Microsoft

Microsoft Ignite

Spotlight on Switzerland

Kongresshaus Zürich

March 9, 2023

Microsoft

Threat Hunting
Attack disruption and SOC empowerment

Ralf Gomeringer
Alex Verboon

Agenda

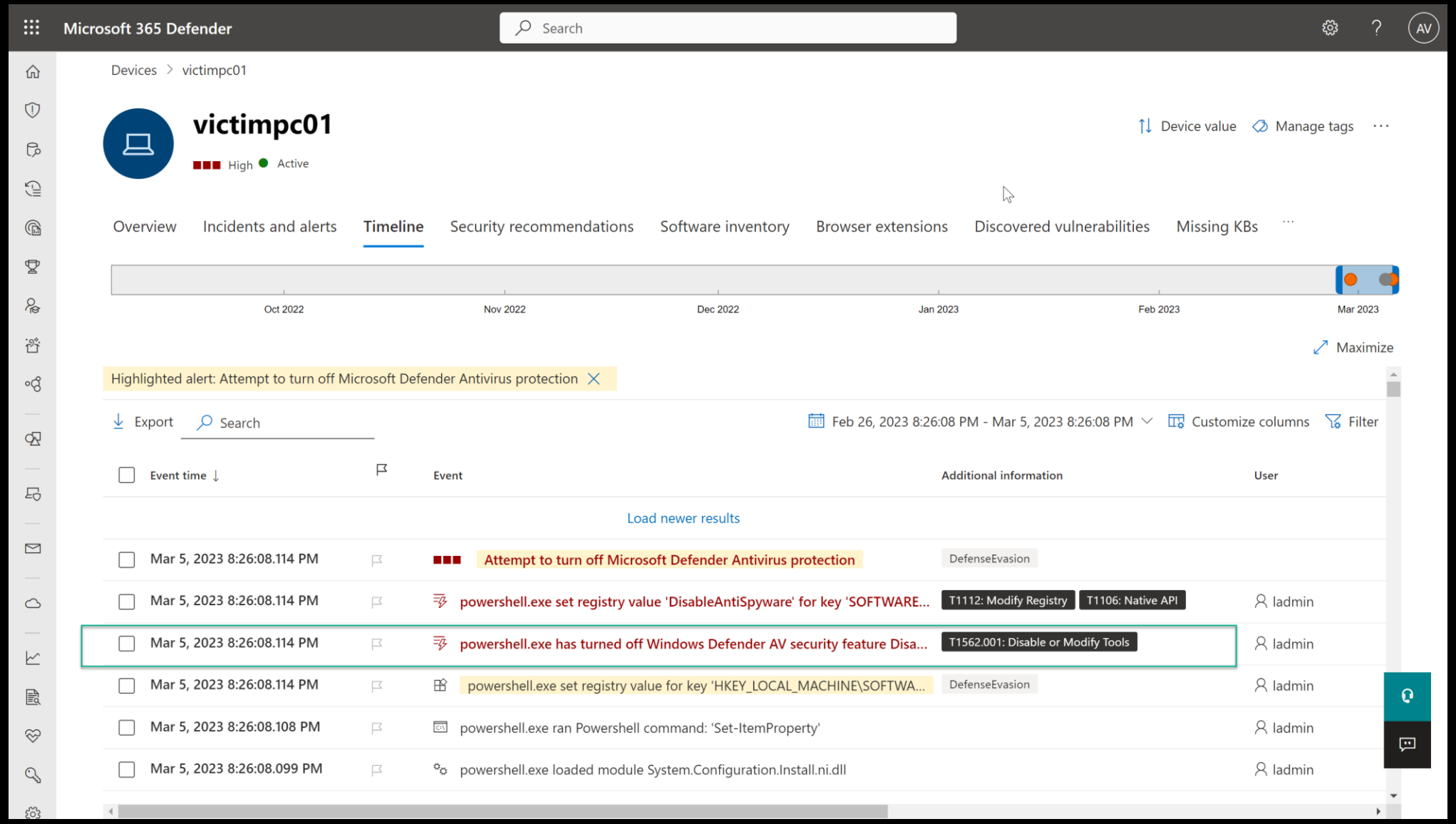
- What is Threat Hunting?
- The benefits of Threat Hunting
- MITRE ATT&CK
- Threat Intelligence Sources
- Threat Hunting & the Microsoft Security Stack
- Demos

What is Threat Hunting

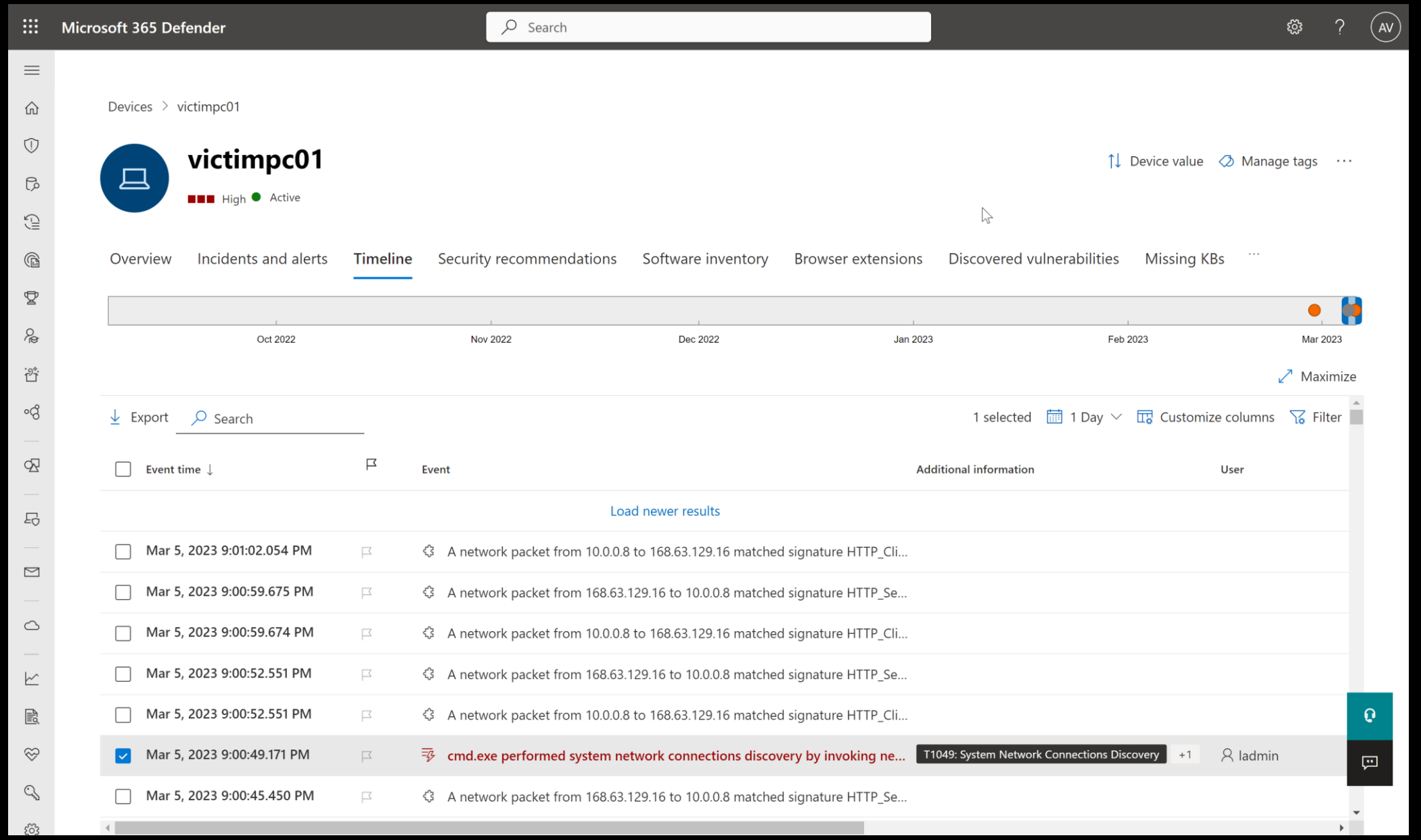
Threat hunting is a **proactive** approach to cybersecurity, predicated on an "**assume breach**" mindset. Just because a breach isn't visible via traditional security tools and detection mechanisms doesn't mean it hasn't occurred. Your threat hunting team doesn't react to a known attack, but rather tries to uncover indications of attack (IOA) that have yet to be detected

Why Threat Hunting

EDR Detections

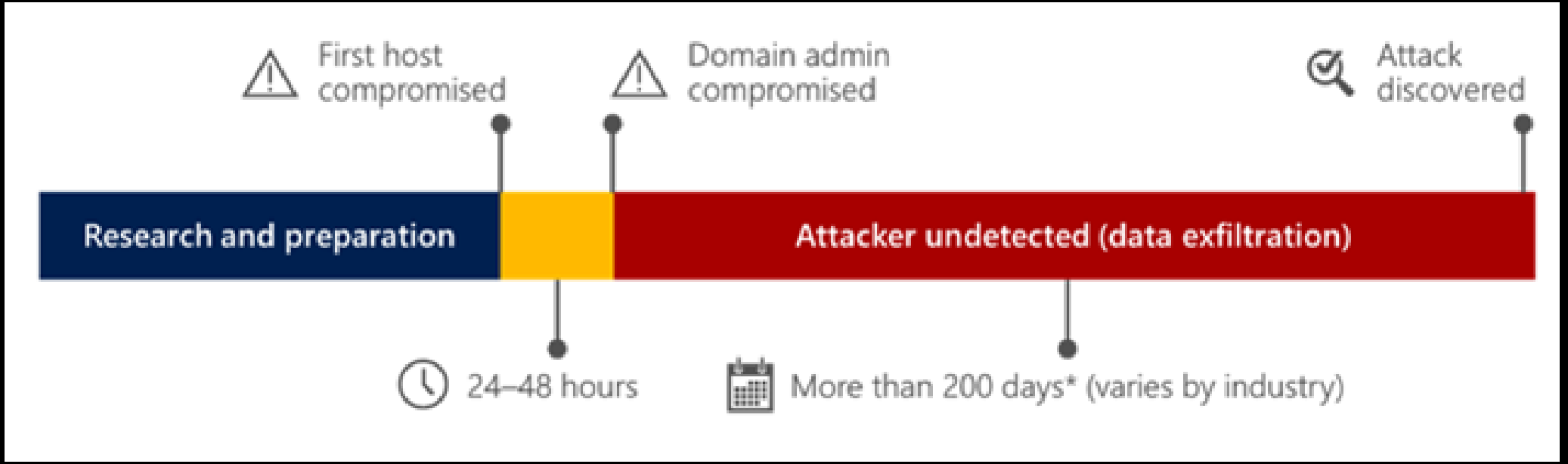


EDR Detections



Dwell Time

The amount of time an attacker spends within the systems under attack, especially the amount of time the attacker spends undetected.



Commodity malware and human-operated attacks.

Commodity malware attacks are the hazards you encounter every day as users click on the wrong link or install the wrong program. In these situations, much of the attack logic is contained within the malware, so remediation is typically as simple as removing the malware, rebuilding the device, and / or potentially resetting the user's credentials.

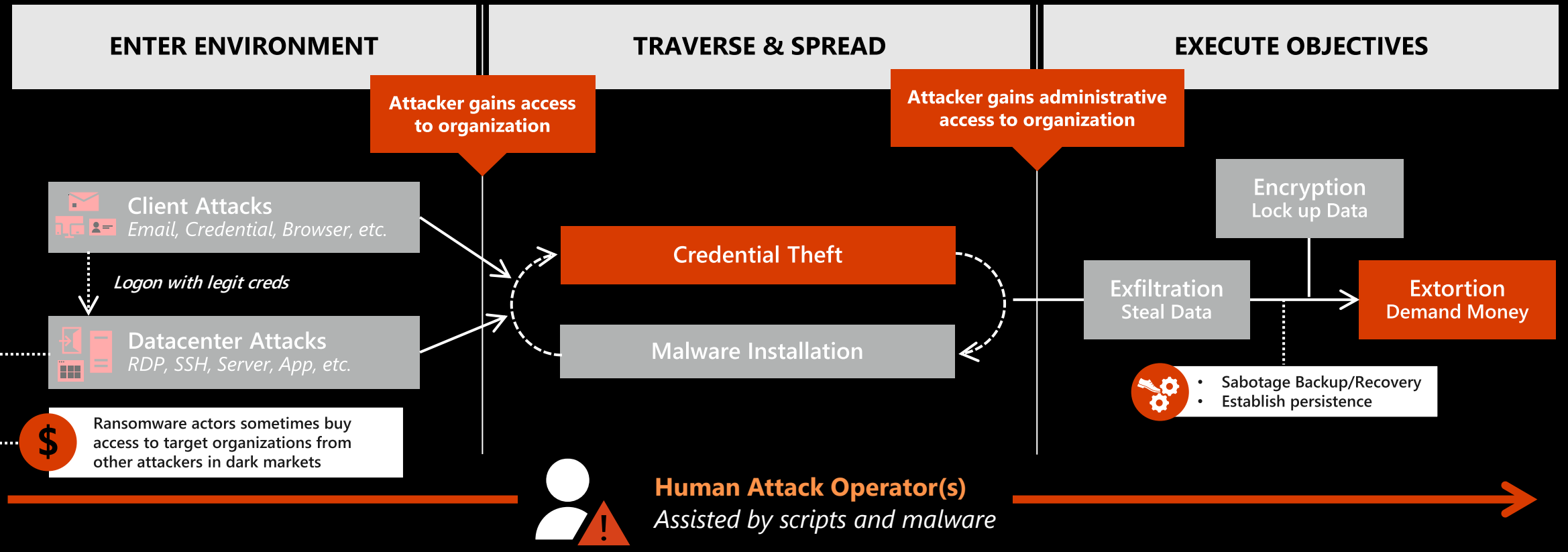
- Leverage highly automated attack techniques
- Focused on infecting large numbers of endpoints
- Delivered using techniques that appearl to many targes

Human-operated attacks invest significantly more effort into the compromise of a specific target than commodity malware attacks. Once attackers gain a foothold within a system, they use their attack experience and motives to decide what to do at each stage based on what they find in their target's network. Because humans are behind these attacks, their impact – and the variety of techniques used – vary significantly.

