



James Graham, PHD

 [/drjamesgraham](https://www.linkedin.com/in/drjamesgraham)

 Cloud Solution Architect



Agenda

- 9:10 - *Opening Keynote*
- 9:35 - *Advanced Threat Hunting*
- 10:30 - *Break I*
- 10:40 - *Live Response*
- 11:40 - *Break II*
- 11:50 - *Power Virtual Agent Lab*
- 12:55 - *Closing*
- 13:00 - *End*



Meet the team



Mark Thomas



James Graham



Ally Turnbull



Jack Lewis



Becky Cholerton



Steve Newby



Christos Ventouris

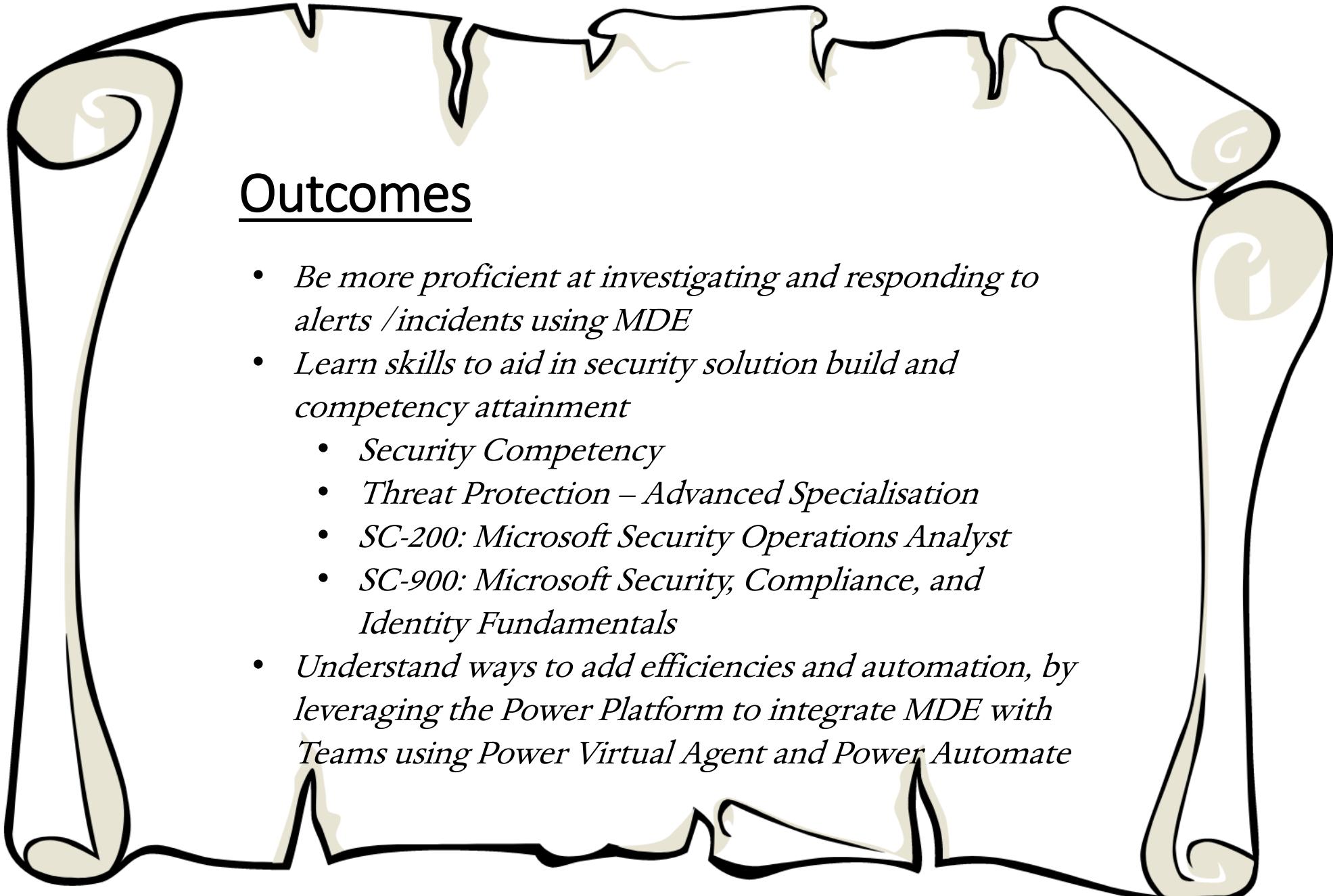


Jaime Lloyd



Rules and Housekeeping

- *Please be patient when asking questions*
- *If it's important, we will post it in the announcements*
- *For lab prerequisites and resources visit
aka.ms/defendermasterclass-repo*
- *Feedback – aka.ms/defendermasterclass-feedback*
- *This event is being recorded – further recordings available at aka.ms/defendermasterclass-recordings*
- *Slides will be made available at the repo*



Outcomes

- *Be more proficient at investigating and responding to alerts /incidents using MDE*
- *Learn skills to aid in security solution build and competency attainment*
 - *Security Competency*
 - *Threat Protection – Advanced Specialisation*
 - *SC-200: Microsoft Security Operations Analyst*
 - *SC-900: Microsoft Security, Compliance, and Identity Fundamentals*
- *Understand ways to add efficiencies and automation, by leveraging the Power Platform to integrate MDE with Teams using Power Virtual Agent and Power Automate*

Microsoft Partner Network Program – Security

Security Competency

Advanced Specializations

Silver Status

Individual Certification Requirements

1 Individual in MS-500 (M365 Security Administration)
OR

AZ-500 (Azure Security Technologies)

Demonstrated Customer Performance

1000 Active Users in M365 security workload

OR

US \$500/month Security Azure customer consumption within previous 12 months

BENEFITS

Internal use rights for M365
Co-marketing MPN benefits

Gold Status

Individual Certification Requirements

4 individuals in MS-500 (M365 Security Admin)
AND

4 individuals in AZ-500 (Azure Security Technologies) (can also be same person)

Demonstrated Customer Performance

4000 Active Users in M365 security workload

OR

US \$1000/month Azure Security customer consumption within previous 12 months

BENEFITS

Internal use rights for M365
Usage incentive eligibility
ECIF* & Customer matching prioritization
Co-marketing MPN benefits

- Threat Protection
- Identity & Access Management
- Information Protection & Governance

*Gold not a requirement for MW EFIC in FY21

Threat Protection advanced specialization

Partners who demonstrate deep knowledge, extensive experience, and proven success deploying Microsoft Threat Protection, Microsoft Cloud App Security, or Azure Sentinel workloads can differentiate their capabilities to customers with the Threat Protection advanced specialization.

<https://aka.ms/PartnerSpecializations>

Requirements	Details
Related competency	Maintain an active Gold Security competency.
Performance	Achieve a minimum of 1,000 Monthly Active User (MAU) growth of Azure Advanced Threat Protection (A-ATP) or Microsoft Cloud App Security (MCAS) in a trailing 12-month period (CPOR data) OR Achieve a minimum of USD 100,000 in Azure Consumed Revenue (ACR) from Azure Sentinel in a trailing 12-month period (Digital Partner of Record, Partner Admin Link, and Cloud Solution Provider data).
Knowledge	Your organization must have at least six individuals who have passed the MS-500: Microsoft 365 Security Administrator exam.
Customer references	Provide three customer references that demonstrate your organization's ability to deploy Microsoft Threat Protection, Microsoft Cloud App Security, or Azure Sentinel workloads. Review our guidelines for customer references before submitting.
Annual renewal	Your advanced specialization and associated benefits will remain in place for one year but require that you keep your gold competency status in place. If you do not maintain your gold competency, you will lose your advanced specialization status. On your renewal date, you will need to meet the current program requirements which may evolve over time.

