

Agenda

- 9:10 - *Opening Keynote*
- 9:40 - *Tenant Access Setup*
- 9:50 - *Break I*
- 10:00 - *Attack Investigation*
- 11:00 - *Break II*
- 11:10 - *Attack Investigation (cont.)*
- 12:00 - *Power Platform Integration Lab*
- 12:50 - *Closing*
- 13:00 - *End*



Meet the team



Mark Thomas



James Graham



Ally Turnbull



Jack Lewis



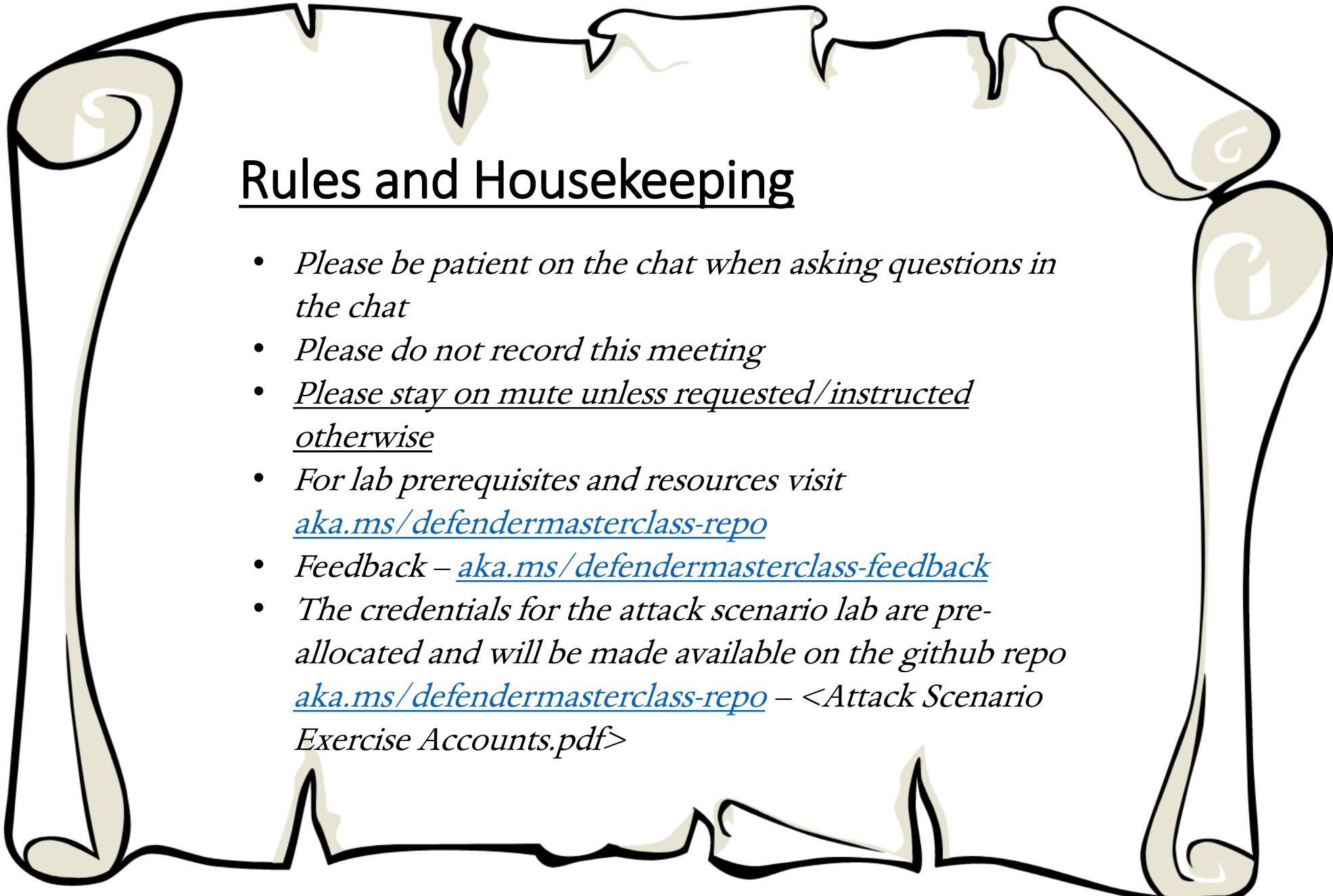
Milad Aslaner



Steve Newby

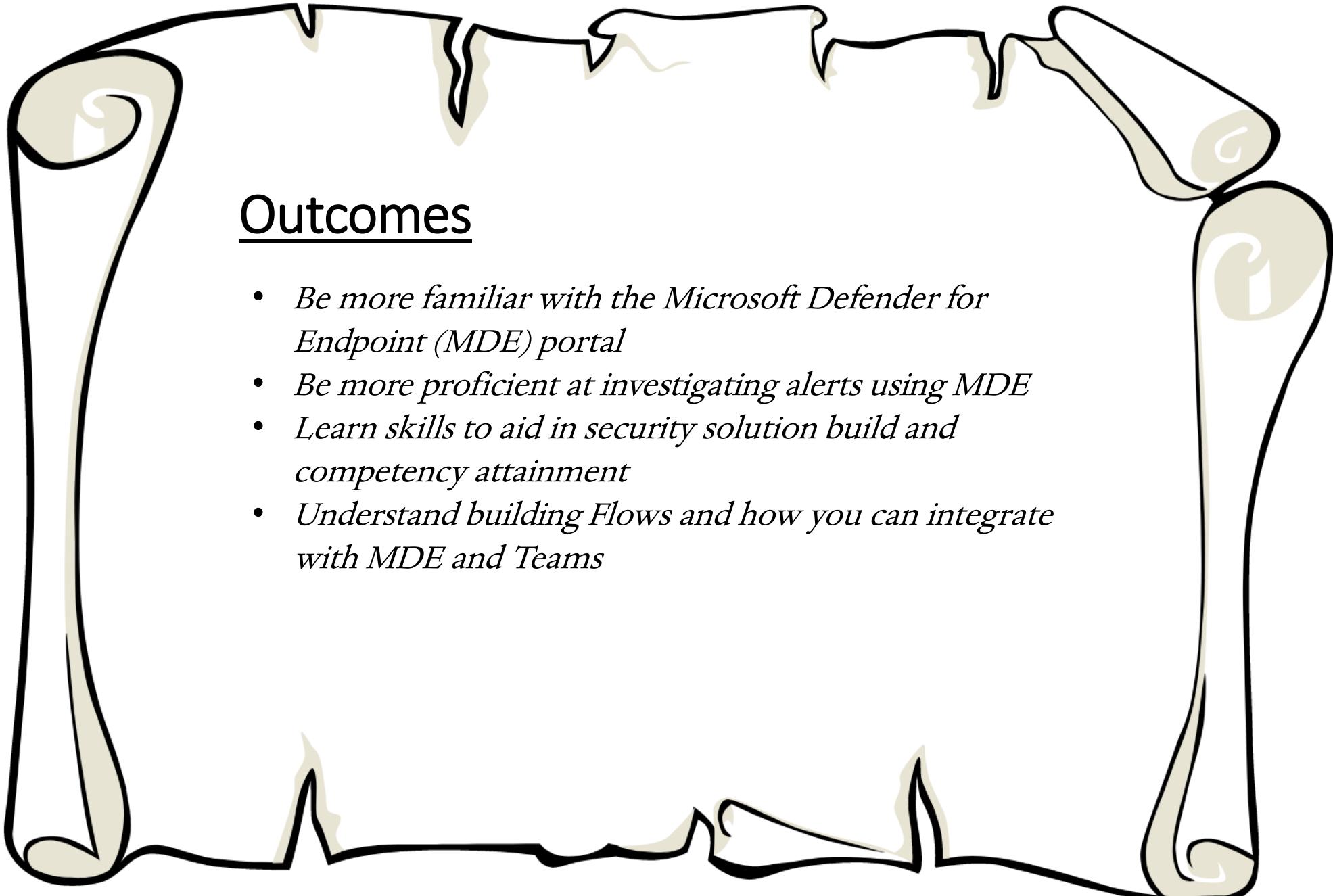


Christos Ventouris



Rules and Housekeeping

- *Please be patient on the chat when asking questions in the chat*
- *Please do not record this meeting*
- *Please stay on mute unless requested/instructed otherwise*
- *For lab prerequisites and resources visit aka.ms/defendermasterclass-repo*
- *Feedback – aka.ms/defendermasterclass-feedback*
- *The credentials for the attack scenario lab are pre-allocated and will be made available on the github repo aka.ms/defendermasterclass-repo – <Attack Scenario Exercise Accounts.pdf>*



Outcomes

- *Be more familiar with the Microsoft Defender for Endpoint (MDE) portal*
- *Be more proficient at investigating alerts using MDE*
- *Learn skills to aid in security solution build and competency attainment*
- *Understand building Flows and how you can integrate with MDE and Teams*



Tenant Access

Disclaimer

- This is a multi-customer, shared training tenant.
- Please do not onboard your own machines, other customers will see the data.
- Please do not put anything PII, offensive, or information that would identify your company in the comments, tags, or any other editable area in the tenant.
- Try to avoid changing data in the tenant such as closing incidents, resolving alerts, etc.