- Focus on specific target
- Evade specific organizational protections
- Uses customized tools designed specifically for the target
- Abuse legitimate administrative tools to evade detection

Source: Microsoft Threat Hunting survival guide

Pattern – Human Operated Ransomware



Benefits of Threat Hunting

- Detect previously unidentified malicious activity
- Improve detection coverage
- Improve security posture
- Bonus:
  - Identify IT policy and compliance violations
  - Identify misconfigurations

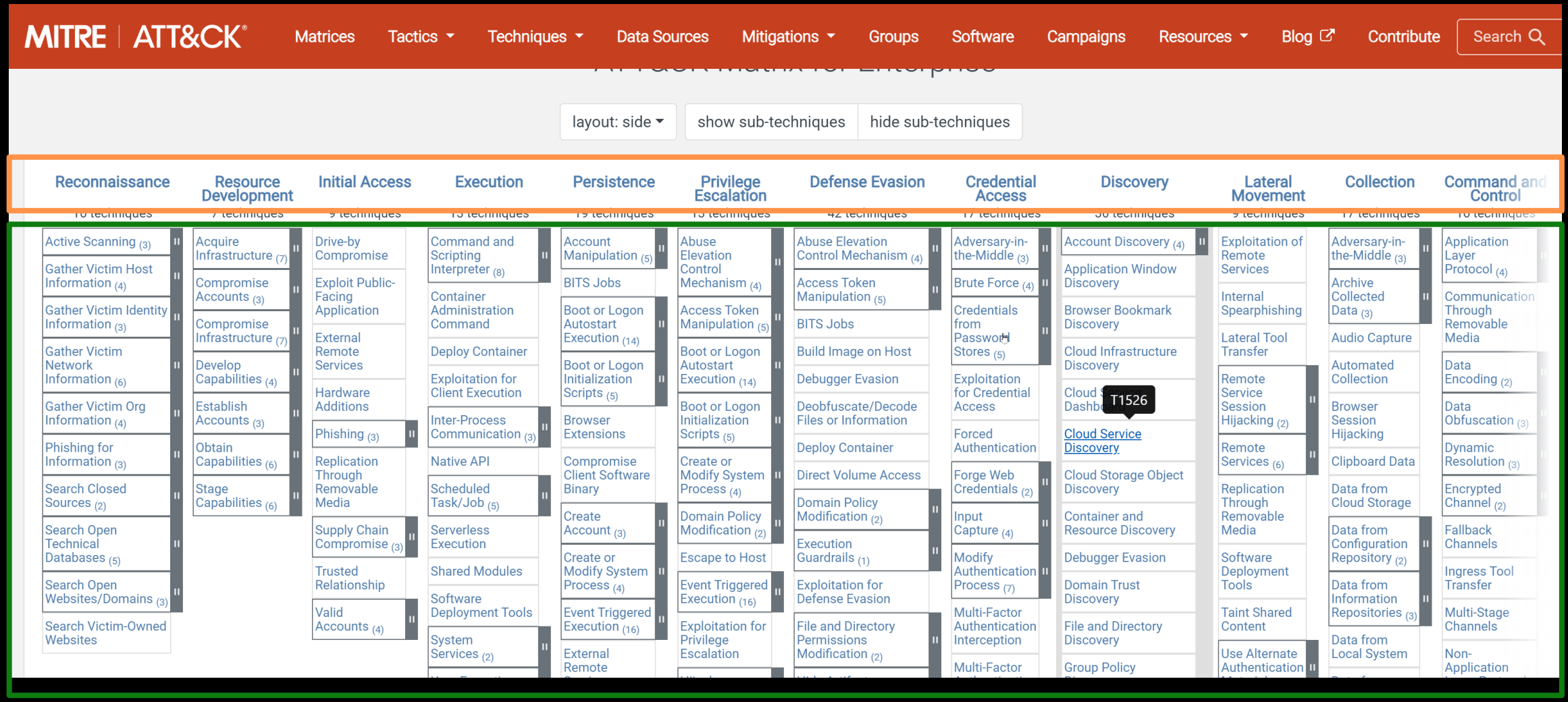
MITRE ATT&CK

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques

Tactics represent the "**why**" of an ATT&CK technique. The tactic is the adversary's tactical objective for performing an action

Techniques represent "**how**" an adversary achieves a tactical objective by performing an action.

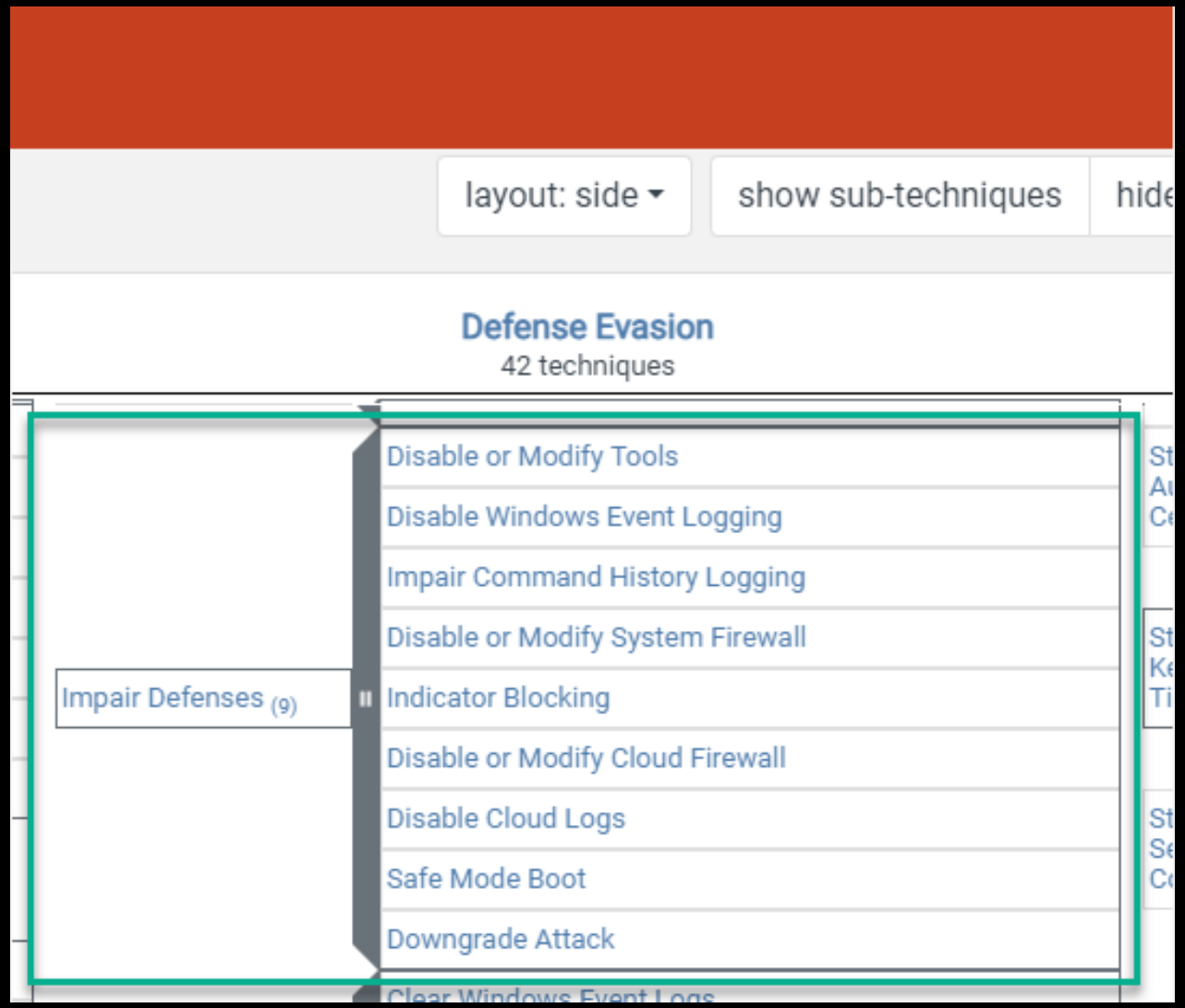
MITRE ATT&CK


MITRE | ATT&CK
Matrices
Tactics
Techniques
Data Sources
Mitigations
Groups
Software
Campaigns
Resources
Blog
Contribute
Search
layout: side
show sub-techniques
hide sub-techniques
Tactics
Techniques
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites
Acquire Infrastructure (7)
Compromise Accounts (3)
Compromise Infrastructure (7)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (6)
Stage Capabilities (6)
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Command and Scripting Interpreter (8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (7)
Multi-Factor Authentication Interception
Multi-Factor
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
T1526
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication
Adversary-in-the-Middle (3)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application

MITRE ATT&CK

Tactics

Techniques



Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior.

Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

MITRE ATT&CK

Impair Defenses

Sub-techniques (9)

ID	Name
T1562.001	Disable or Modify Tools
T1562.002	Disable Windows Event Logging
T1562.003	Impair Command History Logging
T1562.004	Disable or Modify System Firewall
T1562.006	Indicator Blocking
T1562.007	Disable or Modify Cloud Firewall
T1562.008	Disable Cloud Logs
T1562.009	Safe Mode Boot
T1562.010	Downgrade Attack

ID: T1562

Sub-techniques: T1562.001, T1562.002, T1562.003, T1562.004, T1562.006, T1562.007, T1562.008, T1562.009, T1562.010

ⓘ Tactic: Defense Evasion

ⓘ Platforms: Containers, IaaS, Linux, Network, Office 365, Windows, macOS

ⓘ Defense Bypassed: Anti-virus, Digital Certificate Validation, File monitoring, Firewall, Host forensic analysis, Host intrusion prevention systems, Log analysis, Signature-based detection

Version: 1.3

Created: 21 February 2020

Last Modified: 19 October 2022

Threat Intelligence

Microsoft Defender Threat Intelligence

Search

Home > Suspect Raspberry Robin C2 Domains o...

Download Share

Featured 4 months ago

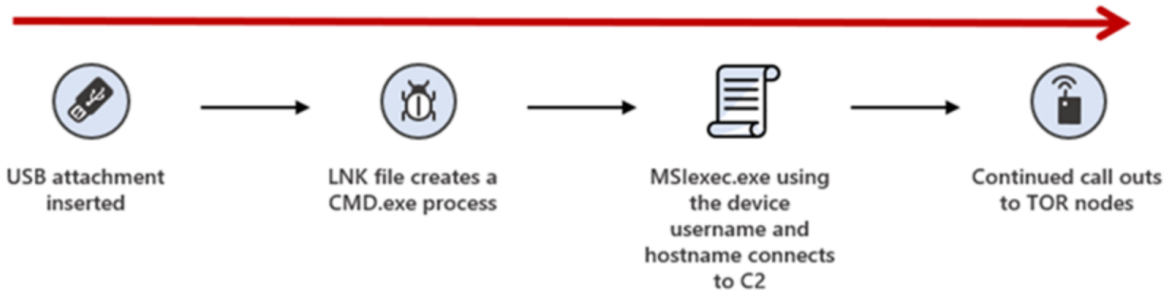
Suspect Raspberry Robin C2 Domains on QNAP Photo Station

MDTI | Enterprise | RaspberryRobin | QNAP | C2 | T1059.003

Description | Public Indicators (10) | Defender TI Indicators (26)

MDTI Threat Intel Brief

As reported earlier by Red Canary, compromised QNAP devices were used for command and control (C2) infrastructure for Raspberry Robin activity. HTTP requests that contain the victim's user and device names are sent to the QNAP device, as well as hosting a malicious DLL that is downloaded and installed to the victim system.



More Intelligence

1 day ago
Batloader Malware Abuses Legitimate Tools ...

2 days ago
#StopRansomware: Royal Ransomware | CISA

2 days ago
Redis Miner Leverages Command Line File H...

2 days ago
Attack Surface: CVE-2023-21529 - Microsoft ...

2 days ago
Activity profile: Remcos delivery through tax ...

