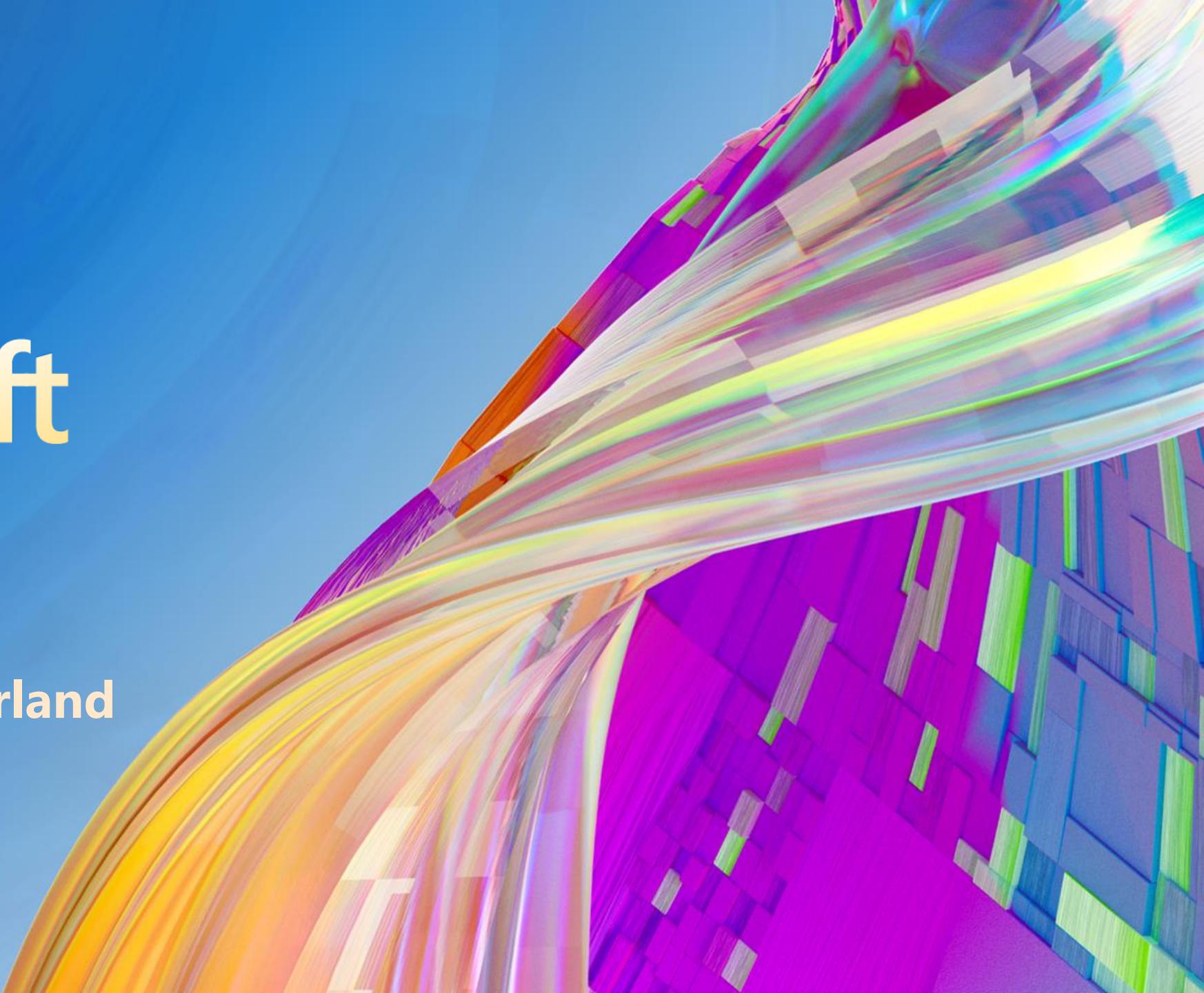




Microsoft Ignite

Spotlight on Switzerland
Kongresshaus Zürich
March 9, 2023





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



**Traditional Focus –
Detections, events, etc.**

Why Threat Hunting

- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command & Control

EDR Detections

Microsoft 365 Defender

Devices > victimpc01

victimpc01

High Active

Device value Manage tags ...

Overview Incidents and alerts Timeline Security recommendations Software inventory Browser extensions Discovered vulnerabilities Missing KBs ...

Oct 2022 Nov 2022 Dec 2022 Jan 2023 Feb 2023 Mar 2023

Maximize

Highlighted alert: Attempt to turn off Microsoft Defender Antivirus protection X

Export Search

Feb 26, 2023 8:26:08 PM - Mar 5, 2023 8:26:08 PM ▾ Customize columns Filter

Event time ↓	Event	Additional information	User
Mar 5, 2023 8:26:08.114 PM	■■■ Attempt to turn off Microsoft Defender Antivirus protection	DefenseEvasion	
Mar 5, 2023 8:26:08.114 PM	powershell.exe set registry value 'DisableAntiSpyware' for key 'SOFTWARE...' T1112: Modify Registry T1106: Native API		ladmin
Mar 5, 2023 8:26:08.114 PM	powershell.exe has turned off Windows Defender AV security feature Disa... T1562.001: Disable or Modify Tools		ladmin
Mar 5, 2023 8:26:08.114 PM	powershell.exe set registry value for key 'HKEY_LOCAL_MACHINE\SOFTWA...	DefenseEvasion	ladmin
Mar 5, 2023 8:26:08.108 PM	powershell.exe ran Powershell command: 'Set-ItemProperty'		ladmin
Mar 5, 2023 8:26:08.099 PM	powershell.exe loaded module System.Configuration.Install.ni.dll		ladmin

Load newer results

...

EDR Detections

Microsoft 365 Defender

Search

Devices > victimpc01

victimpc01
High Active

Overview Incidents and alerts Timeline Security recommendations Software inventory Browser extensions Discovered vulnerabilities Missing KBs ...

Oct 2022 Nov 2022 Dec 2022 Jan 2023 Feb 2023 Mar 2023

Maximize

Export Search 1 selected 1 Day Customize columns Filter

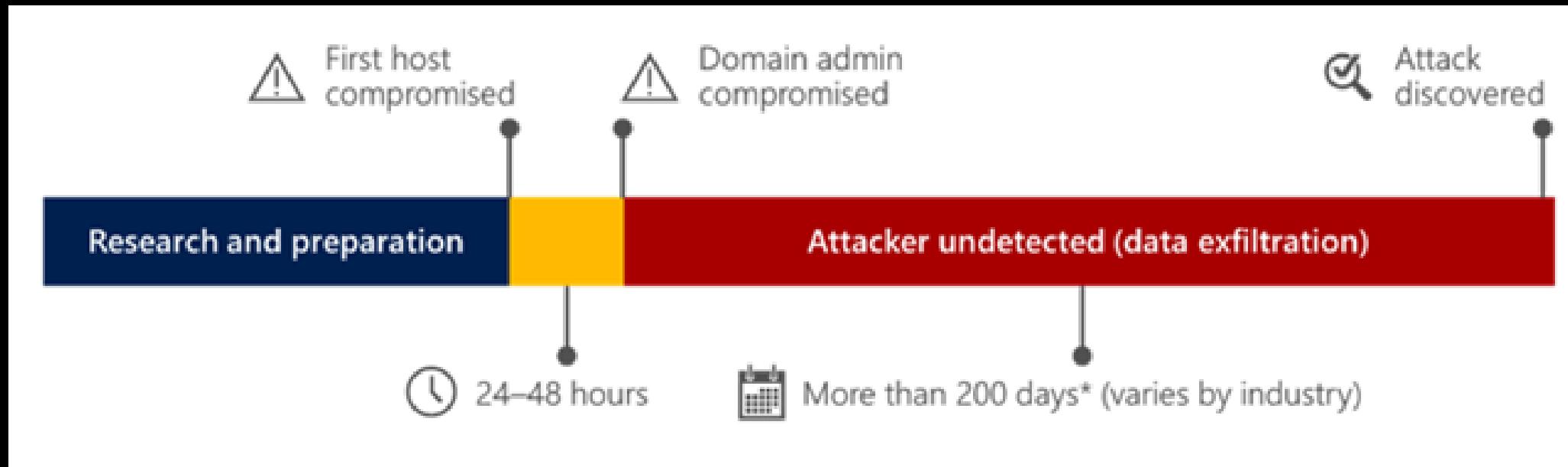
Event time	Event	Additional information	User
Mar 5, 2023 9:01:02.054 PM	<input type="checkbox"/> A network packet from 10.0.0.8 to 168.63.129.16 matched signature HTTP_Cli...		
Mar 5, 2023 9:00:59.675 PM	<input type="checkbox"/> A network packet from 168.63.129.16 to 10.0.0.8 matched signature HTTP_Se...		
Mar 5, 2023 9:00:59.674 PM	<input type="checkbox"/> A network packet from 10.0.0.8 to 168.63.129.16 matched signature HTTP_Cli...		
Mar 5, 2023 9:00:52.551 PM	<input type="checkbox"/> A network packet from 168.63.129.16 to 10.0.0.8 matched signature HTTP_Se...		
Mar 5, 2023 9:00:52.551 PM	<input type="checkbox"/> A network packet from 10.0.0.8 to 168.63.129.16 matched signature HTTP_Cli...		
<input checked="" type="checkbox"/> Mar 5, 2023 9:00:49.171 PM	<input type="checkbox"/> cmd.exe performed system network connections discovery by invoking ne... T1049: System Network Connections Discovery +1 ladmin		
Mar 5, 2023 9:00:45.450 PM	<input type="checkbox"/> A network packet from 168.63.129.16 to 10.0.0.8 matched signature HTTP_Se...		

