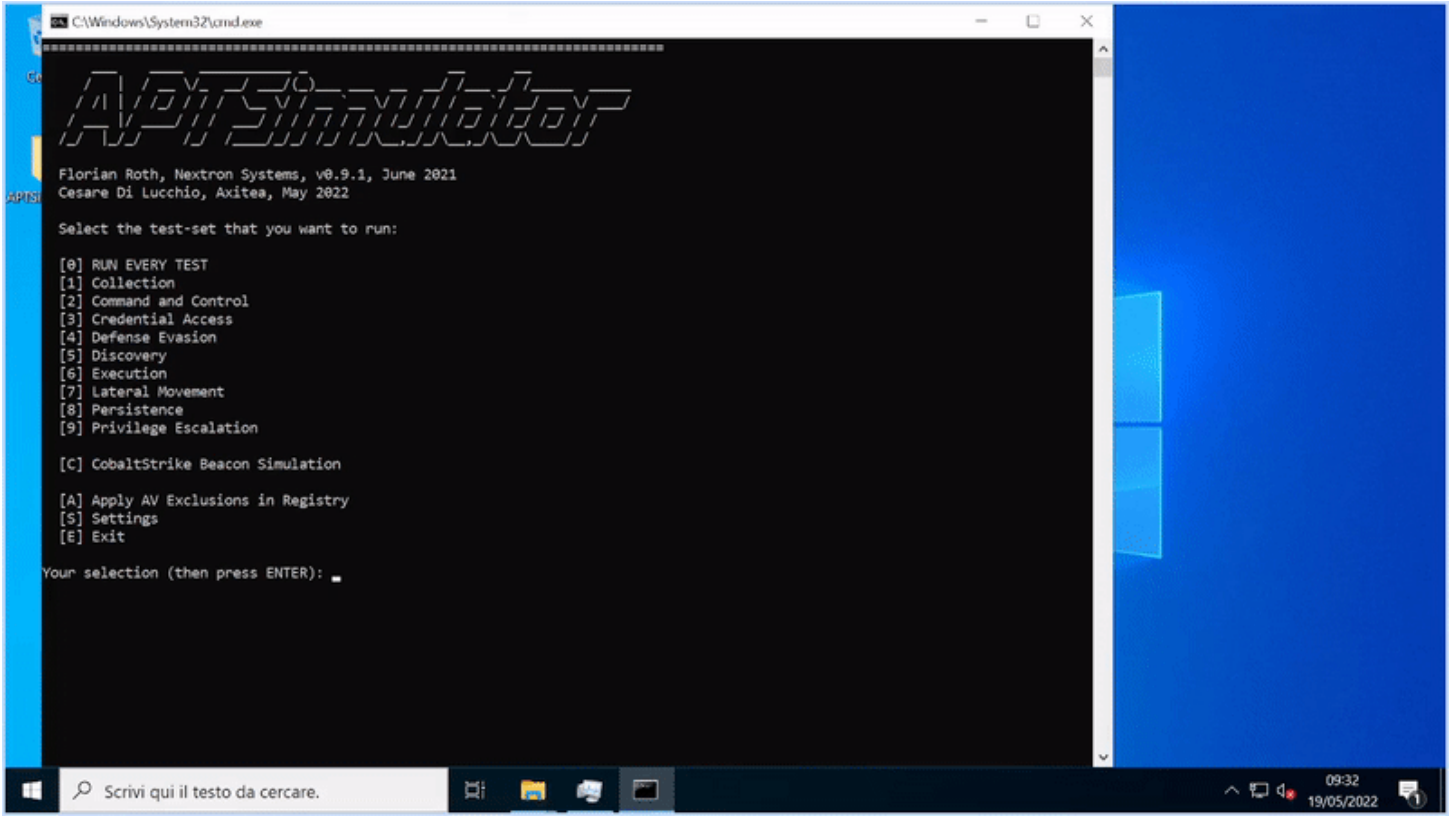


Fonte: Jared Atkinson

Detection

- Rilevamento automatico di azioni sospette
- Rilevamento di ciò che è sconosciuto e possibilità di raccogliere eventi non associati a incidenti
- Rilevamento di attacchi che hanno aggirato i primi controlli
- Rilevamento automatico di minacce basato su threat intelligence proprietaria (IPs, domini, file ecc.)
- APT Simulator

