Crowdsourcing Microsoft Defender coverage

Questionable insights and some rabbit holes

Olaf Hartong

Detection Engineer and Security Researcher

- Purple teaming, Threat hunting
- Security MVP

Former documentary photographer
Father of 2 boys
“I like **warm hugs**”

@olafhartong
github.com/olafhartong
olaf@falconforce.nl
olafhartong.nl / falconforce.nl

SentinelOne Blog

EN

Microsoft | Microsoft Security

Solutions Products Services Partners Resources Contact Sales Start free trial

All Microsoft Search Light Dark

Blog home / Analyst reports

Search the blog

News Analyst reports Microsoft Defender XDR 8 min read

Microsoft 365 Defender demonstrates 100 percent protection coverage in the 2023 MITRE Engenuity ATT&CK® Evaluations: Enterprise

By Tanmay Ganacharya, Partner Director, Security Research, Microsoft 365 Defender

September 20, 2023

Microsoft Defender

Microsoft Defender for Endpoint

Microsoft 365 Defender is now Microsoft Defender XDR. Learn more.

For the fifth consecutive year, Microsoft 365 Defender demonstrated industry-leading extended detection and response (XDR) capabilities in the independent MITRE Engenuity ATT&CK® Evaluations: Enterprise. The attack used during the test highlights the importance of a unified XDR platform and showcases Microsoft 365 Defender as a leading solution, enabled by next-generation protection, industry-first capabilities like automatic attack disruption, and more.

Microsoft 365 Defender demonstrated 100 percent visibility and complete coverage across all stages of the attack and achieved 100 percent protection across both Windows and Linux, showcasing the strong multiplatform capabilities of the solution. These results demonstrate that Microsoft's XDR provides organizations with industry-leading visibility and protection in a world of evolving threats.

CROWDSTR

CrowdSt
100% Vis
MITRE E
Enterpris

September 20, 2023 Mic

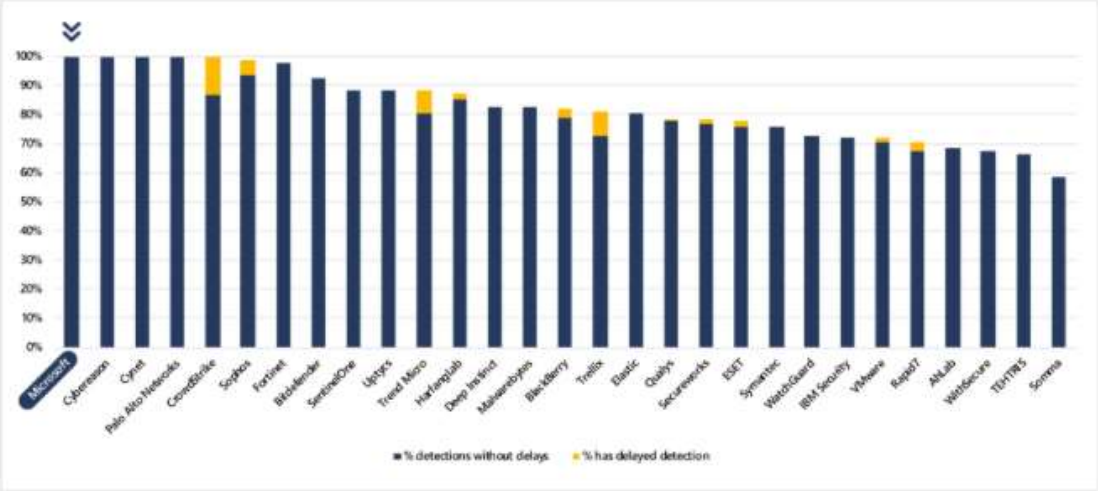
MIT


HE GETS A MITRE ATT&CK SCORE OF 100%
SHE GETS A MITRE ATT&CK SCORE OF 100%
THEY GET A MITRE ATT&CK SCORE OF 100%
EVERYBODY GETS A MITRE ATT&CK SCORE OF 100%
imgflip.com

100 percent visibility across all stages of the attack chain in real-time

In the face of a rapidly evolving threat carried out by adversaries like Turla, the speed of response makes a significant difference in a security team's effectiveness in mitigating an attack. A single delay can mean the difference of your organization's devices getting encrypted or not. Microsoft 365 Defender's XDR platform accelerates the security team's ability to respond by providing real-time, unparalleled breadth and depth of understanding an attack, starting with 100 percent visibility in real-time. This unique breadth of Microsoft's XDR extends across **endpoints, network, hybrid identities, email, collaboration tools, software as a service (SaaS) apps, and data** with centralized visibility, powerful analytics, and automatic attack disruption.

Visibility across the attack



warmhugs

Microsoft Defender

Search

Device inventory > castelblack

castelblack

No known risks Criticality: None

View in map | Device value

Overview | Incidents and alerts | Timeline | Security policies | Security recommendations | Inventories | Discovered vulnerabilities | Missing KBs | Security baselines

Apr 2024 | May 2024 | Jun 2024 | Jul 2024 | Aug 2024

Maximize

Export | Search | 30 Days | Customize columns | Filter

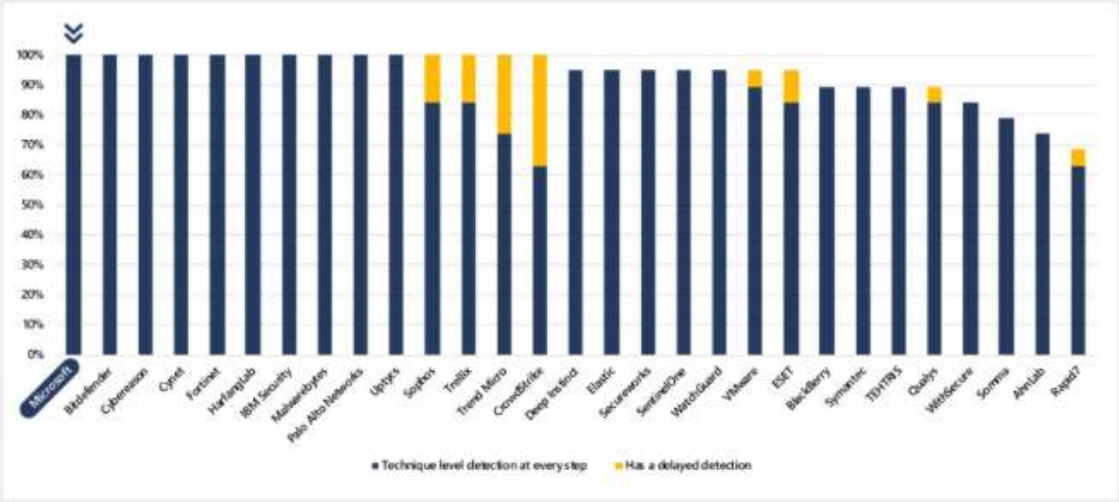
Event time	Event	Additional information	User	Enti
14 Aug 2024 20:21:36.424	Network logon by north\robb.stark from 192.168.56.11:54805 succeeded			nor
14 Aug 2024 20:21:36.423	NORTH.SEVENKINGDOMS.LOCAL\robb.stark signed into a Windows doma...	T1078.002: Domain Accounts	NORTH.SEVENKINGDOMS.LOCAL\robb.stark	NO
14 Aug 2024 20:21:36.423	Network logon by north\robb.stark from 192.168.56.11:54803 succeeded			nor
14 Aug 2024 20:21:36.423	NORTH.SEVENKINGDOMS.LOCAL\robb.stark signed into a Windows doma...	T1078.002: Domain Accounts	NORTH.SEVENKINGDOMS.LOCAL\robb.stark	NO
14 Aug 2024 20:21:36.423	Network logon by north\robb.stark from 192.168.56.11:54804 succeeded			nor
14 Aug 2024 20:21:36.421	NORTH.SEVENKINGDOMS.LOCAL\robb.stark signed into a Windows doma...	T1078.002: Domain Accounts	NORTH.SEVENKINGDOMS.LOCAL\robb.stark	NO
14 Aug 2024 20:21:36.421	Network logon by north\robb.stark succeeded			nor
14 Aug 2024 20:21:36.411	NORTH.SEVENKINGDOMS.LOCAL\robb.stark signed into a Windows doma...	T1078.002: Domain Accounts	NORTH.SEVENKINGDOMS.LOCAL\robb.stark	NO
14 Aug 2024 20:21:36.411	Network logon by north\robb.stark from 192.168.56.11:54802 succeeded			nor
14 Aug 2024 20:21:29.208	A PowerShell interpreter process was launched by SenseIR.exe	T1059.001: PowerShell +1	NT AUTHORITY\system	ser
14 Aug 2024 20:21:24.968	taskhostw.exe created file energy-report.html		nt authority\system	svc
14 Aug 2024 20:21:22.907	svchost.exe created process WmiPrvSE.exe		nt authority\system	ser
14 Aug 2024 20:21:19.322	appidcertstorecheck.exe created process conhost.exe		nt authority\local service	svc
14 Aug 2024 20:21:19.288	svchost.exe created process rundll32.exe		nt authority\system	ser
14 Aug 2024 20:21:19.288	svchost.exe created process appidcertstorecheck.exe		nt authority\system	ser
14 Aug 2024 20:20:36.854	Unknown process received a TCP connection acknowledged request from 19...			192
14 Aug 2024 20:20:36.854	Unknown process received a TCP connection acknowledged request from 19...			192
14 Aug 2024 20:20:36.853	Unknown process received a TCP connection acknowledged request from 19...			192
14 Aug 2024 20:20:36.851	Unknown process received a TCP connection acknowledged request from 19...			192
14 Aug 2024 20:20:36.412	NORTH.SEVENKINGDOMS.LOCAL\robb.stark signed into a Windows doma...	T1078.002: Domain Accounts	NORTH.SEVENKINGDOMS.LOCAL\robb.stark	NO
14 Aug 2024 20:20:36.412	Network logon by north\robb.stark succeeded			nor
14 Aug 2024 20:20:36.399	NORTH.SEVENKINGDOMS.LOCAL\robb.stark signed into a Windows doma...	T1078.002: Domain Accounts	NORTH.SEVENKINGDOMS.LOCAL\robb.stark	NO

Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Learning hub
Trials
Partner catalog
Exposure management
Overview
Attack surface
Exposure insights
Secure score
Data connectors
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Identities
Dashboard
Health issues
Tools
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker

100 percent ATT&CK technique-level detections at every attack stage without delay

As an attack unfolds, security teams need to know what they're up against the moment it's happening. Delayed and incomplete detections make it difficult for analysts to understand the attack in full, providing attackers an opportunity escalate their campaign by moving laterally, stealing credentials, or executing other malicious activities. With Microsoft 365 Defender's 100 percent real-time ATT&CK technique-level coverage, analysts immediately receive relevant details within the alert that describe the attacker's approach, equipping them with the knowledge to effectively and rapidly respond.

Technique level detections at every major step



warmhugs

Microsoft Defender

Home
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Threat intelligence

Collapse Navigation · Suspicious User Account Discovery

Part of incident: Multi-stage incident involving Initial access & Discovery on one endpoint reported by multiple sources. View incident page

workstation · Risk level Medium · Windows10

SEVENKINGDOMS\tywin.lannister

Suspicious User Account Discovery
Low · Detected · New

Manage alert · See in timeline · Tune alert

Alert story · Maximize

Details · Recommendations

Exposure management
Overview
Attack surface
Exposure insights
Secure score
Data connectors

Assets
Devices
Identities

Endpoints
Vulnerability management
Partners and APIs
Configuration management

Identities
Dashboard
Health issues

17:23:16	SharpHound.exe loaded a .NET assembly in memory	Remote execution		
	Suspicious User Account Discovery	Low	Detected	New
	Suspicious System Network Configuration Discov...	Low	Detected	New
	Suspicious System Network Connections Discover...	Low	Detected	New
17:23:16	SharpHound.exe loaded a .NET assembly in memory	Remote execution		
17:23:16	SharpHound.exe ran an LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New
17:23:16	SharpHound.exe performed an exploratory LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New
17:23:16	SharpHound.exe ran an LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New
17:23:16	SharpHound.exe performed an exploratory LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New
17:23:16	SharpHound.exe performed an exploratory LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New

Classify alert

Alert state

Classification: Not Set
Set Classification

Assigned to: Unassigned

Alert details

Category: Discovery

MITRE ATT&CK Techniques: T1033: System Ow... +1 More
View all techniques

Detection source: EDR

Service source: Microsoft Defender for Endpoint

Detection status: Detected

Detection technology: Amsi,Behavior,Network

Generated on: 9 Mar 2024 17:25:10

First activity: 9 Mar 2024 17:22:37

Last activity: 9 Mar 2024 17:23:16

Investigations
Explorer
Review
Campaigns
Threat tracker

17:23:16	SharpHound.exe ran an LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New
17:23:16	SharpHound.exe ran an LDAP query	Remote execution		
	Suspicious LDAP query	Medium	Detected	New
17:23:16	SharpHound.exe performed user account discovery	Remote execution		

Entity Name · Remediation Status · Verdict

powershell.exe (PID: 10...
SharpHound.exe (PID: ...
192.168.1.34

Alert description

warmhugs Microsoft Defender

Alerts > Bloodhound post-exploitation tool was detected (Agentless)

Part of incident: Bloodhound post-exploitation tool was detected (Agentless) on one endpoint View incident page

goad-vm-dc03
Virtual Machine

Bloodhound post-exploitation tool was detected (Agentless)
High | Unknown | New

Manage alert | Link alert to another incident

Alert story | Maximize

13/8/2024
08:03:23

Bloodhound post-exploitation tool was detected (Agentless) on a cloud resource

TenantId	e52fd1d3-fa9f-46b5-9d65-a6232fe98978
Machine Name	goad-vm-dc03
Threat Information	VirTool:MSIL/SharpHound.A HackTool:PowerShell/SharpHound.B
Threat Category	Tool
EffectiveAzureResourceId	/subscriptions/1bfbec58-e3d7-42cb-8d4f-0ee9bd04bee6/resourceGroups/GOAD/providers/Microsoft.Compute/virtualMachines/goad-vm-dc03
CompromisedEntity	goad-vm-dc03
ProductComponentName	Servers
EffectiveSubscriptionId	1bfbec58-e3d7-42cb-8d4f-0ee9bd04bee6

Alert state

Classification: Not Set
Set Classification

Assigned to: Unassigned

Alert details

Category: Execution

MITRE ATT&CK Techniques: -

Detection source: Microsoft Defender for Servers

Service source: -

Generated on: 13 Aug 2024 08:03:44

First activity: 13 Aug 2024 08:03:23

Last activity: 13 Aug 2024 08:03:23

Last activity
13 Aug 2024 08:03:23

Evidence

Entity Name	Remediation Status	Verdict
sharphound-v2.4.1.zip		Suspicious

SOFTWARE

- BloodHound
- BLUELIGHT
- Bonadan
- BONDUPDATER
- BoomBox
- BOOSTWRITE
- BOOTRASH
- BOULDSPY
- BoxCaon
- BrainTest
- BRATA
- Brave Prince
- Bread
- Briba
- Brute Ratel C4
- BS2005
- BUBBLEWRAP
- build_downer
- Bumblebee
- Bundlore
- BUSHWALK
- BusyGasper
- Cachedump
- CaddyWiper
- Cadelspy
- CALENDAR
- Calisto

BloodHound

BloodHound is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.[1][2][3][4]

ID: S0521
Type: TOOL
Platforms: Windows
Version: 1.5
Created: 28 October 2020
Last Modified: 09 August 2023