Load newer results

Q

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.

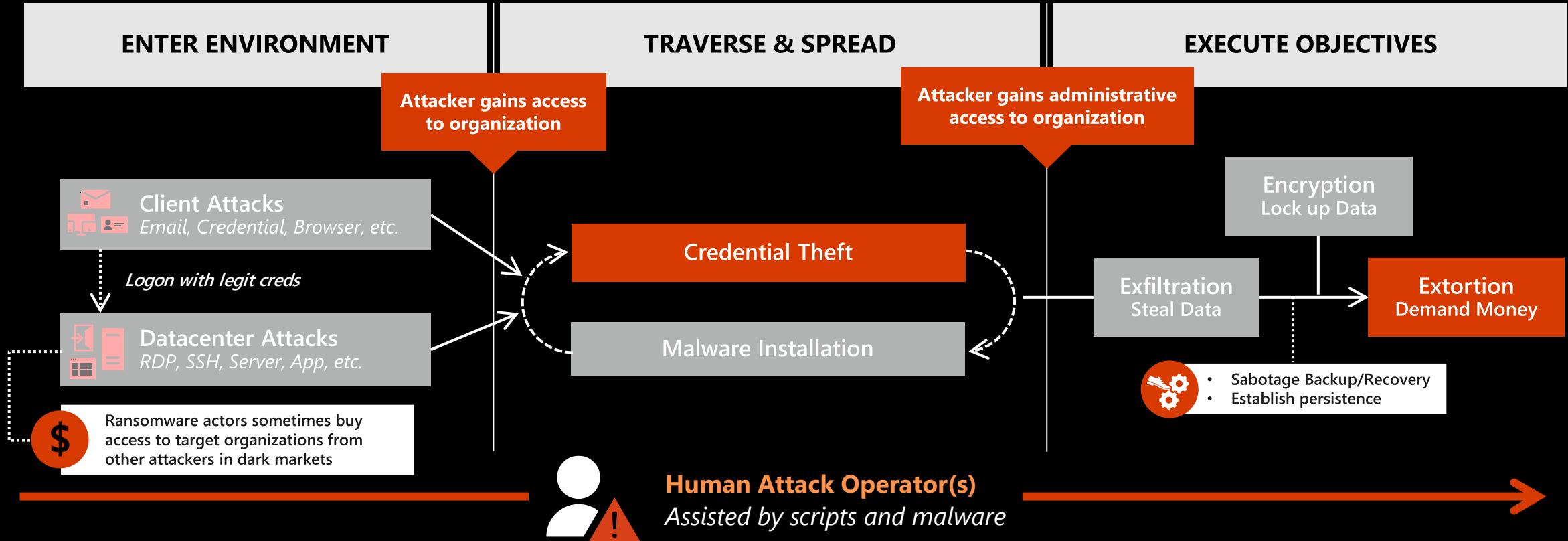
Commodity malware attacks are the hazards you encounter every day as users click on the wrong link or install the wrong program. In these situations, much of the attack logic is contained within the malware, so remediation is typically as simple as removing the malware, rebuilding the device, and / or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

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

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

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 🔎

Tactics

Techniques

layout: side ▾

show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
10 techniques	7 techniques	9 techniques	13 techniques	13 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Token Manipulation (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	BITS Jobs	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Cloud Infrastructure Discovery	Cloud Service Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Debugger Evasion	Deobfuscate/Decode Files or Information	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Cloud Service Discovery	Clipboard Data	Dynamic Resolution (3)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Container and Resource Discovery	Container and Resource Discovery	Container and Resource Discovery	Data from Cloud Storage	Encrypted Channel (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Debugger Evasion	Debugger Evasion	Debugger Evasion	Fallback Channels	Ingress Tool Transfer
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Domain Policy Modification (2)	Execution Guardrails (1)	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Multi-Stage Channels	Non-Application
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Event Triggered Execution (16)	Exploitation for Defense Evasion	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Data from Local System	Use Alternate Authentication
Search Victim-Owned Websites			Software Deployment Tools	External Remote	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Group Policy	Group Policy	Group Policy		

T1526

MITRE ATT&CK

Tactics

Techniques

The screenshot shows the 'Defense Evasion' section of the MITRE ATT&CK framework. At the top, there are three buttons: 'layout: side ▾', 'show sub-techniques', and 'hide'. Below this, the title 'Defense Evasion' is displayed with the subtitle '42 techniques'. A green rectangular box highlights the 'Impair Defenses (9)' category, which is expanded to show the following sub-techniques: Disable or Modify Tools, Disable Windows Event Logging, Impair Command History Logging, Disable or Modify System Firewall, Indicator Blocking, Disable or Modify Cloud Firewall, Disable Cloud Logs, Safe Mode Boot, Downgrade Attack, and Clear Windows Event Logs.

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

Home > Techniques > Enterprise > Impair Defenses



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](#)

① Tactic: [Defense Evasion](#)

① Platforms: Containers, IaaS, Linux, Network, Office 365, Windows, macOS

① 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 ? User icon

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.

```
graph LR; A((USB attachment inserted)) --> B((LNK file creates a CMD.exe process)); B --> C((MSlexec.exe using the device username and hostname connects to C2)); C --> D((Continued call outs to TOR nodes))
```

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

The screenshot shows the Microsoft Defender Threat Intelligence interface. At the top, there's a navigation bar with icons for Home, MDTI, Enterprise, RaspberryRobin, C2, and T1059.003. A search bar is also present. Below the navigation, the page title is "Home > Suspect Raspberry Robin C2 Domains o...". The main content area has tabs for "Description", "Public Indicators (10)", and "Defender TI Indicators (26)". The "Public Indicators" tab is selected. It lists three entries under "Public Indicators":

Type	Name
SHA-256 Hash	57a0ba0158324694abfb3f12b98707d6c1e289ad62d0e4314a904972d490b37f VirusTotal - ANY.RUN - Hybrid Analysis
SHA-256 Hash	992a84ebbe30c4849020c324463b611034496e41c540cb4d7852b5e29799bd57 VirusTotal - ANY.RUN - Hybrid Analysis
SHA-256 Hash	f7b9e262f52af04086b26988ce980dd28cae38f36ca16cc896418dbc0b8f2714 VirusTotal - ANY.RUN - Hybrid Analysis

Below these, there are two more entries:

Domain	Name
Domain	2t.pm
Domain	7d.wf

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

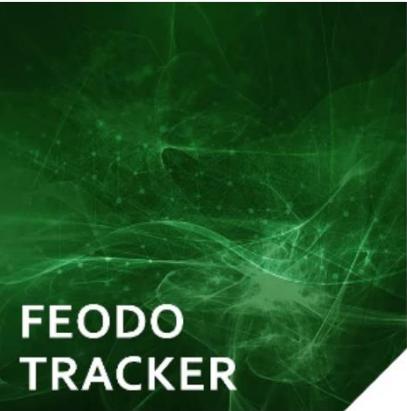
Threat Intelligence Feeds

ABUSE|ch

OUR MISSION OUR PLATFORMS BLOG STATISTICS CONTACT



Sharing malware samples with the community, AV vendors and threat intelligence providers



Tracking botnet C&C infrastructure associated with Emotet, Dridex and TrickBot



Collecting and providing a blocklist for malicious SSL certificates and JA3/JA3s fingerprints



Sharing malware distribution sites with the community, AV vendors and threat intelligence providers



