



SIEM vs EDR

The fight for a holistic and combined approach

Michel de Crevoisier
SOC / Detection lead

 [mdecrevoisier](#)

Bsides Zagreb 2024

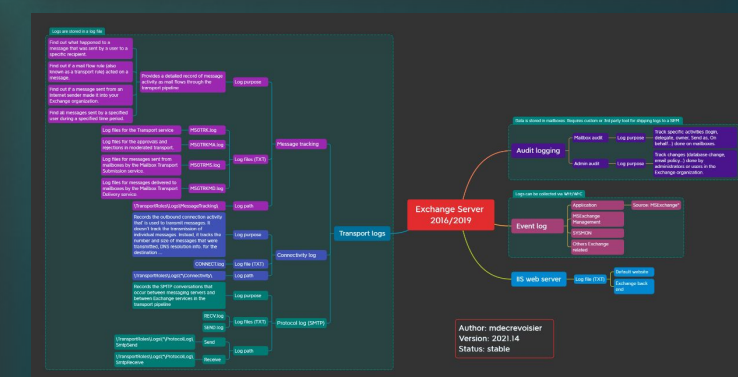
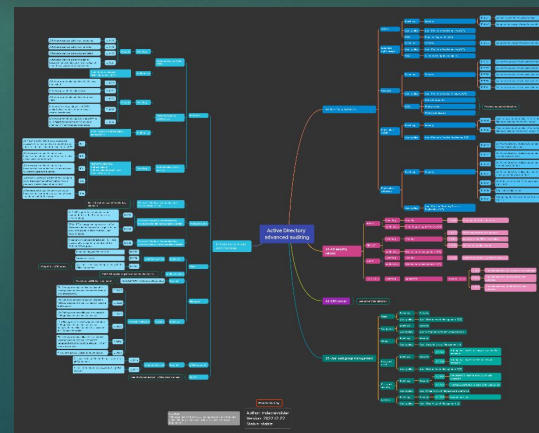
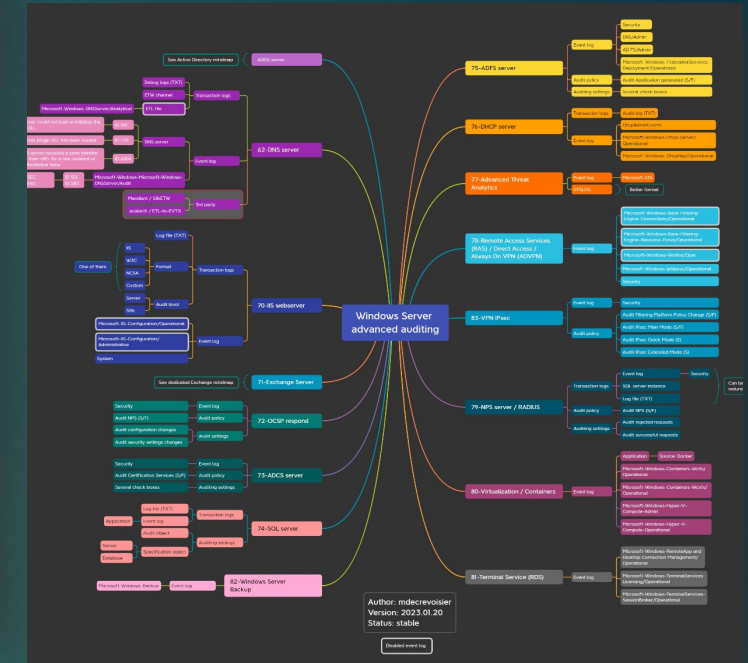
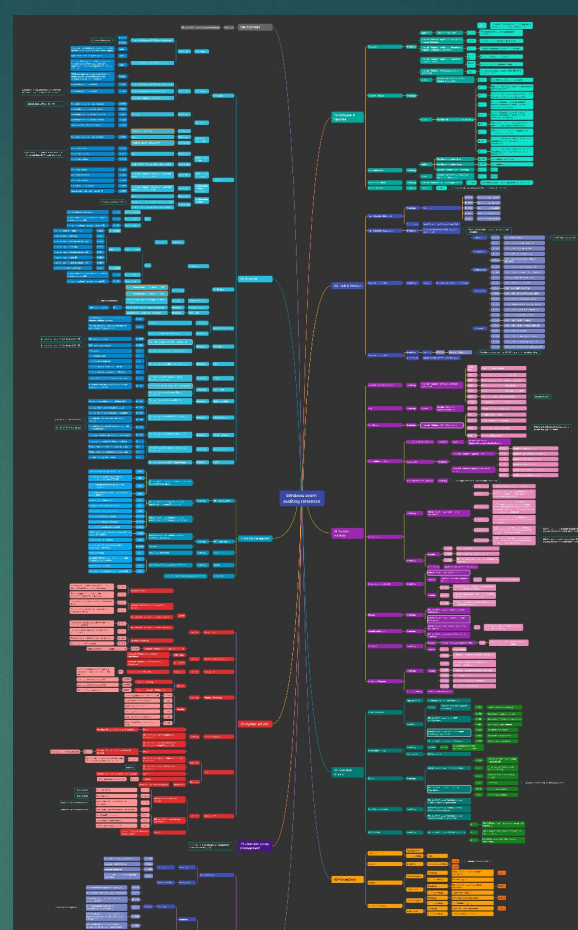


#whoami

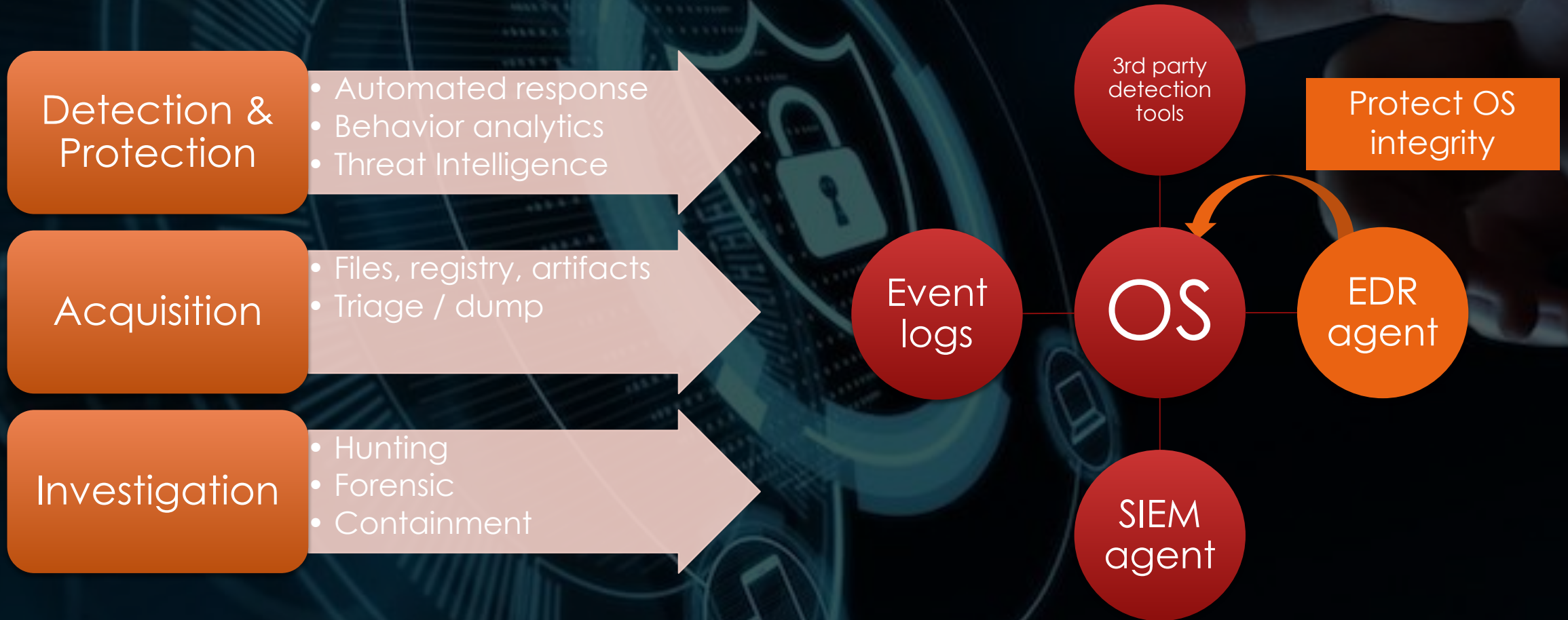
SOC / Detection lead / Senior Security Analyst

- ▶ ex Network & System administrator
- ▶ Threat bounty developer at **SOC PRIME**
- ▶ Guest contributor at **redcanary**
- ▶ Frequent speaker at **BSIDES**
- ▶ Author of several projects:

- ▶ SIGMA-detection-rules (>320 rules)
- ▶ EVT-X-to-MITRE-Attack (>270 samples)
- ▶ Microsoft-eventlog-mindmaps



EDR at a glance



EDR: first prey ?

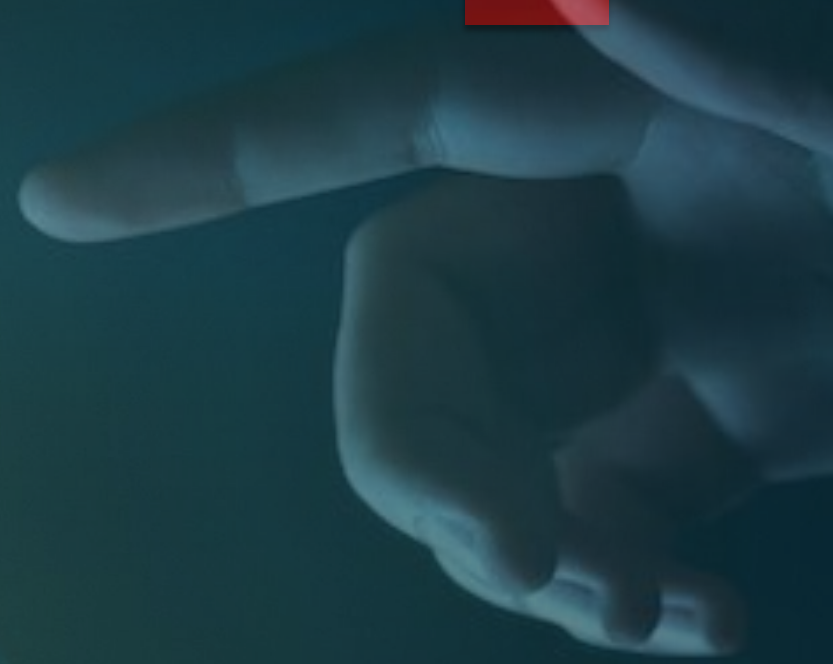
Focus on **evasion** operations



EDR evasion operations

5

Avoiding
the EDR



Hiding in hypervisors



2023-09: Johnson Controls International had a ransomware attack that targeted ESXi servers