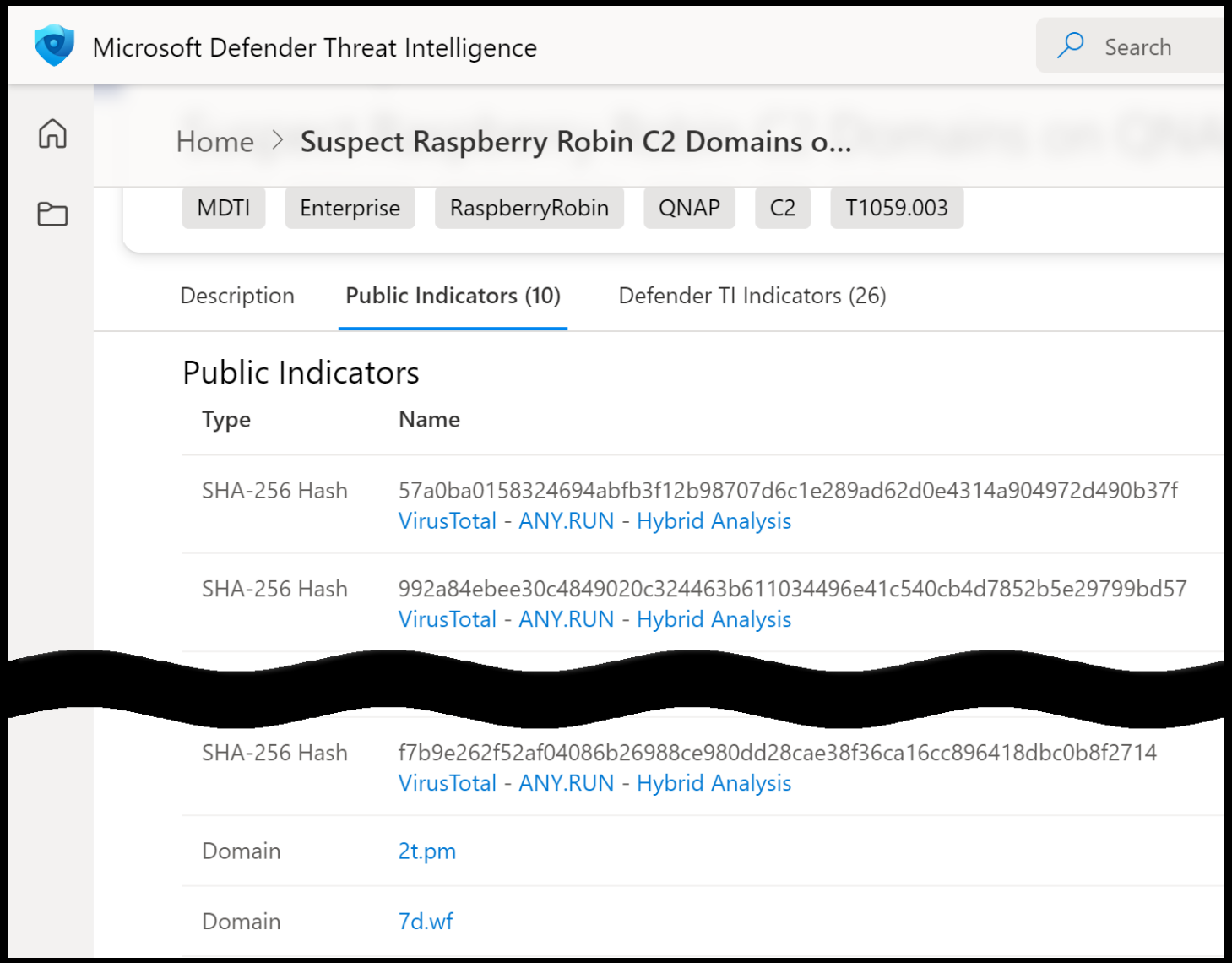
3 days ago
Attack Surface: CVE-2023-21745 - Microsoft ...

3 days ago
BB17 distribution Qakbot (Qbot) activity

1 day ago
GootKit Payload Delivery URLs, February 22 -...

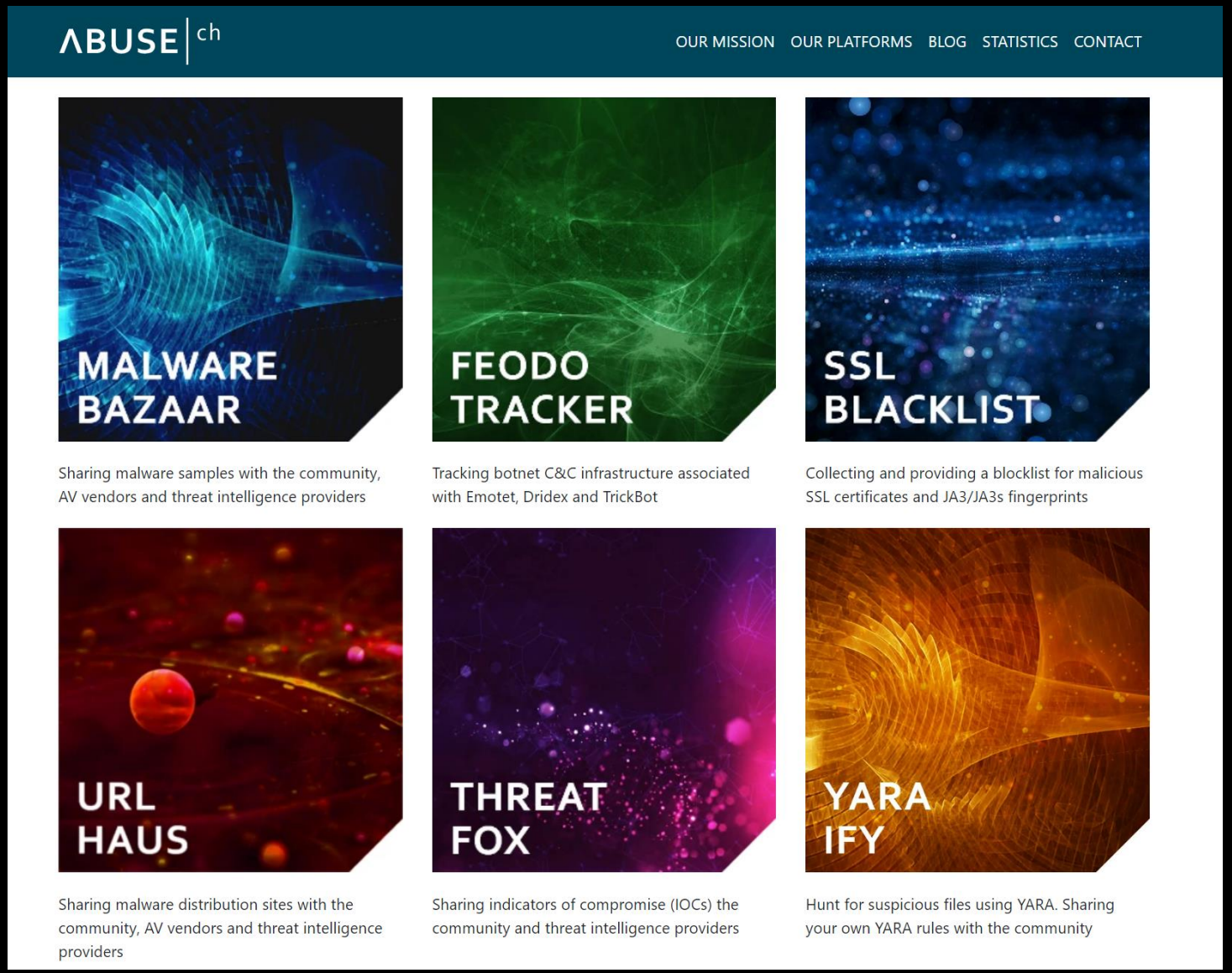
4 days ago
EXFILTRATOR-22 – An Emerging Post-Exploit...

Threat Intelligence



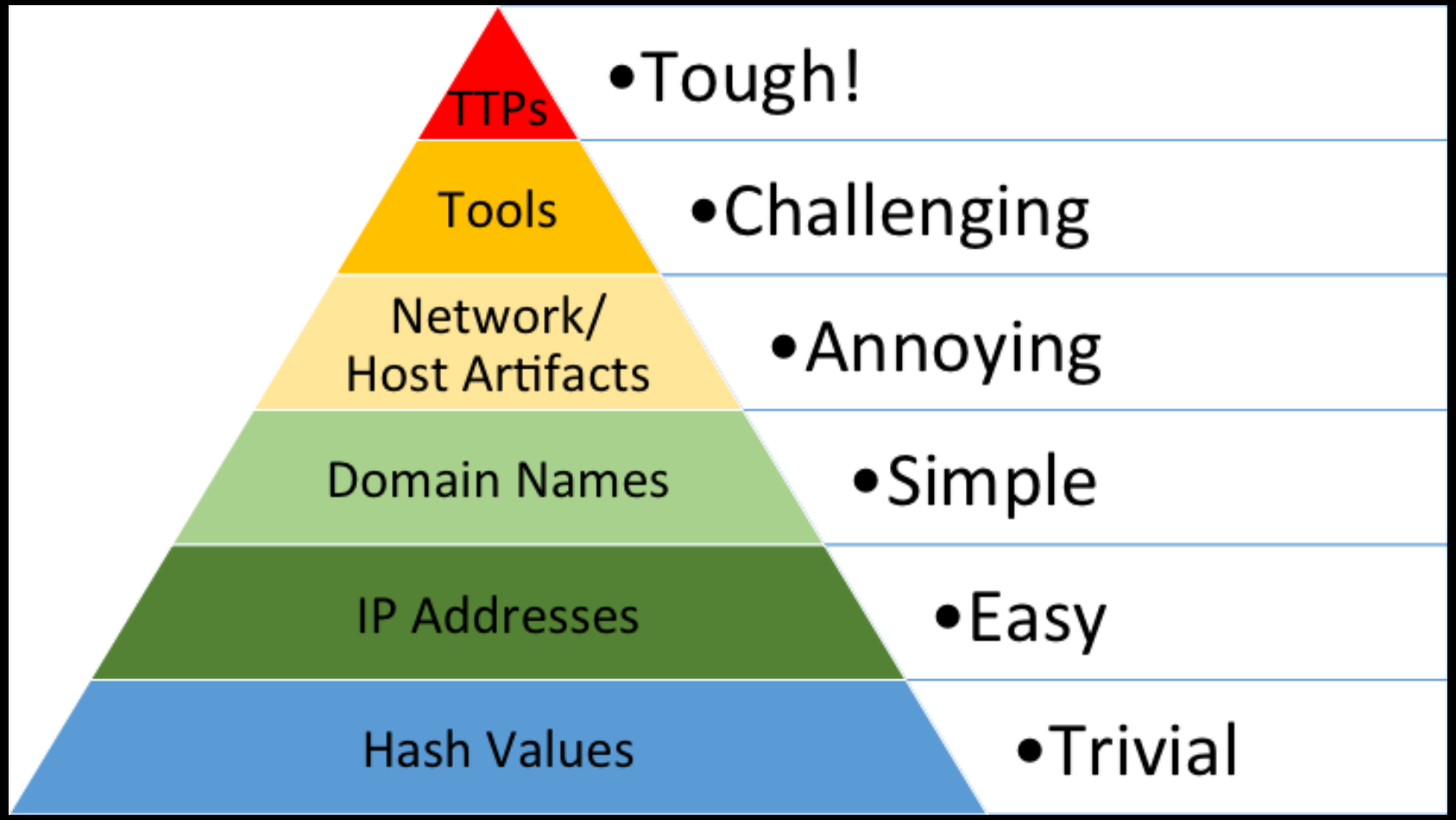
Use Threat Intelligence sources to get insights into used Techniques and IOCs

Threat Intelligence Feeds



The Pyramid of Pain

The Pyramid of Pain is a conceptual model for the effective use of Cyber Threat Intelligence in threat detection operations, with a particular emphasis on increasing the adversaries' cost of operations.



Source: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

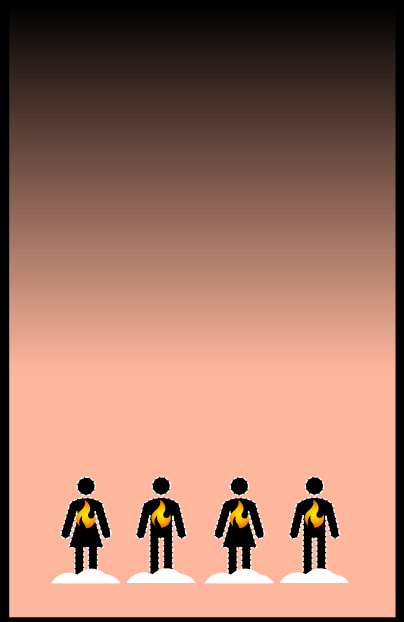
Security Operations Model

Detection Quality and Engineering

Filtering low quality detections is critical!