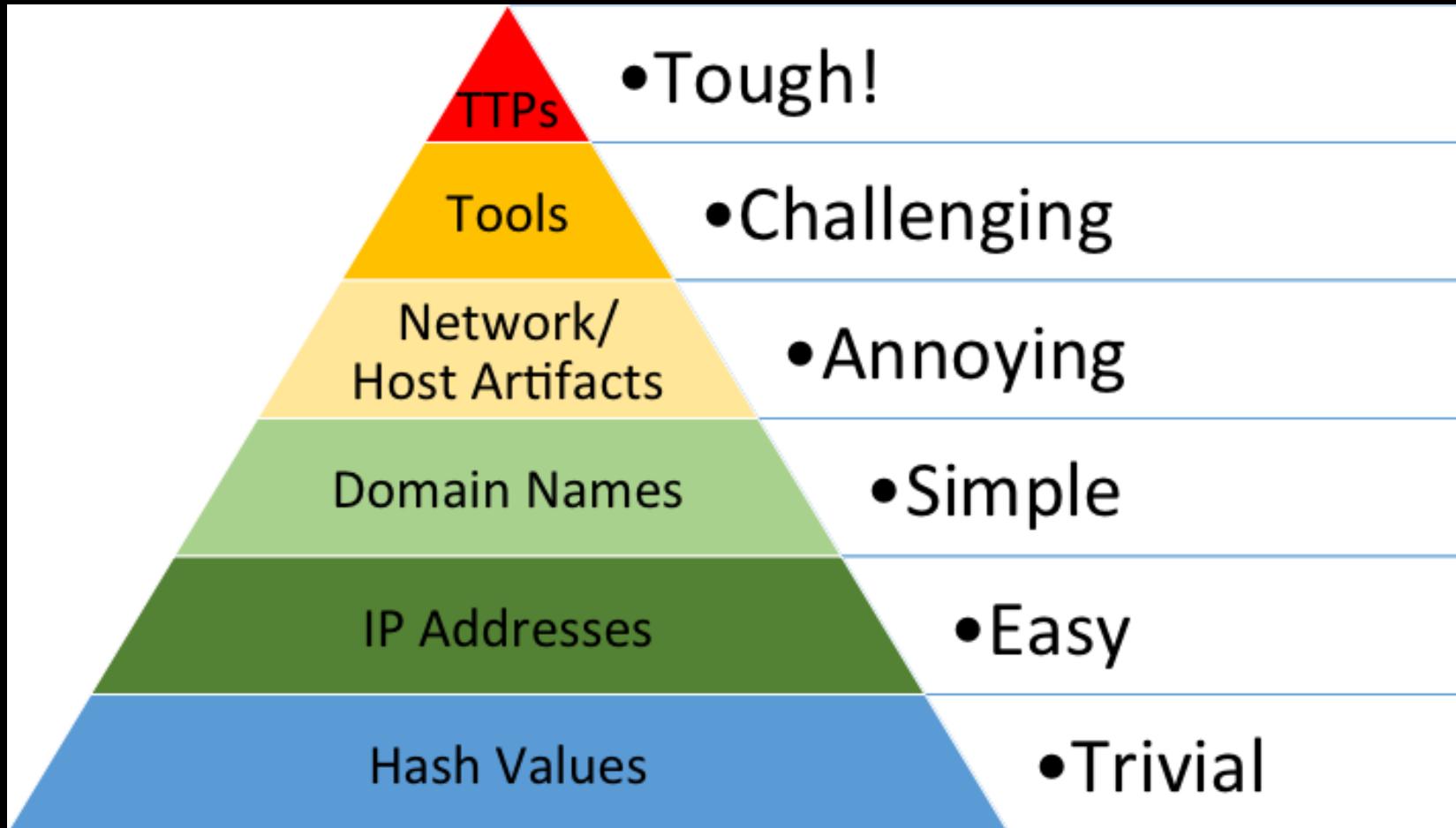
Sharing indicators of compromise (IOCs) the community and threat intelligence providers



Hunt for suspicious files using YARA. Sharing your own YARA rules with the community

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.

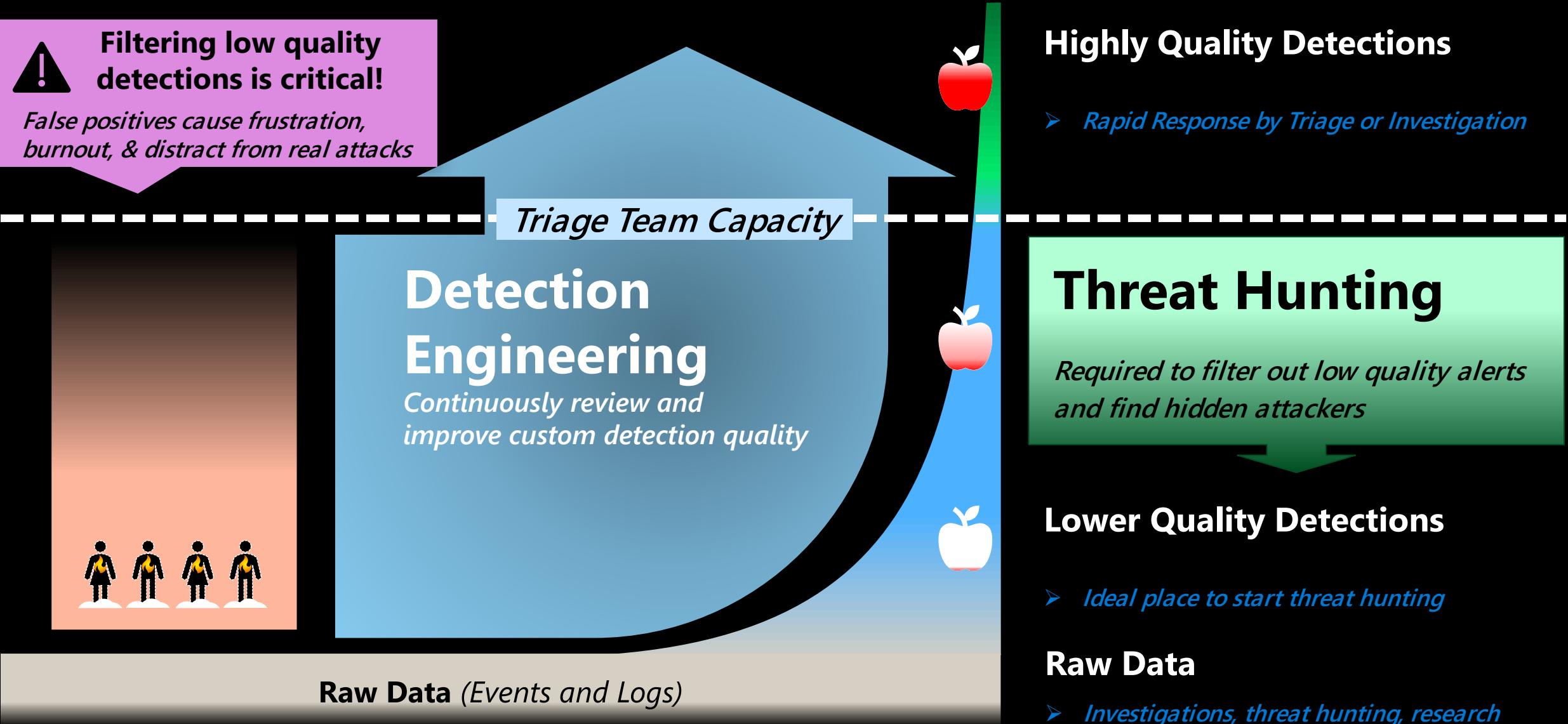


Source: <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

Security Operations Model



Detection Quality and Engineering



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

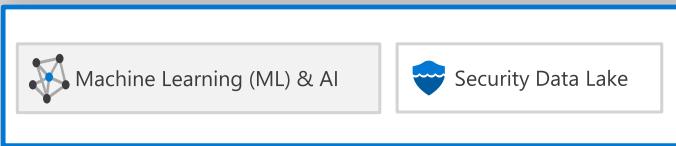
Enumeration of users and groups

Uncommon processes—bottom 5 percent

Threat Hunting & the Microsoft Security Stack

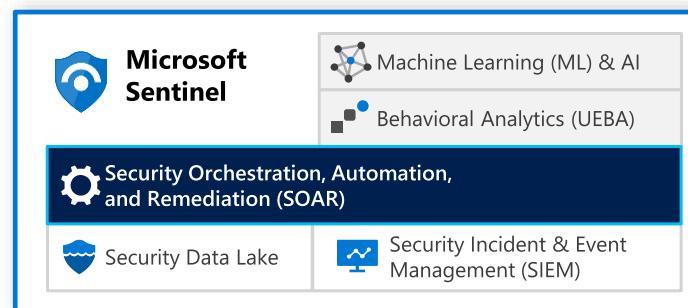
Hunting & ML Model Generation

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

Microsoft Defender - Extended Detection and Response (XDR)

Defender for Cloud

Servers & VMs Containers Azure app services Network traffic SQL IoT & OT ...