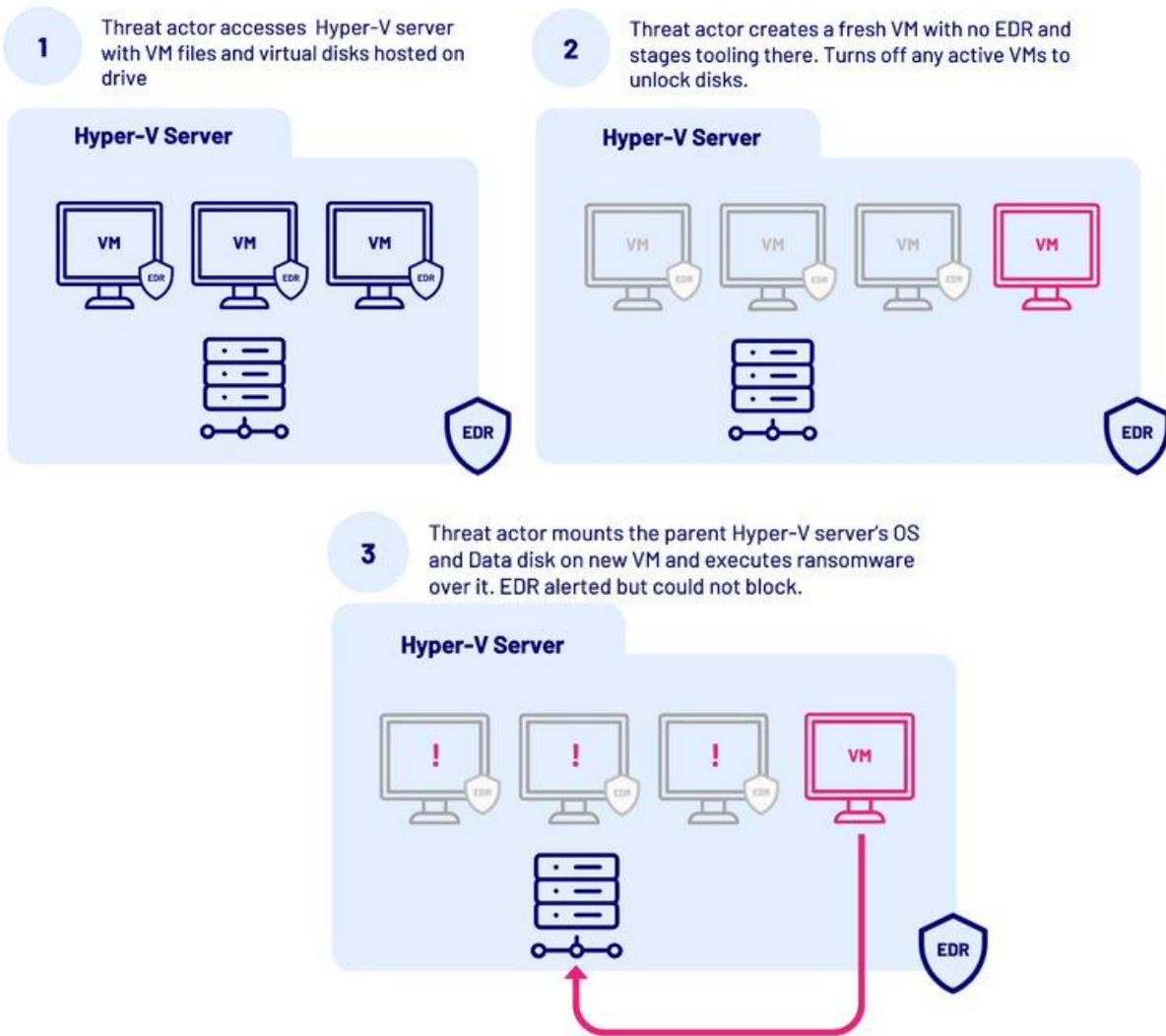
2023-02: Akira ransomware groups targeted Windows Hyper-V servers



2022: Alpha Spidere used Cobalt strike variants on ESXi servers



2022: Scattered Spider used proxy tool RSOCX for persistence on ESXi servers



Source: Weaponising VMs to bypass EDR – Akira ransomware - CyberCX - September 2023

Hiding in network devices

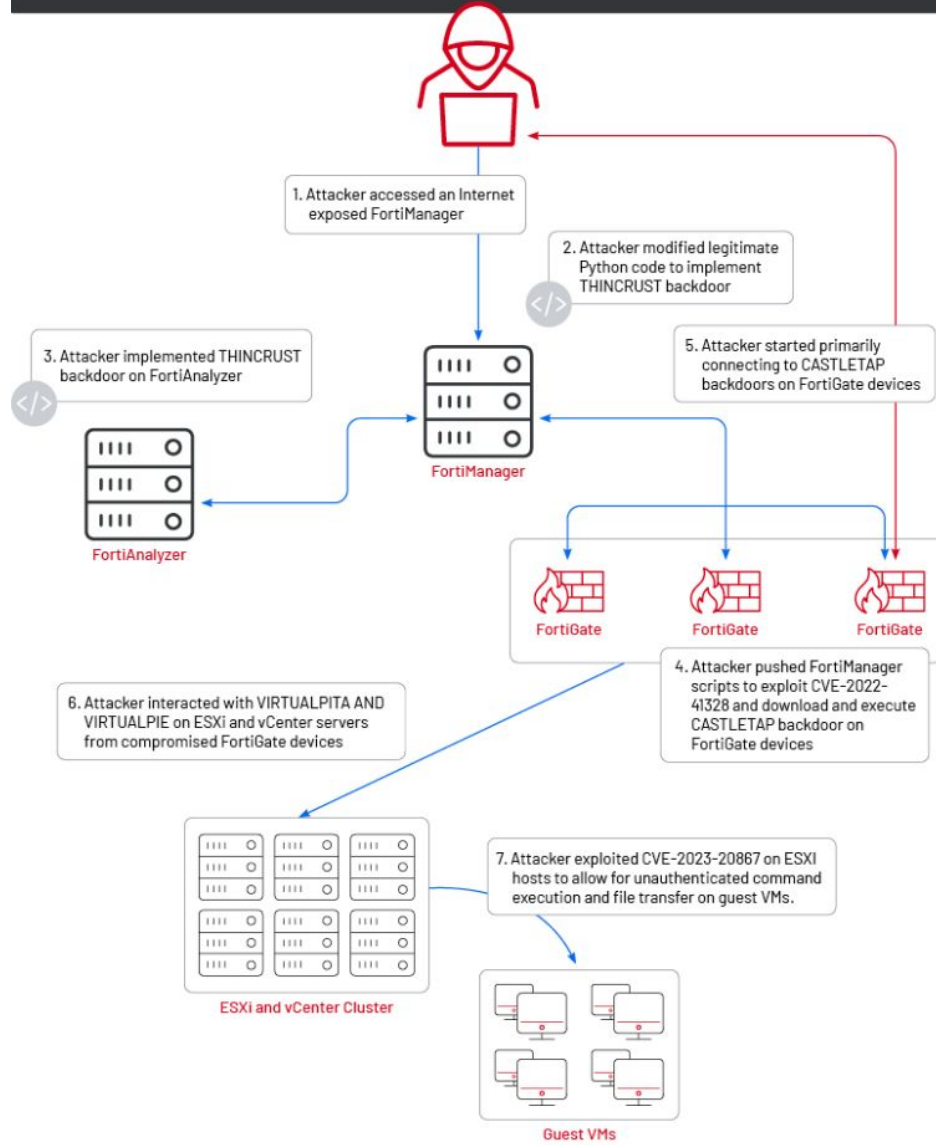
2023-09: BlackTech hacking gang infiltrated Cisco devices (with firmware replacement and SSH backdoor)



2023-07: UNC3886 targeted **FORTINET** VMware devices to remain undetected

2022-10: UNC4841 exploited a 0-day (CVE-2023-2868) in Barracuda Email Security Gateway to establish a reverse shell

UNC3886 EXPLOITED TWO ZERO-DAYS IN COMPLEX OPERATIONS



— Attacker had direct access to the devices after the CASTLETAP backdoor was installed.
— Attacker accessed ESXi and vCenter servers from various compromised FortiGate devices

EDR evasion operations

8

Avoiding
the EDR

EDR
tampering



EDR tampering

★ BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

Bring Your Own [Vulnerable] Driver

2024
Lazarus group

- `appid.sys`: native driver for AppLocker exploited ([Avast](#)). Reported in July 2023 to Microsoft

2024
Kasseika ransomware

- `Martini.sys` / `viragt64.sys` (part of VirIT Agent System developed by TG Soft) ([TrendMicro](#))

2022
Sunlogin driver

- Sunlogin remote control utility (from Oray company) - CNVD-2022-10270 / CNVD-2022-03672 ([ASEC](#))

2022
AMD driver

- AMD's Ryzen master driver v17 ([GitHub](#))
- CPU overclocking control

2022
Scattered Spider

- Intel Ethernet diagnostic drivers `iqvw64.sys` - CVE-2015-2291 ([CrowdStrike](#))

2022
BurntCigar malware

- Signed with a legitimate WHCP certificate ([Sophos](#))

2021
Lazarus group

- Dell DBUtil drivers - CVE-2021-21551 ([ESET](#))

2021
Cuba ransomware

- Avast driver `aswArPot.sys` ([AON](#))

2019
BlackByte ransomware

- Micro-Star's MSI AfterBurner
- Graphics card overclocking utility `RTCORE[32/64].sys` ([Sophos](#))

EDR tampering

★ BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

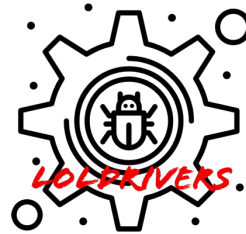
DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation



Bring Your Own [Vulnerable] Driver

```
1845 lines (1845 sloc) | 117 KB
1 title: Vulnerable Driver Load
2 id: 7aaaf4b8-e47c-4295-92ee-6ed40a6f60c8
3 status: experimental
4 description: Detects the load of known vulnerable drivers by hash value
5 references:
6   - https://lolldrivers.io/
7 author: Nasreddine Bencherchali (Nextron Systems)
8 date: 2022/08/18
9 modified: 2023/04/10
10 tags:
11   - attack.privilege_escalation
12   - attack.t1543.003
13   - attack.t1068
14 logsource:
15   product: windows
16   category: driver_load
17 detection:
18   selection_sysmon:
19     Hashes|contains:
20     - 'MD5=64efbffa153b0d53dc1bccda4279299'
21     - 'MD5=d3e40644a91327da2b1a7241606fe559'
22     - 'MD5=1ed043249c21ab201edccb37f1d40af9'
23     - 'MD5=6126065af2fc2639473d12ee3c0c198e'
24     - 'MD5=63e333d64a8716e1ae59f914cb686ae8'
```

Provided with an
API feed
(JSON & CSV)

Name ↕

gameink.sys

krprocesshacker.sys

Learn / Windows / Security /

Microsoft recommended driver block rules

Article • 01/25/2024 • 5 contributors •

Applies to: Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, Windows Server 2016

Feedback

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

Event Tracing for Windows (ETW)



- Introduced in Windows XP
- Built-in logging mechanism
- Allow to observe and troubleshoot system

Windows 11 can produce more than 50K events with 1000 different providers

ETW abuses

- Blind security applications and ETW telemetry
- Used as a sniffer without kernel drivers or callback
- Can help to detect some sandbox detonations