Corp Virtual Training Series (VTS)

Interactive, time-zone-friendly webinar series for Microsoft Partners designed to increase your knowledge of incubation and advanced technical scenarios across Microsoft's cloud solutions. These training opportunities offer chat-based instructors, with deep technical knowledge in a consolidated format and time frame.

- Focused on Microsoft core solution areas:
 - Azure
 - Modern Work and Security
 - Business Applications
- Flexible schedules and self-paced options
- Available to all Microsoft Partners

The screenshot shows the Microsoft VTS landing page. At the top, there's a dark banner with the text "Virtual Training Series" and a subtext "Enhance your technical skills with interactive webinars for core customer technical scenarios." Below the banner is a button labeled "See the schedule >". The main area features a blurred background image of a person working at a computer. Below the image, the heading "Featured trainings" is displayed, followed by a brief description: "These training opportunities provide chat-based instructors with targeted information delivered in a consolidated time frame to enhance your expertise." Four training offerings are listed in a grid:

Thumbnail	Title	Description	Date
	Don't miss these new VTS opportunities	Live VTS offerings – July 2020	2020-06-12
	AZ-900: Microsoft Azure Fundamentals	Recorded VTS - Beginner - 5 hrs 0 min	2020-03-27
	MB-700: Microsoft Dynamics 365 Finance & Operations Apps Solution Architect	Recorded VTS - Advanced - 5 hrs 0 min	2020-06-26
	MS-900: Microsoft 365 Fundamentals	Recorded VTS - Beginner - 4 hrs 0 min	2020-05-22

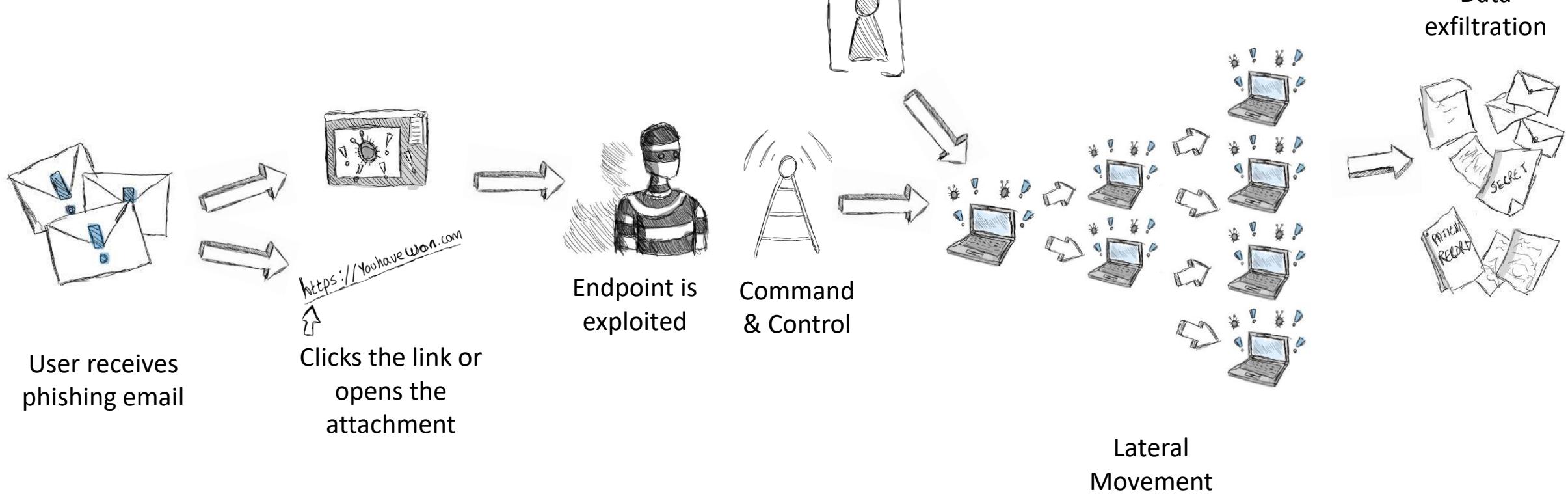
<https://aka.ms/enablevts>

Ninja Self paced training

- [Azure Sentinel ninja training](#)
- [Microsoft Defender ATP ninja training](#)
- [Azure Security \(ASC\) ninja training](#)



Revealing the Microsoft Banksy..



Microsoft Defender Masterclass II

Microsoft Defender for Endpoint

Endpoint Detection & Response



Navigating a shifting world

Conventional security tools have not kept pace



The nature of business and work have changed



Cost of breaches and regulations are increasing



COVID-19 brought unexpected IT challenges

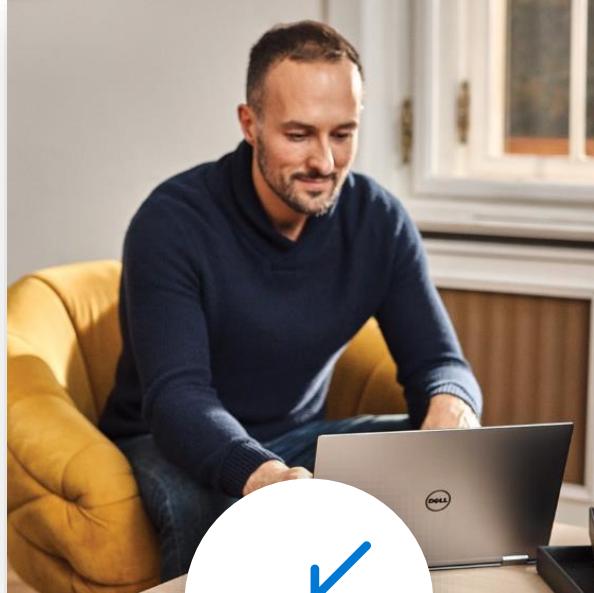
- Rapidly enabling remote work while protecting corporate resources



A new reality needs new principles



Verify explicitly



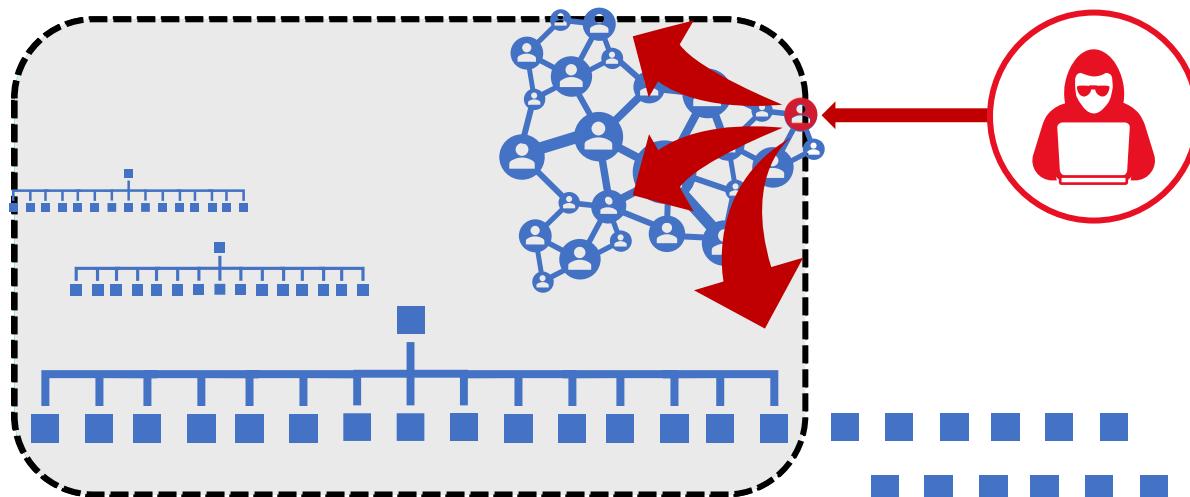
Use least privilege access



Assume compromise

Why are we having a Zero Trust conversation?