APT SIMULATOR EXTENDED



https://github.com/murd00ck/APTSimulatorExtended

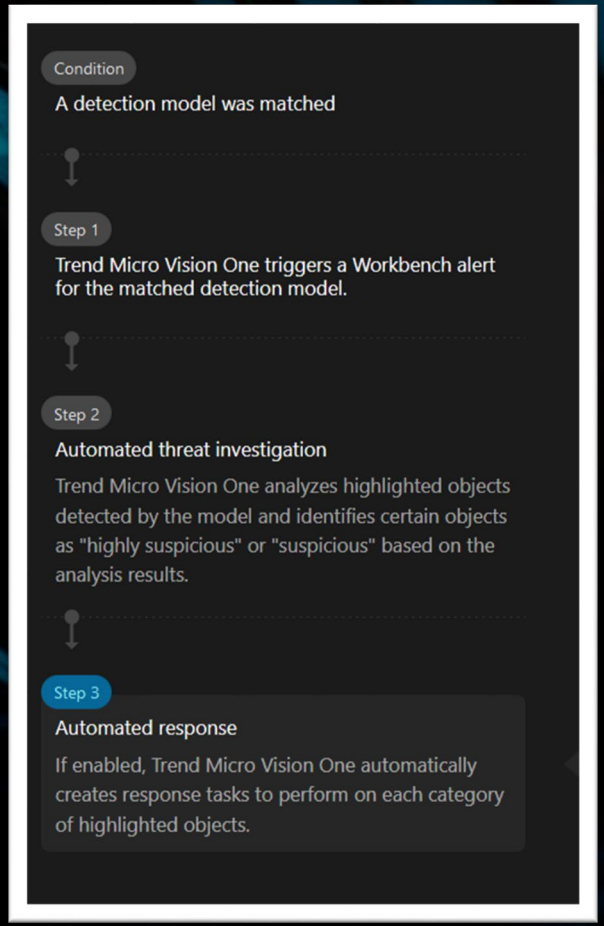
APT SIMULATOR EXTENDED

Risk level	Detection filter	Description	Tactic	Technique
Info	Service Execution via Service Control Manager	Service Control Manager (services.exe) has executed a pro...	TA0002	T1569.002
High	Malware Detection	Malware Detection found in an endpoint.		
Medium	Suspicious File Extraction To Public Directory	Identified suspicious file extraction in Public directory	TA0002	T1204.002
Info	File Deletion - Public Folder	Detects deleting of files in Public Folder	TA0005	T1070.004
High	Possible Credential Dumping Via Command Line	Command-line argument for obtaining login and passwor...	TA0002, TA0005, TA0006, TA0008	T1059.003, T1550.003, T1550.002, T1003, T1212
Low	Account Discovery	A command-line utility was executed to gather information...	TA0007	T1087.001, T1018, T1069.001, T1069.002, T1087.002
Low	Account Discovery on the Domain Controller	A command-line utility was executed to gather information...	TA0007	T1069.002, T1087.002
Low	Account Discovery	A command-line utility was executed to gather information...	TA0007	T1087.001, T1018, T1069.001, T1069.002, T1087.002
Low	Delete Account Using NET Utility	Detect the deletion of a local system or domain account vi...	TA0040	T1531
High	User Creation via Powershell	Detect the addition of new user using powershell	TA0002	T1059.001
Medium	Uncommon Powershell Parameters Used in Command Line	An uncommon powershell parameter in a process was det...	TA0002	T1059.001
Info	Powershell Execution	Powershell Scripting environment which adversaries may a...	TA0002	T1059.001
Low	Account Discovery	A command-line utility was executed to gather information...	TA0007	T1087.001, T1018, T1069.001, T1069.002, T1087.002
Low	Delete Account Using NET Utility	Detect the deletion of a local system or domain account vi...	TA0040	T1531
Low	Create Account Via NET.exe Utility	Detect the creation of a local system or domain account vi...	TA0003	T1136.002, T1136.001
Low	Creation of Local Account via Net.exe	Net user /add command was used to create a local accou...	TA0003	T1136.001
Info	Execution of Windows Command Line Interface	Windows Command Line Interface (cmd.exe), was execute...	TA0002	T1059.003
High	Possible C2 Connection via Powercat	Detects C2 connection via powercat	TA0011	T1095
High	Possible C2 Connection via Powercat	Detects C2 connection via powercat	TA0011	T1095
High	Possible C2 Connection via Powercat	Detects C2 connection via powercat	TA0011	T1095
High	Possible C2 Connection via Powercat	Detects C2 connection via powercat	TA0011	T1095
Low	Possible Network Discovery via Powercat	Detects the execution of powercat	TA0007	T1016

https://github.com/murd00ck/APTSimulatorExtended

response

- Capacità di response della soluzione
- Integrazione con piattaforme SIEM, SOAR
- Integrazione con sistemi di ticketing
- Root cause analysis
- Funzionalità di reporting



PPT IMPACT

- Tempi e modalità di deployment della soluzione
- Requisiti hardware
- La soluzione utilizza infrastruttura in Cloud?
- Qual è l'impatto sugli endpoint nell'utilizzo di query per acquisire la telemetria o per inviarla?

Platform	Editions	Processor
Windows 11 (64-bit) October 2021 Release (21H2)	• Enterprise • Education • Pro • Home	2 CPU cores
Windows 10 (32/64-bit) November 2021 Update (21H2)	• Enterprise • Education • Pro • Home	2 CPU cores
Windows 8.1 (32/64-bit)	• Enterprise • Education • Pro	2 CPU cores

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