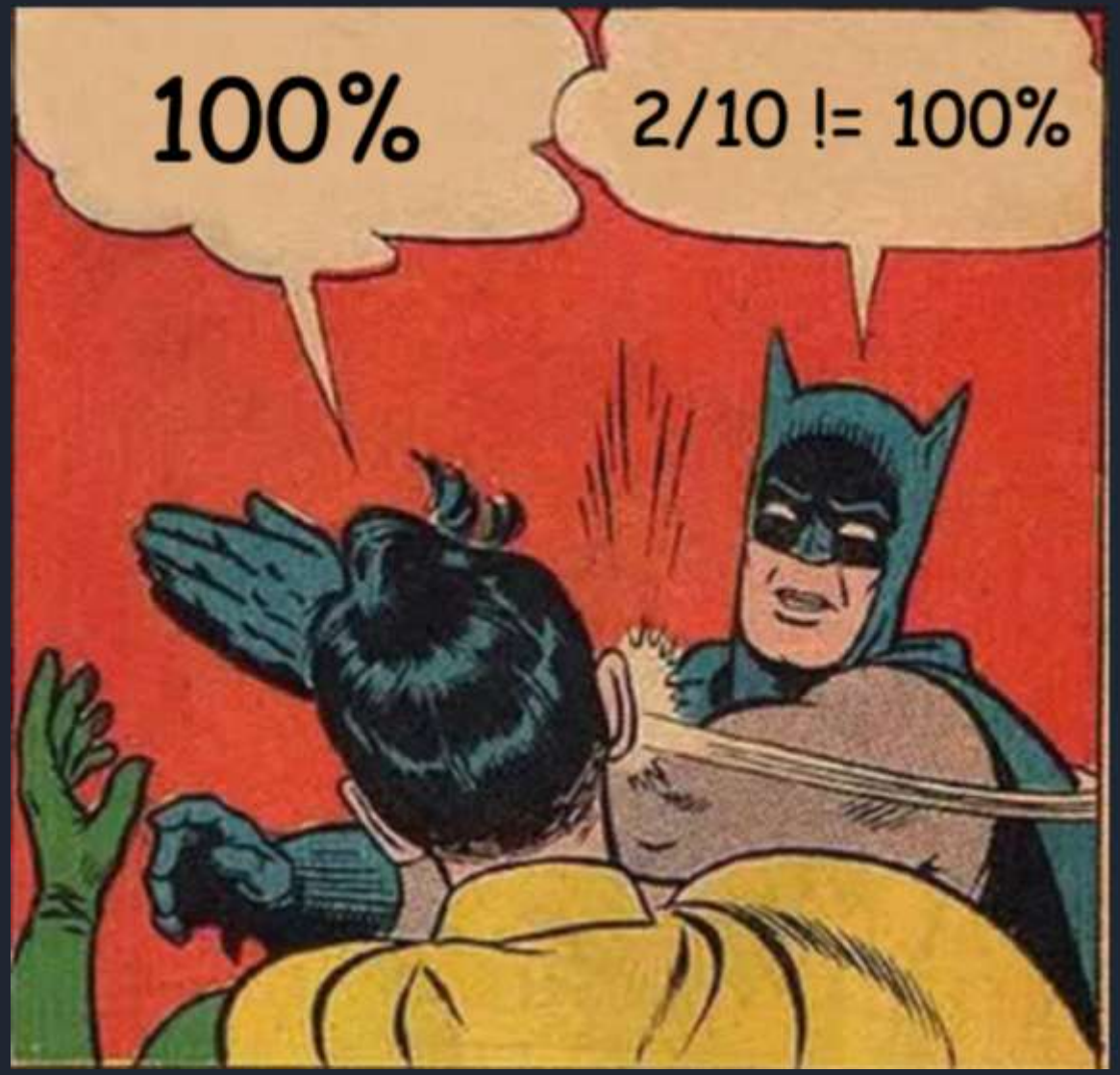
Version Permalink

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	BloodHound can identify users with local administrator rights.[2]
		.002	Account Discovery: Domain Account	BloodHound can collect information about domain users, including identification of domain admin accounts.[2]
Enterprise	T1560		Archive Collected Data	BloodHound can compress data collected by its SharpHound ingestor into a ZIP file to be written to disk.[1][4]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	BloodHound can use PowerShell to pull Active Directory information from the target environment.[2]
Enterprise	T1482		Domain Trust Discovery	BloodHound has the ability to map domain trusts and identify misconfigurations for potential abuse.[2]
Enterprise	T1615		Group Policy Discovery	BloodHound has the ability to collect local admin information via GPO.[1]
Enterprise	T1106		Native API	BloodHound can use .NET API calls in the SharpHound ingestor component to pull Active Directory data.[1]
Enterprise	T1201		Password Policy Discovery	BloodHound can collect password policy information on the target environment.[2]
Enterprise	T1069	.001	Permission Groups Discovery: Local Groups	BloodHound can collect information about local groups and members.[3]
		.002	Permission Groups Discovery: Domain Groups	BloodHound can collect information about domain groups and members.[3]
Enterprise	T1018		Remote System Discovery	BloodHound can enumerate and collect the properties of domain computers, including domain controllers.[2]
Enterprise	T1033		System Owner/User Discovery	BloodHound can collect information on user sessions.[2]

Tried to do the math



Curious, what is it covering?

Built some basic KQL, with that output I wanted to:

- Gather out of the box detections, with their technique mappings
- Get this from as many environments as possible
- Analyze it to understand the real life coverage

KQLHunter

```
AlertInfo
| where Timestamp > ago(30d)
| join AlertEvidence on AlertId
| extend Techniques=parse_json(AttackTechniques)
| where DetectionSource != "Custom detection"
| mv-expand Techniques
```

Title	DetectionSource	Techniques	Timestamp	Category	Severity	AttackTechniques
Multiple VM creation activiti...	Cloud App Security	Resource Hijacking (T1496)	2024-08-28T12:35:43.328Z	Impact	Low	["Resource Hijacking (T149...
An active 'Mythagent' malw...	Antivirus		2024-07-31T07:24:59.0008...	Malware	Low	
An active 'Mythagent' malw...	Antivirus		2024-07-31T07:24:59.0041...	Malware	Low	
A process was injected with...	EDR	Process Injection (T1055)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
A process was injected with...	EDR	Dynamic-link Library Injection (T1055.001)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
A process was injected with...	EDR	Portable Executable Injection (T1055.002)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
A process was injected with...	EDR	Thread Execution Hijacking (T1055.003)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
A process was injected with...	EDR	Asynchronous Procedure Call (T1055.004)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
A process was injected with...	EDR	Process Hollowing (T1055.012)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
A process was injected with...	EDR	PowerShell (T1059.001)	2024-07-29T13:57:19.11386...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process launch ...	EDR	Rundll32 (T1218.011)	2024-07-29T13:57:27.41101...	DefenseEvasion	Medium	["Rundll32 (T1218.011)"]
Suspicious process injectio...	EDR	Process Injection (T1055)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process injectio...	EDR	Dynamic-link Library Injection (T1055.001)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process injectio...	EDR	Portable Executable Injection (T1055.002)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process injectio...	EDR	Thread Execution Hijacking (T1055.003)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process injectio...	EDR	Asynchronous Procedure Call (T1055.004)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process injectio...	EDR	Thread Local Storage (T1055.005)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Suspicious process injectio...	EDR	Process Hollowing (T1055.012)	2024-07-29T14:23:36.058...	DefenseEvasion	Medium	["Process Injection (T1055)"...
Unusual number of failed si...	EDR		2024-07-30T08:13:27.6770...	CredentialAccess	Medium	
Process memory dump	EDR	OS Credential Dumping (T1003)	2024-08-05T00:34:45.542...	SuspiciousActivity	High	["OS Credential Dumping (T...
Process memory dump	EDR	Credentials from Password Stores (T1555)	2024-08-05T00:34:45.542...	SuspiciousActivity	High	["OS Credential Dumping (T...

KQLHunter

```
AlertInfo
| where Timestamp > ago(180d)
| join AlertEvidence on AlertId
| extend Techniques=parse_json(AttackTechniques)
| where DetectionSource != "Custom detection"
| mv-expand Techniques
| summarize arg_min(Timestamp,*) by Title, DetectionSource, tostring(Techniques)
| project Timestamp,Title,DetectionSource,Techniques
| where isnotempty( Techniques)
```

Timestamp	Title	DetectionSource	TechniqueId	TechniqueName
2024-08-28T12:35:43.328Z	Multiple VM creation activities	Cloud App Security	T1496	Resource Hijacking
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1055	Process Injection
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1055.001	Dynamic-link Library Injection
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1055.002	Portable Executable Injection
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1055.003	Thread Execution Hijacking
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1055.004	Asynchronous Procedure Call
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1055.012	Process Hollowing
2024-07-29T13:57:19.113865Z	A process was injected with potentially malicious code	EDR	T1059.001	PowerShell
2024-07-31T07:24:57.3753819Z	A process was injected with potentially malicious code	EDR	T1620	Reflective Code Loading
2024-07-31T08:57:02.6986435Z	Suspicious User Account Discovery	EDR	T1033	System Owner/User Discovery
2024-07-31T08:57:02.6986435Z	Suspicious User Account Discovery	EDR	T1059.001	PowerShell
2024-07-31T08:57:02.6986435Z	Suspicious User Account Discovery	EDR	T1087.001	Local Account
2024-07-31T08:57:02.6986435Z	Suspicious User Account Discovery	EDR	T1620	Reflective Code Loading
2024-07-29T13:57:27.4110116Z	Suspicious process launch by Rundll32.exe	EDR	T1218.011	Rundll32
2024-07-29T14:23:36.0584848Z	Suspicious process injection observed	EDR	T1055	Process Injection
2024-07-29T14:23:36.0584848Z	Suspicious process injection observed	EDR	T1055.001	Dynamic-link Library Injection