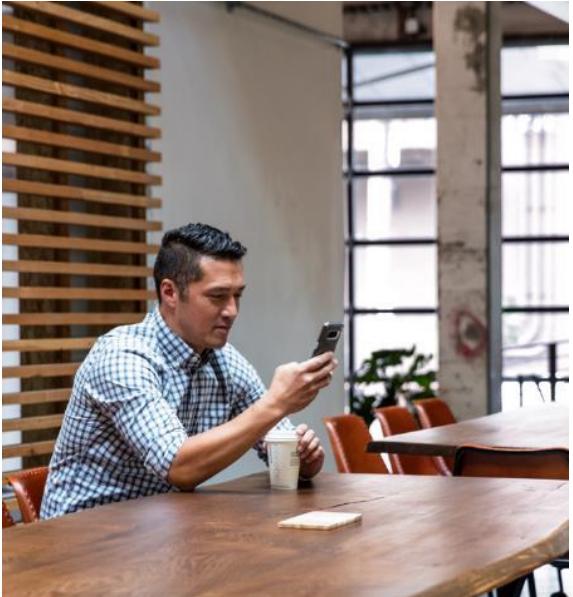
Access Control: Keep **Assets** away from **Attackers**



1. **IT Security is complex**
 - Many devices, users & connections
2. **“Trusted network” security strategy**
 - Initial attacks were network based
 - *Seemingly* simple and economical
 - Accepted lower security within the network
3. **Assets increasingly leave the network**
 - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
 - Phishing and credential theft
 - Security teams often overwhelmed

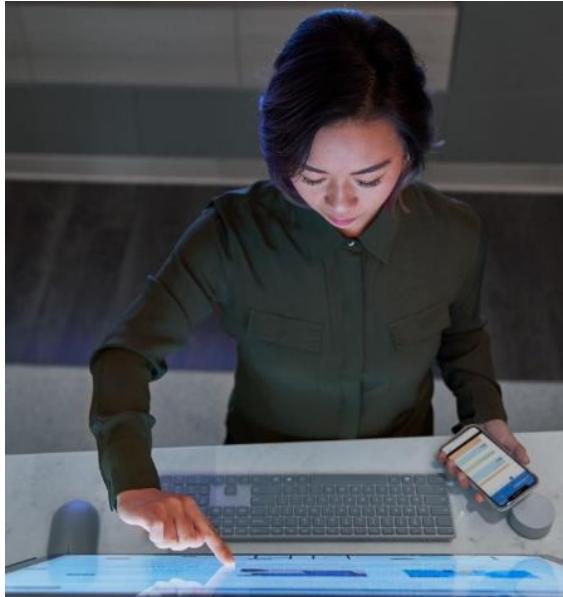


Microsoft Security Pillars



Identity and access management

Secure access for a connected world



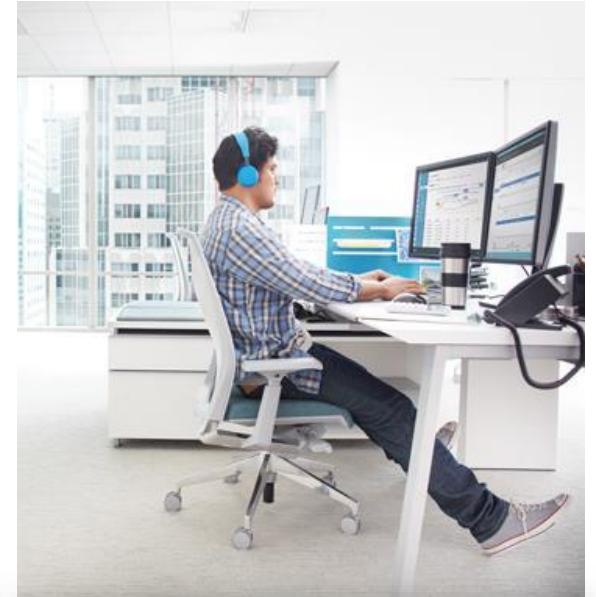
Threat protection

Stop attacks with integrated and automated SIEM and XDR



Information protection

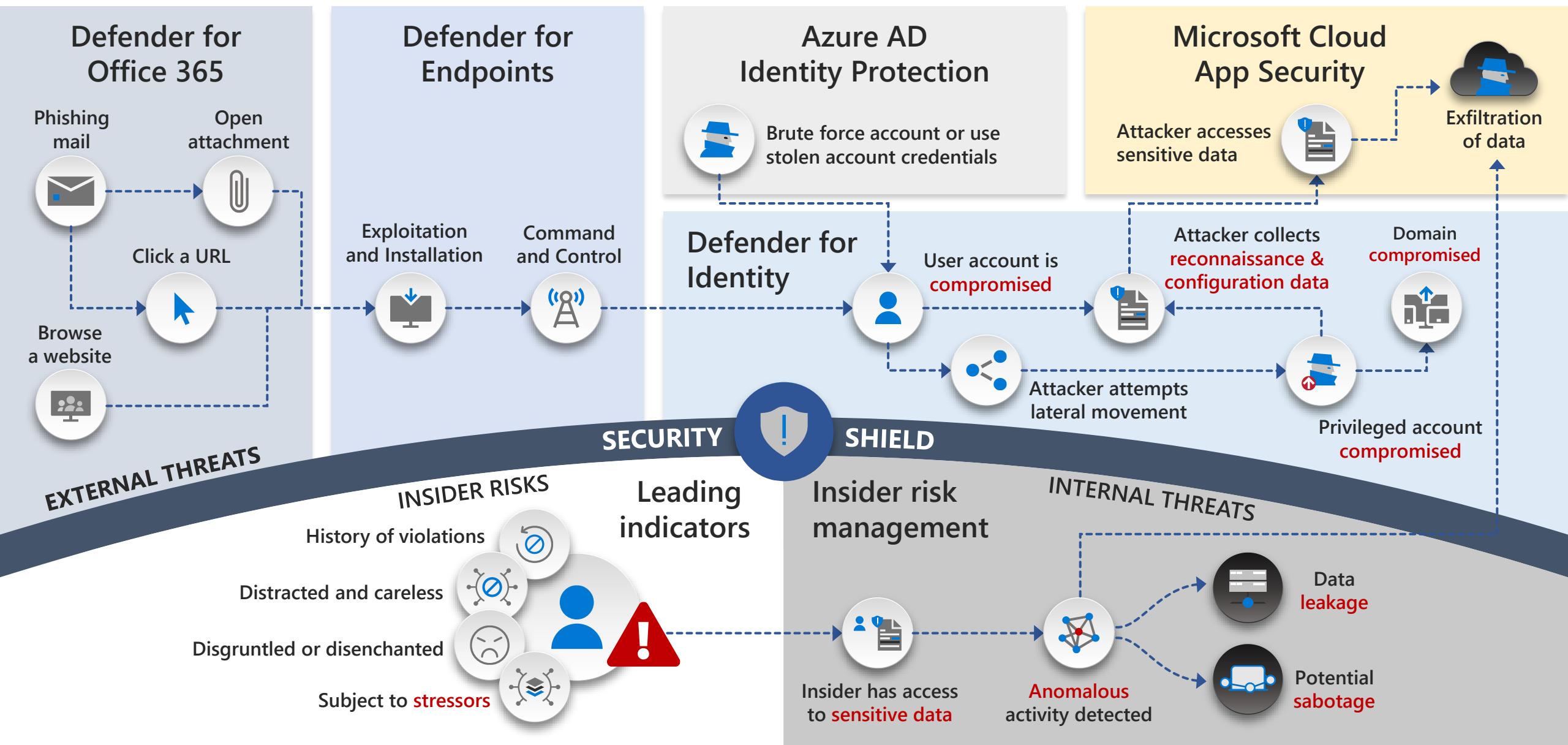
Protect sensitive data and manage insider risks with intelligence