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding sensors

Blocking communications

DLL unhooking

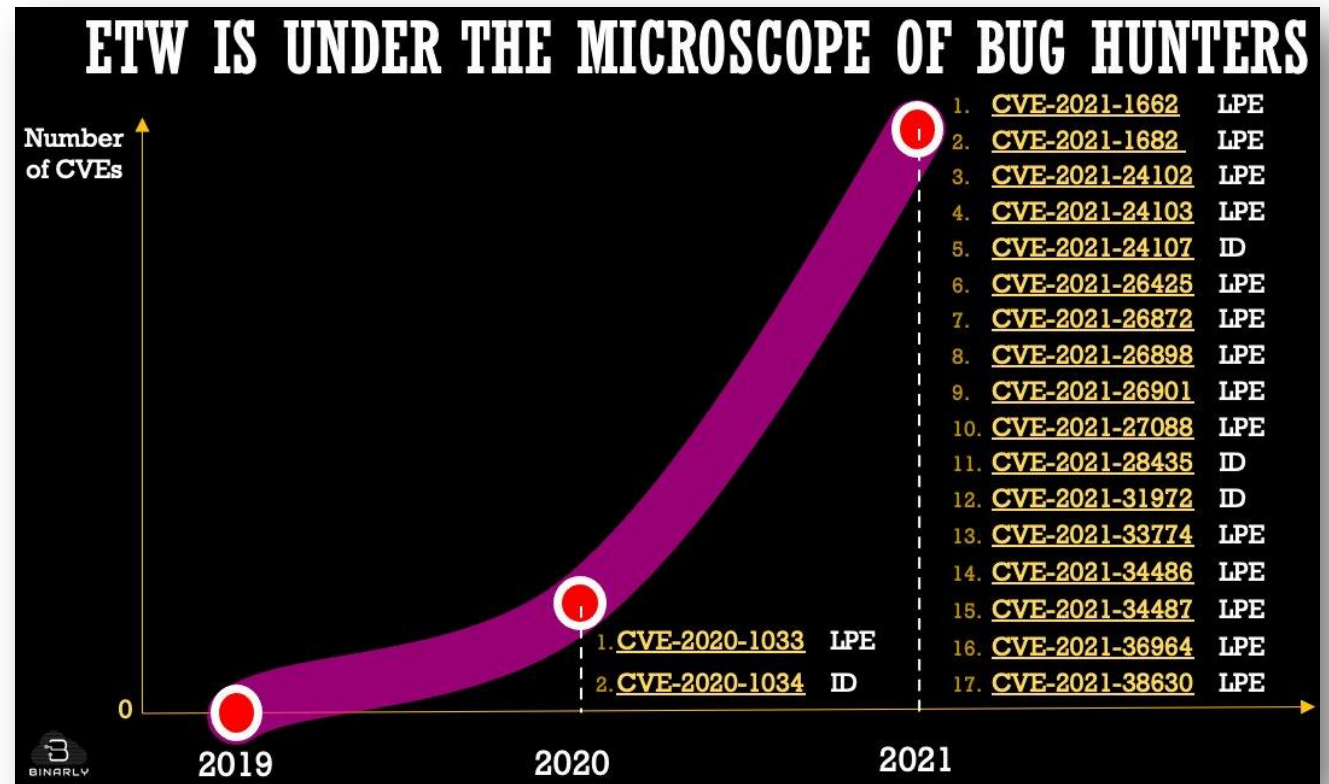
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object Manipulation

ETW vulnerabilities evolution



Source: Design issues of modern EDRs: bypassing ETW-based solutions – Binarly.io - November 2021

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding sensors

Blocking communications

DLL unhooking

Kernel callbacks

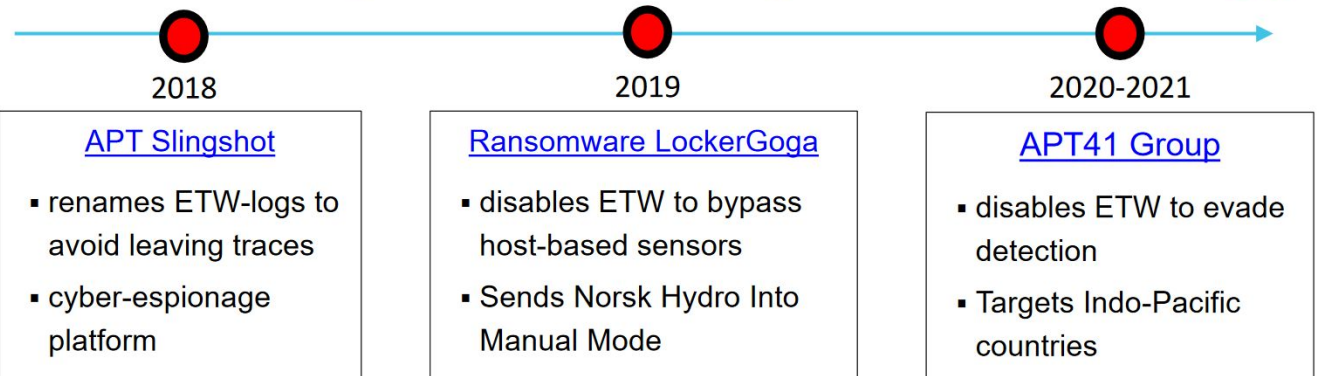
File/driver deletion

Process injection

Direct Kernel Object Manipulation

ETW malware examples

Malware Examples of evading ETW-based logging



Defense Evasion (post-exploitation) Frameworks:

- [SharpSploit](#) disable ETW monitoring for current process
- [ScareCrow](#) – payload creation framework bypasses EDR
- [EDR Evasion](#) – about 10 examples of blocking ETW logging

[MITRE ATT&CK – Impair Defenses](#)

- Indicator Blocking
- Disable Cloud Logs

#BHEU @BlackHatEvents

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding sensors

Blocking communications

DLL unhooking

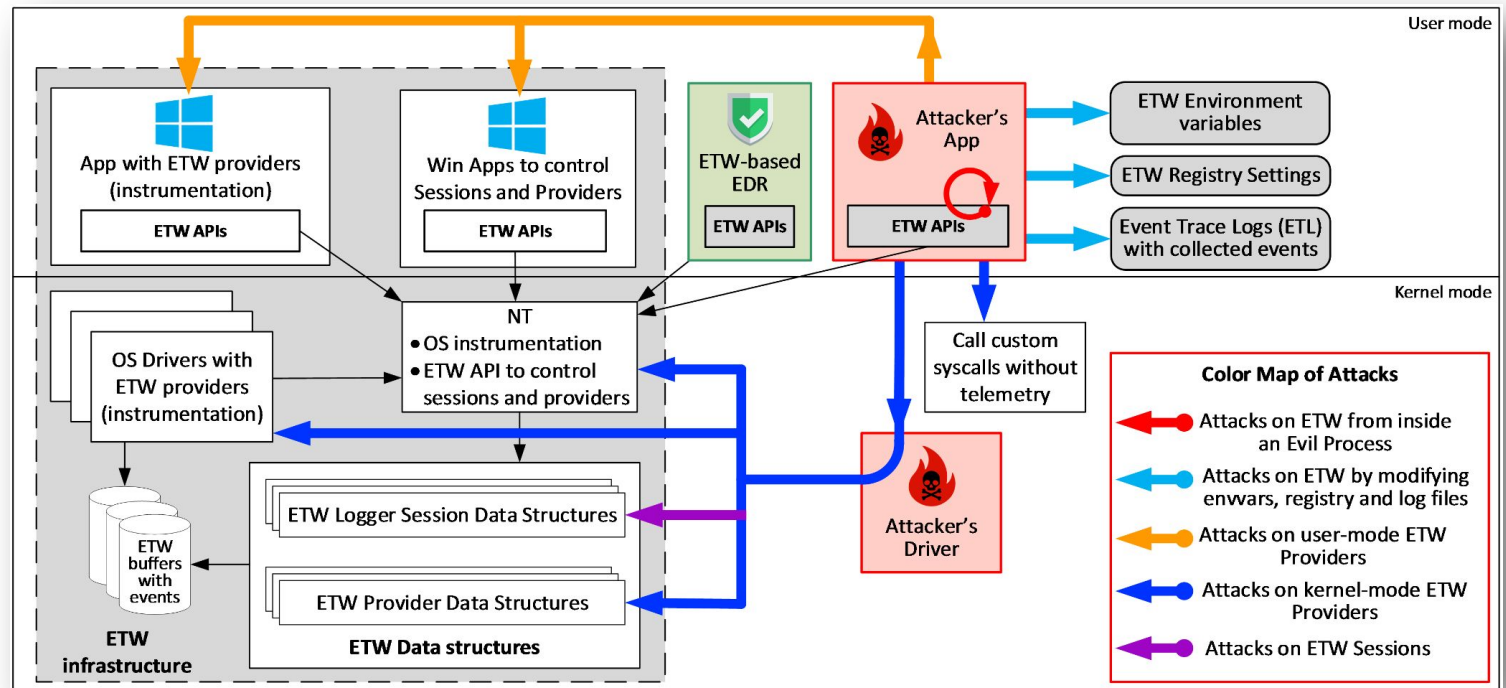
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object Manipulation

ETW attack surface



Source: Attacks on ETW Blind EDR Sensors – Blackhat Nov. 2021

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

★ AMSI bypass

DLL side loading

Blinding sensors

Blocking communications

DLL unhooking

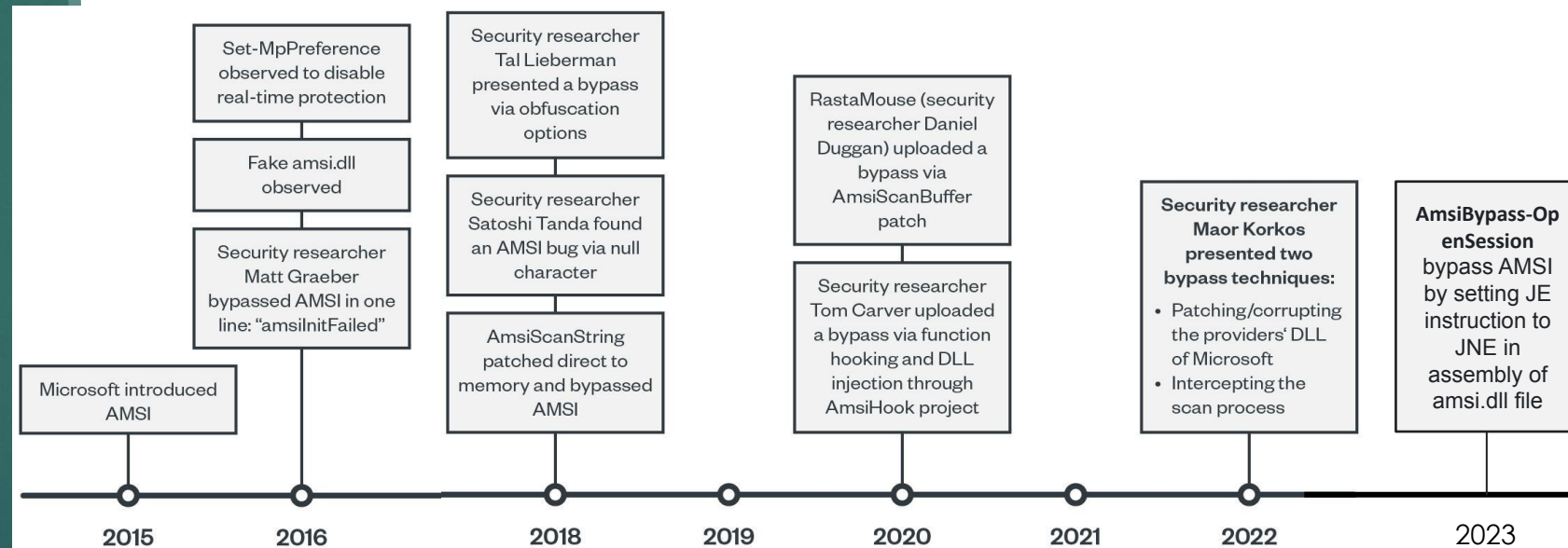
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object Manipulation

Antimalware Scan Interface (AMSI) bypass evasion techniques evolution



Source: Detecting Windows AMSI bypass techniques
TrendMicro - December 2022

Source: AMSI bypass new way
2023

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

★ DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernal callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

DLL side loading

DLL Hijacking manipulates a trusted application into executing an unauthorized DLL.

HijackLibs

Enter the name of a DLL or EXE here...