2024-08-05T00:34:45.5425905Z	Process memory dump	EDR	T1003	OS Credential Dumping
2024-08-05T00:34:45.5425905Z	Process memory dump	EDR	T1555	Credentials from Password Stores
2024-08-05T00:34:45.5428465Z	Anomaly detected in ASEP registry	EDR	T1112	Modify Registry
2024-08-05T00:34:45.5428465Z	Anomaly detected in ASEP registry	EDR	T1547.001	Registry Run Keys / Startup Folder

KQL, with some data extension

...and sort of make all the MS product renames sensible

```
SecurityAlert
| where TimeGenerated > ago(180d)
| extend Techniques=parse_json(Techniques)
| where ProviderName in ("MDATP", "MCAS", "IPC", "Azure Advanced Threat Protection", "MicrosoftThreatProtection")
| where AlertType != "CustomDetection"
| mv-expand Techniques
| where isnotempty( Techniques)
| extend DetectionSource = case(AlertType == "WindowsDefenderAtp","EDR",
                                AlertType == "WindowsDefenderAv", "Antivirus",
                                AlertType == "MTP","EDR",
                                ProviderName == "MicrosoftThreatProtection", "M365D",
                                ProviderName == "MCAS", "CloudApp",
                                ProviderName == "Azure Advanced Threat Protection", "Defender for Cloud",
                                ProviderName == "IPC","Entra Identity Protection", "?" )
| where not(AlertType matches regex @"(\w{8}-\w{4}-\w{4}-\w{4}-\w{12})")
| distinct Title=DisplayName, TechniqueId=tostring(Techniques), AlertType, DetectionSource
```

I asked a lot of trusted people to share

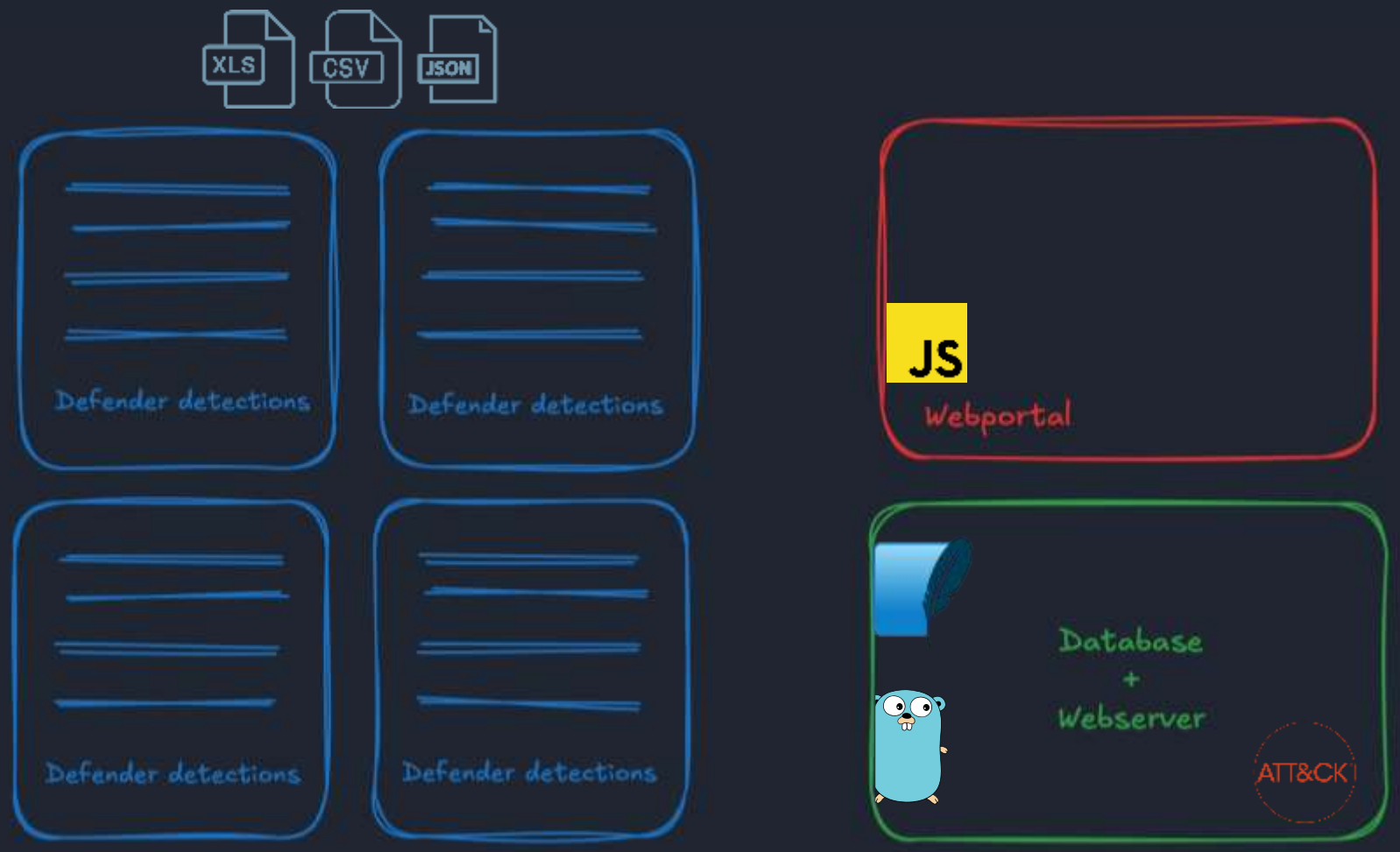
Received data from ~ 1500 tenants (over time)

What to do with all this data

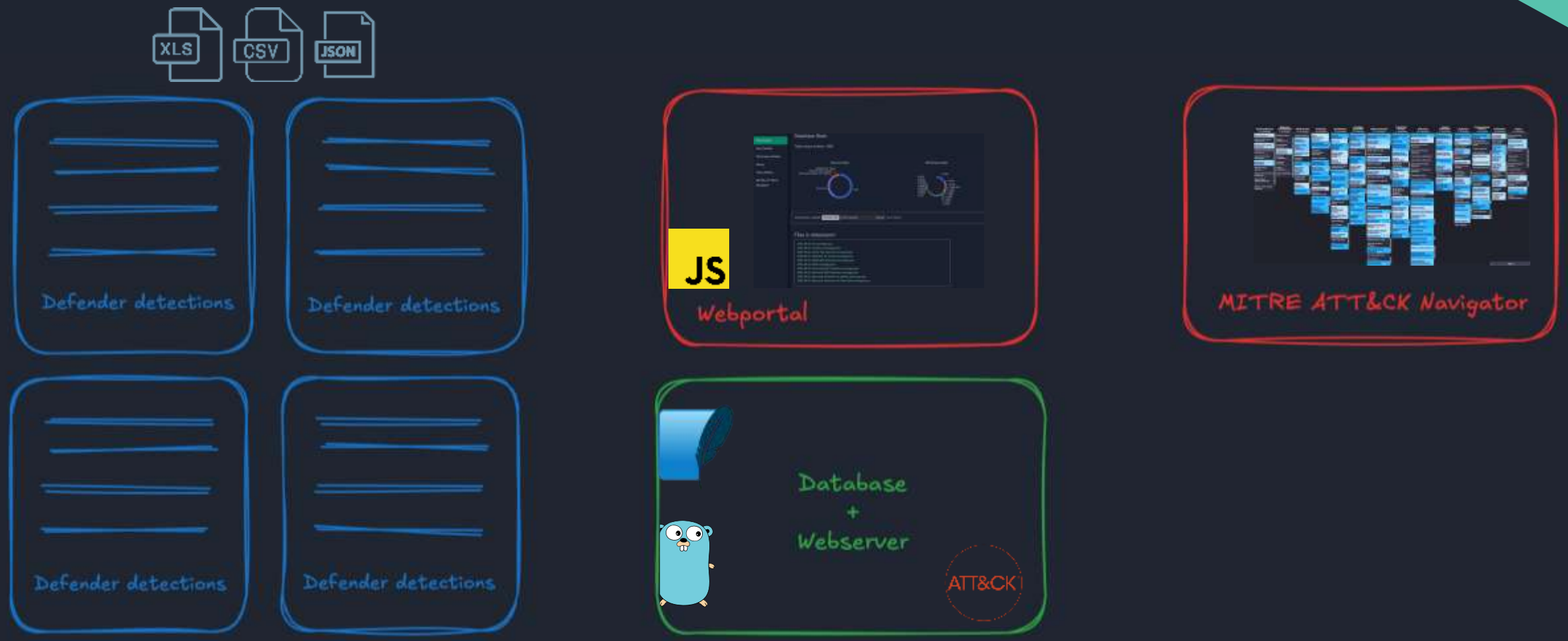
- Deduplicate the data
- Store it in a database
- Make it queryable and generate ATT&CK heatmaps to analyze them.