Cloud Security & Posture Management

Safeguard your multi-cloud resources with insights and guidance

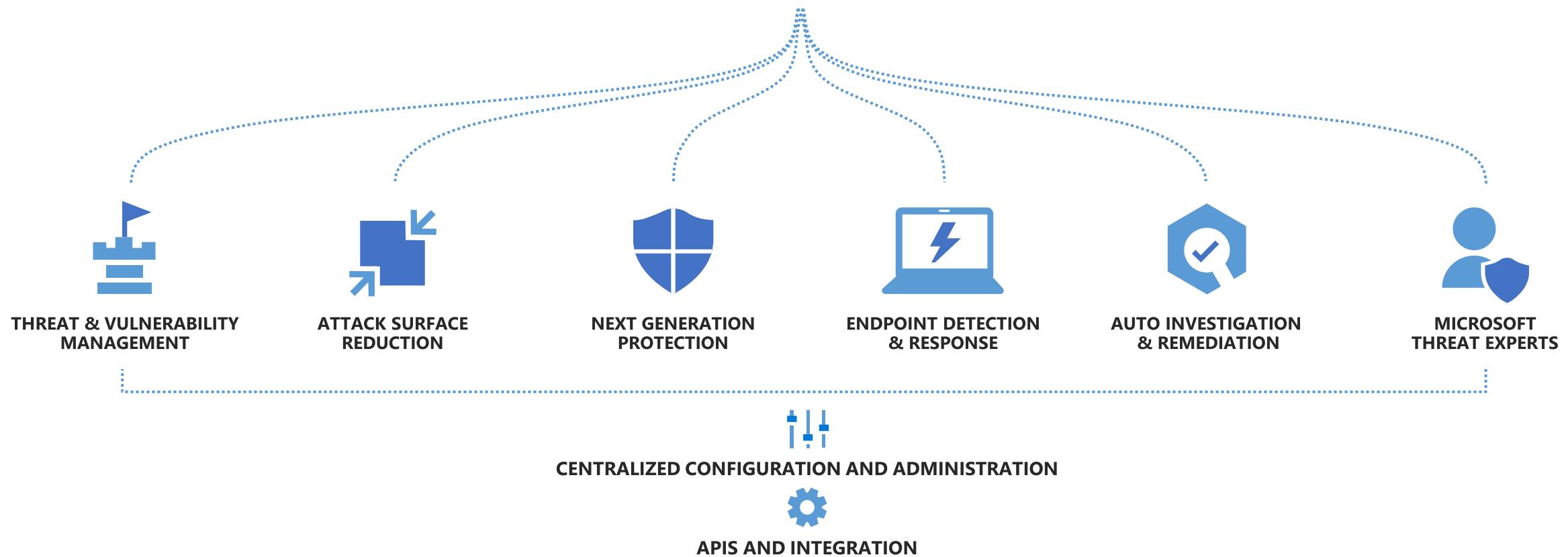
Internal and external protection across the threat kill chain





Microsoft Defender for Endpoint

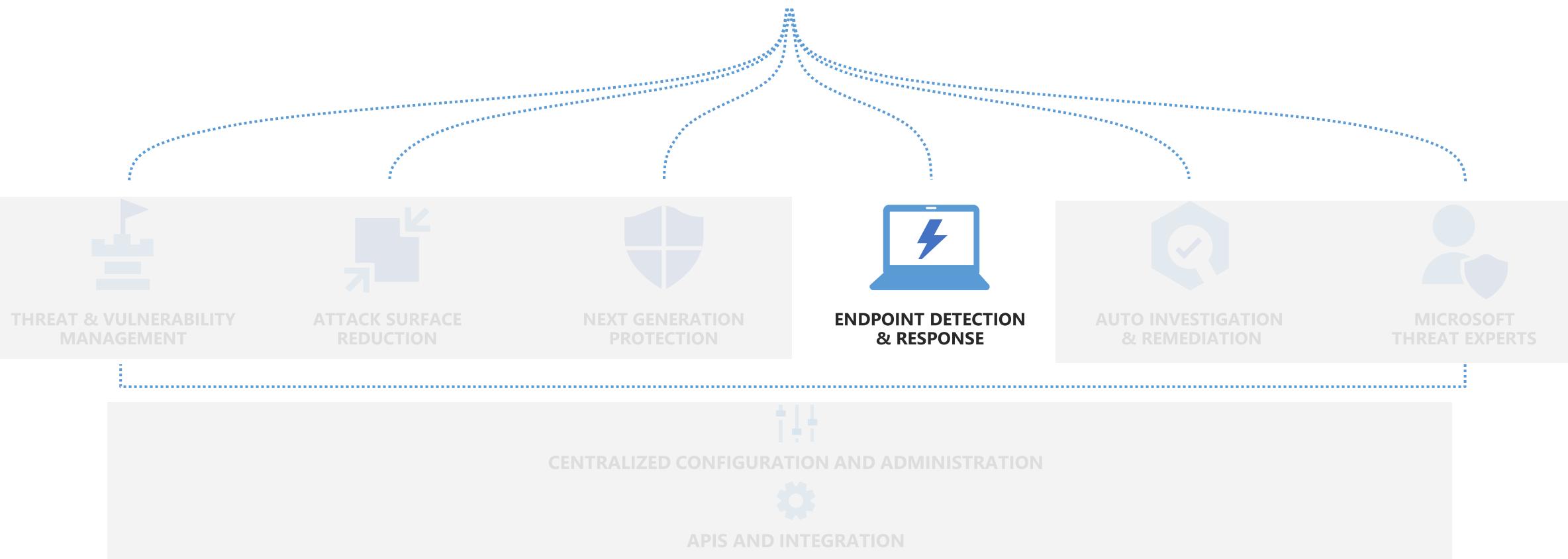
Built-in. Cloud-powered.





Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Endpoint Detection & Response