Sideloadng Environment Variable Phantom Search Order

Latest entries:

[nvsmartmax.dll](#) [safestore32.dll](#) [formdll.dll](#) [opera_elf.dll](#) [rjyplatform.dll](#)

[shellchromeapi.dll](#) [sensapi.dll](#) [acrodistdll.dll](#) [classicexplorer32.dll](#)

[dbgmodel.dll](#)

By vendor:

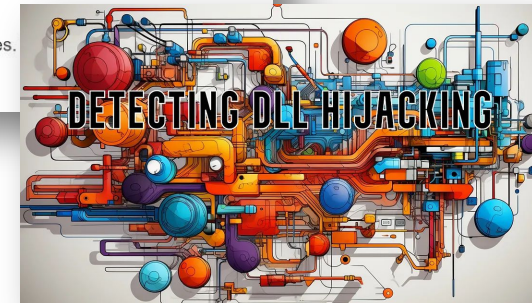
Microsoft ⁴²² McAfee ⁴ Symantec ³ Trend Micro ³ HP ² VMWare ² Adobe ¹ Asus ¹ Avast ¹

Baidu ¹ BitDefender ¹ Cisco ¹ Classic Shell ¹ CyberArk ¹ F-Secure ¹ Google ¹ Lenovo ¹

LogMeIn ¹ Luxand ¹ Mozilla ¹ npm ¹ Nvidia ¹ Opera ¹ Palo Alto ¹ Python ¹ Razer ¹ Smadav ¹

Sophos ¹ Toshiba ¹ Unity ¹ VentaFax ¹ Vivaldi ¹ VLC ¹ x64dbg ¹

The database contains 386 *Sideloadng*, 89 *Environment Variable*, 12 *Phantom* and 9 *Search Order* entries. hijacking entries, click [here](#).



Source: Detect DLL Hijacking techniques from HijackLibs with Splunk – DetectFYI – Oct. 2023

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

DLL side loading

★ Blinding sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object Manipulation

Blinding EDR sensors

Event Trace (ETW) patch

Removing the DLL hooks

Removing kernel callbacks

Block EDR outbound traffic (EDR silencer)

Set MaxConnections to 0 for internal communication between process and driver

EDR evasion operations

18

Avoiding
the EDR

EDR
tampering

Blending
into the
environment



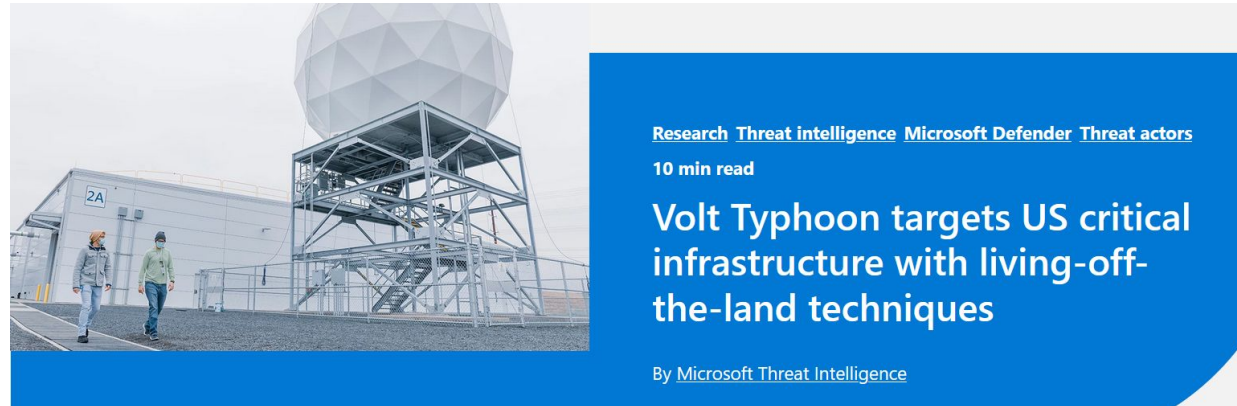
EDR blending

★ LOLBINS

WSL (Subsystem
for Linux)

Remote services
or software

Living of the land binaries (LOLBINS)



Source: Volt Typhoon - Microsoft May 2023

Binary	Function					
	Compile	Decode	Download	Execute	Modify System Settings	Reconnaissance
Rundll32				■		
Regsvr32				■		
Msiexec				■		
Mshhta				■		
Certutil		■	■		■	
MSBuild	■			■		
WMIC				■	■	■
WmiPrvSe				■		

Source: 8 LOLBINS every threat hunter should know – CrowdStrike – March 2023

EDR blending

★ LOLBINS

WSL (Subsystem
for Linux)

Remote services
or software

Living of the land binaries (LOLBINS)

LOLBAS

☆ Star 5,323



Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib. More information on programmatically accessing this project can be found on the [API page](#).

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).













If you are looking for UNIX binaries, please visit [gtfobins.github.io](https://github.com/gtfobins/gtfobins).

Search among 178 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
AspNet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At
Atbroker.exe	Execute	Binaries	T1218: System Binary Proxy Execution



A great collection of resources to thrive off the land

logo	link	description
	https://br0k3nlab/LoFP/	Living off the False Positive is an autogenerated collection of false positives sourced from some of the most popular rule sets. The information is categorized along with ATT&CK techniques, rule source, and data source.
	https://loldrivers.io	Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks
	https://gtfobins.github.io	GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems
	https://lolbas-project.github.io	The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques
	https://lots-project.com	Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain
	https://filesec.io	File extensions being used by attackers
	https://malapi.io	MalAPI.io maps Windows APIs to common techniques used by malware
	https://hijacklibs.net	This project provides an curated list of DLL Hijacking candidates
	https://wadcoms.github.io	WADComs is an interactive cheat sheet, containing a curated list of offensive security tools and their respective commands, to be used against Windows/AD environments
	https://www.loobins.io	Living Off the Orchard: macOS Binaries (LOOBins) is designed to provide detailed information on various built-in macOS binaries and how they can be used by threat actors for malicious purposes
	https://lolapps-project.github.io	This project was made because exploitation isn't limited to binaries using command line techniques. Both built-in and third-party applications have been used & abused for adversarial gain since the dawn of time, and knowing these methods can help when all else fail.
		Curated list of known malicious bootloaders for various operating systems. The project

Living off the living off the land

EDR blending

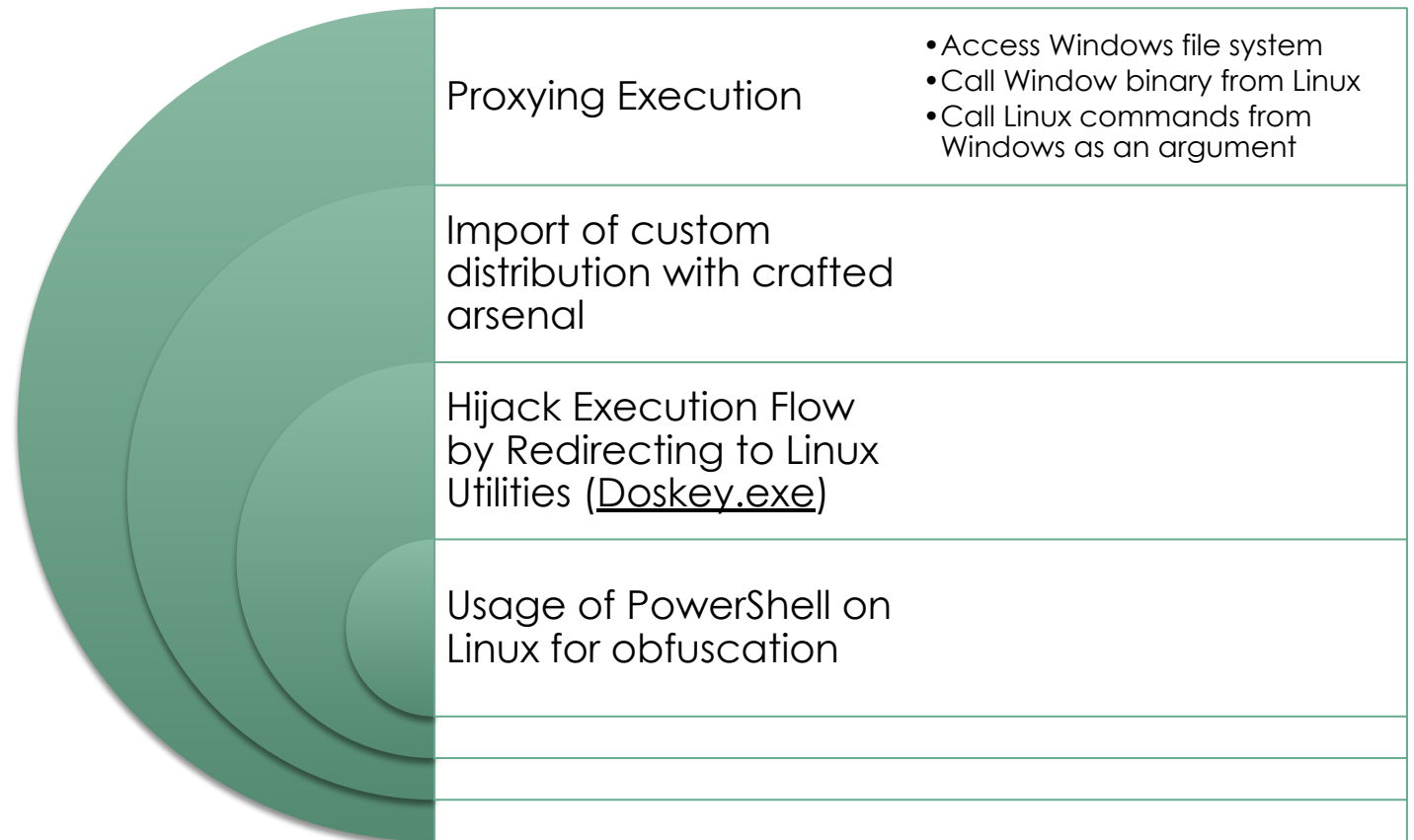
LOLBINS

★ WSL (Subsystem for Linux)

Remote services or software



Windows Subsystem for Linux (WSL)



Source: Attack Tactics, Techniques & Procedures using Windows Subsystem for Linux
Qualys – December 2022

EDR blending

LOLBINS

★ WSL (Subsystem for Linux)

Remote services or software



Windows Subsystem for Linux (WSL)

```
SubjectUserSid S-1-5-21-2249913968-[REDACTED]
SubjectUserName D[REDACTED]
SubjectDomainName K[REDACTED]
SubjectLogonId 0x326810
NewProcessId 0x616c
NewProcessName C:\Users\D[REDACTED]\AppData\Local\Packages\KaliLinux.54290C8133FEE_ey8k8hqnwqnmq\LocalState\rootfs\usr\bin\truncate
TokenElevationType %%1938
ProcessId 0x6edc
CommandLine truncate -s 0 dpkg.log
TargetUserSid S-1-0-0
TargetUserName -
TargetDomainName -
TargetLogonId 0x0
ParentProcessName C:\Users\D[REDACTED]\AppData\Local\Packages\KaliLinux.54290C8133FEE_ey8k8hqnwqnmq\LocalState\rootfs\usr\bin\bash
MandatoryLabel S-1-16-8192
```

WSL commands re-transcription in process execution events logs



The Defender for Endpoint for **WSL2 plug-in** enables Defender for Endpoint to provide more visibility into all running WSL containers, by plugging into the isolated subsystem.
December 2023

EDR blending



Remote services / Remote software

LOLBINS

WSL (System for Linux)

★ Remote services or software

Category of legitimate tools

#	Category	Example	
1	MS Native Tools	PowerShell, PsExec, WMI, MSBuild, ...	Techniques are being well researched.
2	Pentest Tools	Cobalt Strike, Mimikatz, Bloodhound, ...	AV products are making effort to detect them.
3	Commercial Tools	AnyDesk, Splashtop, Rclone(MEGA), ...	Our focus on this presentation

Target RMM tools



Target SYNC tools



Source: Analysis on legit tools abused in human operated ransomware – Trend Micro – 2023