Defender for Identity

Azure AD Identity Protection

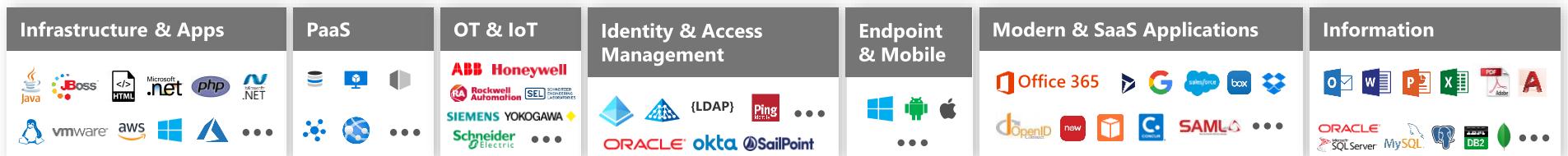
Defender for Endpoint

Defender for Office 365

Defender for Cloud Apps

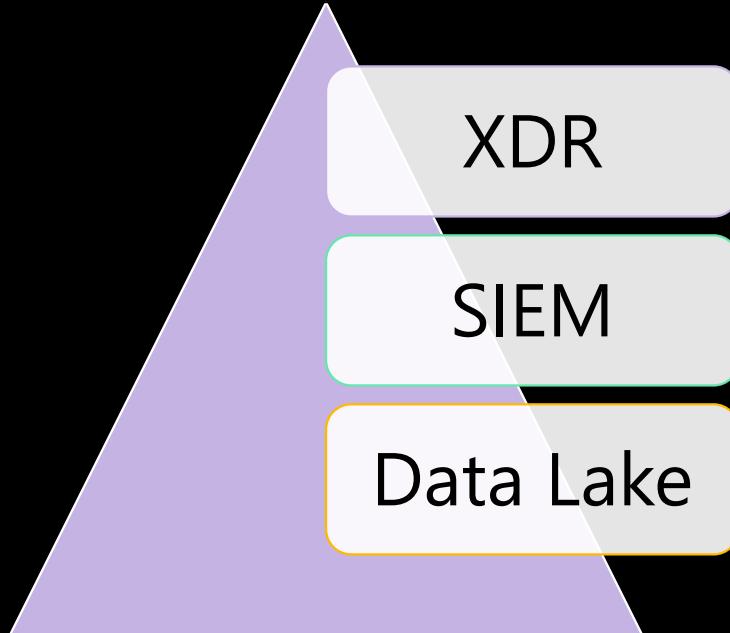
Microsoft 365 Defender

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

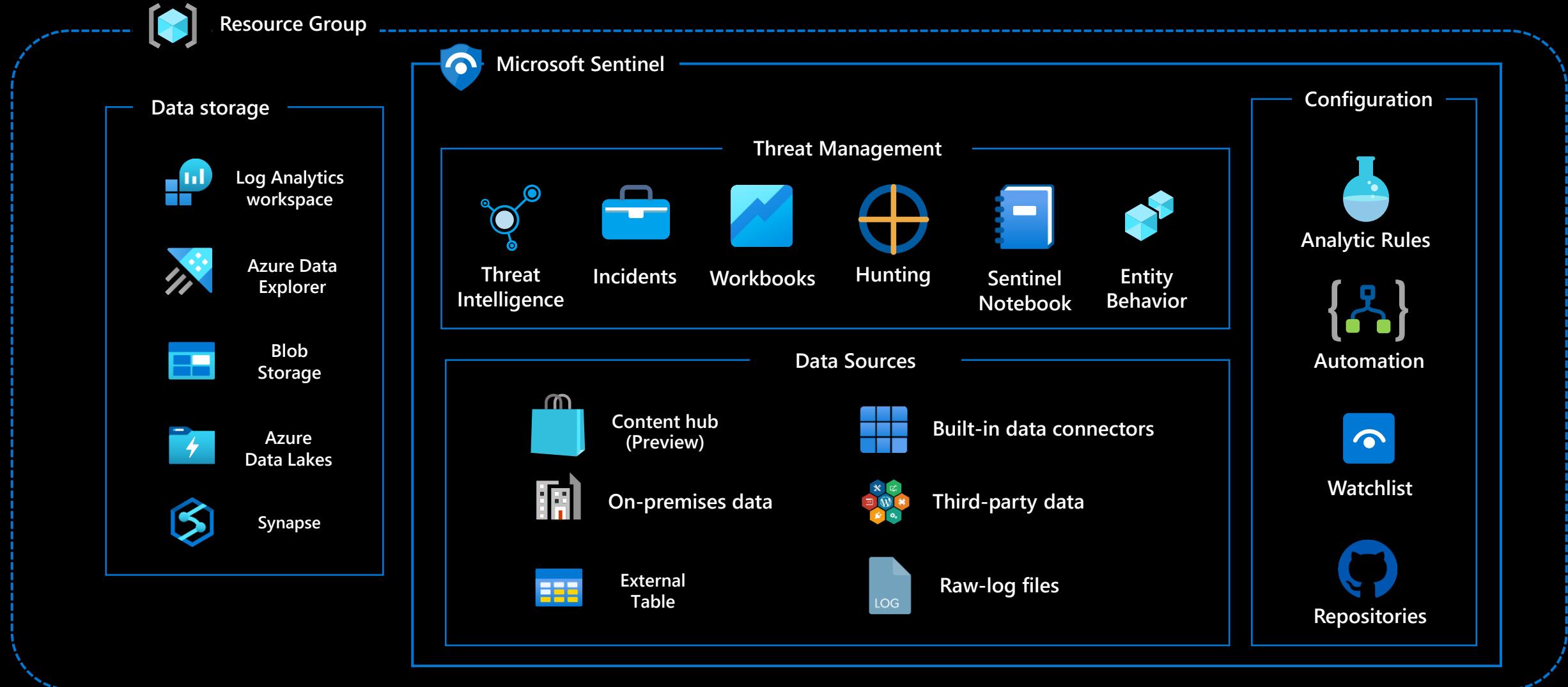
- Build queries with the integrated query builder
- Customize and create your own hunting queries using KQL
- Create custom detections with attached response actions
- Query raw data from endpoints, identity, mail and cloud apps

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a sidebar with navigation icons and sections like Schema, Shared queries, and Test. The main area is titled "Advanced hunting" with tabs for "Get started" and "PowerShell downloads". A "Run query" button is highlighted. Below it is a code editor containing KQL (Windows PowerShell Query Language) for finding PowerShell execution events. The results table shows 15 items per page, with 1-15 of 15 total. The columns are EventTime, ComputerName, and InitiatingProcessFileName. The data includes various log entries such as "msticex-srv.msticex.net cmd.exe" and "tk5-3wp03r0809.cfdev.nttest.microsoft.com cmd.exe".

```
// Finds PowerShell execution events that could involve a download.
ProcessCreationEvents
| where EventTime > ago(7d)
| where FileName in ("powershell.exe", "POWERSHELL.EXE", "powershell_ise.exe", "POWERSHELL_ISE.EXE")
| where ProcessCommandLine has ".Net.WebClient"
or ProcessCommandLine has "DownloadFile"
or ProcessCommandLine has "Invoke-WebRequest"
or ProcessCommandLine has "Invoke-Shellcode"
or ProcessCommandLine contains "http:"
project EventTime, ComputerName, InitiatingProcessFileName, FileName, ProcessCommandLine
top 100 by EventTime
```

EventTime	ComputerName	InitiatingProcessFileName
12/2/2019 12:02:32 PM	msticex-srv.msticex.net	cmd.exe
12/2/2019 12:01:32 PM	msticex-srv.msticex.net	cmd.exe
12/2/2019 12:01:32 PM	msticex-srv.msticex.net	cmd.exe
12/2/2019 12:01:31 PM	msticex-srv.msticex.net	cmd.exe
12/2/2019 2:51:10 AM	tk5-3wp03r0809.cfdev.nttest.microsoft.com	cmd.exe
12/2/2019 2:47:26 AM	tk5-3wp03r0813.cfdev.nttest.microsoft.com	cmd.exe
12/2/2019 19:26:27 PM	tk5-3wp03r0801.cfdev.nttest.microsoft.com	cmd.exe
12/1/2019 18:35:42 PM	tk5-3wp03r0809.cfdev.nttest.microsoft.com	cmd.exe
12/1/2019 18:35:42 PM	tk5-3wp03r0813.cfdev.nttest.microsoft.com	cmd.exe
12/1/2019 18:35:42 PM	tk5-3wp03r0823.cfdev.nttest.microsoft.com	cmd.exe
12/1/2019 18:35:41 PM	tk5-3wp03r0823.cfdev.nttest.microsoft.com	cmd.exe

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

The screenshot shows the Microsoft Sentinel Hunting interface. At the top, there are navigation links: Refresh, Last 24 hours, New Query, and Run all queries. Below that, there are three main sections: Total Queries (93), My Bookmarks (2), and Live Stream Results (1). A MITRE ATT&CK™ section displays various tactics across different data sources. The main area is titled "Suspicious network traffic p" and lists several built-in hunting queries. Each query entry includes the name, provider, data source, results count, and tactics. To the right of the list, there's a detailed sidebar for the first query: "Suspicious network traffic patterns" (Custom Query, Microsoft, CommonSecurityLog, 0 results, Persistence tactic). The sidebar also shows the query's description, creation time (11/1/2019), creator (sfender@microsoft.com), and a query editor. It includes filters for Entities (IP, Account, Host) and Tactics (Initial Access, Credential Access, Discovery, Persistence, Command and Control, Exfiltration, Persistence, Initial Access, Credential Access, Discovery, Persistence, Command and Control, Exfiltration). Buttons for "Run Query" and "View Results" are at the bottom of the sidebar.