False positives cause frustration, burnout, & distract from real attacks

Triage Team Capacity



Detection Engineering

Continuously review and improve custom detection quality

Raw Data *(Events and Logs)*

Highly Quality Detections

- *Rapid Response by Triage or Investigation*

Threat Hunting

Required to filter out low quality alerts and find hidden attackers

Lower Quality Detections

- *Ideal place to start threat hunting*

Raw Data

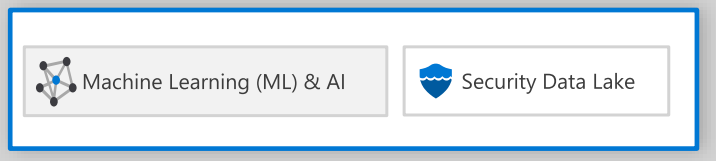
- *Investigations, threat hunting, research*

Examples

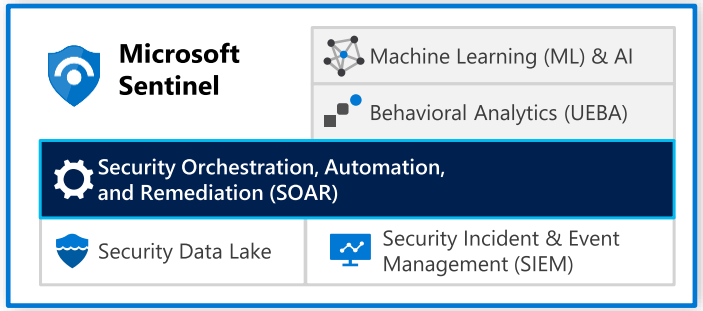
anomalous inbox rules created by user
anomalous bursts of outbound emails to previously unseen domains
unusual login events associated with highly privileged accounts
Ports Usage
Suspicious domains
PowerShell downloads
Azure Active Directory sign-ins from new locations
Host with new log-ins
Enumeration of users and groups
Uncommon processes—bottom 5 percent

Threat Hunting & the Microsoft Security Stack

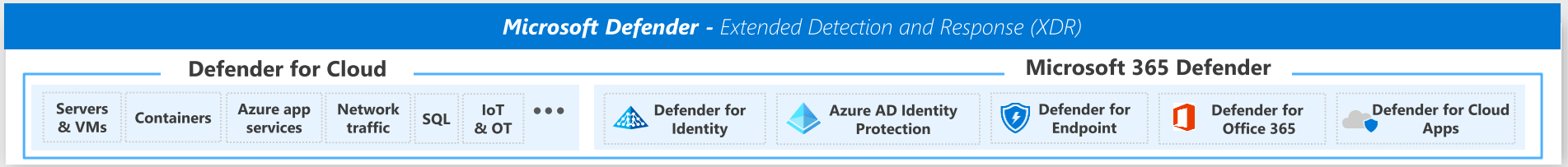
Hunting & ML Model Generation
Historic Hunting and ML training



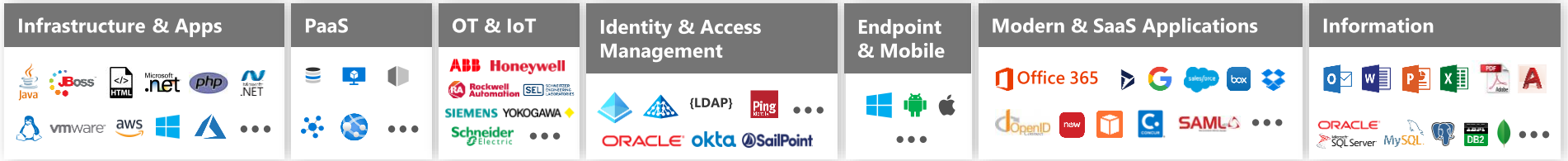
Multi-Source Hunting
Hunting on multiple data sources on longer timeframes



Purpose-Built Hunting
Hunting on XDR dataset to enhance on lower quality detections

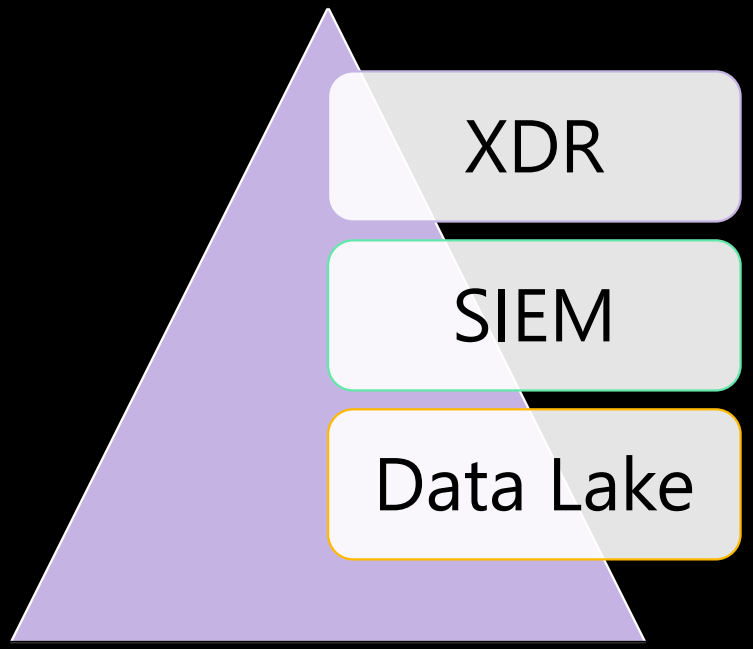


Raw Data
Security & Activity Logs



Hunting ecosystem and technologies

Based on our Use Cases and maturity , we can hunt on different datasets:



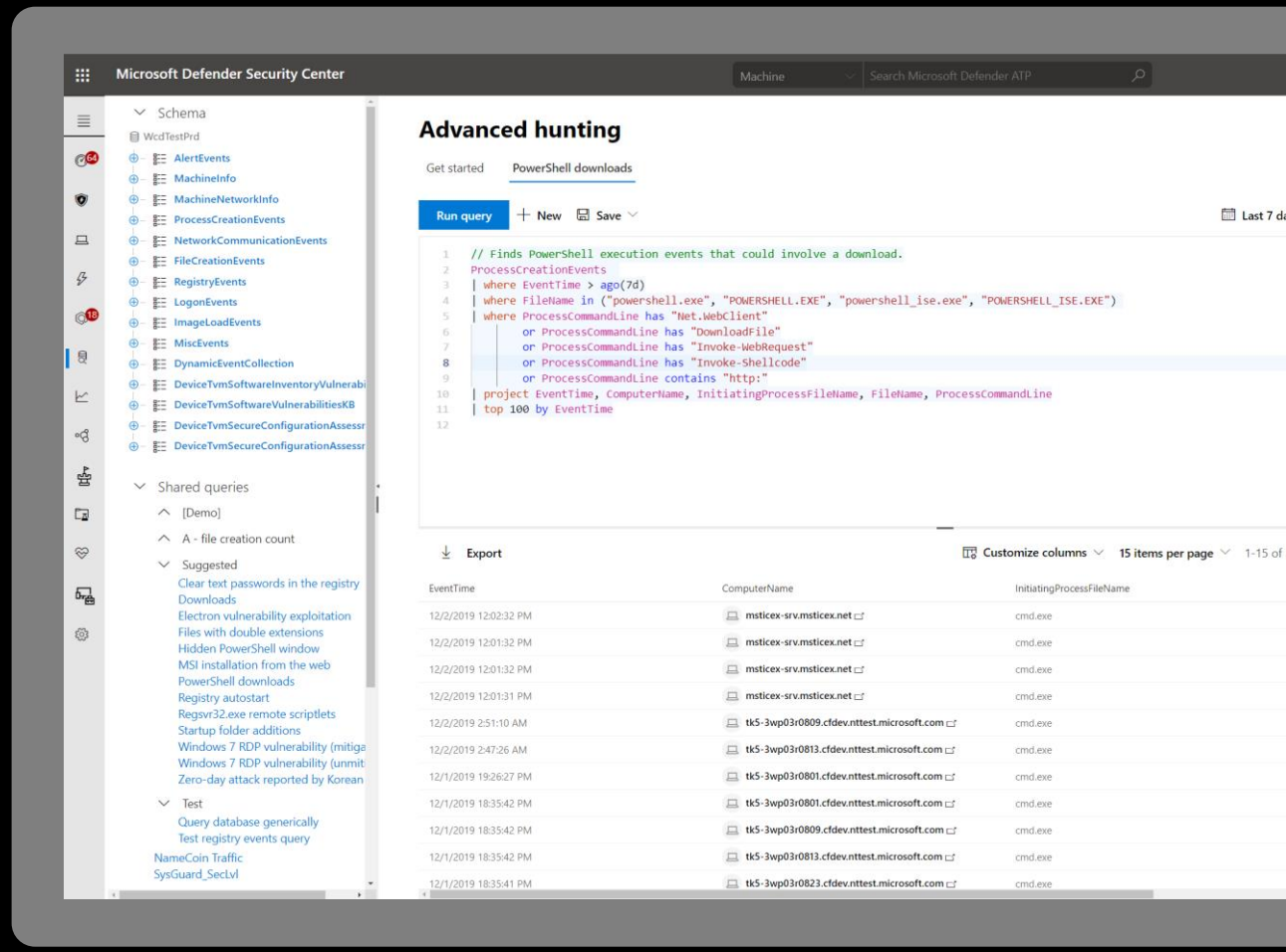
Microsoft 365 Defender Advanced Hunting
- Limited to XDR data within retention time (days of data)
- Low entry barrier with guided experiences

Microsoft Sentinel: Hunting Queries, LAW queries, Notebooks
- Large data set in LAW (months to years of data)
- Advanced knowledge required
- More flexibility of working with data (i.e. Jupyter)

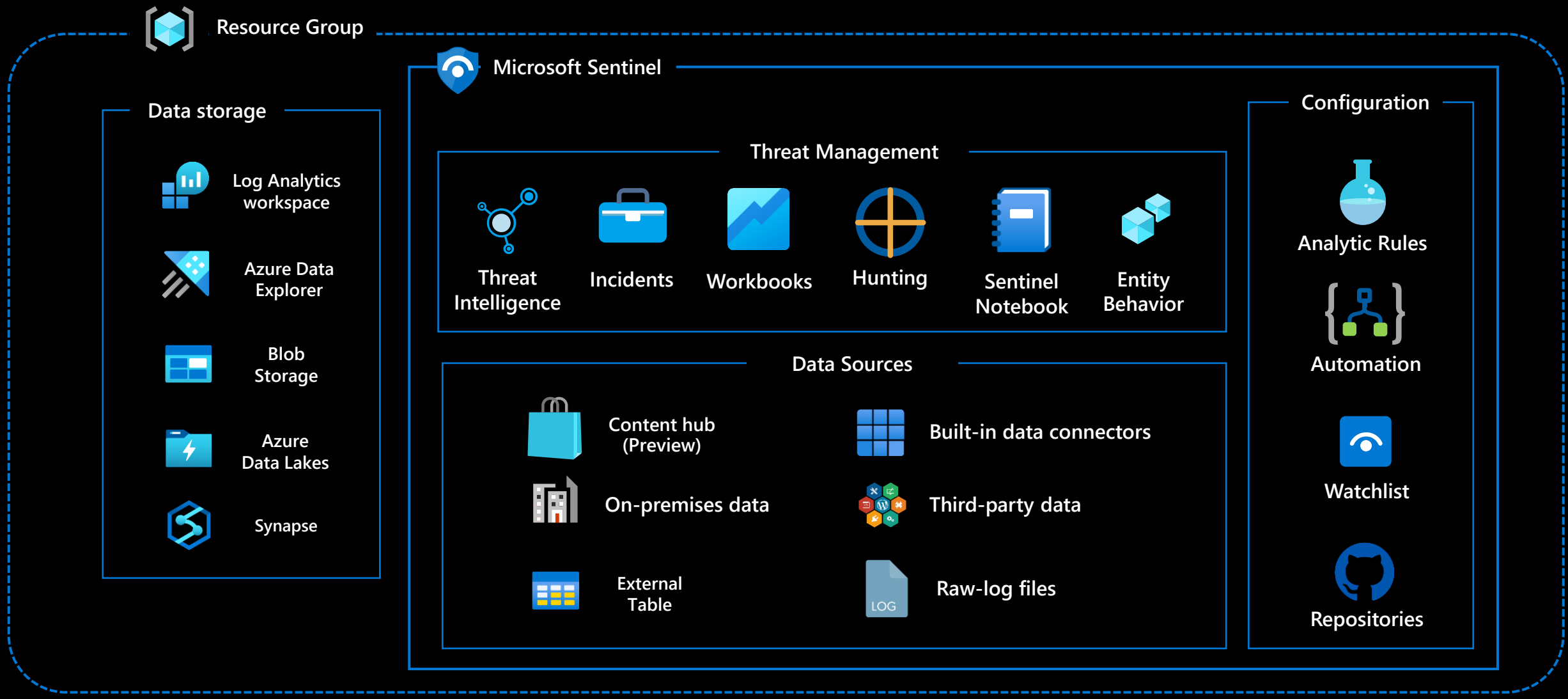
ADX or Azure Data Lake + Azure Synapse + Azure Databricks
- Data set becomes almost unlimited (decades of data)
- Data Scientists to work on the data might be required
- Full flexibility of languages and tools (R, Python, Spark, etc.)