EDR evasion operations

Avoiding the EDR

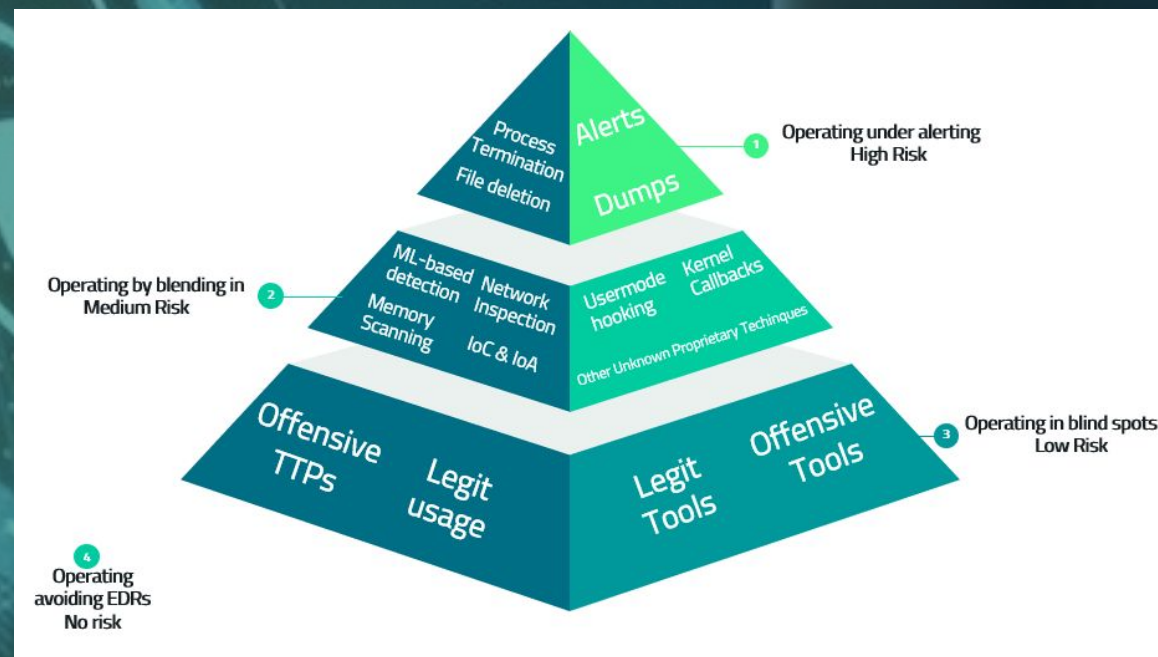
EDR tampering

Blending into the environment

Operating in blind spots



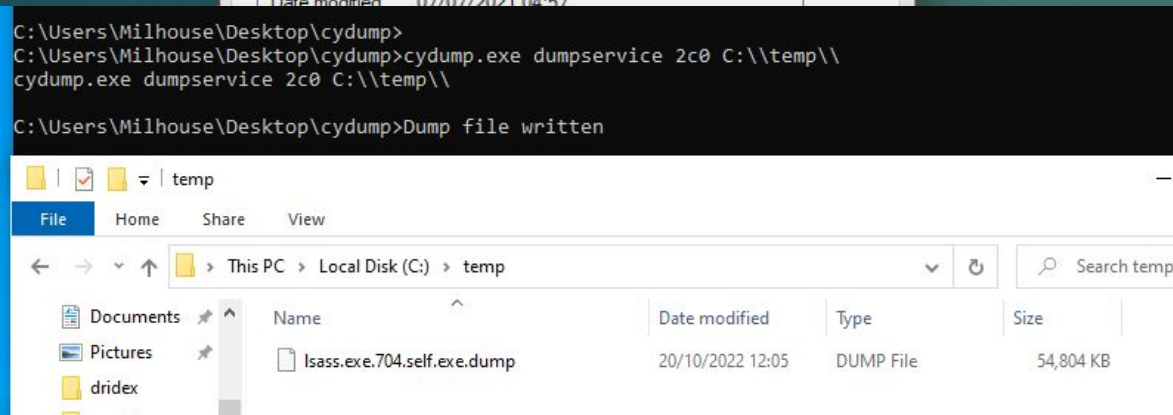
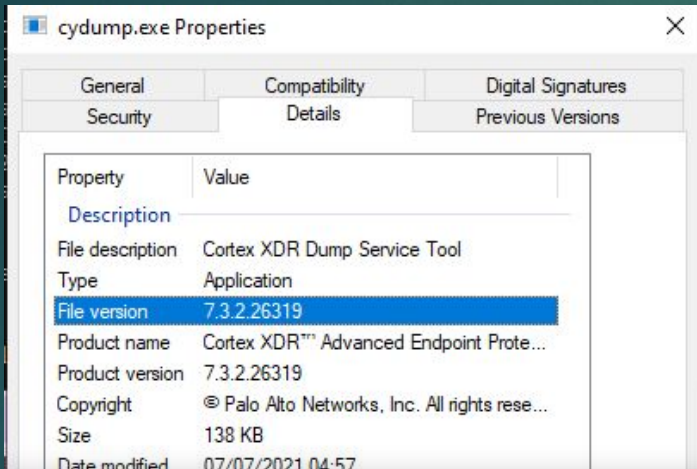
Attacker's pyramid of pain - Mapping risk levels to EDR evasion category



Source: Living-Off-the-Blindspot - Operating into EDRs' blindspot September 2022



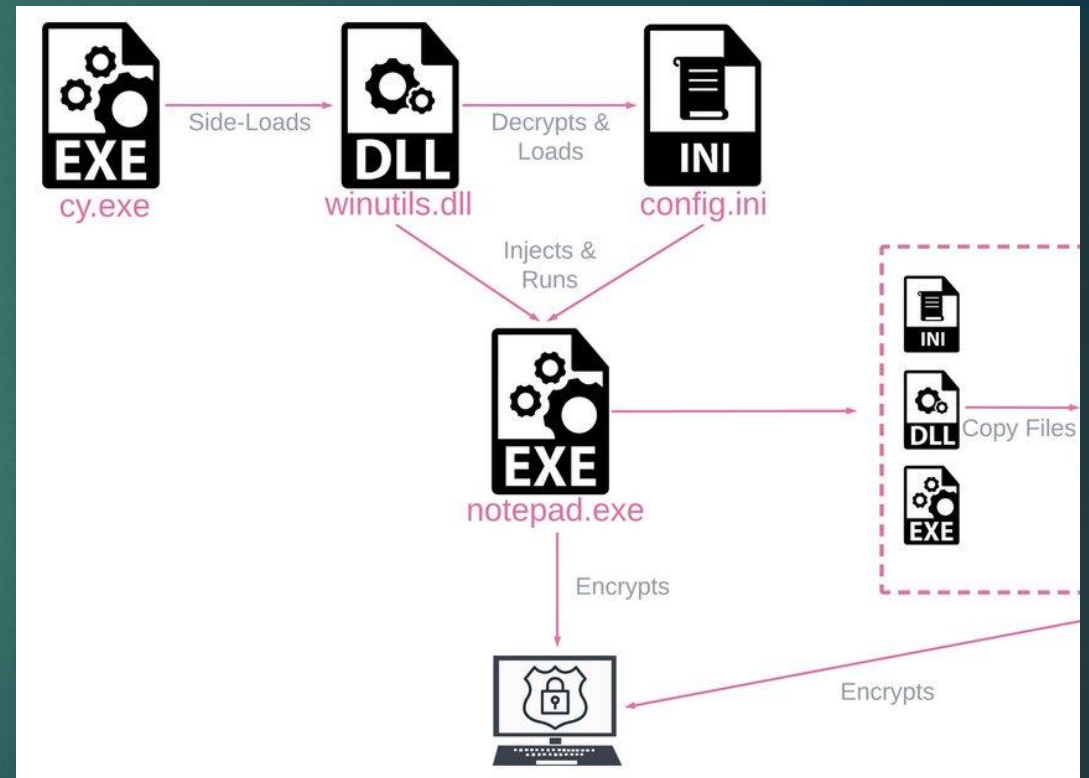
Dumping LSASS with **Palo Alto Cortex XDR** "cydump.exe" tool (patched in July 2021)



Source: Randsec – July 2022



DLL sideloading with **Palo Alto Cortex XDR** "cy.exe" tool



Source: "Rorschach: a new sophisticated ransomware" - Checkpoint – April 2023

EDR



“Uses a CoSetProxyBlanket to call the dump function in SentinelAgent.exe to dump a PID to disk. Requires local admin.”

```
[11/18/2023 00:00:29] Trying to dump SentinelAgent to 'C:\Windows\temp\' ...  
[11/18/2023 00:00:29] Initializing SentinelHelper COM object...  
[11/18/2023 00:00:29] SentinelHelper COM object initialized successfully  
[11/18/2023 00:00:29] Fetching SentinelAgent ProcessId...  
[11/18/2023 00:00:29] SentinelAgent Found: 3420
```

Name	Date modified	Type	Size
_SentinelAgentKernel.dmp	11/18/2023 12:00 AM	Memory Dump File	1,024 KB
_SentinelAgentUser.dmp	11/18/2023 12:00 AM	Memory Dump File	381,045 KB
vdagent.log	11/17/2023 11:39 PM	Text Document	40 KB
vdservice.log	11/17/2023 8:54 PM	Text Document	4 KB

Source: Adam Svoboda – Nov. 2023

EDR



cross platform, LLVM base, bypass statis



OKTA breach: LAPSUS downloaded “Process Hacker” and terminated the **FireEye HX** service agent.
(was tamper protection on ?)



Offensive Rust – More and more ransomware groups abused it since 2022
(cross platform, LLVM base, bypass static analysis...)

Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
2022-01-19 19:45:39	Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01 19:47:58	UserProfileSvcEop.exe downloaded from hxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:31:19	Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED]	Maintain Presence
2022-01-20 18:32:32	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 18:39:43	Bing search for Process Explorer by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:40:04	Process Explorer executed by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:43:51	Bing search for Process Hacker by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:01	Process Hacker downloaded from hxps://github.com by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:17	Process Hacker execution by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:46:22	FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED]	Establish Foothold
2022-01-20 18:46:55	Bing search for Mimikatz by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:48:28	Mimikatz downloaded from hxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:50:10	Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED]	Escalate Privileges

The screenshot shows a Windows Security window in the background with 'Virus & threat protection' active. In the foreground, a terminal window titled 'C:\Users\Admin\Desktop\rusty_fense.exe' displays the following output:

```
Hello from Rust
Want to see a trick:
[*] We're not gonna touch any EDR Hooks
[*] We're not gonna patch ETW or AMSI
[*] We're not gonna use custom syscalls
[*] We're not gonna encrypt shellcode
[*] We're gonna use a standard alloc method to execute shellcode
[*] Allocating space
[*] Copying shellcode into new section
[*] Changing shellcode's permissions
[*] Executing shellcode
```

Below the terminal is a Cobalt Strike interface showing a table of active sessions:

external	inter...	listener	user	computer	note	process	pid	arch	last	sleep
15.158...	172.16...	Research	Admin	...	rusty_fe...	5756	x64	8s	10 seconds	

At the bottom, an 'Event Log X' window shows the following entries:

```
02/20 14:39:46 *** Matt has left.
02/20 14:39:55 *** Matt has joined.
02/20 14:39:59 *** initial beacon from Admin@172.16.144.138 (...
```

Source: @BillDemirkapi - January 2022

Source: A closer look at rust based malware - February 2023

EDR configuration extraction

29

```
python XDRConfExtractor.py demo.ldb

#####
Description:
The password has at least 9 or more characters and must contain letters, number
For more information see: https://mrd0x.com/cortex-xdr-analysis-and-bypass/

AGENT SALT:      79q3mds4r67261zfmnobp1
AGENT HASH:      5b12f604e592035f4a3e8b3da6ceff4d2afacd3c642981deba53d5e3ed6672
a57bc0a00247c
```

MITRE | **ATT&CK™** | T1518.001 - Software Discovery: Security Software Discovery

- | | | |
|---|--|---|
| Uninstall Password Hash & Salt | Excluded Signer Names | DLL Security Exclusions & Settings |
| Office Files Security Exclusions & Settings | Credential Gathering Module Exclusions | Webshell Protection Module Exclusions |
| Child process Execution chain Exclusions | Behavioral Threat Module Exclusions | Local Malware Scan Module Exclusions |
| Memory Protection Module Status | Global Hash Exclusions | Ransomware Protection Module Modus & Settings |

EDR offensive / defensive tools

30

Terminator

- Relay on Zemana Anti-Malware driver ([GitHub](#))
- Used by Akira group

EDR Snowblat ([Sandblast](#) fork)

- Drivers & EDR process communication deactivation ([GitHub](#))

EDR silencer

- ([source](#)) vs EDR noise maker ([source](#))

Chimera

- DLL sideloading ([GitHub](#)) with encrypted shellcode

CrimsonEDR

- identify specific malware patterns and leverage diverse detection methods (unhook, ETW patch, AMSI patch...)