Detect and investigate advanced persistent attacks



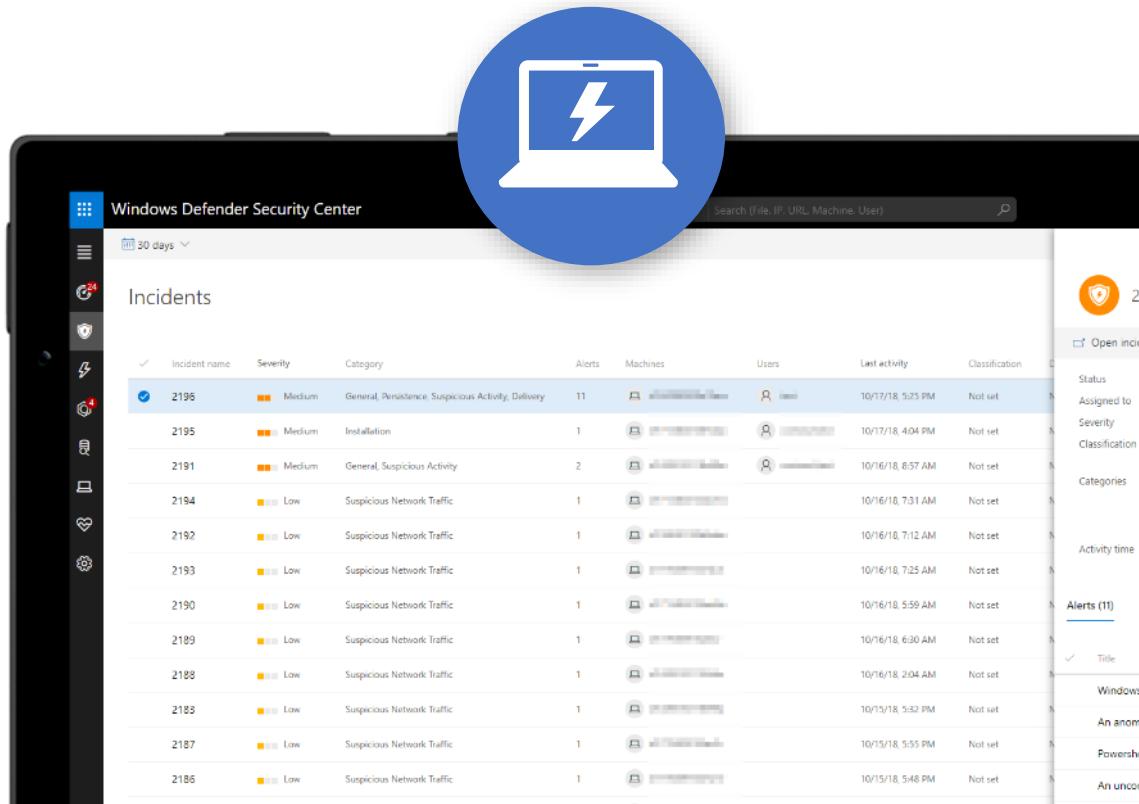
Correlated behavioral alerts



Investigation & hunting over 6 months of data



Rich set of response actions



The screenshot shows the Windows Defender Security Center interface. At the top, there's a search bar and a navigation menu. Below it, a large blue circular icon contains a white laptop with a lightning bolt, symbolizing a threat. The main area is titled 'Incidents' and displays a list of 15 entries. Each entry includes columns for Incident name, Severity, Category, Alerts, Machines, Users, Last activity, and Classification. The list shows various types of incidents such as 'General Persistence' and 'Suspicious Activity'. On the right side of the screen, there are several filter and search options, including dropdown menus for Status, Severity, Classification, Categories, and Activity time, along with a link to 'Alerts (11)'.



Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation.

Triage & Investigation

Understand what was alerted

Alert investigation experience provides detailed description, rich context, full process execution tree.

Investigate device activity

Full machine timeline to drill into activities, filter and search.

Rich supporting data & tools

Supporting profiles for files, IPs, URLs including org & world prevalence, deep analysis sandbox.

Expand scope of breach

In-context pivoting to other affected machines/users.

The screenshot displays several windows from the Microsoft Defender for Endpoint platform:

- File Analysis:** Shows details for a file named "control.exe". It includes SHA1, SHA256, and MD5 hashes, along with a timestamp of Aug 15, 2019, at 5:39:38.755 PM. The event type is "ProcessCreated" under "SuspiciousActivity".
- Alert Details:** An alert titled "COM hijacking" is shown, indicating it's part of an incident. It provides severity (Medium), category (Persistence), detection source (EDR), and detection technology (Behavioral). A "Recommended actions" section lists steps to validate the alert.
- Machine Timeline:** A timeline for machine "apt29-client3" from July 2019 to September 2019. It highlights an "Event of type [CollectInvestigationPackageResponse] observed on machine" on Aug 15, 2019, at 8:38:10.497 PM.
- Alert Process Tree:** A diagram showing the execution flow of processes. It starts with "sdclt.exe", which creates "control.exe", which then creates "powershell.exe". "powershell.exe" runs "reg.exe", which creates registry keys under "HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run".
- Device Details:** Provides information about the machine, including domain ("apt29.org"), OS ("Windows 10 x64 Version 1903 Build 18362"), and health state ("Inactive"). It also shows first seen (Aug 13, 2019, 1:34:05 PM) and last seen (Aug 21, 2019, 5:08:29 PM) times.
- Filters:** A sidebar on the right allows users to filter events by various categories such as Event group (Any, ASR events, Alert related events, etc.), Persistence, and Executed.

Incident

Narrates the end-to-end attack story

Reconstructing the story

The broader attack story is better described when relevant alerts and related entities are brought together.

Incident scope

Analysts receive better perspective on the purview of complex threats containing multiple entities.

Higher fidelity, lower noise

Effectively reduces the load and effort required to investigate and respond to attacks.

The screenshot displays two views of the Microsoft Defender Security Center interface. The top view shows a list of incidents over the last 30 days, with columns for Incident name, Severity, Categories, Active alerts, Machines, Detection sources, First activity, Last activity, and Status. Several incidents are listed, each with a red severity icon. The bottom view is a detailed summary for Incident 77196, which is marked as 'Active'. This summary includes:

- Overview:** Shows 11 active alerts, 3 MITRE attack categories (Initial access, Execution, Persistence), and 10 entities found.
- Alerts and categories:** A bar chart showing the distribution of alert categories across multiple machines.
- Scope:** Details the affected device as 'desktop-bga19q8' with a high risk level.
- Evidence:** A timeline of events from November 28, 2019, showing suspicious activities like PowerShell command lines and Microsoft Word behavior.

[Announcement blog](#)

Advanced hunting with custom detection and custom response

The screenshot shows the Microsoft Defender Security Center interface, specifically the Advanced hunting section. The left sidebar contains navigation links for Schema, Shared queries, and Test. The main area displays a PowerShell query for detecting PowerShell downloads over the last 7 days. The results table shows 15 items per page, with 1-15 of 100 total. The columns are EventTime, ComputerName, InitiatingProcessFileName, and FileName. The results list multiple entries where cmd.exe initiated a powershell.exe process. The right side features filters for ComputerName, InitiatingProcessFileName, FileName, and ProcessCommandLine.