Hunting in Defender 365

- Build queries with the integrated query builder
- Customize and create your own hunting queries using KQL
- Create custom detections with attached response actions
- Query raw data from endpoints, identity, mail and cloud apps

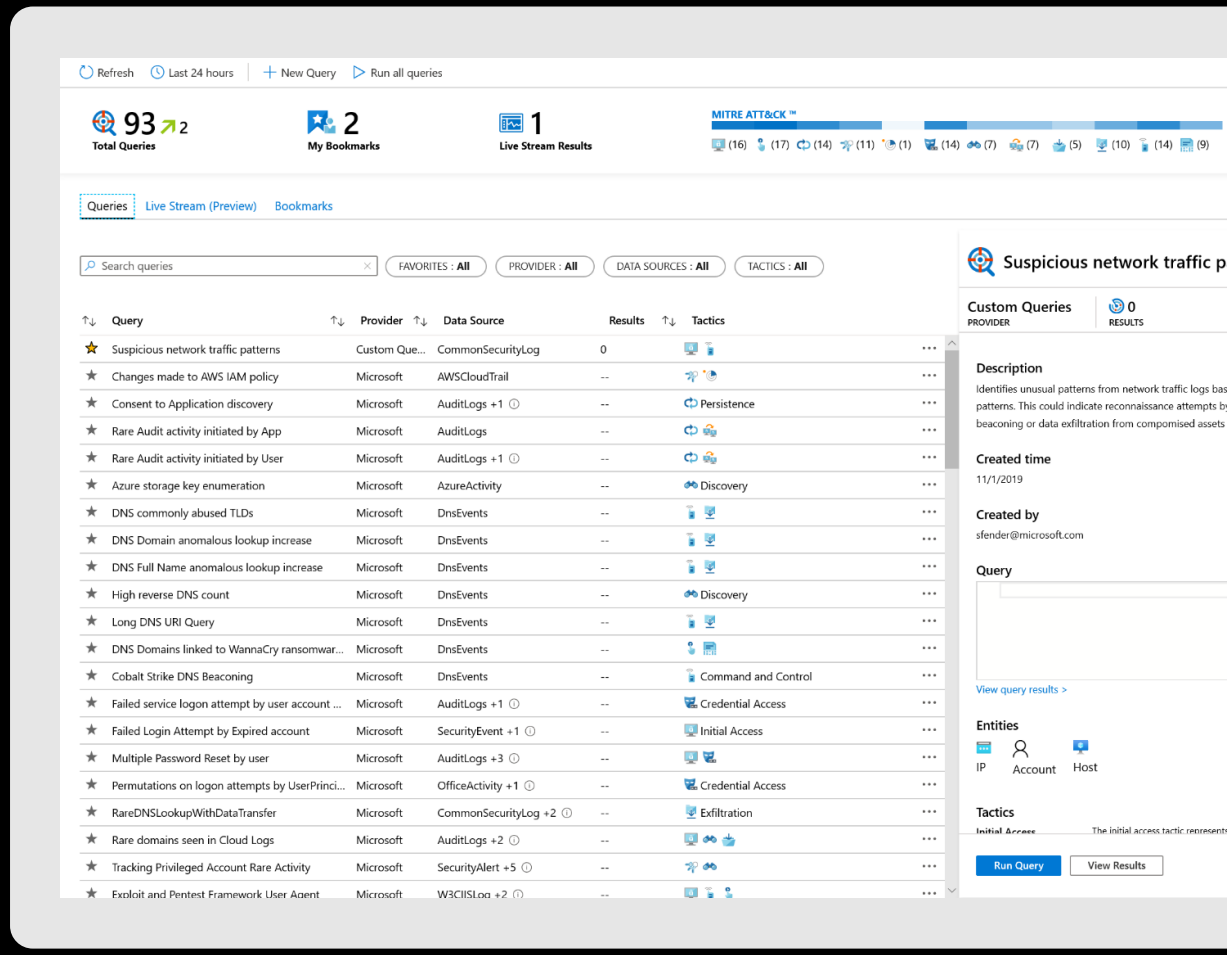


Microsoft Sentinel Core Capabilities



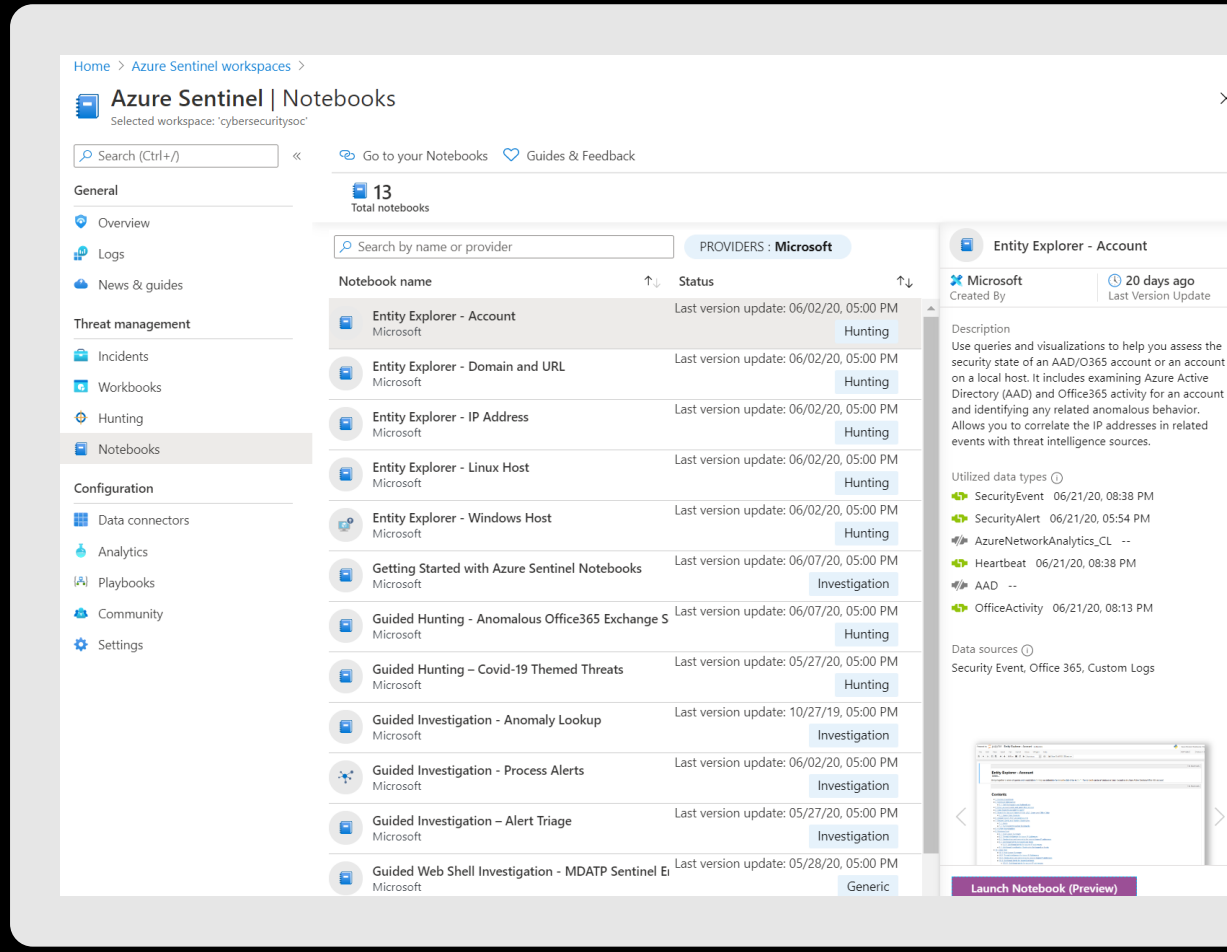
Hunting in Sentinel with the Hunting interface

- Run built-in threat hunting queries—no prior query experience required
- Customize and create your own hunting queries using KQL
- Integrate hunting and investigations
- Use bookmarks and live stream to manage your hunts