Query	Provider	Data Source	Results	Tactics
Suspicious network traffic patterns	Custom Que...	CommonSecurityLog	0	Persistence
Changes made to AWS IAM policy	Microsoft	AWSCloudTrail	--	
Consent to Application discovery	Microsoft	AuditLogs +1	--	Persistence
Rare Audit activity initiated by App	Microsoft	AuditLogs	--	
Rare Audit activity initiated by User	Microsoft	AuditLogs +1	--	
Azure storage key enumeration	Microsoft	AzureActivity	--	Discovery
DNS commonly abused TLDs	Microsoft	DnsEvents	--	
DNS Domain anomalous lookup increase	Microsoft	DnsEvents	--	
DNS Full Name anomalous lookup increase	Microsoft	DnsEvents	--	
High reverse DNS count	Microsoft	DnsEvents	--	Discovery
Long DNS URI Query	Microsoft	DnsEvents	--	
DNS Domains linked to WannaCry ransomwar...	Microsoft	DnsEvents	--	
Cobalt Strike DNS Beacons	Microsoft	DnsEvents	--	Command and Control
Failed service logon attempt by user account ...	Microsoft	AuditLogs +1	--	Credential Access
Failed Login Attempt by Expired account	Microsoft	SecurityEvent +1	--	Initial Access
Multiple Password Reset by user	Microsoft	AuditLogs +3	--	
Permutations on logon attempts by UserPrinci...	Microsoft	OfficeActivity +1	--	Credential Access
RareDNSLookupWithDataTransfer	Microsoft	CommonSecurityLog +2	--	Exfiltration
Rare domains seen in Cloud Logs	Microsoft	AuditLogs +2	--	
Tracking Privileged Account Rare Activity	Microsoft	SecurityAlert +5	--	
Exploit and Pentest Framework User Agent	Microsoft	W3CISLoa +2	--	

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, ...

The screenshot shows the Azure Sentinel Notebooks interface. At the top, there's a navigation bar with 'Home > Azure Sentinel workspaces >'. The main title is 'Azure Sentinel | Notebooks' with a note 'Selected workspace: 'cybersecuritysoc''. Below the title is a search bar 'Search (Ctrl+ /)' and a link 'Go to your Notebooks'. A 'Guides & Feedback' button is also present.

The interface includes several sections:

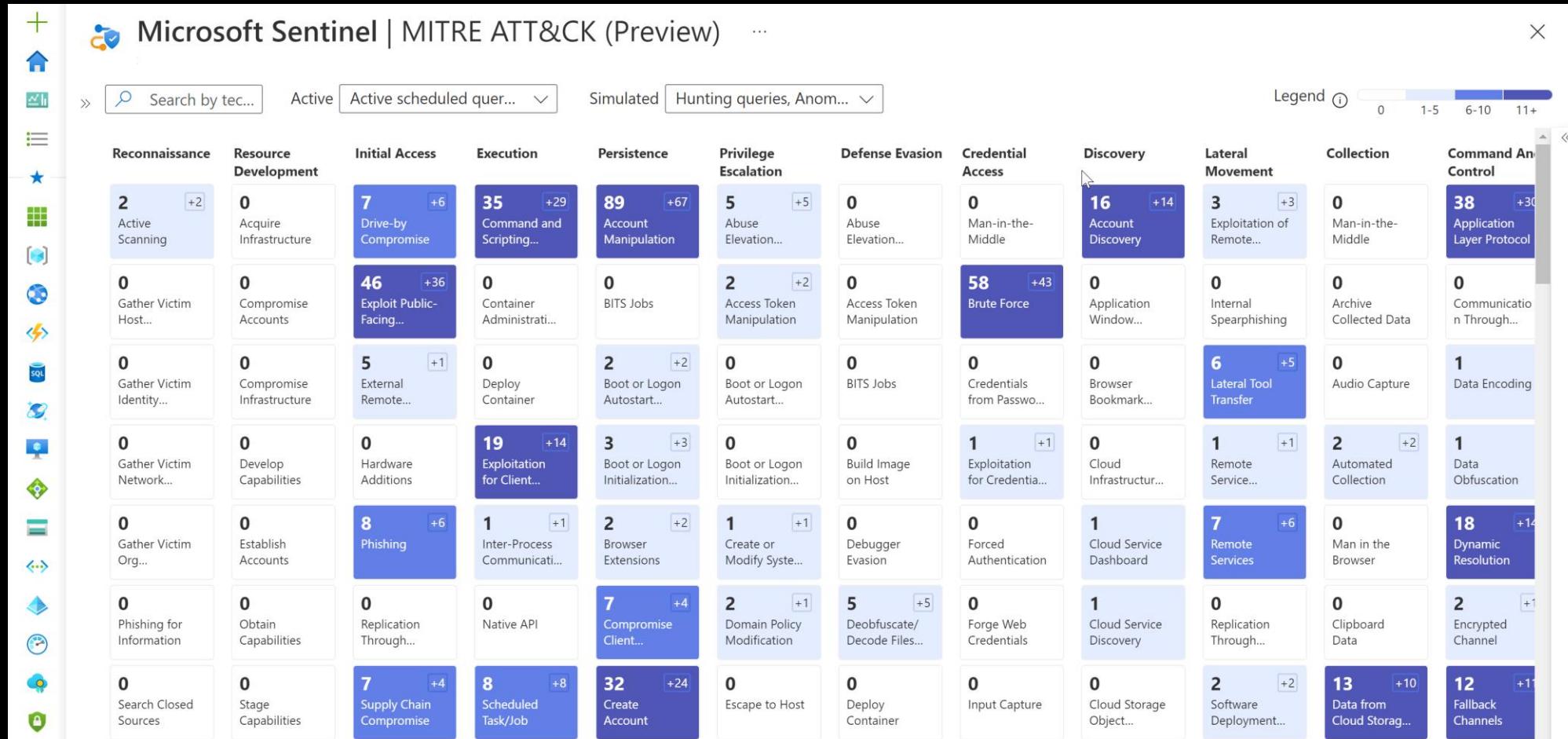
- General:** Includes links for 'Overview', 'Logs', 'News & guides', and 'Notebooks' (which is currently selected).
- Threat management:** Includes links for 'Incidents', 'Workbooks', 'Hunting', and 'Notebooks'.
- Configuration:** Includes links for 'Data connectors', 'Analytics', 'Playbooks', 'Community', and 'Settings'.