Run query + New Save Last 7 days Create detection rule

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

Filters

ComputerName

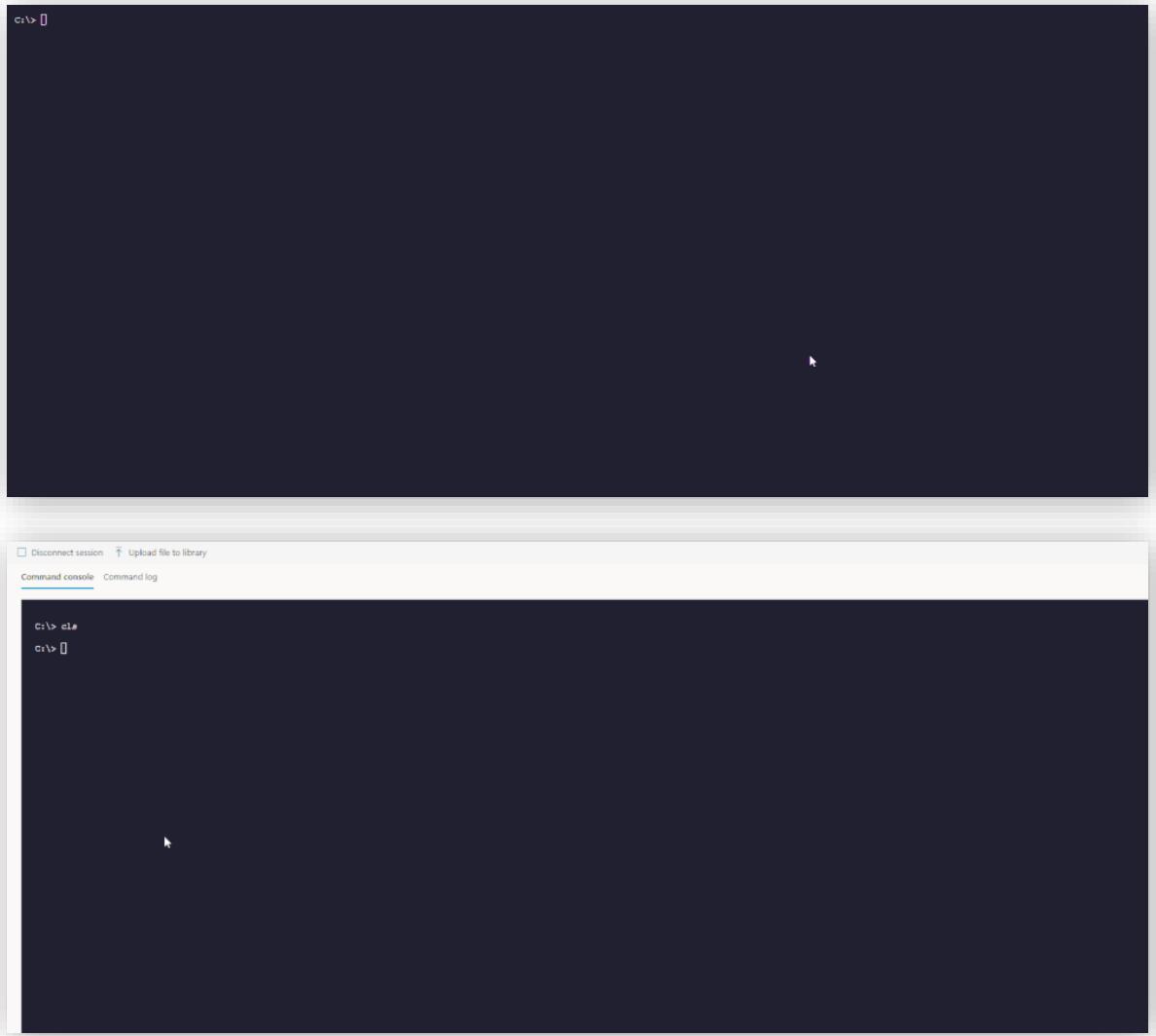
InitiatingProcessFileName

FileName

ProcessCommandLine

Live Response

- Real-time live connection to a remote system
- Leverage Microsoft Defender for Endpoint Auto IR library (memory dump, MFT analysis, raw filesystem access, etc.)
 - Extended remediation command + easy undo
- Full audit
- Extendable (write your own command, build your own tool)
- RBAC+ Permissions
- Git-Repo (share your tools)



Threat Analytics

See how you do against major threats

Threat to posture view

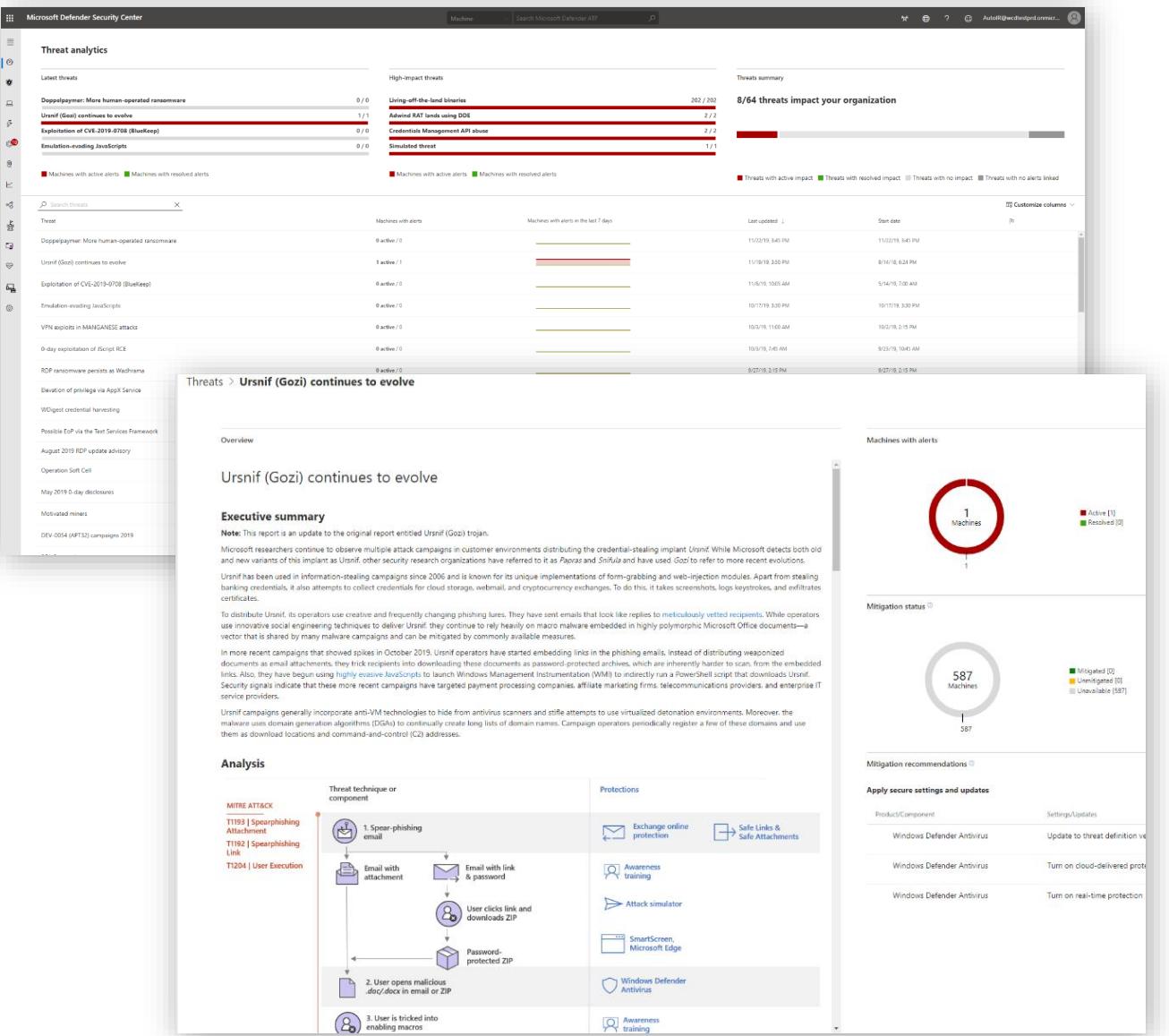
See how you score against significant and emerging campaigns with interactive reports.

Identify unprotected systems

Get real-time insights to assess the impact of the threat on your environment.

Get guidance

Provides recommended actions to increase security resilience, to prevention, or contain the threat.



Break





Lab Preparation

For the next exercise please use your own demo tenant.