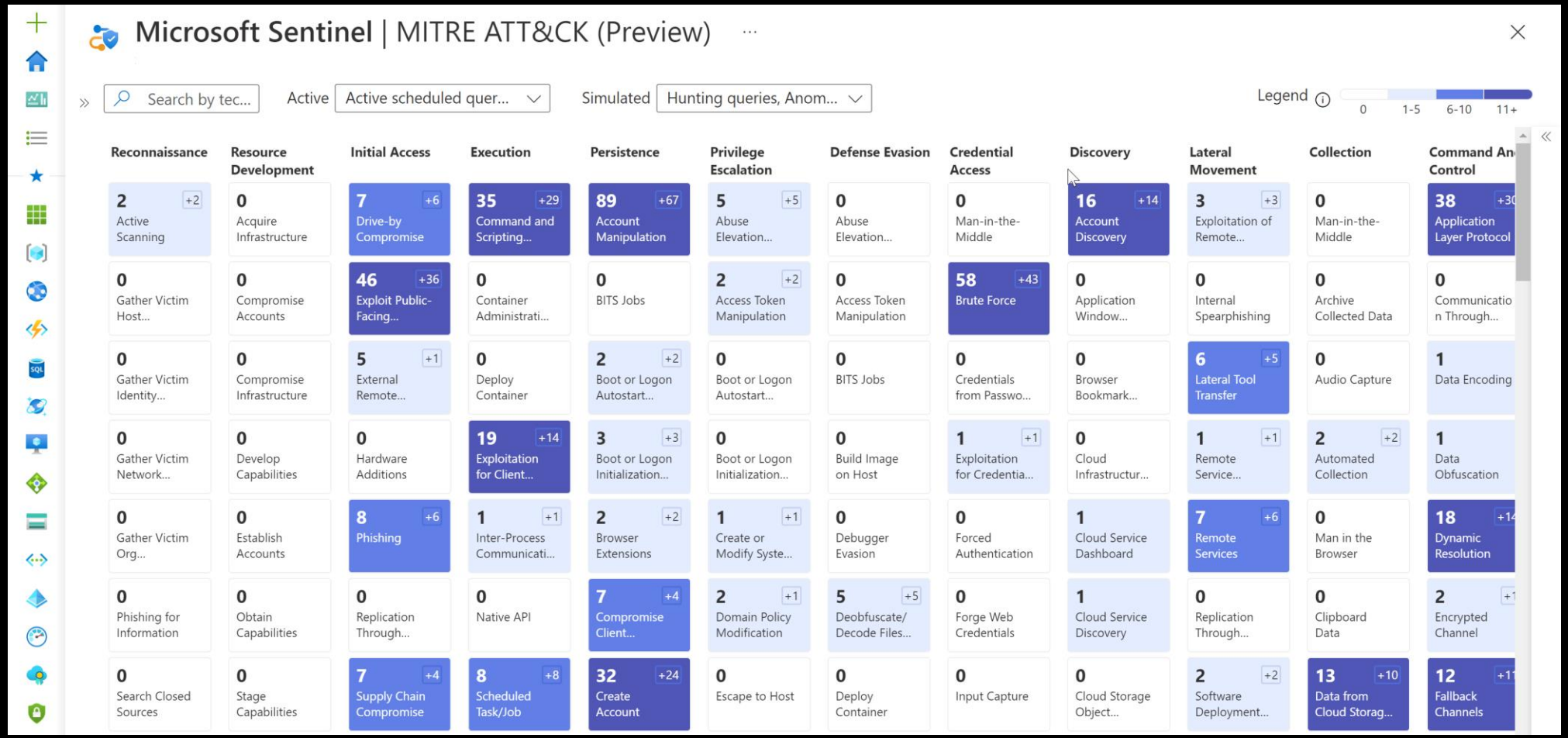


Jupyter notebooks for advanced hunting in Sentinel

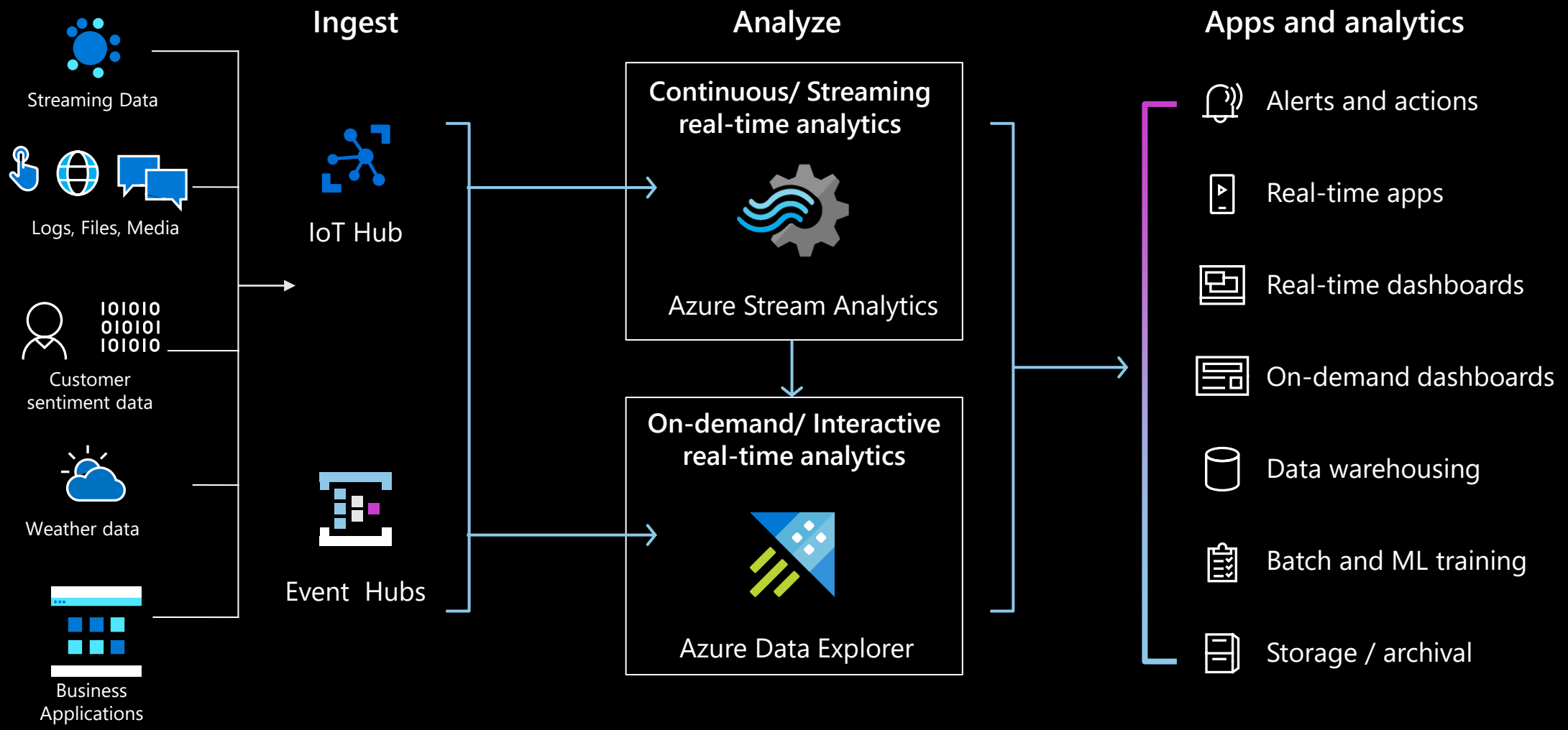
- Run in Azure Machine Learning (or Synapse)
- Use sample templates to help you get started
- Save as sharable HTML/JSON
- Query Microsoft Sentinel data and bring in external data sources
- Use your language of choice—Python, SQL, KQL, R, …



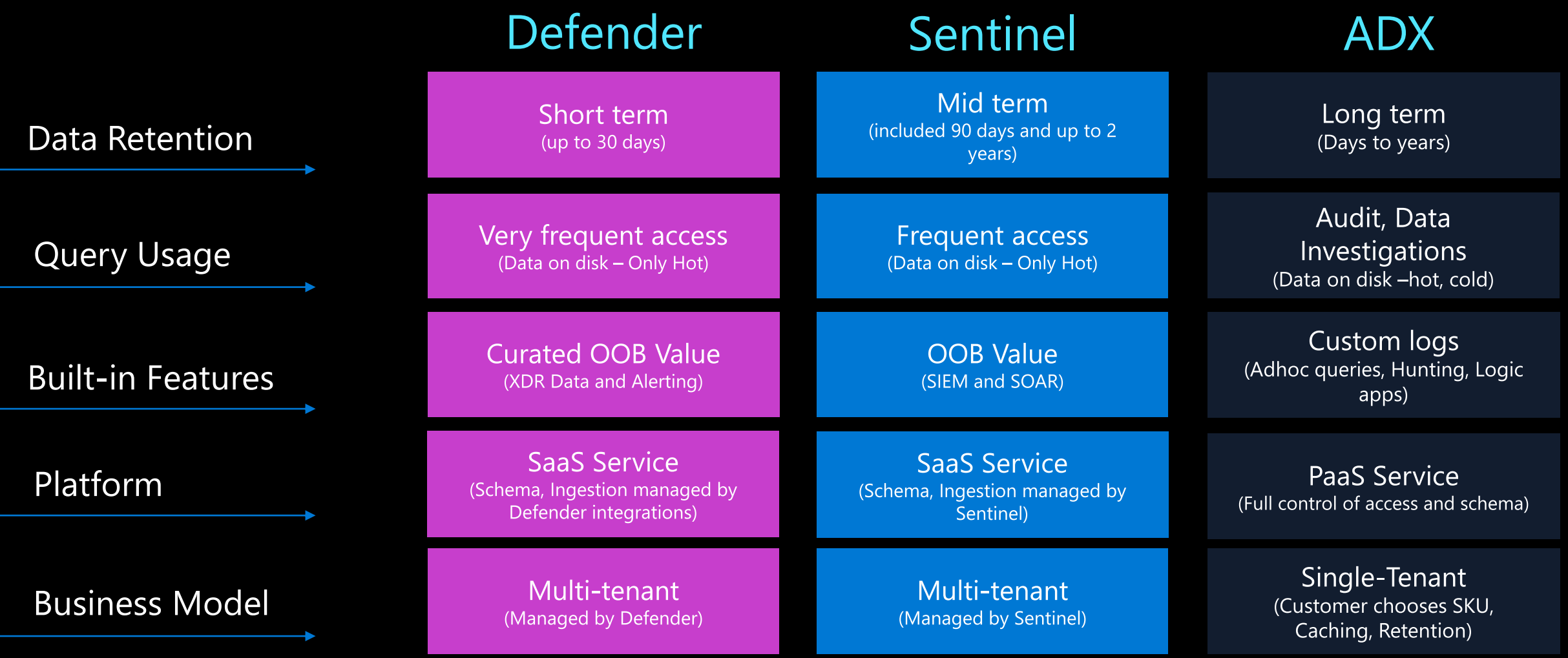
MITRE ATT&CK in Sentinel



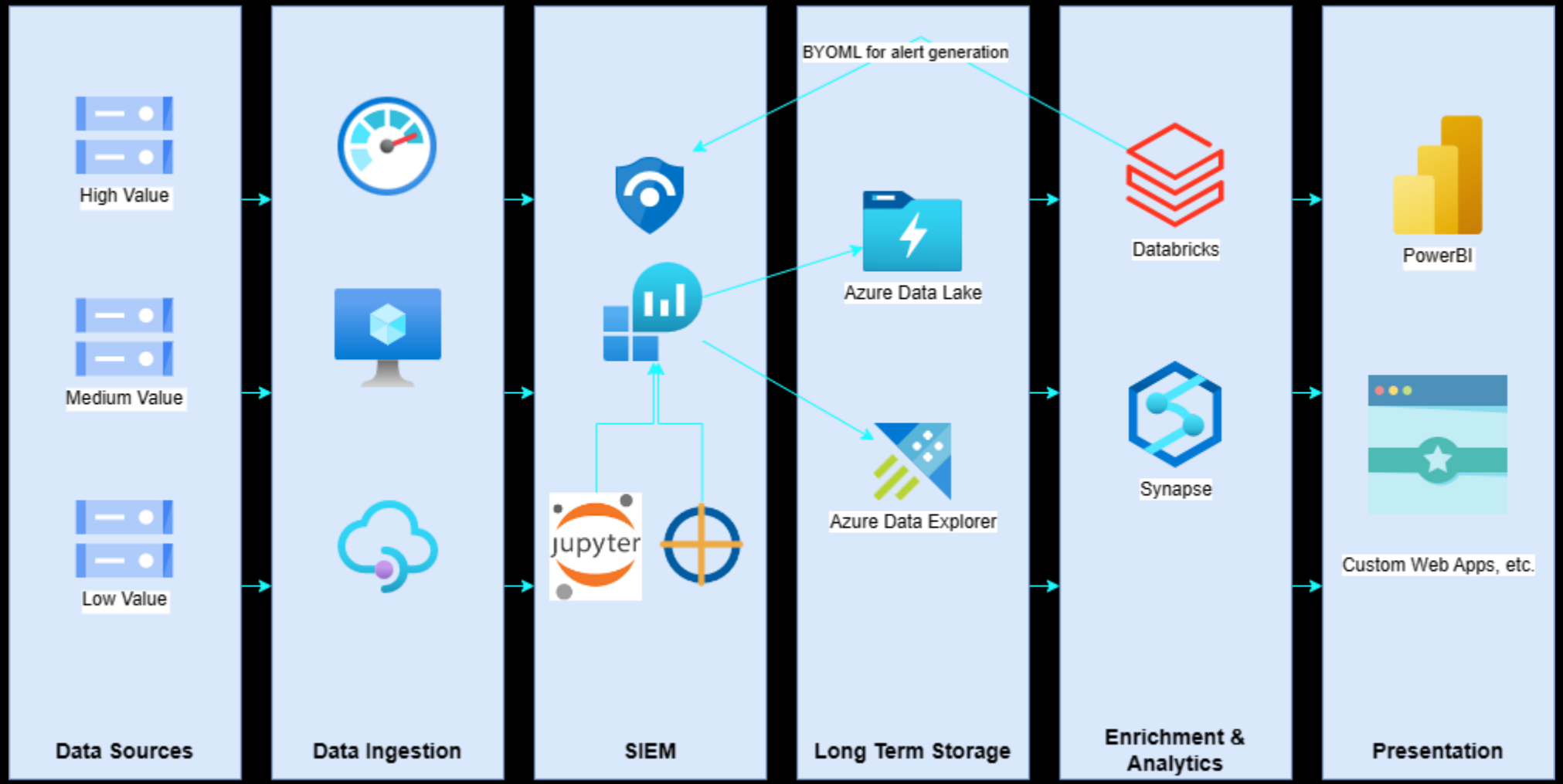
Using ADX for real-time analytics



Defender and/or ADX or/and Sentinel LAW



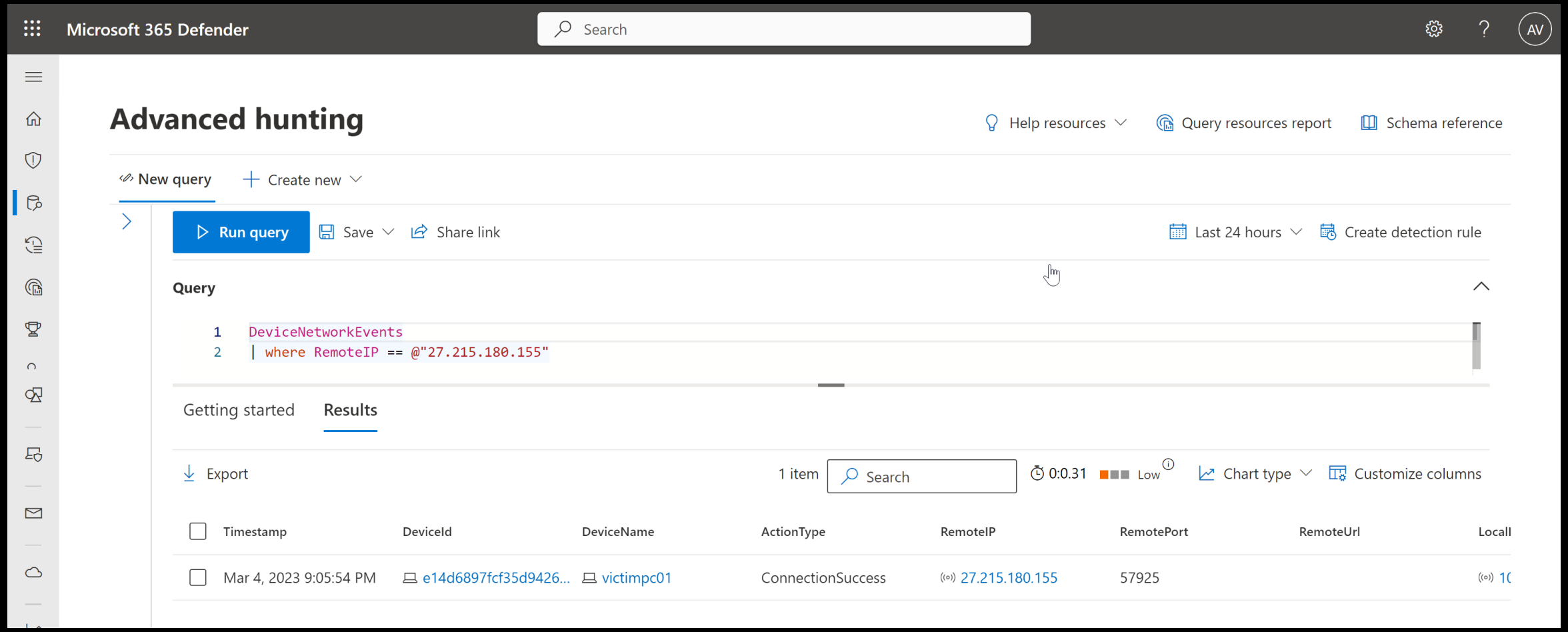
Hunting Tiers in the MSFT Stack (an example)