Who is monitoring the EDR ?

Identify EDR weak points

- Process monitoring
 - EDR may be **tampered** or **disabled**
 - Not all devices** can be enrolled
 - Ensure a **constant coverage** over time
 - Air gapped** devices without internet access
 - EDR may have shorter **retention** time
 - EDR may implemented filters, or collect partial data

Telemetry Feature Category	Sub-Category	Carbon Black	CrowdStrike	Cybereason	ESET Inspect	Elastic	Harfanglab	LimaCharlie	MDE
Process Activity	Process Creation	Green	Green	Green	Green	Green	Green	Green	Green
	Process Termination	Orange	Green	Green	Green	Green	Red	Green	Green
	Process Access	Green	Green	Green	Green	Green	Red	Green	Green
	Image/Library Loaded	Green	Green	Green	Green	Green	Red	Green	Green
	Remote Thread Creation	Green	Green	Green	Green	Green	Red	Green	Green
File Manipulation	Process Tampering Activity	Orange	Green	?	Red	Green	Red	Green	Green
	File Creation	Green	Green	Green	Green	Green	Red	Green	Green
	File Opened	Green	Green	Red	Red	Green	Red	Red	Red
	File Deletion	Green	Green	Green	Green	Green	Red	Green	Green
	File Modification	Green	Green	Red	Green	Green	Red	Green	Green
User Account Activity	File Renaming	Green	Green	Green	Green	Green	Red	Red	Green
	Local Account Creation	Red	Green	Red	Green	Red	Red	Red	Green
	Local Account Modification	Red	Orange	Red	Green	Red	Red	Red	Green
	Local Account Deletion	Red	Green	Red	Green	Red	Red	Red	Green
	Account Login	Red	Green	Green	Green	Green	Red	Orange	Green
Network Activity	Account Logoff	Red	Green	Green	Green	Green	Red	Red	Red
	TCP Connection	Green	Green	Green	Green	Green	Red	Green	Green
	UDP Connection	Green	Green	Green	Red	Green	Red	Green	Green
	URL	Red	Green	Red	Green	Orange	Red	Orange	Green
Hash Algorithms	DNS Query	Green	Green	Green	Green	Green	Red	Green	Green
	File Downloaded	Red	Green	Orange	Orange	Red	Red	Orange	Green
	MD5	Green	Green	Green	Green	Green	Green	Green	Green
	SHA	Green	Green	Green	Green	Green	Green	Green	Green
	IMPHASH	Red	Red	Red	Red	Orange	Green	Red	Red
	Key/Value Creation	Green	Orange	Orange	Green	Green	Red	Green	Green

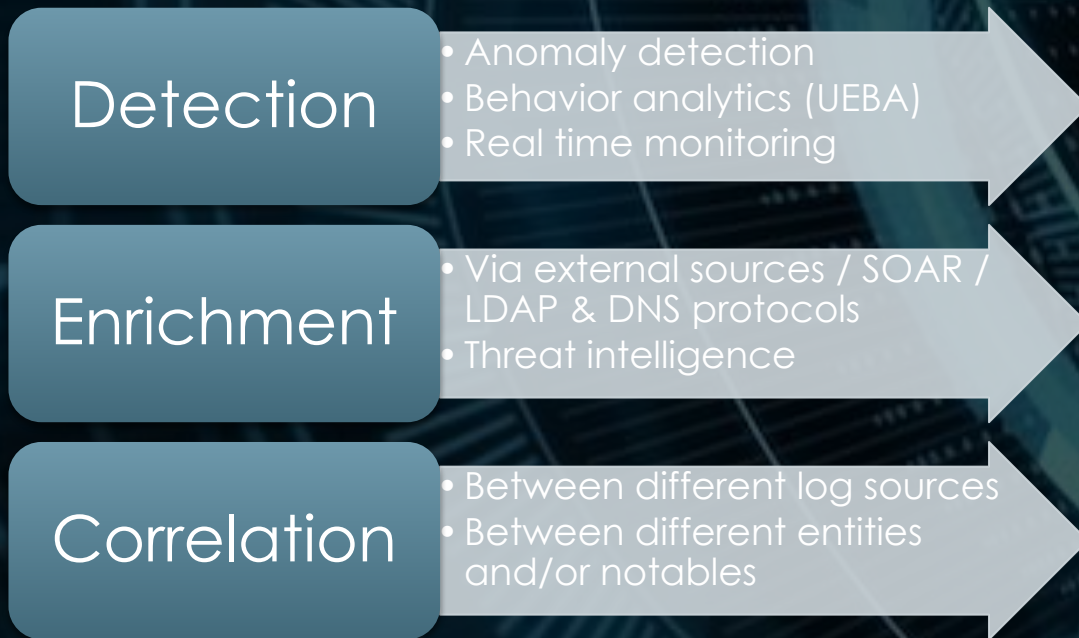
Source: 4688-Sysmon (Github project) – reprise99

Source: EDR telemetry (Github project) - Tsale



SIEM at the rescue

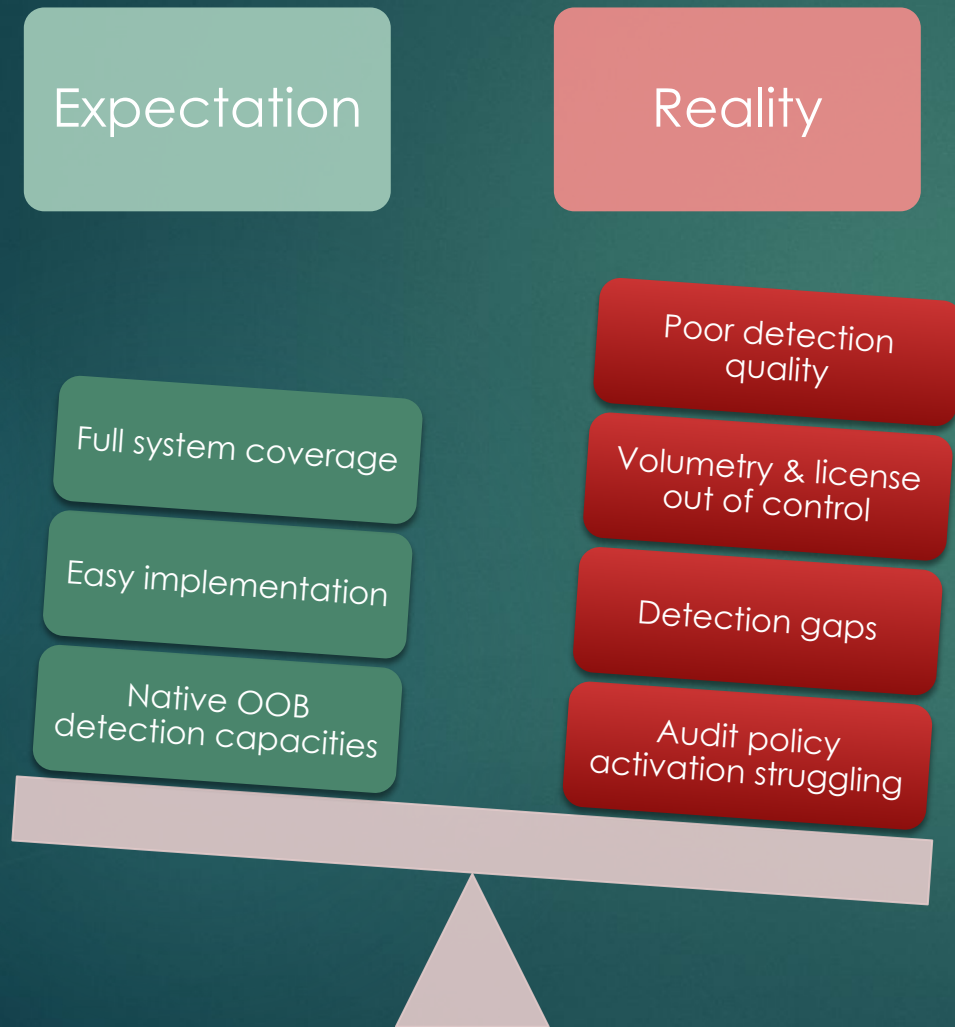
SIEM at a glance



Read and forward logs

SIEM implementation challenges

35



Buy a SIEM

Enable OOB detections

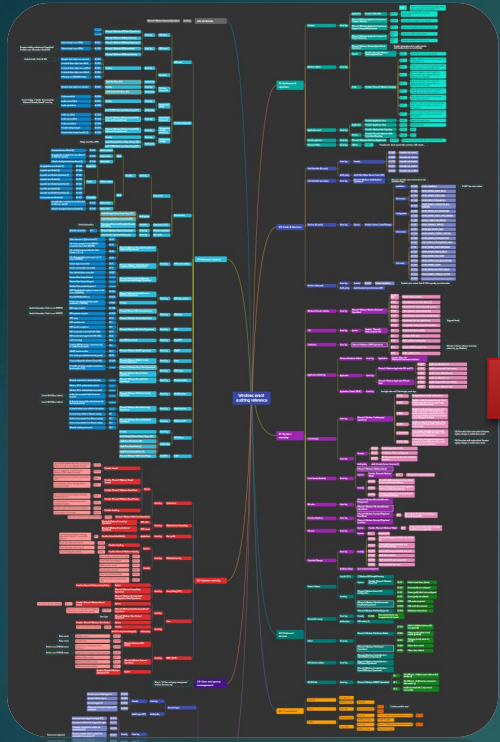
Tune detections down and keep engineers busy normalizing data

Add a MITRE stamp to each detection and deliver a kickass presentation to the board



imgflip.com

Log collection toolkit (Windows)



Category	Subcategory	Outcome	To collect	Event ID	Event Description	TTP ID	TTP Name
None	None	Yes	1100	Event logging service has shut down	11562.002	Disable Windows Event Logging	
		Yes	1101	Audit events have been dropped by the transport.	10770.001	Indicator Removal on Host	
		Yes	1102	Event log cleared	11562.002	Disable Windows Event Logging	
		Yes	1104	Security log is now full	11562.002	Disable Windows Event Logging	
		Yes	1105	Event log automatic backup	11562.002	Disable Windows Event Logging	
		Yes	1108	The event logging service encountered an error	11562.002	Disable Windows Event Logging	
		Success	4774	An account was mapped for logonsuccess			
		Success	4776	The computer attempted to validate the credentials for an account			
		Failure	4775	An account could not be mapped for logon			
		Failure	4774	An account was mapped for logon			
Account Logon	Audit Credential Validation	Success	4776	The computer attempted to validate the credentials for an11110	brutforce		
		Failure	4777	The domain controller failed to validate the credentials for an11110	brutforce		
		Yes	4822	NTLM authentication failed because the account was a me11078.002	Valid Accounts: Domain Accounts		
		Yes	4823	NTLM authentication failed because access control restrict11078.002	Valid Accounts: Domain Accounts		
		Success	4768	A Kerberos authentication ticket [TGT] was requested	11558	Steal or Forge Kerberos Tickets	
		Success/Noisy	4768	A Kerberos authentication ticket [TGT] was requested	11110	brutforce	
		Success	4771	Kerberos preauthentication failed	11110	brutforce	
		Failure	4772	A Kerberos authentication ticket request failed	11110	brutforce	
		Failure	4824	A Kerberos ticket granting ticket [TGT] was denied because11078.002	Valid Accounts: Domain Accounts		
		Failure	4824	Kerberos preauthentication by using DES or RC4 failed because11078.002	Valid Accounts: Domain Accounts		
Kerberos Service Ticket Operations	Kerberos Authentication Service	Success/Noisy	4769	A Kerberos service ticket was requested	11558	Steal or Forge Kerberos Tickets	
		Success	4770	A Kerberos service ticket was renewed	11558	Steal or Forge Kerberos Tickets	
		Success	4769	A Kerberos service ticket was requested	11558	Steal or Forge Kerberos Tickets	
		Success	4770	A Kerberos service ticket was renewed	11558	Steal or Forge Kerberos Tickets	
		Success	4769	A Kerberos service ticket was requested	11558	Steal or Forge Kerberos Tickets	
		Success	4770	A Kerberos service ticket was renewed	11558	Steal or Forge Kerberos Tickets	
		Success	4769	A Kerberos service ticket was requested	11558	Steal or Forge Kerberos Tickets	
		Success	4770	A Kerberos service ticket was renewed	11558	Steal or Forge Kerberos Tickets	
		Success	4769	A Kerberos service ticket was requested	11558	Steal or Forge Kerberos Tickets	
		Success	4770	A Kerberos service ticket was renewed	11558	Steal or Forge Kerberos Tickets	