The central area displays a list of 13 total notebooks, each with a thumbnail, name, provider (Microsoft), last version update, and status (e.g., Hunting, Investigation). The notebooks listed are:

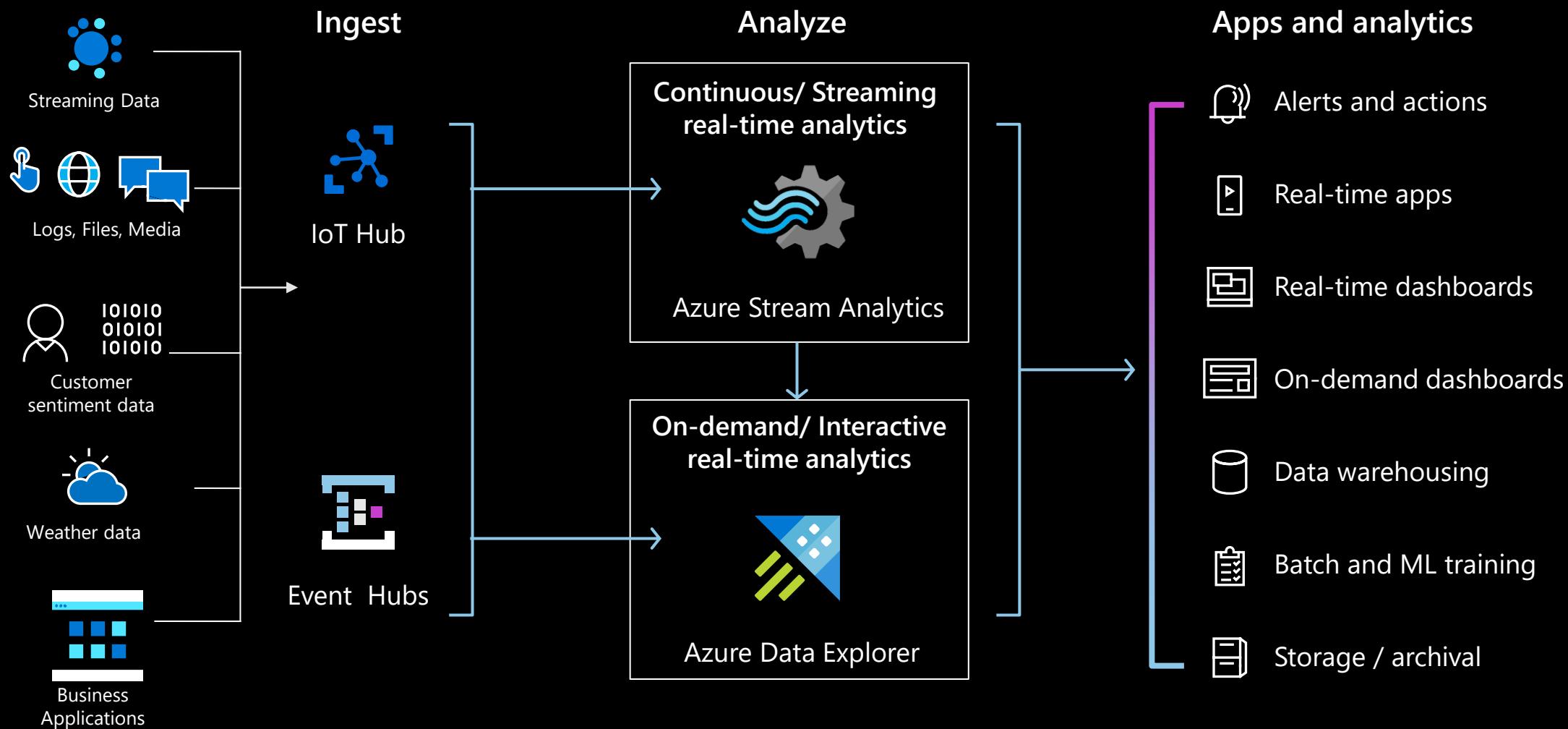
- Entity Explorer - Account (Microsoft) - Last version update: 06/02/20, 05:00 PM - Hunting
- Entity Explorer - Domain and URL (Microsoft) - Last version update: 06/02/20, 05:00 PM - Hunting
- Entity Explorer - IP Address (Microsoft) - Last version update: 06/02/20, 05:00 PM - Hunting
- Entity Explorer - Linux Host (Microsoft) - Last version update: 06/02/20, 05:00 PM - Hunting
- Entity Explorer - Windows Host (Microsoft) - Last version update: 06/02/20, 05:00 PM - Hunting
- Getting Started with Azure Sentinel Notebooks (Microsoft) - Last version update: 06/07/20, 05:00 PM - Investigation
- Guided Hunting - Anomalous Office365 Exchange S (Microsoft) - Last version update: 06/07/20, 05:00 PM - Hunting
- Guided Hunting - Covid-19 Themed Threats (Microsoft) - Last version update: 05/27/20, 05:00 PM - Hunting
- Guided Investigation - Anomaly Lookup (Microsoft) - Last version update: 10/27/19, 05:00 PM - Investigation
- Guided Investigation - Process Alerts (Microsoft) - Last version update: 06/02/20, 05:00 PM - Investigation
- Guided Investigation - Alert Triage (Microsoft) - Last version update: 05/27/20, 05:00 PM - Investigation
- Guided Web Shell Investigation - MDATP Sentinel Ei (Microsoft) - Last version update: 05/28/20, 05:00 PM - Generic

On the right side, there's a sidebar titled 'Entity Explorer - Account' which provides a detailed description of the notebook, its utilized data types (SecurityEvent, SecurityAlert, AzureNetworkAnalytics_CL, Heartbeat, AAD, OfficeActivity), and its data sources (Security Event, Office 365, Custom Logs). Below the sidebar, there's a preview of the notebook content and a 'Launch Notebook (Preview)' button.

MITRE ATT&CK in Sentinel



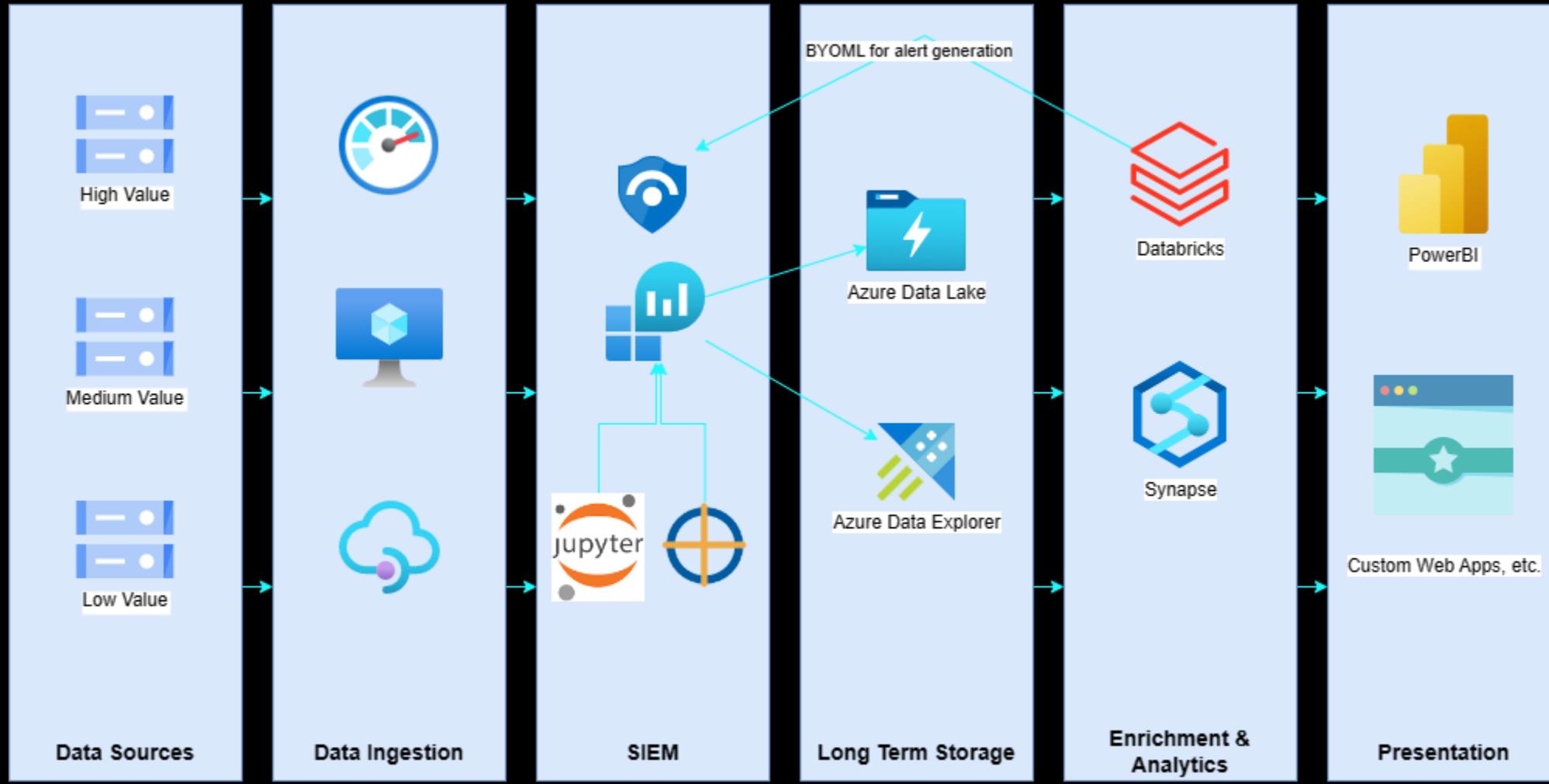
Using ADX for real-time analytics



Defender and/or ADX or/and Sentinel LAW

	Defender	Sentinel	ADX
Data Retention	Short term (up to 30 days)	Mid term (included 90 days and up to 2 years)	Long term (Days to years)
Query Usage	Very frequent access (Data on disk – Only Hot)	Frequent access (Data on disk – Only Hot)	Audit, Data Investigations (Data on disk – hot, cold)
Built-in Features	Curated OOB Value (XDR Data and Alerting)	OOB Value (SIEM and SOAR)	Custom logs (Adhoc queries, Hunting, Logic apps)
Platform	SaaS Service (Schema, Ingestion managed by Defender integrations)	SaaS Service (Schema, Ingestion managed by Sentinel)	PaaS Service (Full control of access and schema)
Business Model	Multi-tenant (Managed by Defender)	Multi-tenant (Managed by Sentinel)	Single-Tenant (Customer chooses SKU, Caching, Retention)