Demos

Threat Hunting – IP Address

Hunting for IP Address



Threat Hunting – Valid Accounts

[Valid Accounts: Domain Accounts, Sub-technique T1078.002 - Enterprise | MITRE ATT&CK®]

```
let ADPrivGroups = dynamic(["Access Control Assistance Operators",
"Account Operators","Administrators","ADSyncAdmins","ADSyncBrowse",
"ADSyncOperators","ADSyncPasswordSet","Allowed RODC Password Replication Group","Backup Operators",
"Cert Publishers","Certificate Service DCOM Access","Cloneable Domain Controllers","Cryptographic Operators",
"Denied RODC Password Replication Group","Distributed COM Users","DnsAdmins","DnsUpdateProxy","Domain Admins",
"Domain Controllers","Domain Guests","Enterprise Admins","Enterprise Key Admins","Enterprise Read-only Domain Controllers","Event Log Readers","Group Policy
"Hyper-V Administrators","IIS_IUSRS","Incoming Forest Trust Builders","Key Admins","Network Configuration Operators","Performance Log Users","Performance Mor
"Print Operators","Protected Users","RAS and IAS Servers","RDS Endpoint Servers","RDS Management Servers","RDS Remote Access Servers",
"Read-only Domain Controllers","Remote Desktop Users","Remote Management Users","Replicator",
"Schema Admins","Server Operators","Storage Replica Administrators""Terminal Server License Servers","Windows Authorization Access Group"]);
IdentityDirectoryEvents
| where TimeGenerated > ago(30d)
| where ActionType == "Group Membership changed"
| extend Actor = tostring(AdditionalFields ['ACTOR.ACCOUNT'])
| extend Operation = iff(AdditionalFields contains "TO.GROUP","Add",iff(AdditionalFields contains "FROM.GROUP","Remove","Undefined"))
| extend ChangedGroup = iff(Operation == "Add", AdditionalFields['TO.GROUP'],iff(Operation == "Remove", AdditionalFields['FROM.GROUP'],"Undefined"))
| project TimeGenerated , ActionType , Operation , ChangedGroup, Actor, TargetAccountUpn
| where ChangedGroup in(ADPrivGroups)
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	ActionType	Operation	ChangedGroup	Actor	TargetAccountUpn
2.2.2023, 12:15:40.556	Group Membership changed	Add	Domain Admins	[redacted]	[redacted]

User Added to Domain Admin Group

Threat Hunting – Commonly used Port

[Commonly Used Port, Technique T0885 - ICS | MITRE ATT&CK®]

```
1
2  //iana_port_assignments
3  // Service Name,Port Number,Transport Protocol,Description,Assignee,Contact,Registration Date,Modification Date,Reference,Service Code,Unauthorized Use Reported,Assignme
4  let iana_port_assignments = (externaldata(ServiceName:string,PortNumber:int ,Transport:string,Protocol:string,Description:string) [@"https://www.iana.org/assignments/se
5  with (format="csv",ignoreFirstRecord=true));
6  iana_port_assignments
7  | join kind=rightouter (DeviceNetworkEvents)
8  on $left. PortNumber == $right.RemotePort
9  | where isnotempty( PortNumber)
10 | summarize EventCount=count() by PortNumber,RemotePort, ServiceName
11 | sort by PortNumber
```

Results | Chart | Add bookmark

PortNumber	RemotePort	ServiceName	EventCount
0	0		32
11	11	systat	2
21	21	ftp	1'074
22	22	ssh	495
23	23	telnet	278

Threat Hunting – Commonly used Port

[Commonly Used Port, Technique T0885 - ICS | MITRE ATT&CK®]

New Query 3* | New Query 4*

Run | Time range : Set in query | Save | Share | New alert rule | Export | Pin to | Format query

```
14  DeviceNetworkEvents
15  | where TimeGenerated > ago(90d)
16  | where RemoteIPType == 'Public'
17  | where RemotePort == 22
18  | project TimeGenerated,  InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
19
20  DeviceNetworkEvents
21  | where TimeGenerated > ago(90d)
22  | where RemoteIP contains [redacted].84"
23  | project TimeGenerated,  InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
24
25  DeviceNetworkEvents
26  | where TimeGenerated > ago(90d)
27  | where RemoteUrl contains [redacted].ch"
28  | project TimeGenerated,  InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
29
30  DeviceNetworkEvents
31  | where TimeGenerated > ago(90d)
32  | where RemoteIP contains [redacted].5"
33  | project TimeGenerated,  InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	InitiatingProcessCommandLine	RemoteIP	RemoteUrl	ActionType
19.12.2022, 08:11:42.982	[redacted].ch	[redacted].84	[redacted].ch	ConnectionFailed
4.1.2023, 18:46:02.588	"msedge.exe" --type=utility --utility-sub-type=...	[redacted].5	[redacted].ch	ConnectionSuccess

Threat Hunting – Remote Desktop

[Remote Services: Remote Desktop Protocol, Sub-technique T1021.001 - Enterprise | MITRE ATT&CK®]

```
13
14 DeviceNetworkEvents
15 | where TimeGenerated > ago(90d)
16 | where RemoteIPType == 'Public'
17 // | where LocalPort == 3389
18 | where RemotePort == 3389
19 | project TimeGenerated,  InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingProcessAccountName
20 // | summarize count() by DeviceName
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	InitiatingProcessComman...	RemoteIP	RemoteUrl	ActionType	DeviceName	LocalPort	InitiatingP
27.12.2022, 11:40:02.984	"mstsc.exe"	[redacted]	[redacted]	ConnectionFailed	[redacted]	61'556	[redacted]
7.12.2022, 06:43:57.721	mstsc.exe -Embedding			ConnectionFailed		55'452	
1.1.2023, 15:19:06.261	"mstsc.exe" "C:\Users\0chelee...			ConnectionFailed		62'002	

Threat Hunting – Account Discovery

[Net, Software S0039 | MITRE ATT&CK®]

[Account Discovery: Domain Account, Sub-technique T1087.002 - Enterprise | MITRE ATT&CK®]

```
DeviceProcessEvents
| where TimeGenerated > ago(30d)
| extend cmd = parse_command_line(InitiatingProcessCommandLine,"windows")
| where InitiatingProcessFileName == 'net.exe'
| mv-expand cmd
| summarize count() by tostring(cmd)

let netcommands = dynamic(["stop","accounts","domain","bits",'config','session']);
DeviceProcessEvents
| where TimeGenerated > ago(30d)
| extend cmd = parse_command_line(InitiatingProcessCommandLine,"windows")
| where InitiatingProcessFileName == 'net.exe'
| mv-expand cmd
| where cmd has_any (netcommands)
| project TimeGenerated,DeviceName,AccountName, InitiatingProcessCommandLine, cmd
| where cmd contains "domain"
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	DeviceName	AccountName	InitiatingProcessCommandL...	cmd
3.3.2023, 18:07:11.208	[redacted]	[redacted]	net user [redacted] /domain	/domain

Threat Hunting – Top 10 abused domains

The 10 Most Abused Top Level Domains

Threat Hunting – Files originating from suspicious sources

Analyzing file downloads (executables, scripts, macros)

```
let excludedomains = dynamic(["microsoft.com","sharepoint.com","dell.com","office.net","adobe.com"]);
let fileextensions = dynamic(["exe","ps1","xlsm","scr","bat","cmd"]);
DeviceFileEvents
| where isnotempty( FileOriginUrl)
| project TimeGenerated, FileName, FileOriginUrl
| extend tld = tostring(split(FileOriginUrl, ".")[-1])
| extend PU = parse_url(FileOriginUrl)
| extend Timestamp = TimeGenerated
| project Timestamp, FileName, FileOriginUrl, PU
| evaluate bag_unpack(PU,columnsConflict='keep_source') : (Timestamp:timespan, FileName:string,Host:string,FileOriginUrl:string )
| extend FileExtension = extract("\\.([0-9A-Za-z]+)(?:[\\?#]|$)", 1, FileName)
| extend domain = extract(@"(\w+\.\w+)$", 1, Host)
```

Results | Chart | Add bookmark

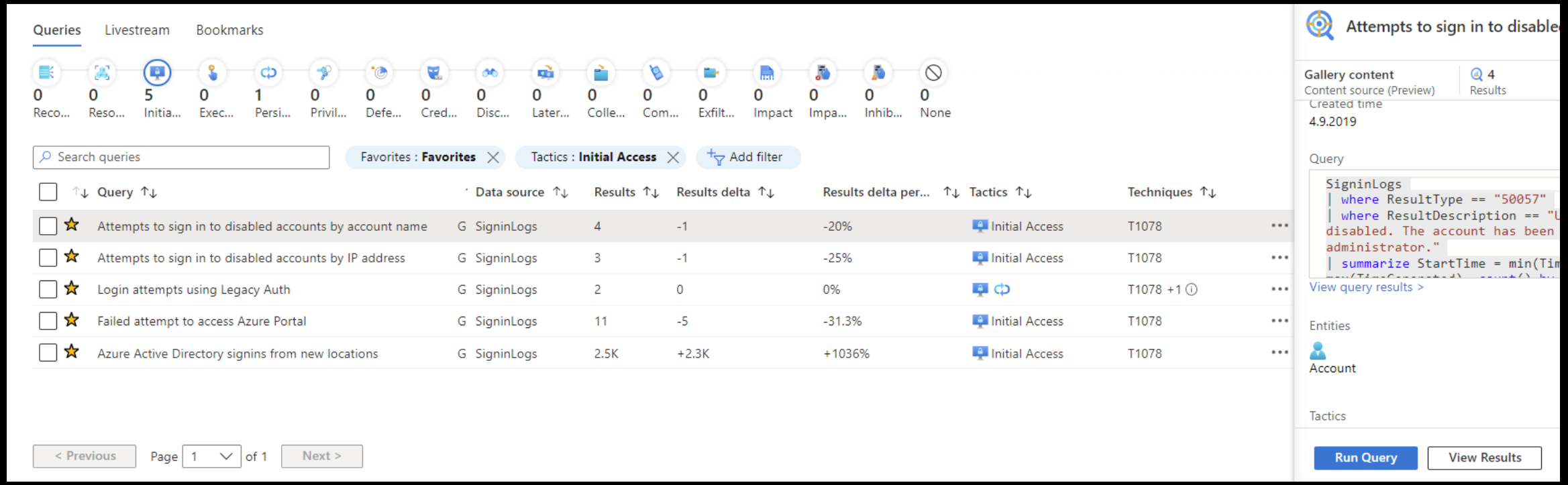
domain	FileName	FileExtension	FileOriginUrl
[redacted]			
earth.li	putty.exe	exe	https://the.earth.li/~sgtatham/putty/0.78/w64/putty.exe
lastpass.com	$RC7RFAL.exe	exe	https://download.cloud.lastpass.com/windows_installer/LastPassInstaller.exe
nanocad.ru	$R1B8UD4.exe	exe	https://ftp.nanocad.ru/free_en/NCE50_2007_.exe
[redacted]			