Microsoft Defender Security Center

Getting logged in

<https://securitycenter.microsoft.com>

<<user>>@hunter1337.onmicrosoft.com

Password: DieTrickbot1!

Break

Back at 11:01am (GMT)

<https://securitycenter.microsoft.com>

<<user>>@hunter1337.onmicrosoft.com

Password DieTrickbot1!

Questions doc is on the github repo –
answers uploaded at 12pm GMT

*The credentials for the attack scenario lab are pre-allocated and are available on the github repo [aka.ms/defendermasterclass-repo](https://github.com/aka.ms/defendermasterclass-repo) –
<Attack Scenario Exercise Accounts.pdf>*

If you don't see your name – pick a spare at the bottom of the list

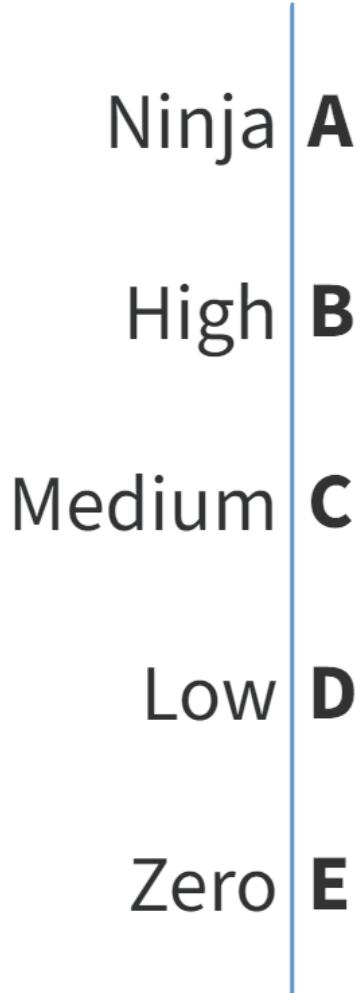




Microsoft Defender for Endpoint

Overview

How familiar are you with the Defender for Endpoint portal?



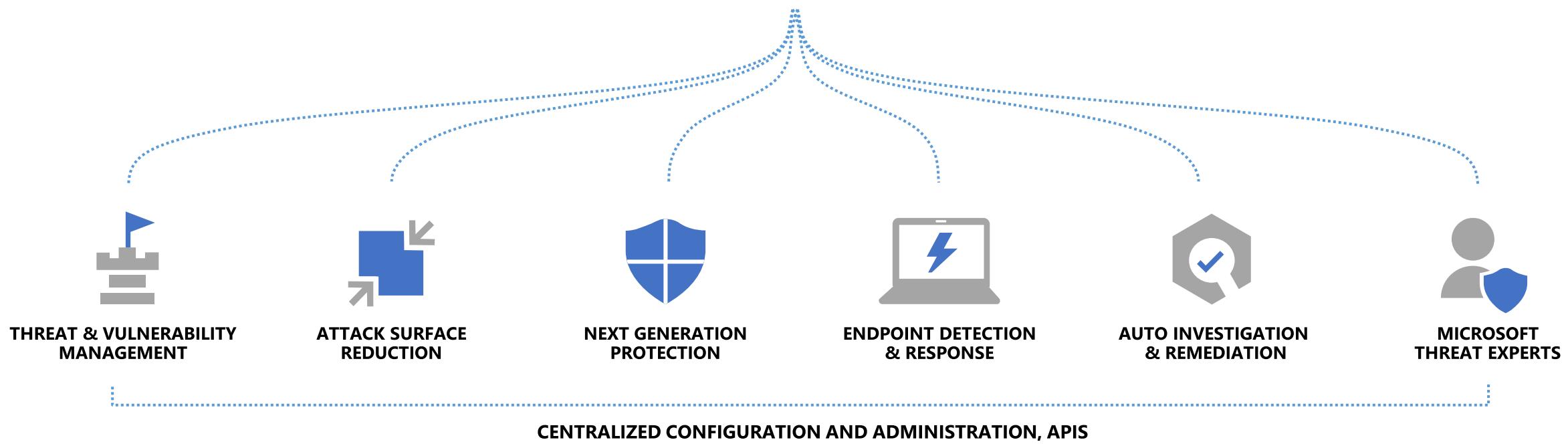
Do you currently have an MDR offering?