Hunting Tiers in the MSFT Stack (an example)



Demos

Threat Hunting – IP Address

Hunting for IP Address

Microsoft 365 Defender Search Help resources Query resources report Schema reference

New query Create new Run query Save Share link Last 24 hours Create detection rule

Advanced hunting

```
1 DeviceNetworkEvents  
2 | where RemoteIP == @"27.215.180.155"
```

Getting started Results

Export 1 item 0:31 Low Chart type Customize columns

Timestamp	DeviceId	DeviceName	ActionType	RemoteIP	RemotePort	RemoteUrl	Locall
Mar 4, 2023 9:05:54 PM	e14d6897fcf35d9426...	victimpc01	ConnectionSuccess	(o) 27.215.180.155	57925		(o) 10

Threat Hunting – Valid Accounts

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

```
1 let ADPrivGroups = dynamic(["Access Control Assistance Operators",
2 "Account Operators", "Administrators", "ADSyncAdmins", "ADSyncBrowse",
3 "ADSyncOperators", "ADSyncPasswordSet", "Allowed RODC Password Replication Group", "Backup Operators",
4 "Cert Publishers", "Certificate Service DCOM Access", "Cloneable Domain Controllers", "Cryptographic Operators",
5 "Denied RODC Password Replication Group", "Distributed COM Users", "DnsAdmins", "DnsUpdateProxy", "Domain Admins",
6 "Domain Controllers", "Domain Guests", "Enterprise Admins", "Enterprise Key Admins", "Enterprise Read-only Domain Controllers", "Event Log Readers", "Group Policy
7 "Hyper-V Administrators", "IIS_IUSRS", "Incoming Forest Trust Builders", "Key Admins", "Network Configuration Operators", "Performance Log Users", "Performance Mon
8 "Print Operators", "Protected Users", "RAS and IAS Servers", "RDS Endpoint Servers", "RDS Management Servers", "RDS Remote Access Servers", .....
9 "Read-only Domain Controllers", "Remote Desktop Users", "Remote Management Users", "Replicator",
0 "Schema Admins", "Server Operators", "Storage Replica Administrators", "Terminal Server License Servers", "Windows Authorization Access Group"]);
1 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 //iana_port_assignments
2 //·Service·Name,Port·Number,Transport·Protocol,Description,Assignee,Contact,Registration·Date,Modification·Date,Reference,Service·Code,Unauthorized·Use·Reported,Assignme
3 let·iana_port_assignments = (externaldata(ServiceName:string,PortNumber:int·,Transport:string,Protocol:string,Description:string)·.[@https://www.iana.org/assignments/service-names-and-numbers]
4 with·(format="csv",ignoreFirstRecord=true));
5 iana_port_assignments
6 |·join·kind=rightouter·(DeviceNetworkEvents)
7 on·$left·.PortNumber == ··$right.RemotePort·
8 |·where·isnotempty(·PortNumber)
9 |·summarize·EventCount=count()·by·PortNumber,RemotePort,·ServiceName
10 |·sort·by·PortNumber
11 |
```

Results		Chart	Add bookmark	
	PortNumber ↑↓	RemotePort	ServiceName	EventCount
<input type="checkbox"/>	> 0	0		32
<input type="checkbox"/>	> 11	11	systat	2
<input type="checkbox"/>	> 21	21	ftp	1'074
<input type="checkbox"/>	> 22	22	ssh	495
<input type="checkbox"/>	> 23	23	telnet	278

Threat Hunting – Commonly used Port

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

The screenshot shows a log search interface with a query editor at the top and a results table below.

Query Editor:

```
2* 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 .84"
23 | project TimeGenerated, InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
24
25 DeviceNetworkEvents
26 | where TimeGenerated > ago(90d)
27 | where RemoteUrl contains .ch"
28 | project TimeGenerated, InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
29
30 DeviceNetworkEvents
31 | where TimeGenerated > ago(90d)
32 | where RemoteIP contains .5"
33 | project TimeGenerated, InitiatingProcessCommandLine, RemoteIP,RemoteUrl, ActionType, DeviceName, LocalPort, InitiatingPr
```

Results Table:

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]	InitiatingProcessCommandline	RemoteIP	RemoteUrl	ActionType	DeviceName	LocalPort	InitiatingP
27.12.2022, 11:40:02.984	"mstsc.exe"			ConnectionFailed		61'556	
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®

```
1 DeviceProcessEvents
2 | where TimeGenerated > ago(30d)
3 | extend cmd = parse_command_line(InitiatingProcessCommandLine,"windows")
4 | where InitiatingProcessFileName == 'net.exe'
5 | mv-expand cmd
6 | summarize count() by tostring(cmd)
7
8 let netcommands = dynamic(["stop","accounts","domain","bits",'config','session']);
9 DeviceProcessEvents
0 | where TimeGenerated > ago(30d)
1 | extend cmd = parse_command_line(InitiatingProcessCommandLine,"windows")
2 | where InitiatingProcessFileName == 'net.exe'
3 | mv-expand cmd
4 | where cmd has_any (netcommands)
5 | project TimeGenerated,DeviceName,AccountName, InitiatingProcessCommandLine, cmd
6 | where cmd contains "domain"
7
```

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



Run query Save Share link

Query

```
1 // search for domains based on the 10 Most Abused Top Level Domains
2 // https://www.spamhaus.org/statistics/tlds/
3 let abusedTLD = dynamic(["rest", "okinawa", "live", "beauty", "bar", "fit", "gq", "cf", "zone", "top"]);
4 DeviceNetworkEvents
5 | where isnotempty(RemoteUrl)
6 | extend tld = tostring(split(RemoteUrl, ".")[-1])
7 | where tld in~ (abusedTLD)
8 | summarize
9 | ... StartTime = min(Timestamp),
10 | ... EndTime = max(Timestamp),
11 | ... NameCount = count()
12 | ... by RemoteUrl, RemoteIP, tld
13 | order by NameCount desc
```

Threat Hunting – Files originating from suspicious sources

Analyzing file downloads (executables, scripts, macros)

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

Results Chart Add bookmark 🔍

domain FileName FileExtension ↑↓ FileOriginUrl

...

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]			
[REDACTED]			

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

Threat Hunting in Sentinel

Hunting Queries

Queries Livestream Bookmarks

0 0 5 0 1 0 0 0 0 0 0 0 0 0 0 0 0

Reco... Reso... Initia... Exec... Persi... Privil... Defe... Cred... Disc... Later... Colle... Com... Exfilt... Impact Impa... Inhib... None

Search queries Favorites : Favorites Tactics : Initial Access Add filter

	↑↓ Query ↑↓	↑↓ Data source ↑↓	Results ↑↓	Results delta ↑↓	Results delta per... ↑↓	Tactics ↑↓	Techniques ↑↓
<input type="checkbox"/>	Attempts to sign in to disabled accounts by account name	G SigninLogs	4	-1	-20%	Initial Access	T1078
<input type="checkbox"/>	Attempts to sign in to disabled accounts by IP address	G SigninLogs	3	-1	-25%	Initial Access	T1078
<input type="checkbox"/>	Login attempts using Legacy Auth	G SigninLogs	2	0	0%	Initial Access	T1078 +1 ⓘ
<input type="checkbox"/>	Failed attempt to access Azure Portal	G SigninLogs	11	-5	-31.3%	Initial Access	T1078
<input type="checkbox"/>	Azure Active Directory signins from new locations	G SigninLogs	2.5K	+2.3K	+1036%	Initial Access	T1078

< Previous Page 1 of 1 Next >

Attempts to sign in to disable

Gallery content Content source (Preview) Created time 4.9.2019

Query

```
SigninLogs  
| where ResultType == "50057"  
| where ResultDescription == "U  
disabled. The account has been  
administrator."  
| summarize StartTime = min(Tim  
View query results >
```