I suck at Excel so, I started building a tool

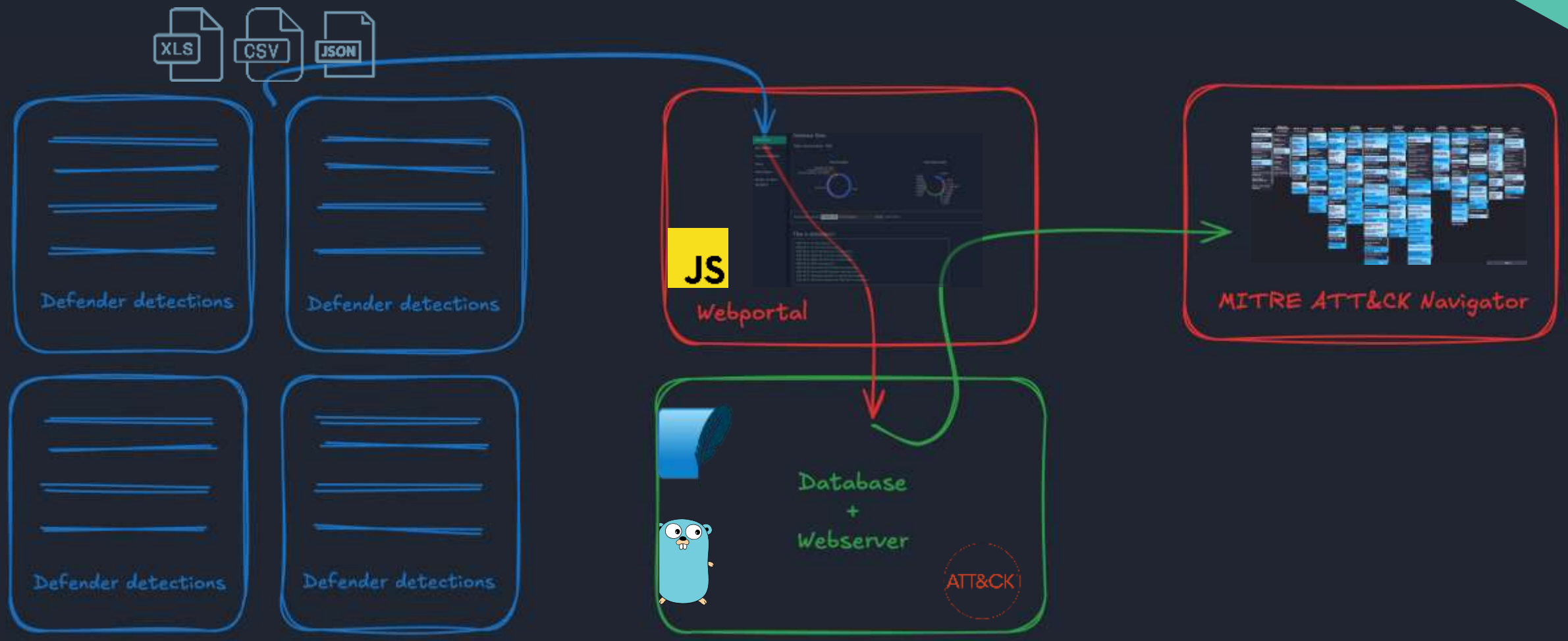
Storing the data



Visualizing the data



Data flow


XLS
CSV
JSON
Defender detections
Defender detections
Defender detections
Defender detections
JS
Webportal
MITRE ATT&CK Navigator
Database
+
Webserver
ATT&CK

Downloads

Alert Details

Technique Details

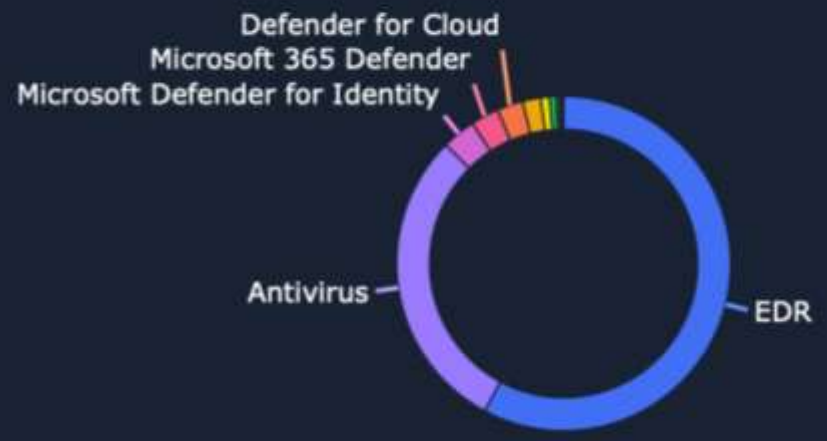
Query

Database Stats

Total unique entries: 1990

Source stats

Technique stats



2024-08-31-Cloud App Security-coverage.json
2024-08-31-Defender for Cloud-coverage.json
2024-08-31-DefenderForServers-coverage.json
2024-08-31-EDR-coverage.json
2024-08-31-Entra Identity Protection-coverage.json
2024-08-31-Microsoft 365 Defender-coverage.json
2024-08-31-Microsoft Defender for Identity-coverage.json
2024-08-31-Microsoft Defender for Office 365-coverage.json

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques

Redacted

Coverage maps per product

Redacted

- Downloads
- Alert Details
- Technique Details
- Query
- Tactic Matrix
- MITRE ATT&CK Navigator

Top alert titles

Redacted

Count
41
23
17
15
15
14
14
13
13
12

1 to 20 of 893 Page 1 of 45

TechniqueId	DetectionS...	Title	Name	Detection
T1027	EDR	A suspicious file was observed	Obfuscated Files or Information	Detection of file obfus
T1204.002	EDR	A suspicious file was observed	User Execution: Malicious File	Monitor the execution
T1204	EDR	A suspicious file was observed	User Execution	Monitor the execution
T1053	EDR	A suspicious file was observed	Scheduled Task/Job	Monitor scheduled tas
T1021	EDR	A suspicious file was observed	Remote Services	Correlate use of login
T1071	EDR	A suspicious file was observed	Application Layer Protocol	Analyze network data
T1489	EDR	A suspicious file was observed	Service Stop	Monitor processes an
T1218	EDR	A suspicious file was observed	System Binary Proxy Execution	Monitor processes an
T1543	EDR	A suspicious file was observed	Create or Modify System Process	Monitor for changes to
T1027.002	EDR	A suspicious file was observed	Obfuscated Files or Information: Software Packing	Use file scanning to lo

Page Size: 20 1 to 17 of 17 Page 1 of 1

- Downloads
- Alert Details
- Technique Details
- Query
- Tactic Matrix
- MITRE ATT&CK Navigator

	T1204.002	EDR	A suspicious file was observed	User Execution: Malicious File	Monitor the execution
	T1204	EDR	A suspicious file was observed	User Execution	Monitor the execution
	T1053	EDR	A suspicious file was observed	Scheduled Task/Job	Monitor scheduled tas
	T1021	EDR	A suspicious file was observed	Remote Services	Correlate use of login
	T1071	EDR	A suspicious file was observed	Application Layer Protocol	Analyze network data
☑	T1489	EDR	A suspicious file was observed	Service Stop	Monitor processes an
	T1218	EDR	A suspicious file was observed	System Binary Proxy Execution	Monitor processes an
	T1543	EDR	A suspicious file was observed	Create or Modify System Process	Monitor for changes tc
	T1027.002	EDR	A suspicious file was observed	Obfuscated Files or Information: Software Packing	Use file scanning to lo

Page Size: 20 | 1 to 17 of 17 | Page 1 of 1

Details

TechniqueId: T1489

DetectionSource: EDR

MITRE ATT&CK information:

Alert Title: A suspicious file was observed

Technique Name: Service Stop

Detection: Monitor processes and command-line arguments to see if critical processes are terminated or stop running. Monitor for edits for modifications to services and startup programs that correspond to services of high importance. Look for changes to services that do not correlate with known software, patch cycles, etc. Windows service information is stored in the Registry at HKLM\SYSTEM\CurrentControlSet\Services. Systemd service unit files are stored within the /etc/systemd/system, /usr/lib/systemd/system/, and /home/.config/systemd/user/ directories, as well as associated symbolic links. Alterations to the service binary path or the service startup type changed to disabled may be suspicious. Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. For example, ChangeServiceConfigW may be used by an adversary to prevent services from starting.(Citation: Talos Olympic Destroyer 2018)

Mitigation: Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.