Columns

2s 698ms | Display time (UTC+00:00) | Query details | 46 - 55 of 879

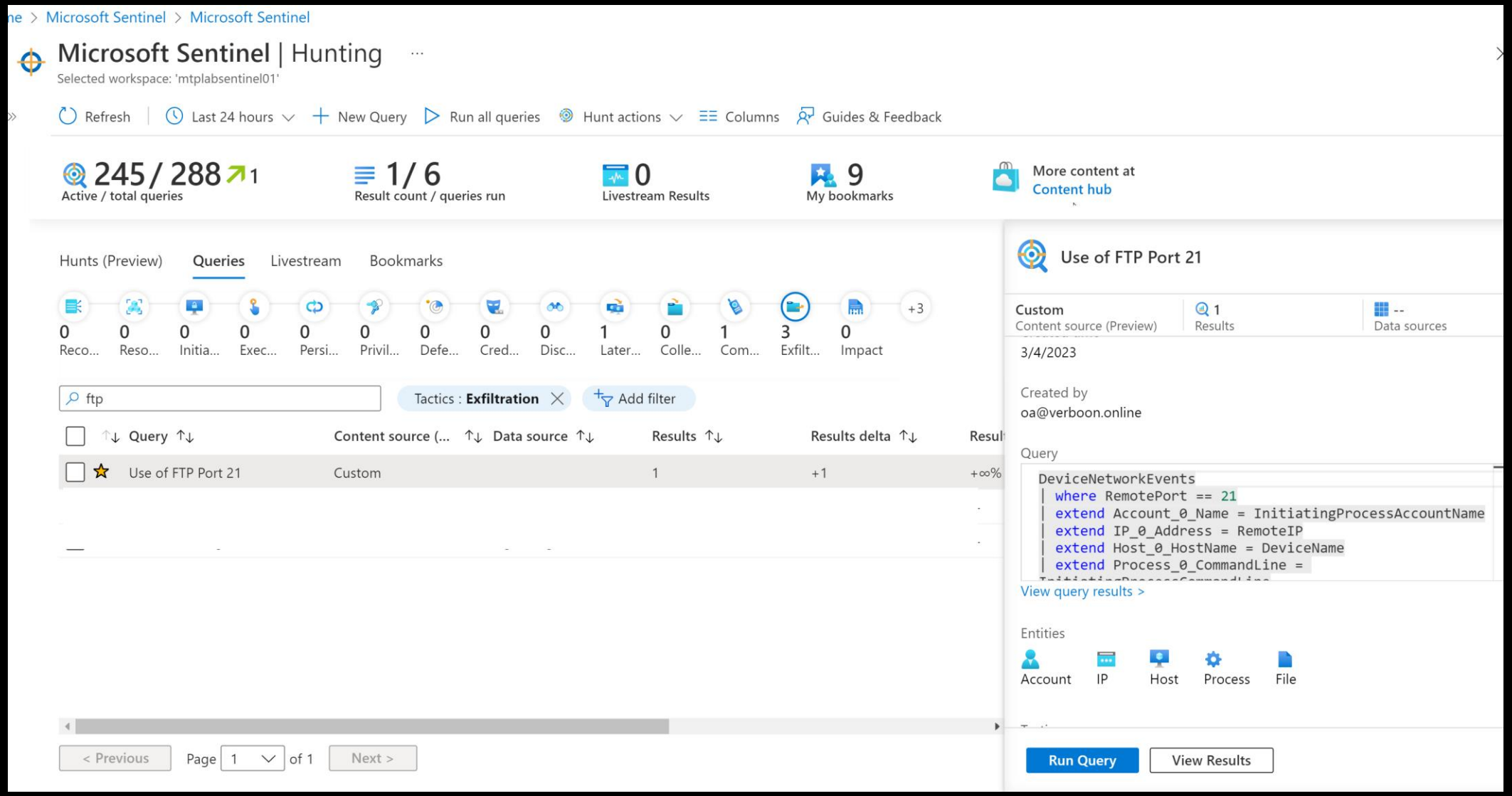
Threat Hunting in Sentinel

Hunting Queries



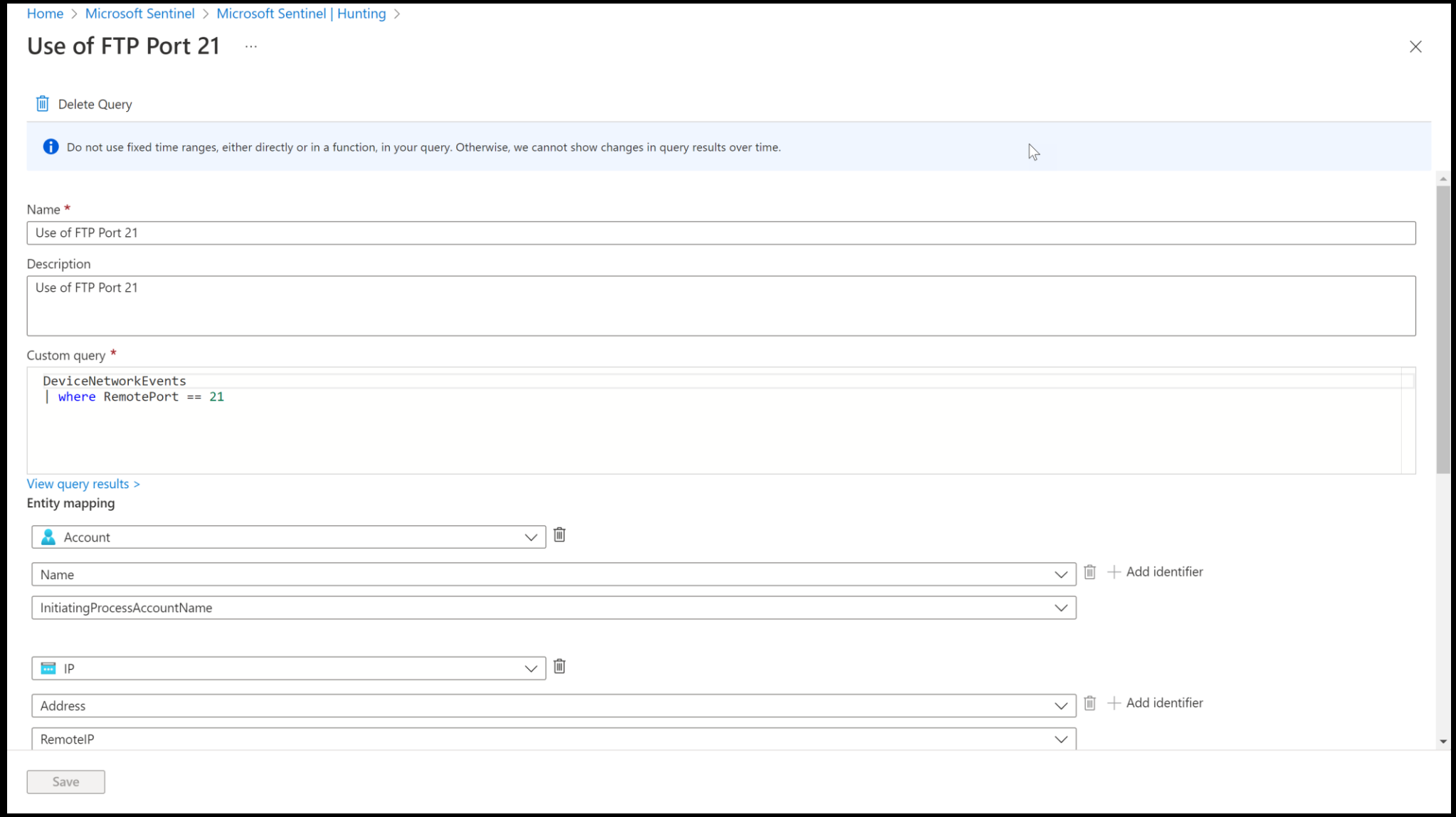
Threat Hunting in Microsoft Sentinel

Hunting Queries



Threat Hunting in Microsoft Sentinel

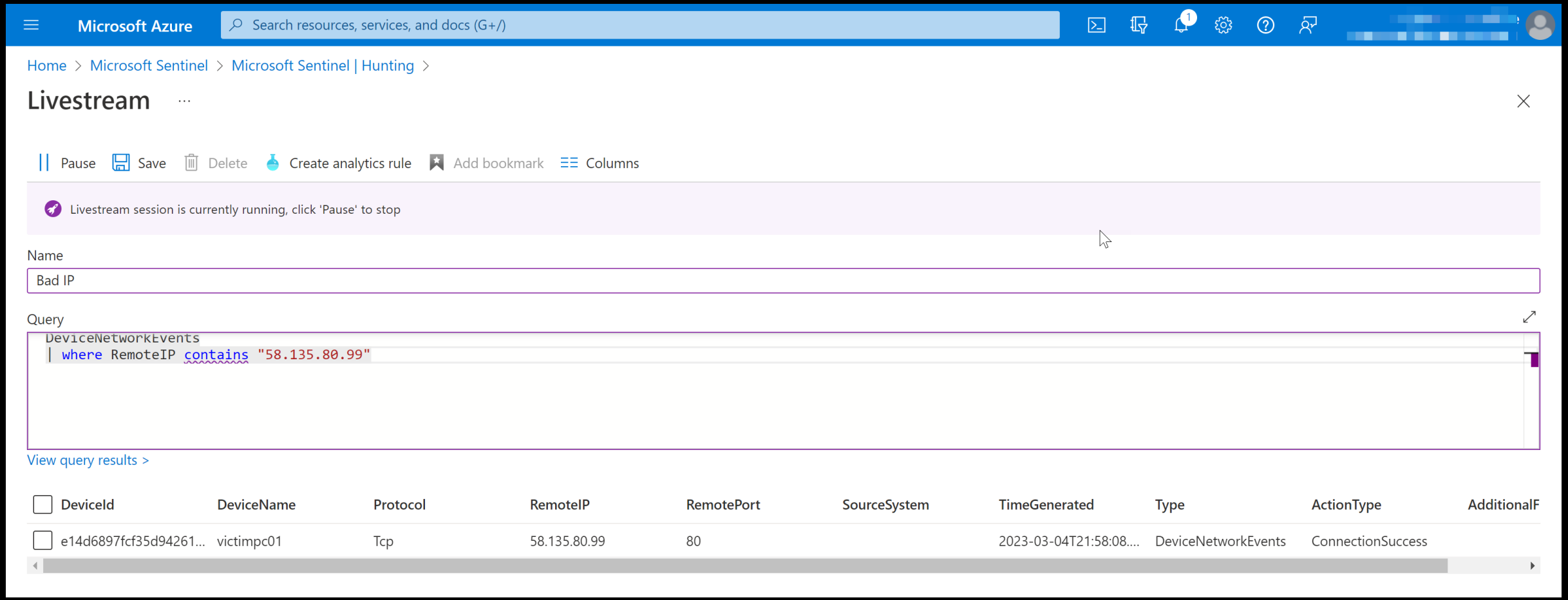
Hunting Queries



Identify activity on Port 21 (FTP)

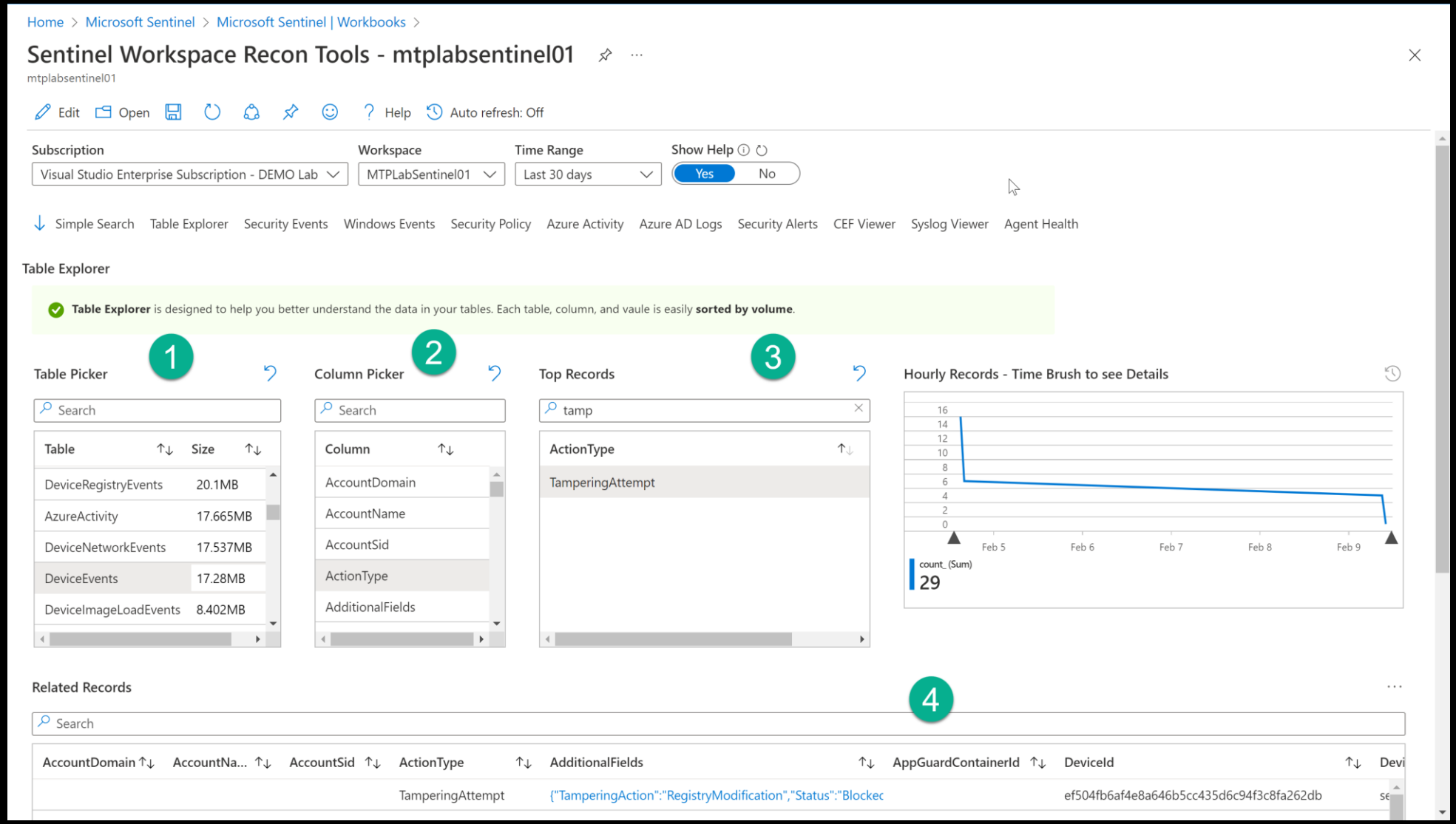
Threat Hunting in Microsoft Sentinel

Live Stream



Threat Hunting in Microsoft Sentinel

Not (yet) comfortable with KQL? Use the Sentinel Workspace Recon Tools workbook



Microsoft

Additional Resources

THREAT HUNTING SURVIVAL GUIDE – Microsoft

The art and science behind Microsoft threat hunting: Part 1 - Microsoft Security Blog

Threat hunting: Part 1—Why your SOC needs a proactive hunting team (microsoft.com)

Improving AI-based defenses to disrupt human-operated ransomware - Microsoft Security Blog