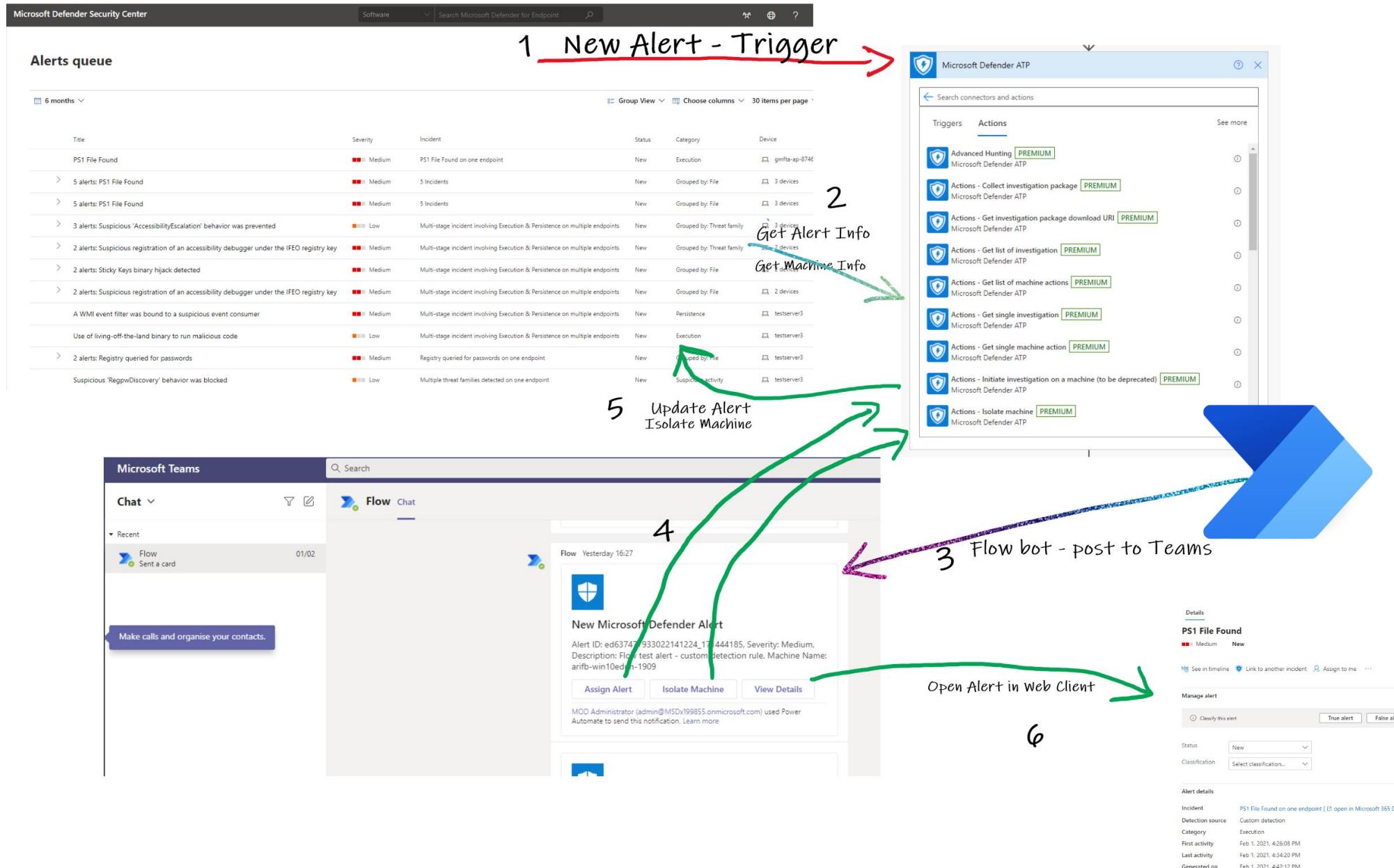
Please head over to:

aka.ms/defendermasterclass-repo

You will need:

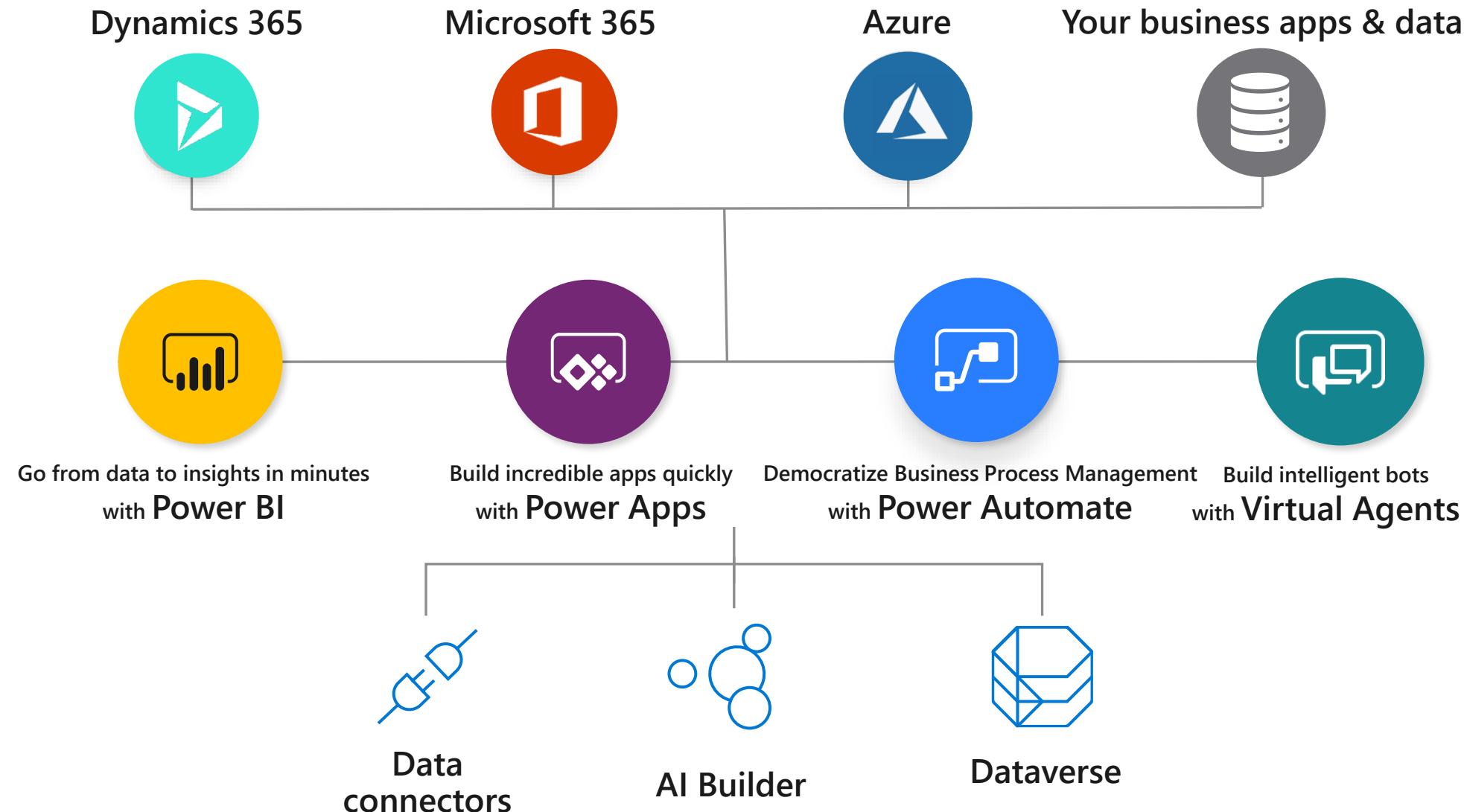
1. Defender Masterclass – Labs Getting Started
2. Defender Masterclass 2 - Multitenant Teams Bot Microsoft Defender Integration Lab
3. Defender Masterclass 2 - Customer Tenant Credentials

Defender for Endpoint Automation

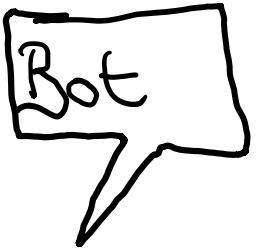


Microsoft Power Platform - Analyse. Act. Automate.