So what else is deemed suspicious ?

Title	Count
Suspicious sequence of exploration activities	41
A suspicious file was observed	17
Suspicious behavior by cmd.exe was observed	14
Suspicious User Account Discovery	13
Suspicious PowerShell command line	13
Suspicious remote activity	12
Suspicious remote PowerShell execution	12
Suspicious LDAP query	12
Suspicious file registered as a service	11
Suspicious System Network Configuration Discovery	11

Page Size: 20 | 1 to 20 of 195 | Page 1 of 10

So what else is deemed suspicious ?

Query alert mapping details

Suspicious | Search | Generate ATT&CK JSON

TechniqueId	DetectionSource	Title	Name	Detection	Mitigation
T1018	EDR	Suspicious LDAP query	Remote System Discovery	System and network dis…	#N/A
T1069	EDR	Suspicious LDAP query	Permission Groups Disc…	System and network dis…	#N/A
T1087	EDR	Suspicious LDAP query	Account Discovery	System and network dis…	Prevent admin
T1087.002	EDR	Suspicious LDAP query	Account Discovery: Dom…	System and network dis…	Prevent admin
T1135	EDR	Suspicious LDAP query	Network Share Discovery	System and network dis…	Enable Windo
T1558.003	EDR	Suspicious LDAP query	Steal or Forge Kerberos …	Enable Audit Kerberos S…	Enable AES K
T1033	EDR	Suspicious User Accoun…	System Owner/User Dis…	`System and network dis…	#N/A
T1106	EDR	Suspicious User Accoun…	Native API	Monitoring API calls may…	On Windows 1
T1049	EDR	Suspicious System Net…	System Network Conne…	System and network dis…	#N/A
T1106	EDR	Suspicious System Net…	Native API	Monitoring API calls may…	On Windows 1
T1135	EDR	Suspicious System Net…	Network Share Discovery	System and network dis…	Enable Windo
T1033	EDR	Suspicious LDAP query	System Owner/User Dis…	`System and network dis…	#N/A
T1082	EDR	Suspicious LDAP query	System Information Disc…	System and network dis…	#N/A
T1016	EDR	Suspicious System Net…	System Network Config…	System and network dis…	#N/A
T1106	EDR	Suspicious System Net…	Native API	Monitoring API calls may…	On Windows 1
T1204.002	EDR	Suspicious file similar to …	User Execution: Malicio…	Monitor the execution of …	On Windows 1
T1003	EDR	Suspicious RDP session	OS Credential Dumping	### Windows Monitor for..	Manage the a
T1021.001	EDR	Suspicious RDP session	Remote Services: Remo…	Use of RDP may be legit…	Audit the Rem
T1555	EDR	Suspicious RDP session	Credentials from Passw…	Monitor system calls, file…	The password
T1003.001	EDR	Suspicious access to LS…	OS Credential Dumping:…	Monitor for unexpected …	On Windows 1

Page Size: 20 | 1 to 20 of 611 | Page 1 of 31

So what else is deemed suspicious ?

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact

Redacted

What does it look like without the suspicious ones?

Create Layer from Other Layers

Select layers to inherit properties from

domain*
Enterprise ATT&CK MITRE ATT&CK v15

Select the domain for the new layer. Only layers of the same domain and version can be merged.

score expression
b - a

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here . Leave blank to initialize scores to 0. Here's a list of available layer variables:

- a (Suspicious)
- b (Observed Defender Coverage)

gradient
Observed Defender Coverage

Select which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

coloring
Observed Defender Coverage

Select which layer to import manually assigned colors from. Leave blank to initialize with no colors.

comments
Observed Defender Coverage

Select which layer to import comments from. Leave blank to initialize with no comments.

links
Observed Defender Coverage

Select which layer to import technique links from. Leave blank to initialize without links.

metadata
Observed Defender Coverage

Select which layer to import technique metadata from. Leave blank to initialize without metadata.

states
Observed Defender Coverage

Select which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.

filters
Observed Defender Coverage

Select which layer to import filters from. Leave blank to initialize with no filters.

legend
Observed Defender Coverage

Select which layer to import the legend from. Leave blank to initialize with an empty legend.

Create layer

What does it look like without the suspicious ones?

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	16 techniques	9 techniques	14 techniques

Redacted

What does it look like without the suspicious ones?

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	16 techniques	9 techniques	14 techniques

Redacted

Red teaming

SOAPHound — tool to collect Active Directory data via ADWS

January 26, 2024

Nikos Karouzos

No data … so no coverage?

Since when is it detectable ?

Microsoft | Microsoft Security Intelligence Threats Blogs Downloads Submissions Help All Microsoft Search

Attention: We have transitioned to a new AAD or **Microsoft Entra ID** from the week of May 20, 2024. In case your tenant requires admin consent, please refer to this document located at **Overview of user and admin consent - Microsoft Entra ID | Microsoft Learn** and grant access to App ID: 6ba09155-cb24-475b-b24f-b4e28fc74365 with graph permissions for Directory.Read.All and User.Read for continued access. While the app may appear unverified, you can confirm its legitimacy by verifying the App ID provided.

We're gradually updating threat actor names in our reports to align with the new weather-themed taxonomy.
Learn about Microsoft threat actor names

Published Feb 14, 2024 | Updated Not applicable

HackTool:MSIL/SoapHound!MSR

Detected by Microsoft Defender Antivirus

Aliases: No associated aliases

Summary

Microsoft Defender Antivirus detects and removes this threat.

This threat can perform a number of actions of a malicious actor's choice on your device.

Find out ways that malware can get on your device.

VirTool:MSIL/SoapHound.A

Alert level: Severe
Status: Active
Date: 9/8/2024 10:30 AM
Category: Tool
Details: This program is used to create viruses, worms or other malware.

Learn more

Affected items:

file: C:\Users\imaginebox\Downloads\SOAPHound.exe

OK

Detection but no techniques

```
23  AlertInfo
24  | where Timestamp > ago(180d)
25  | join AlertEvidence on AlertId
26  | extend Techniques=parse_json(AttackTechniques)
27  | where DetectionSource != "Custom detection"
28  | mv-expand Techniques
29  | summarize arg_min(Timestamp,*) by Title, DetectionSource, tostring(Techniques)
```

Getting started | Results | Query history

Export | Show empty columns | 6 items | Search | 00:00.134 | Low | Chart type | Customize columns | Full screen

Filters: Add filter

Title	DetectionSource	Techniques	Timestamp	AlertId	Category	S
SOAPHound tool activity	EDR		8 Sep 2024 12:27:41	da25f2cf5f-292c-473...	SuspiciousActivity	M
An active 'SoapHound' malware was detected	Antivirus		8 Sep 2024 12:27:01	daa2aeefca-38bd-45...	Malware	L
'SoapHound' malware was detected	Antivirus		8 Sep 2024 12:27:01	da25888e76-2248-43...	Malware	I
An active 'SoapHound' malware process was detected while executing	Antivirus		8 Sep 2024 12:26:29	dac2623c07-eded-44...	Malware	L

What percentage of alerts has techniques tagged ?

DetectionSource	HasTechniquePercentage	NoTechniquePercentage
Antivirus	10.87	89.13
EDR	92.31	7.69
CloudApp	29.03	70.97
Defender for Cloud	100	0
Entra Identity Protection	37.5	62.5
Other	16.67	83.33

Based on an environment with 100k endpoints.
Similar amounts are observed in other tenants

What are we missing here ?