Entities

Account

Tactics

Run Query View Results

Threat Hunting in Microsoft Sentinel

Hunting Queries

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Hunting

Selected workspace: 'mtplabsentinel01'

Refresh | Last 24 hours | New Query | Run all queries | Hunt actions | Columns | Guides & Feedback

245 / 288 ↗1 1 / 6 0 Livestream Results 9 My bookmarks More content at Content hub

Hunts (Preview) Queries Livestream Bookmarks

0 Reco... 0 Reso... 0 Initia... 0 Exec... 0 Persi... 0 Privil... 0 Defe... 0 Cred... 0 Disc... 1 Later... 0 Colle... 1 Com... 3 Exfilt... 0 Impact +3

ftp Tactics : Exfiltration Add filter

Query Content source Data source Results Results delta Results

Use of FTP Port 21 Custom 1 +1 +∞%

Custom 1 Results Data sources

3/4/2023

Created by
oa@verboon.online

Query

```
DeviceNetworkEvents
| where RemotePort == 21
| extend Account_0_Name = InitiatingProcessAccountName
| extend IP_0_Address = RemoteIP
| extend Host_0_HostName = DeviceName
| extend Process_0_CommandLine =
    ...additional ProcessCommandLine...
```

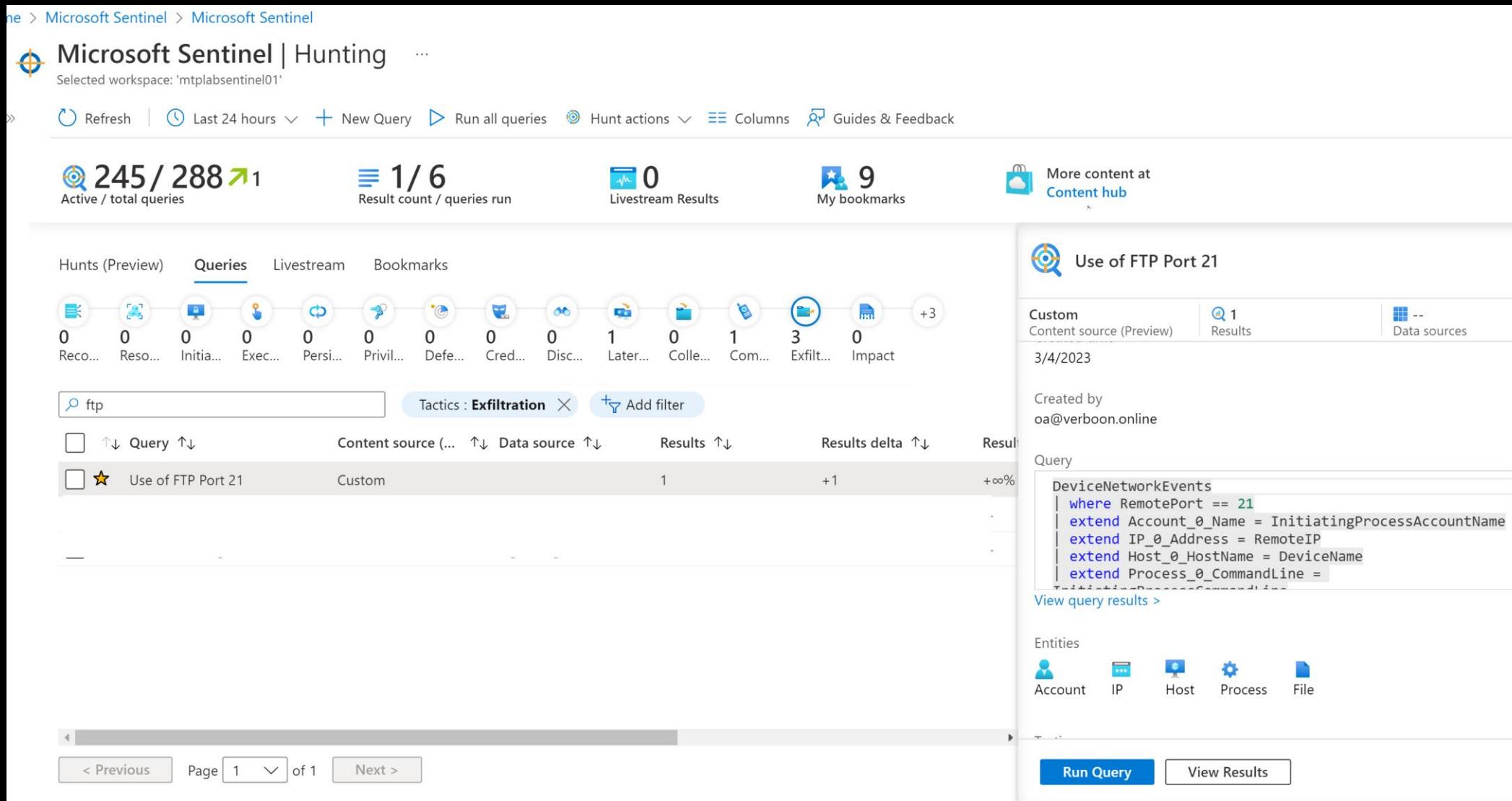
[View query results >](#)

Entities

Account IP Host Process File

< Previous Page 1 of 1 Next >

Run Query View Results



Threat Hunting in Microsoft Sentinel

Hunting Queries

Home > Microsoft Sentinel > Microsoft Sentinel | Hunting >

Use of FTP Port 21

Delete Query

ⓘ Do not use fixed time ranges, either directly or in a function, in your query. Otherwise, we cannot show changes in query results over time.

Name *
Use of FTP Port 21

Description
Use of FTP Port 21

Custom query *

```
DeviceNetworkEvents  
| where RemotePort == 21
```

[View query results >](#)

Entity mapping

Account

Name	<input type="button" value="–"/>	<input type="button" value="+ Add identifier"/>
InitiatingProcessAccountName	<input type="button" value="–"/>	

IP

Address	<input type="button" value="–"/>	<input type="button" value="+ Add identifier"/>
RemoteIP	<input type="button" value="–"/>	

Identify activity on Port 21 (FTP)

Threat Hunting in Microsoft Sentinel

Live Stream

The screenshot shows the Microsoft Sentinel Livestream interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Microsoft Sentinel > Microsoft Sentinel | Hunting > Livestream'. The main area is titled 'Livestream' and shows a message: 'Livestream session is currently running, click 'Pause' to stop'. There's a 'Name' field containing 'Bad IP' and a 'Query' field with the following Kusto query:

```
DeviceNetworkEvents  
| where RemoteIP contains "58.135.80.99"
```

Below the query, there's a link 'View query results >' and a table showing the results of the query. The table has columns: DeviceId, DeviceName, Protocol, RemoteIP, RemotePort, SourceSystem, TimeGenerated, Type, ActionType, and AdditionalF. One row is visible, showing:

DeviceId	DeviceName	Protocol	RemoteIP	RemotePort	SourceSystem	TimeGenerated	Type	ActionType	AdditionalF
e14d6897fcf35d94261...	victimpc01	Tcp	58.135.80.99	80		2023-03-04T21:58:08....	DeviceNetworkEvents	ConnectionSuccess	

Threat Hunting in Microsoft Sentinel

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

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

Sentinel Workspace Recon Tools - mtplabsentinel01

mtplabsentinel01

Edit Open Refresh Help Auto refresh: Off

Subscription: Visual Studio Enterprise Subscription - DEMO Lab | Workspace: MTPLabSentinel01 | Time Range: Last 30 days | Show Help: Yes

Simple Search Table Explorer Security Events Windows Events Security Policy Azure Activity Azure AD Logs Security Alerts CEF Viewer Syslog Viewer Agent Health

Table Explorer

Table Picker (1) Column Picker (2) Top Records (3) Hourly Records - Time Brush to see Details (4)

Table Explorer is designed to help you better understand the data in your tables. Each table, column, and value is easily sorted by volume.

Table Picker:

Table	Size
DeviceRegistryEvents	20.1MB
AzureActivity	17.665MB
DeviceNetworkEvents	17.537MB
DeviceEvents	17.28MB
DeviceImageLoadEvents	8.402MB

Column Picker:

Column
AccountDomain
AccountName
AccountSid
ActionType
AdditionalFields

Top Records:

ActionType
TamperingAttempt

Hourly Records - Time Brush to see Details:

Feb 5 Feb 6 Feb 7 Feb 8 Feb 9

count_(Sum) 29

Related Records:

AccountDomain	AccountNa...	AccountSid	ActionType	AdditionalFields	AppGuardContainerId	DeviceId	Devi
TamperingAttempt	{"TamperingAction": "RegistryModification", "Status": "Blockec	ef504fb6af4e8a646b5cc435d6c94f3c8fa262db					



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](#)