One low-code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone applications – both cloud and on-premises



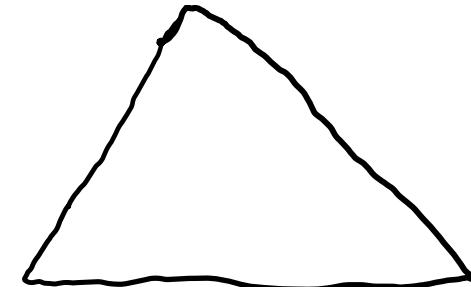
Partner AAD



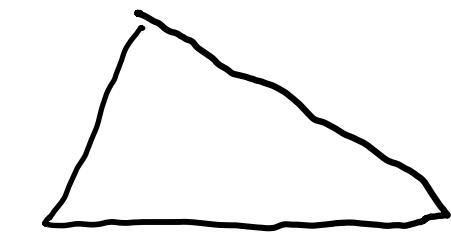
Roles:
DFFE(Alert: Read: All,
Score: Read: All)



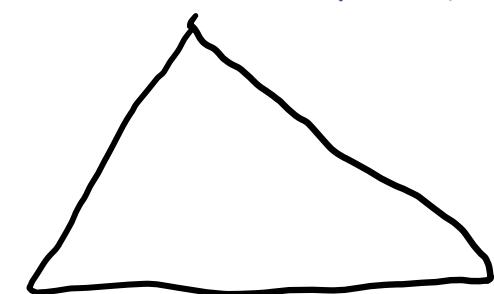
Contoso AAD



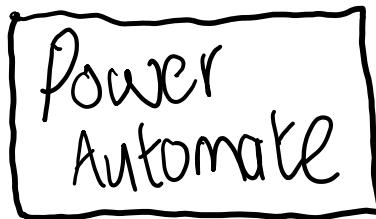
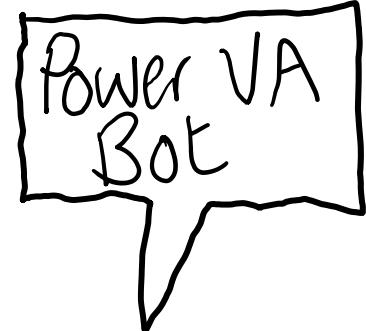
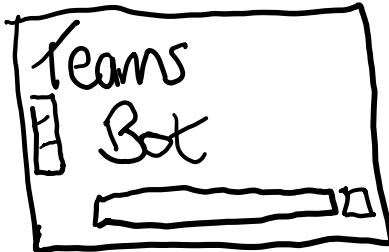
Tailspin AAD



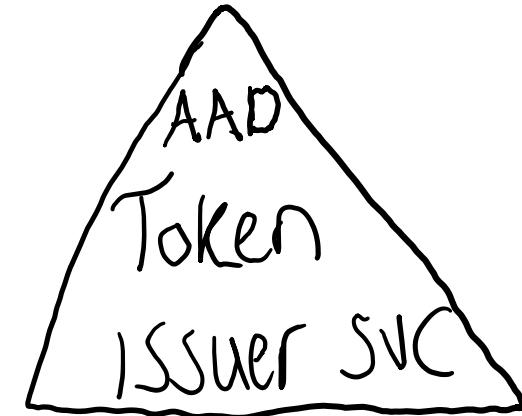
Northwind AAD



Partner



Azure AD



Defender for Endpoint
API service

Score Resource

Alerts Resource

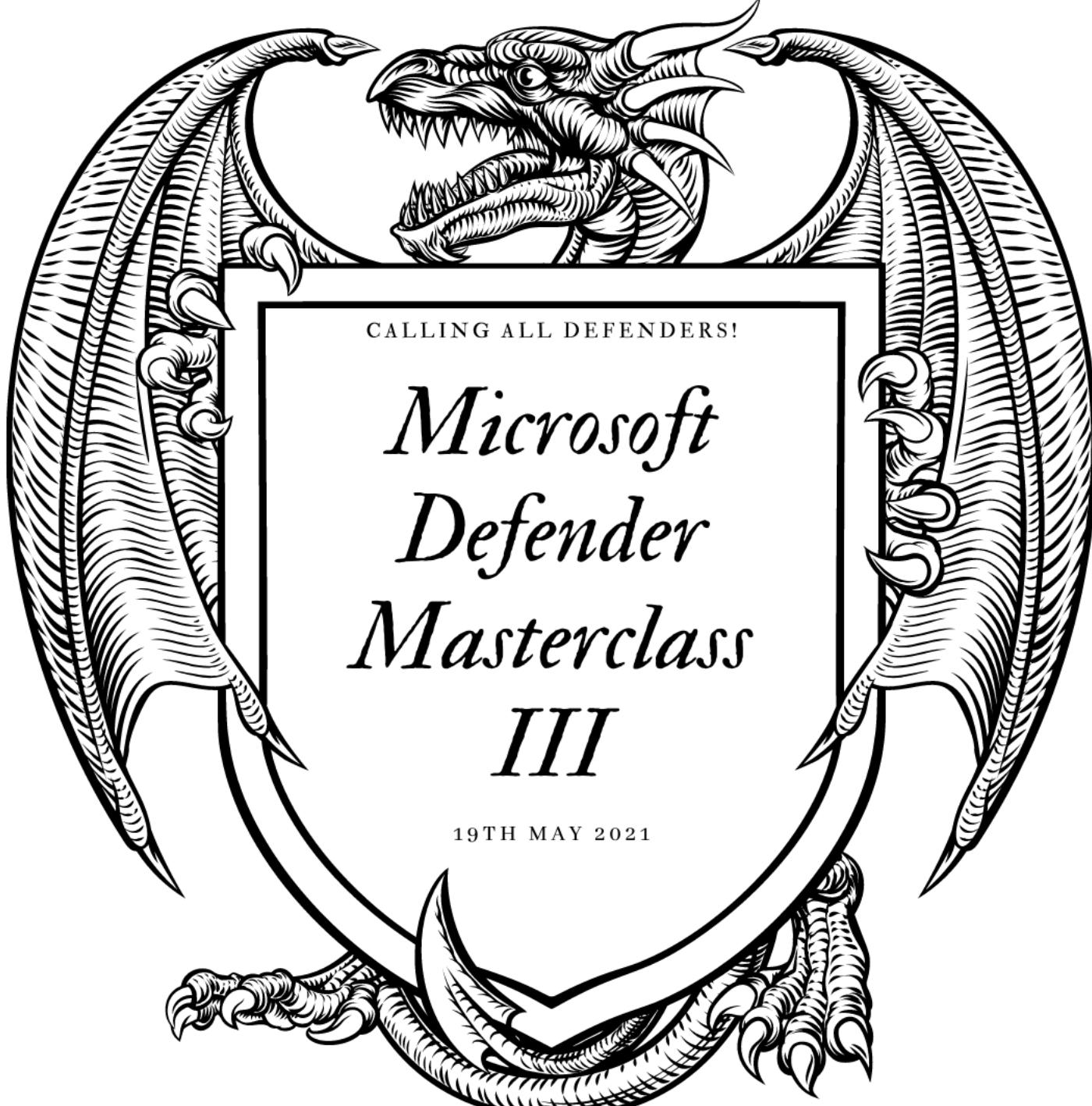
Thank you!

 aka.ms/jacklewis

Jack Lewis
Jack.Lewis@microsoft.com



Register your bravery at
aka.ms/defendermasterclass3-reg



Capture the Flag Finale
aka.ms/defendermasterclass4-reg



aka.ms/defendermasterclass-on-demand

aks.ms/defendermasterclass3-reg

aka.ms/defendermasterclass4-reg

aka.ms/defendermasterclass-feedback

Thank you everyone!