Preconfigured group policy objects

Enable auditing

Increase log size

Enable disabled event logs

```

WinEventLog://Microsoft-Windows-Authentication/ProtectedUser-Client]
disabled = 0
whitelist = 104,304
# !!! EVENT LOG FILE DISABLED PER DEFAULT !!!
# ID 104: The security package on the client does not contain the credentials
# ID 304: The security package does not store the Protected User's credentials

[WinEventLog://Microsoft-Windows-Authentication/ProtectedUserFailures-Domain]
disabled = 0
whitelist = 100,104
# !!! EVENT LOG FILE DISABLED PER DEFAULT !!!
# ID 100: An NTLM sign-in failure occurs for an account that is in the Protected
# ID 104: DES or RC4 encryption types are used for Kerberos authentication

[WinEventLog://Microsoft-Windows-Authentication/ProtectedUserSuccesses-Domain]
disabled = 0
whitelist = 303
# !!! EVENT LOG FILE DISABLED PER DEFAULT !!!
# ID 303: A Kerberos ticket-granting-ticket (TGT) was successfully issued for

[WinEventLog://Microsoft-Windows-NTLM/Operational]
disabled = 0
whitelist = 8004
# ID 8004: Domain Controller Blocked Audit: Audit NTLM authentication to the

# -----
# Specific channels - RDP
# -----

[WinEventLog://Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational]
disabled = 0
whitelist = 104,131,140,168,169
# ID 104: Client timezone is [1] hour from UTC / MITRE TTP T1021.001 - Remote
# ID 131: The server accepted a new UDP/TCP connection from client [IP]:Port
# ID 140: Connection failed; bad username or password / MITRE TTP T1021
# ID 168: Connection failed; bad username or password / MITRE TTP T1021
# ID 169: Connection failed; bad username or password / MITRE TTP T1021
# ID 104: CTSSUC_CTRSSOUR_T2 [1] WORK_ALSOU_OIC \ WILSE_Lib_17831-007 - HWK

```

Source: Splunk Windows baseline
<https://github.com/mdecrevoisier/Splunk-input-windows-baseline>

Source: Microsoft eventlog mindmap
<https://github.com/mdecrevoisier/Microsoft-eventlog-mindmap>

Source: Microsoft auditing baseline
<https://github.com/mdecrevoisier/Windows-auditing-baseline>



Covers more than 70 different event logs with event ID description and MITRE ATT&CK mapping: Exchange, MS SQL, Bitlocker, DNS Server, IIS, RDP, WinRM, WMI, ADFS, Winsock, Office ...



Source: SIGMA detection rules
<https://github.com/mdecrevoisier/SIGMA-detection-rules>

Struggling with log volume/EPS?



37

Apply noise reduction

Use SYSMON

Use different collecting baselines « full / light »

• Enable the « triggering vs attesting approach »

- Enable new type of detections
- Extend log collection perimeter (if restricted)
- Increase detection for offensive action against EDR



Collecting baseline strategy

38

Full collecting baseline

- ▶ Process execution
- ▶ Powershell (modern)
- ▶ Login (success and failures)
- ▶ Kerberos (success and failure)
- ▶ + *light baseline* (aka « triggering VS attesting events »)

Light collecting baseline

- ▶ RDP activity + denied access
- ▶ Failed logins, success login (interactive, RDP, Pass the hash)
- ▶ Service & task creation
- ▶ Local user & groups
- ▶ SSH/WinRM authentication
- ▶ Server roles: SQL Server, ADFS, ADCS/PKI, NPS, Exchange, IIS
- ▶ Misc: drivers, Bitlocker, Printer, Firewall configuration, BITS, WMI, Defender (threats), VHD/ISO, audit policy change, event log, password reset/lockout, AppLocker ...
- ▶ Process exec with focus on LOLBINS

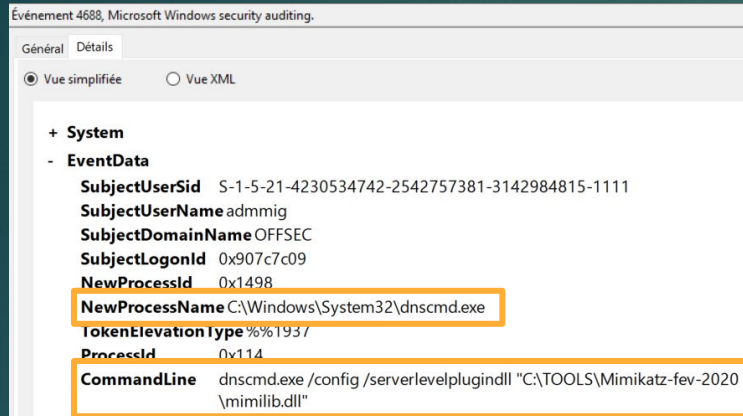


DC: ~1-2GB
Server: ~300-700MB
(per day)

Server: <5MB
(per day)

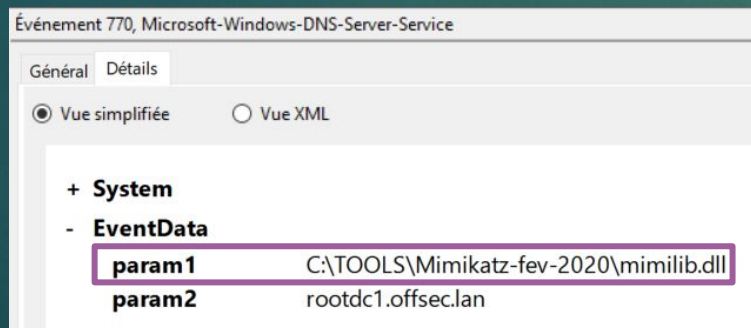
Server: ~20-50MB
(per day)

Triggering vs attesting events



Event log: Security.evtx

T1574.002: Hijack Execution Flow: DLL Side-Loading



Event log: DNS Server.evtx

Triggering

Good security context and documentation

Provides a larger scope of TIP coverage

Risk of detection failure due to improper detection, auditing or obfuscation

Do not confirm triggering actions at 100%

Auditing configuration required

Attesting

Poor structure and lack of documentation

Some event log are disabled per default

Attest with high probability results from triggering actions

Nearly no auditing configuration required

Lighter detection queries (hardware)

Increasing visibility with hidden treasures

40

MITRE | ATT&CK™



T1574.002 - Hijack Execution Flow:
DLL Side-Loading

PrintNightmare vulnerability

ID 321 | 354 | 808 (Printer)

T1048 - Exfiltration Over Alternative
Protocol

BITS client activity

ID 59-60 (BITS client)

T1574.002 - Hijack Execution Flow:
DLL Side-Loading

DNS DLL server plugin load

ID 150 | 770 (DNS Server)

T1505.004 - Server Software
Component: IIS Components

New IIS module loaded

ID 29 (IIS Operational)

T1505.002 - Server Software
Component: Transport Agent

New transport agent deployed

ID 1 | 6 (Exchange Mgmt)

T1562.004 - Impair Defenses:
Disable or Modify System Firewall

New "any/any" firewall rule

ID 2004 | 2005 (Advanced Firewall)

T1543.003 - Create or Modify
System Process: Windows Service

New service installed

ID 4697 (Security) / 7045 (System)

Increasing visibility for EDR tampering

41



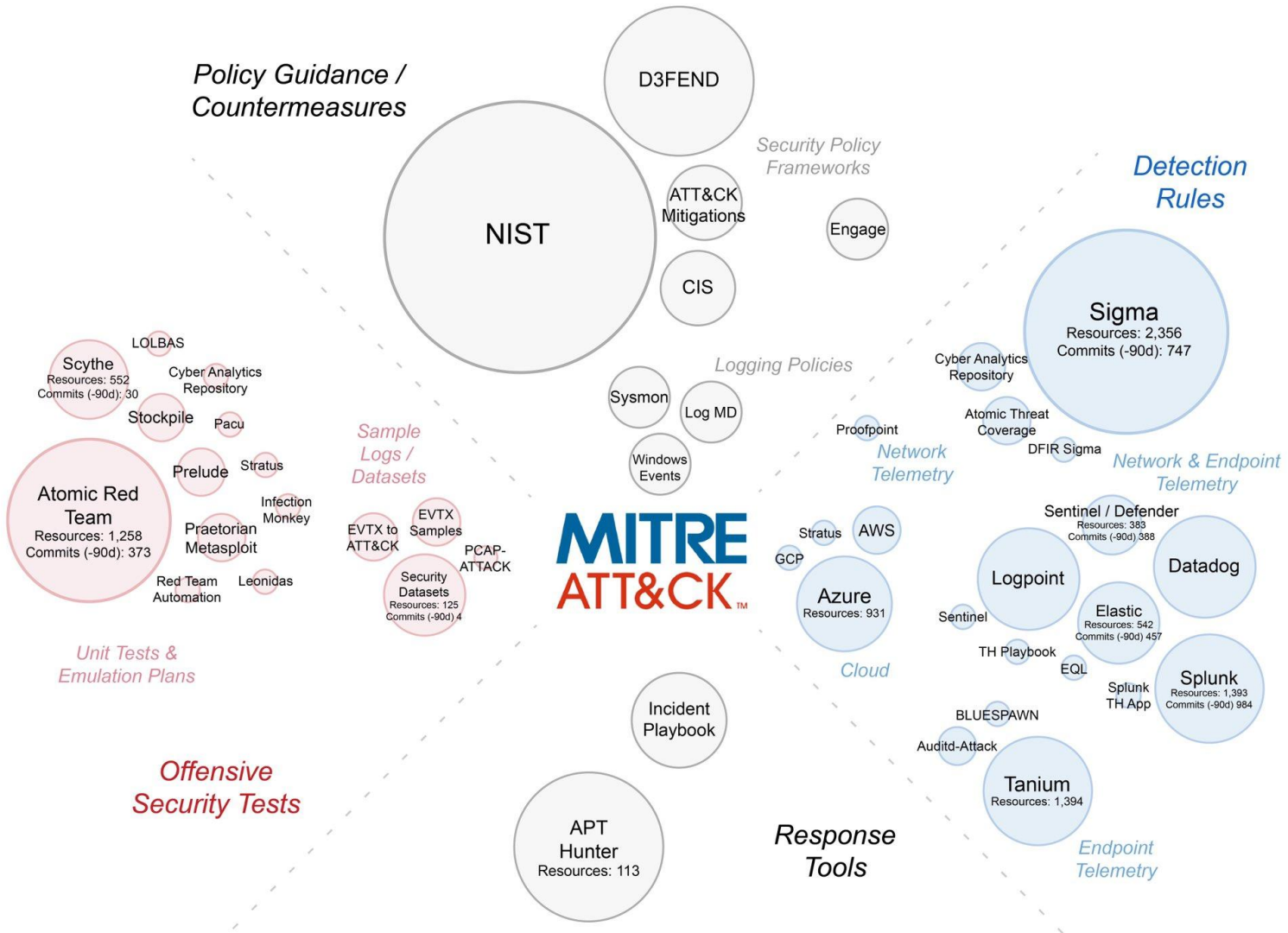
Approach	Threat	TTP ID		Event log	Event ID	ID Desc
Avoiding EDR	Evasion	T1090	Proxy	WinINet-Config	5600	Proxy config. Changed
		T1572	Protocol Tunneling (eg: via RDP)	Terminal Services	1149	User authentication succeeded
Tampering EDR	BYOVD	T1068	Privilege escalation	SYSMON	6	Driver load
		T1543.00	Create or Modify a Windows Service	Security/System	4697/7045	Service creation
	DLL sideloading	T1574.002	Hijack Execution Flow: DLL Side-Loading	SYSMON	7	Image load
	AMSI	T1562.001	Impair Defenses: Disable or Modify Tools	SYSMON	7	Image load
				SYSMON	13/14	Registry events
	Defender bypass/ tampering	T1562.001	Impair Defenses: Disable or Modify Tools	Defender	5007	Exclusion
				SYSMON	13/14	Registry events
				Defender	3002	Protection failure
	Defender	T1562.001	Impair Defenses: Disable or Modify Tools	Defender	5004	Configuration change
				SYSMON	13/14	Registry events
	ETW bypass	T1562.006	Impair Defenses: Indicator Blocking	SYSMON	13/14	Registry events
	NG wiper/symlink	T1547.009	Boot or Logon Autostart : Shortcut modif.	SYSMON	11	File creation
SYSMON/Security				1/4688	Process execution	
Security				4664	Hard link creation	
LOLBINS	T1218	System Binary Proxy Execution	SYSMON/Security	1/4688	Process execution	
	T1127	Trusted dev Utilities Proxy exec.	Application:MsilInstaller	11707	Product installed	
WSL	T1564.006	Hide Artifacts: Run Virtual Instance	Setup:Windows-Servicing	9	New package turned on	
Blending EDR	Replicate company tools	T1021.001	Remote services: RDP	Terminal Services	131	Connection from <ip>
				Terminal Services	1149	User authentication succeeded
		T1021.004	Remote Services: SSH	OpenSSH	4	SSH server listening on
Configuration	Config. extraction	T1518.001	Security Software Discovery	SYSMON/Security	1/4688	Process execution