- Yes with Defender for Endpoints **A**
- Yes with other 3rd party products **B**
- No **C**
- Building a new MDR / Evaluating MDR **D**



Microsoft Defender for Endpoint

Built-in. Cloud-powered.

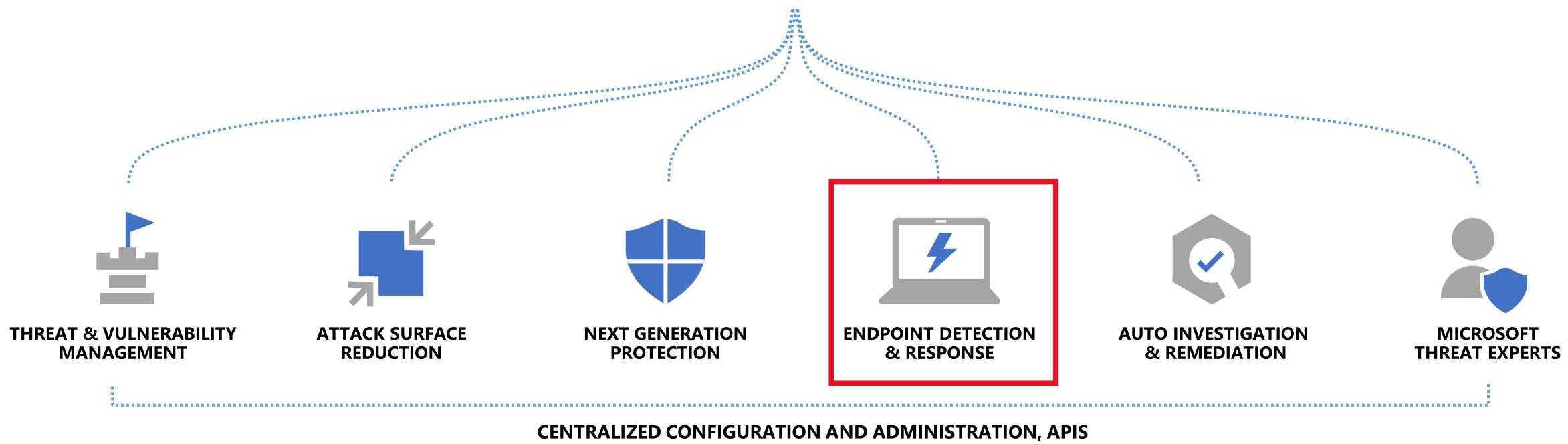


| | | | |
|-----------------------------------|-------------------------------|------------------------|--------------------------|
| Embedded into the OS | Best of breed EPP , EDR | Vulnerability analysis | Cross suite integrations |
| World class anti-tampering | Support for W7/8, non-Windows | Secure score & CA | Data separation, RBAC |
| Deep data collection & 6m storage | Integrated config mgmt. | Automation | Cloud expertise |



Microsoft Defender for Endpoint

Built-in. Cloud-powered.



| | | | |
|-----------------------------------|-------------------------------|------------------------|--------------------------|
| Embedded into the OS | Best of breed EPP , EDR | Vulnerability analysis | Cross suite integrations |
| World class anti-tampering | Support for W7/8, non-Windows | Secure score & CA | Data separation, RBAC |
| Deep data collection & 6m storage | Integrated config mgmt. | Automation | Cloud expertise |



Microsoft Defender for Endpoint

Attack Scenarios



Scenario 1

Microsoft Defender Security Center

Incidents

1-3 < > 30 days Choose co

| Incident name ↑ | Severity | Investigation state | Categories |
|--|----------|------------------------|---------------------------------------|
| > Scenario 1 - Zack the Bitcoin Maniac | Low | 2 investigation states | Unwanted software |
| > Scenario 2 - The Final Countdown | Medium | 2 investigation states | Execution, Persistence, Privileg... |
| > Scenario 3 - AutoIR | Medium | 2 investigation states | Initial access, Execution, Persist... |

