

# edr 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

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

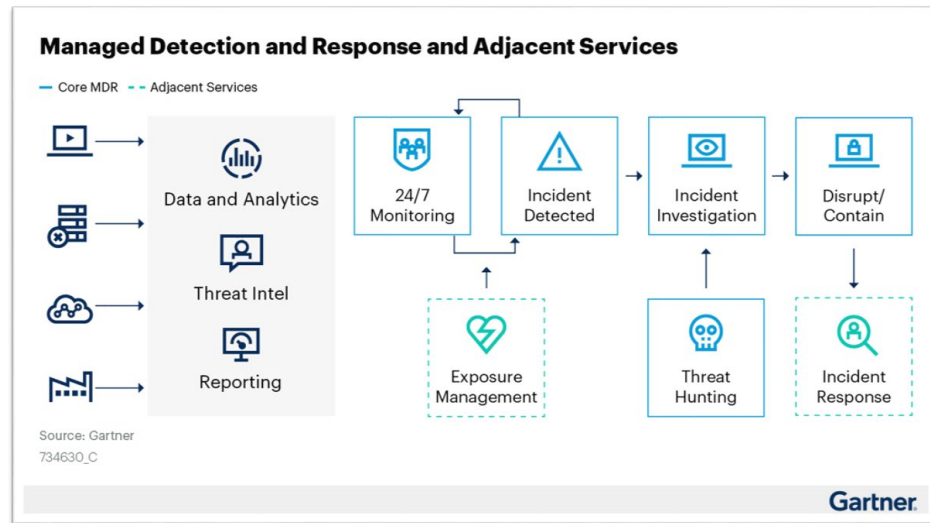
**+35%**

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



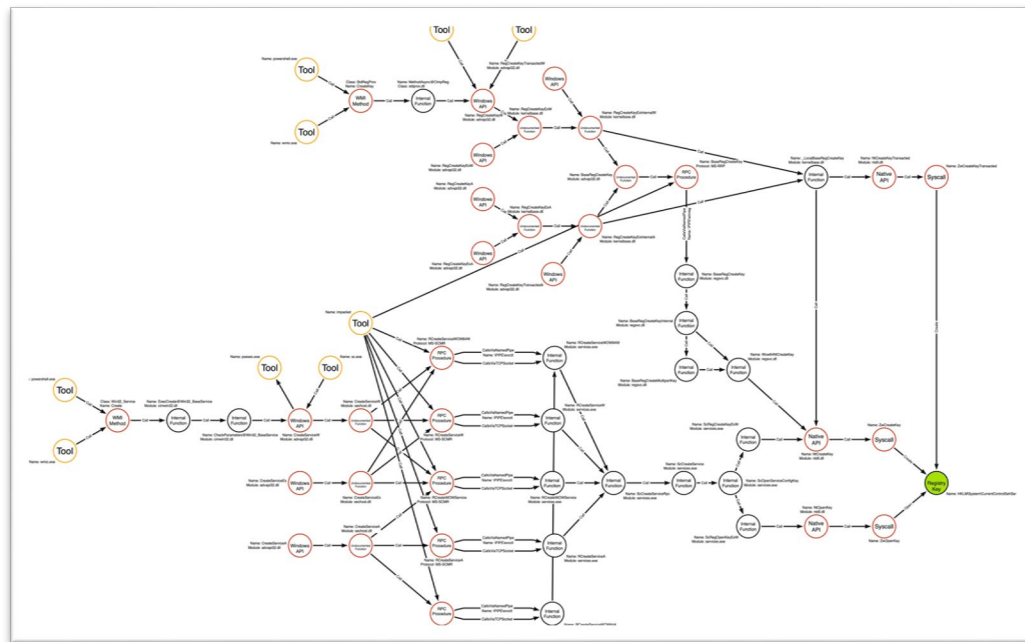
## DRIVER DI SCELTA

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

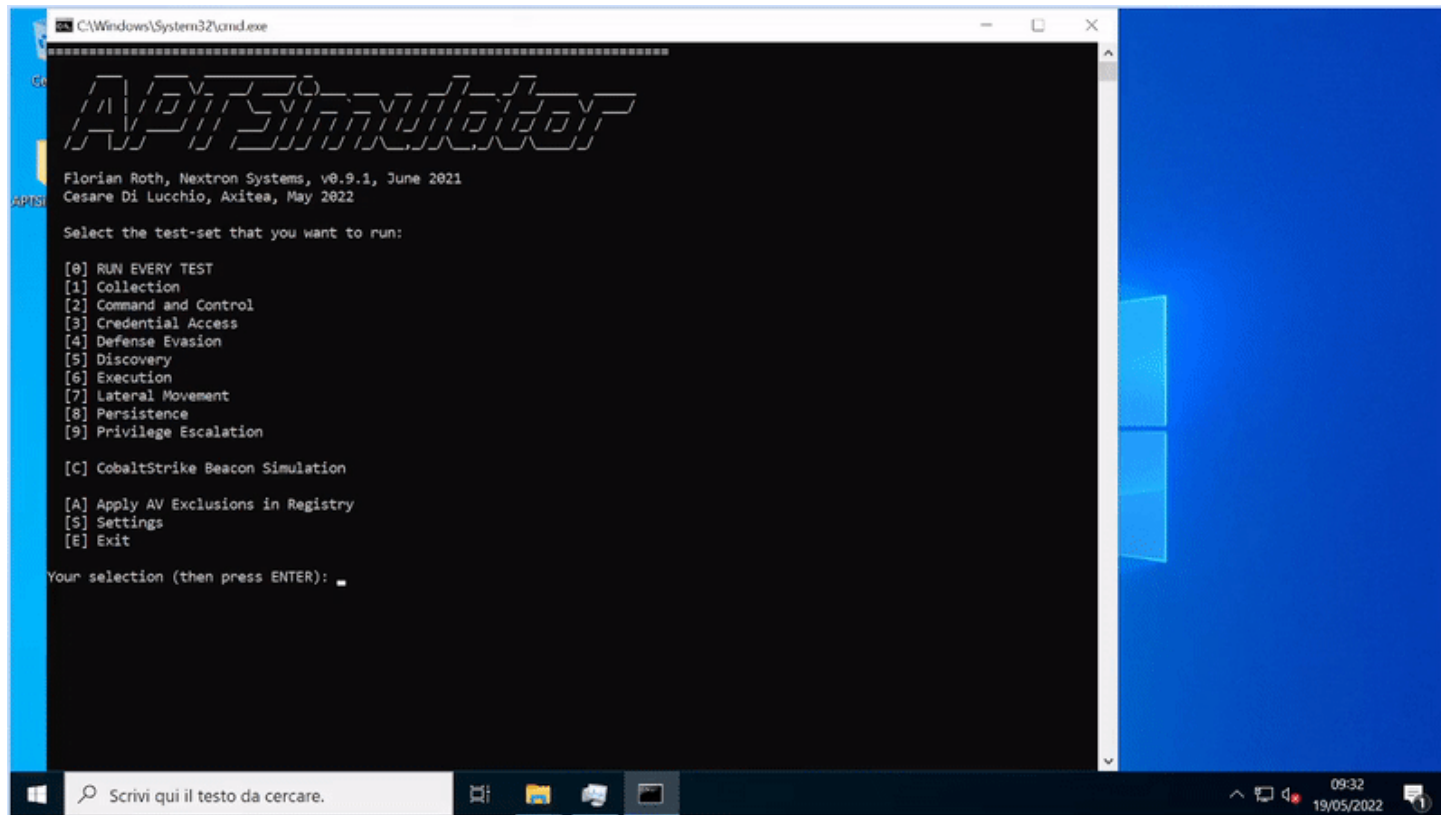


# DETECTION

- 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

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

# APT SIMULATOR extended





# APT SIMULATOR extended

Risk level	①	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

## response

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

### Condition

A detection model was matched

### Step 1

Trend Micro Vision One triggers a Workbench alert for the matched detection model.

### Step 2

#### Automated threat investigation

Trend Micro Vision One analyzes highlighted objects detected by the model and identifies certain objects as "highly suspicious" or "suspicious" based on the analysis results.

### Step 3

#### Automated response

If enabled, Trend Micro Vision One automatically creates response tasks to perform on each category of highlighted objects.

## 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)	<ul style="list-style-type: none"><li>• Enterprise</li><li>• Education</li><li>• Pro</li><li>• Home</li></ul>	2 CPU cores
Windows 10 (32/64-bit) November 2021 Update (21H2)	<ul style="list-style-type: none"><li>• Enterprise</li><li>• Education</li><li>• Pro</li><li>• Home</li></ul>	2 CPU cores
Windows 8.1 (32/64-bit)	<ul style="list-style-type: none"><li>• Enterprise</li><li>• Education</li><li>• Pro</li></ul>	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