Detection validation

ASSESSING YOUR DEFENSES

Control Validation Resource Ecosystem

Public resources aligned with common descriptions of adversary behavior (MITRE ATT&CK)



Control validation resource ecosystem

Source: Control Compass – May 2022

EDR assessment tools



Atomic Red team
(Red Canary)



Attack range
(Splunk)

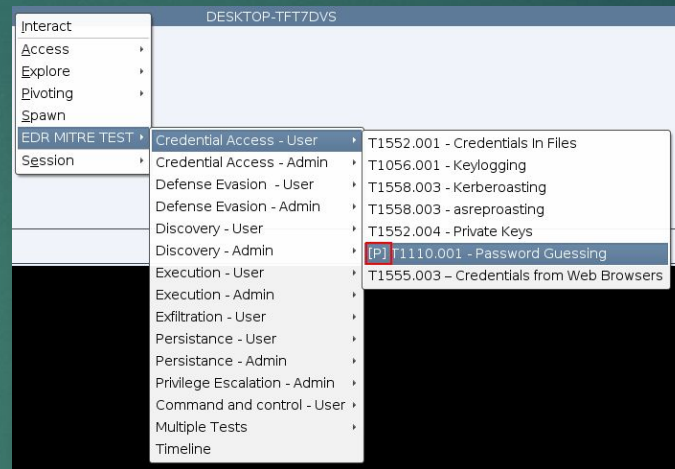


APT Simulator
(Nextron)

Caldera
(MITRE)



Threatest
(Datadog)

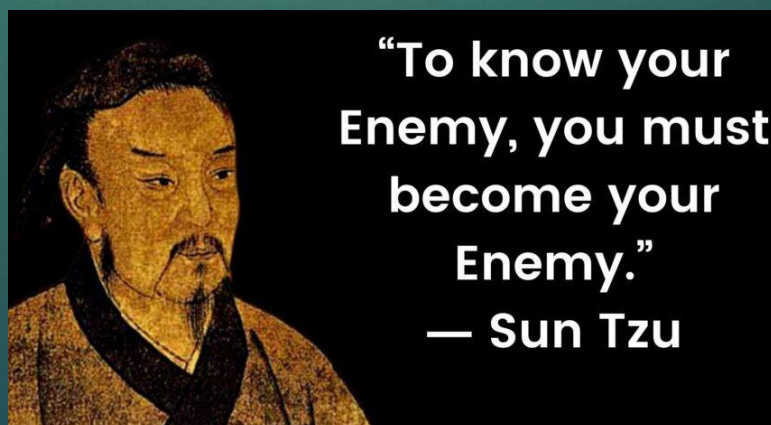


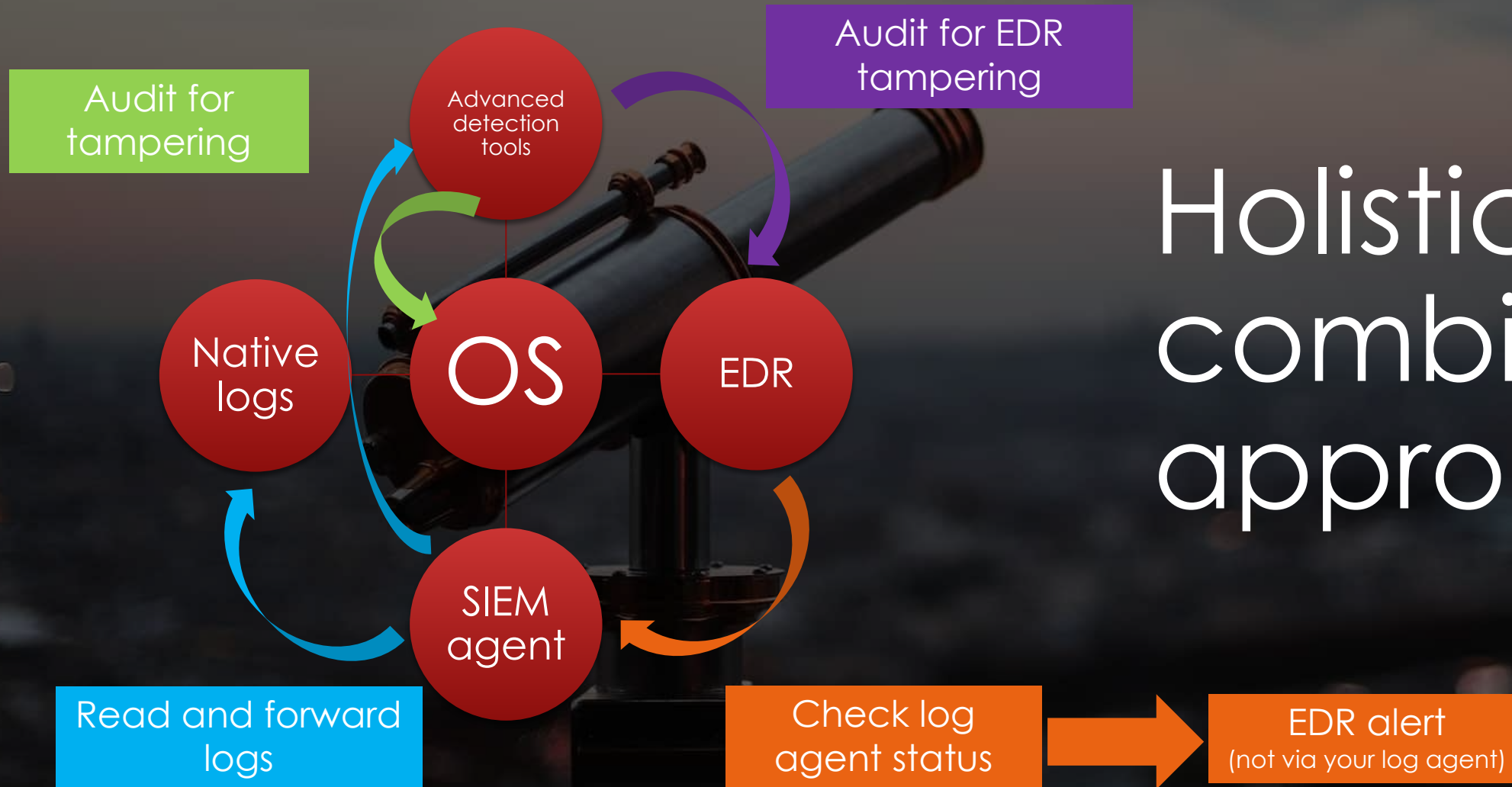
EDR-test

- A good alternative to Atomic Red Team not using PowerShell

Pyramid

- Perform offensive tasks by leveraging Python evasion techniques





Holistic and combined approach

BlackMamba: a polymorphic threat

46

“Exploits large language model to synthesize polymorphic keylogger functionality on-the-fly, dynamically modifying the benign code at runtime - all without any command-and-control infrastructure.”

BACK
TO THE FUTURE

Source: Blackmamba, using AI to generic polymorphic malware - HYAS - Mars 2023

BlackMamba: a polymorphic threat

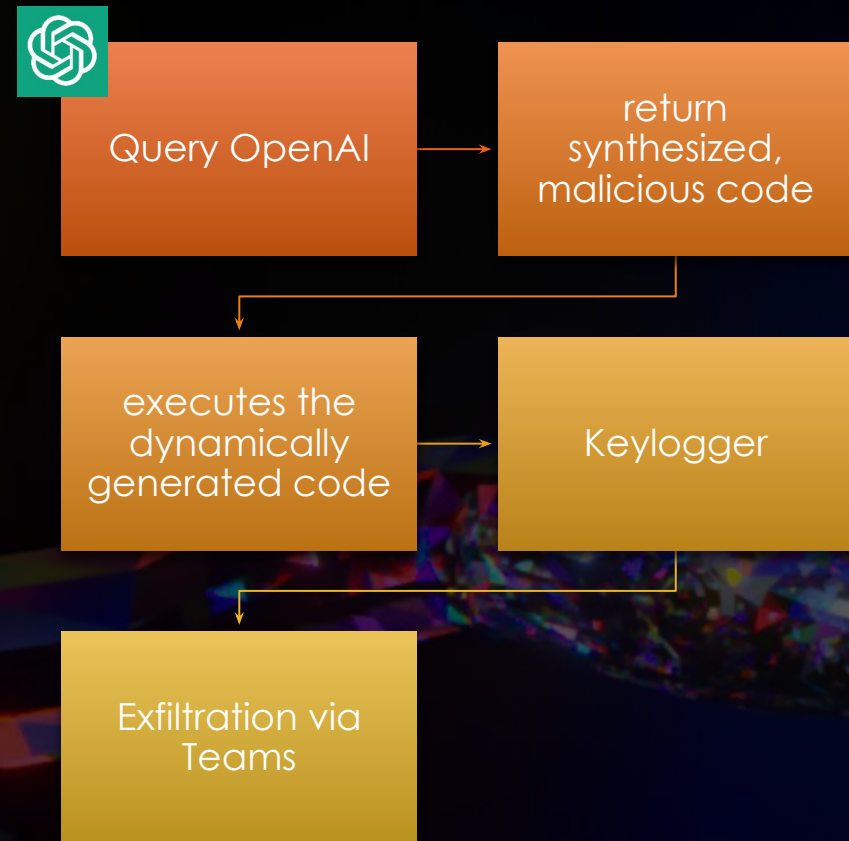
47

C2 removal

- intelligent automation and attacker-bound data through a benign communication channel

Leverage AI code

- synthesize new malware variants, by changing the code and evade detection algorithms.



BACK
TO THE FUTURE

Source: Blackmamba, using AI to generic polymorphic malware - HYAS - Mars 2023

Thank you!