Title	count_
Ransomware-linked threat actor detected	1
Potential C2 Connection Behavior	1
Suspicious activity linked to a financially motivated threat actor detected	1
Potential human-operated malicious activity	1
A file or network connection related to a ransomware-linked emerging threat activity group detected	1
Pistachio Tempest threat activity group detected	1
Information stealing malware activity	1
Connection to adversary-in-the-middle (AiTM) phishing site	1
Suspicious malware activity detected	1

Title	count_
Defender detection bypass	1
SOAPHound tool activity	1
ROADtools redteam framework	1
Compromised account conducting hands-on-keyboard attack	1

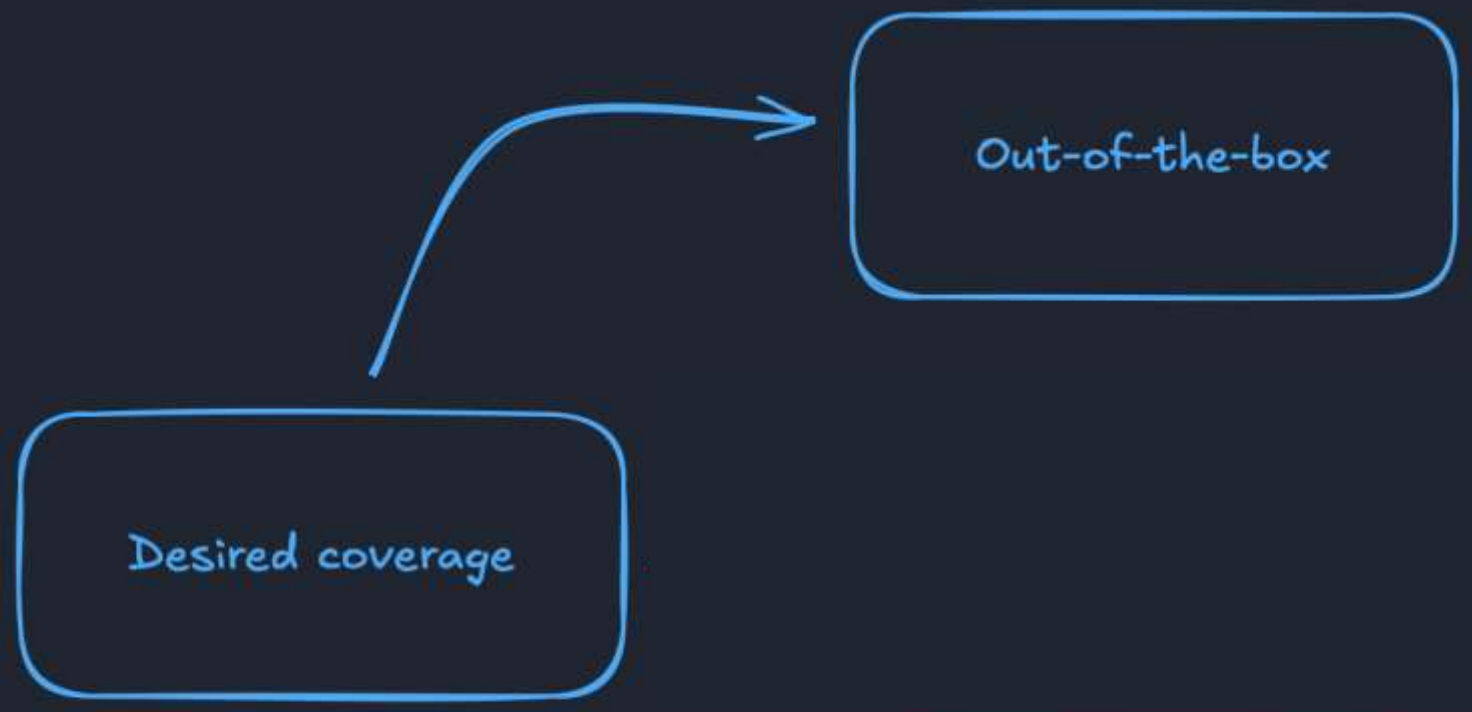
What about all these AV misses?

Title	count_
An active 'AzBloodHnd' malware process was detected while executing	1
'AzBloodHnd' malware was detected and was active	
An active 'AzBloodHnd' malware was detected	
'NSudo' hacktool was prevented	
An active 'Kekeo' malware was detected	
'Kekeo' malware was detected	
An active 'Kekeo' malware process was detected while executing	
An active 'KrbAttack' malware was detected	
'KrbAttack' malware was detected and was active	
An active 'KrbAttack' malware process was detected while executing	
'Covent' malware was detected	
An active 'KrbAttack' malware was blocked	
'KrbAttack' malware was blocked and was active	
'Vigorf' malware was detected	
'SoapHound' malware was prevented	
'Wacapew' malware was prevented	
An active 'NetCat' hacktool was detected	
An active 'NetCat' hacktool process was detected while executing	

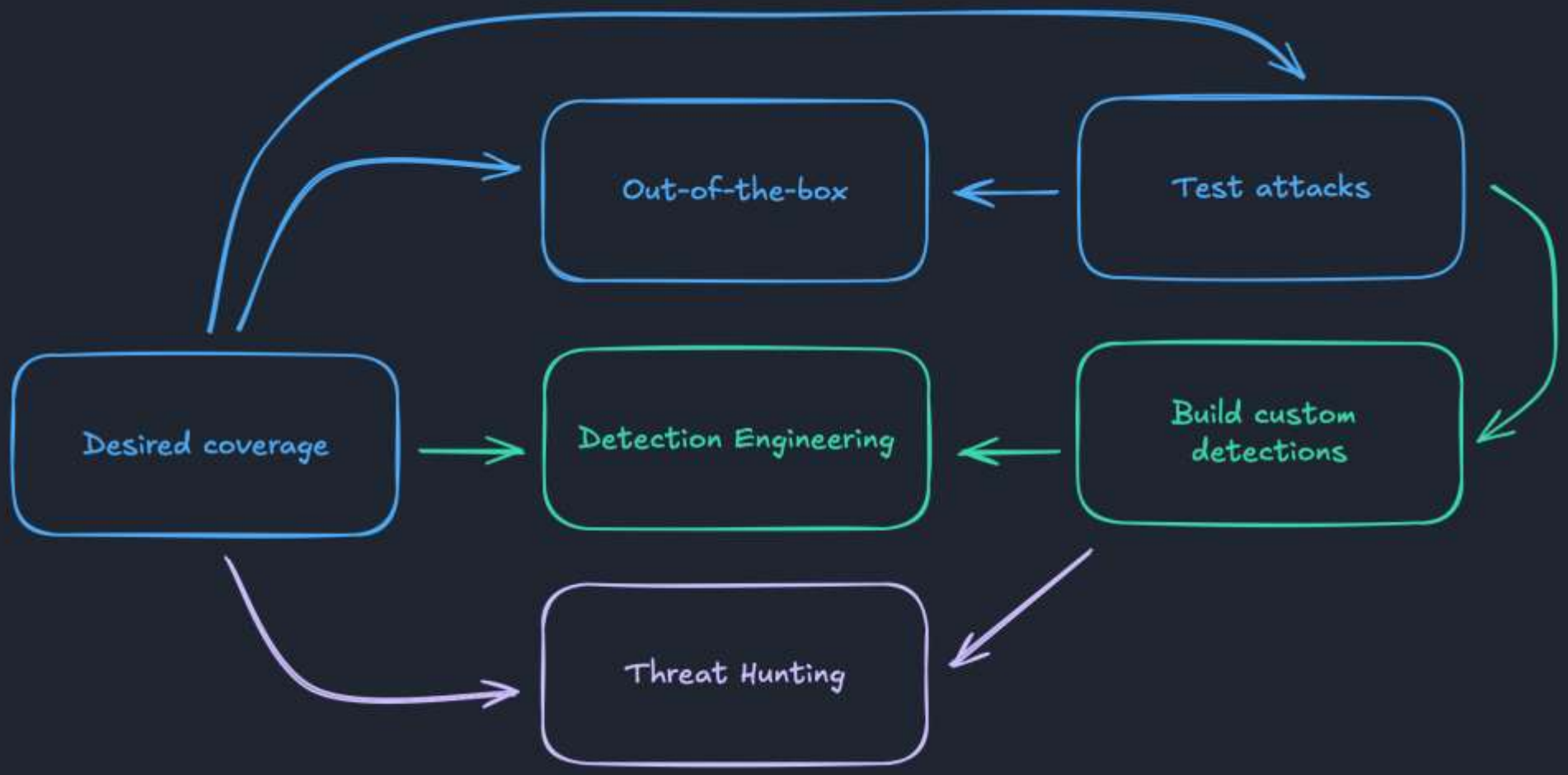
Title
'Conficker' malware was prevented
'BrowserKnocker' malware was detected
'Vigua' unwanted software was detected
'CeeInject' malware was detected
'OfferCore' unwanted software was detected during a scheduled scan
'Dobex' malware was detected
'MyWebSearch' unwanted software was detected
'Dobex' malware was prevented
Unwanted software was detected in an iso disc image file
'Lodi' malware was prevented
'Smsthief' malware was prevented
'Gendows' hacktool was detected during a scheduled scan
'MicTrayDebugger' malware was prevented on a Microsoft SQL server
An active 'AutoKMS' hacktool process was detected while executing

What can we learn from this data?

What can we learn from this data?



What can we learn from this data?



Build custom detections

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques

Redacted

Augment out of the box coverage

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	16 techniques	9 techniques	14 techniques

Redacted

What can we learn from this data?

Technique mapping is …

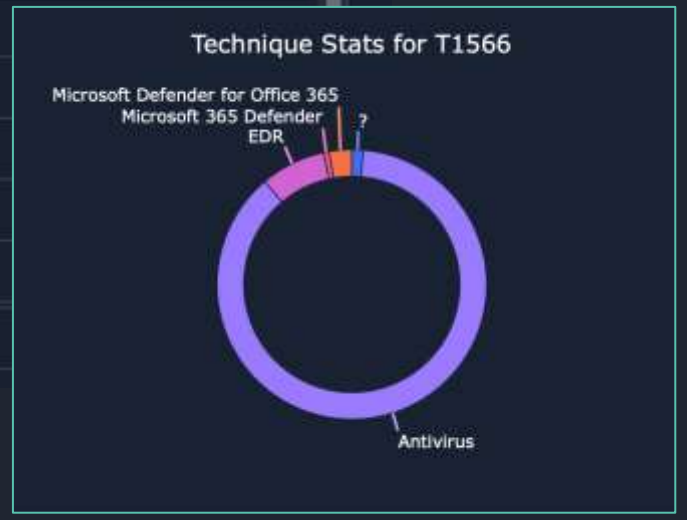
- in some cases, spot on
- in some EDR cases, incomplete. For AV many.
- in some cases, overly generous
- sometimes there and sometimes not for the same alerts ?!

Most tagged attack techniques

T1566(.002) - Phishing + Spearphishing Link

Title	DetectionSource
'Ulthar' malware was prevented	Antivirus
'VBInject' malware was prevented	Antivirus
Email messages from a campaign removed after delivery	Microsoft Defender for Office 365
'ZkarletFlash' malware was prevented	Antivirus
Connection to Storm-0485 adversary-in-the-middle (AiTM) phishing site	EDR
A file or network connection related to threat actor Storm-1575 has been detected	EDR
'Vigorf' malware was detected	Antivirus
'Vigorf' malware was prevented	Antivirus
User clicked a malicious link in Teams chat	Microsoft 365 Defender
Malicious link shared in Teams chat	Microsoft 365 Defender

Page Size: 20 1 to 20 of 374



Most tagged attack techniques

T1204 - User Execution

Title	DetectionSource
Suspicious file similar to known attacker malware	EDR
A suspicious file was observed	EDR
A Windows shortcut with unusual characteristics was opened	EDR
Suspicious attachment opened	Microsoft 365 Defender
A suspicious file was observed	EDR
A Windows shortcut with unusual characteristics was opened	EDR
Suspicious attachment opened	EDR
Suspicious small binary	EDR
Malicious document detected	EDR
A link file (LNK) with unusual characteristics was opened	EDR

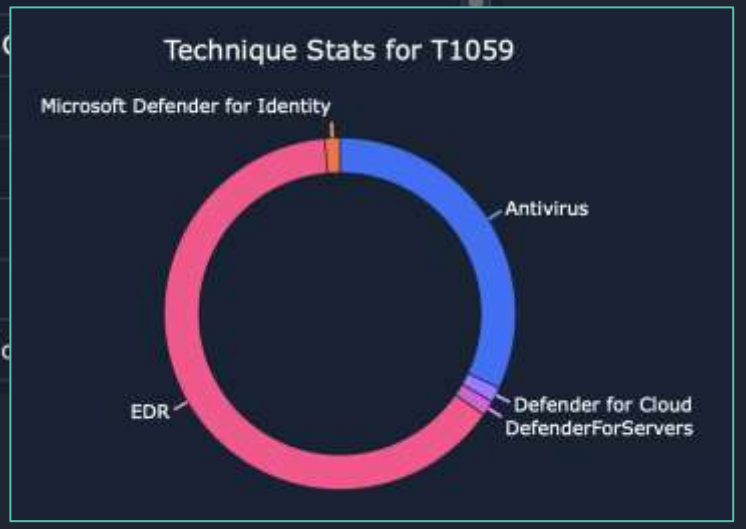
Page Size: 20 1 to 20 of 123

Most tagged attack techniques

T1059 - Command and Scripting Interpreter

Title	DetectionSource
Activity that might lead to credential and token theft	EDR
Possible initial access via OneNote	EDR
PowerShell created possible reverse TCP shell	EDR
'PsAttack' hacktool was prevented	Antivirus
Suspicious activity by living-off-the-land binary	EDR
Remote code execution attempt	Defender for (
'Meterp' malware was detected	Antivirus
Suspicious Remote System Discovery	EDR
Suspicious Permission Groups Discovery	EDR
Possible Metasploit activity	EDR

Page Size: 20 41 to 60 c

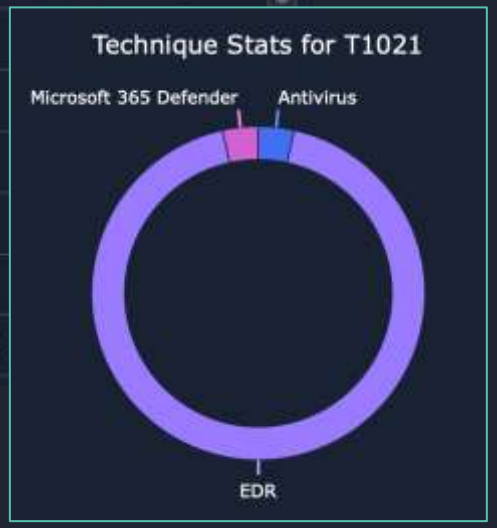


Most tagged attack techniques

T1021 - Remote Services

Title	DetectionSource
Suspicious RDP session	EDR
Compromised account conducting hands-on-keyboard attack	EDR
'ADSync' malware was detected during lateral movement	EDR
Lateral movement using RDP blocked	Microsoft 365 Defender
Lateral movement using remote logon by contained user blocked on multiple devices	Microsoft 365 Defender
Remote Desktop session	EDR
Suspicious remote activity	EDR
Impacket toolkit	Antivirus
Low-reputation arbitrary code executed by signed executable	EDR
Low-reputation arbitrary code executed by signed executable	EDR

Page Size: 20 1 to 20 of 83



Top mitigations from ATT&CK

Based on the top 10 techniques in the detections

- Anti-virus can automatically quarantine suspicious files.
- On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent executable files from running unless they meet a prevalence, age, or trusted list criteria and to prevent Office applications from creating potentially malicious executable content by blocking malicious code from being written to disk. Note: cloud-delivered protection must be enabled to use certain rules. (Citation: win10_asr)
- Audit applications and their permissions to ensure access to data and resources are limited based upon necessity and principle of least privilege.
- Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

Wrapping up

- I won't make these details public, for obvious reasons.
- I recently started tracking first seen occurrences for detections.
- While these details help you focus your detection effort, you still need to test to make sure the out-of-the-box detections catch what you care about.
- Make sure to also have some regression tests in there, MS not only changes product names but also can remove or change detections.

Thank you!

Together. Secure. Today.

olaf@falconforce.nl

https://falconforce.nl

@olafhartong
@falconforceteam

https://linkedin.com/in/olafhartong
https://linkedin.com/company/falconforce