Scenario 1

Microsoft Defender Security Center

Manage incident [?](#) Consult a threat expert

Incidents > **Scenario 1 - Zack the Bitcoin Maniac**

Alerts (3) Devices (1) Investigations (2) Evidence [beta](#) Graph [beta](#)

Grouped view [Choose columns](#) 30

| First activity ↑ | Title | Severity | Status | Linked by | Category |
|------------------|---|------------------|--------|-----------|------------|
| 1/6/21, 5:58 PM | 'CoinMiner' unwanted software was detected | Informational... | New | 2 reasons | Unwanted s |
| 1/6/21, 6:24 PM | Digital currency mining literals have been observed | Low | New | Same file | Unwanted s |
| 1/6/21, 6:26 PM | An active 'CoinMiner' unwanted software was blocked | Low | New | 2 reasons | Unwanted s |

What happened?

- Zach really wants to mine bitcoins on his corporate machine
- When Defender AV blocks the miner, he disables real-time protection
- He then downloads and runs the coin miner again
- Whilst mining, Defender AV real-time protection starts up again, detects the miner is running, blocks it and quarantines it

Break

Back at xx

For the next exercise please use your own
demo tenant





Scenario 2

Microsoft Defender Security Center

Incidents

1-3 < > 30 days Choose co

| Incident name ↑ | Severity | Investigation state | Categories |
|--|----------|------------------------|---------------------------------------|
| > Scenario 1 - Zack the Bitcoin Maniac | Low | 2 investigation states | Unwanted software |
| > Scenario 2 - The Final Countdown | Medium | 2 investigation states | Execution, Persistence, Privileg... |
| > Scenario 3 - AutoIR | Medium | 2 investigation states | Initial access, Execution, Persist... |

Scenario 2

Microsoft Defender Security Center

57

Consult a threat expert

Incidents > Scenario 2 - The Final Countdown

Alerts (23) Devices (3) Investigations (0) Evidence (24) Graph beta

Grouped view Choose columns 30 items

| First activity | Title | Severity | Status | Linked by | Category |
|-------------------|--|----------|--------|-------------|---------------|
| > 1/6/21, 6:52 PM | 7 alerts: Suspicious PowerShell command line | Medium | New | 3 reasons | Group |
| > 1/6/21, 6:52 PM | 2 alerts: Suspicious PowerShell command line | Medium | New | Same device | Group |
| 1/6/21, 6:52 PM | Suspicious service registration | Medium | New | Same device | Persistent |
| 1/6/21, 6:52 PM | Known attack framework activity was observed | Medium | New | Same device | Execution |
| 1/6/21, 6:52 PM | Echo command over pipe on localhost | Low | New | Same device | Privileged |
| 1/6/21, 6:54 PM | Powershell made a suspicious network connection | Low | New | Same device | Communication |
| 1/6/21, 6:54 PM | A malicious PowerShell Cmdlet was invoked on the machine | Medium | New | Same device | Execution |
| 1/6/21, 6:55 PM | WDigest configuration change | Low | New | Same device | Credential |
| 1/6/21, 6:58 PM | Network mapping for reconnaissance | Medium | New | Same device | Discovery |

Scenario 2 - Activity

1. What device does the incident start with?
2. What is the PowerShell running in the first Suspicious PowerShell Alert?
3. On which machines does cleanup.ps1 exist?
4. How was the suspicious service registered on device trn-w2k12-1?
5. What is the impact of the Wdigest configuration change?

Scenario 2 - Activity

6. Advanced Hunting: Find all machines where
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\Wdigest\UseLogonCredential was changed from 0 to 1
7. What users have logged into the device? (BONUS Advanced Hunting: Did any other users log on to the device within 30 minutes of the Wdigest registry change?)
8. What URL did PowerShell make a suspicious network connection to and what tool was executed?
9. What devices have Suspicious Task Scheduler activity and what processes were involved?
10. What executable does the suspicious scheduled tasks run?

Scenario 2 - Activity

11. In the device timeline what key actions does the file browserhelp.exe perform?
12. Advanced Hunting: Find PowerShell events that could involve a download.

What happened?

- An attacker brute forces sysadmin on trn-w2k12-1
- Meterpreter to the device and waits for someone to log in.
- Margo logs in and her credentials are stolen
- Margo's credentials are used to remote PowerShell to trn-win10-1 and trn-win10-2
- Schedules a task to run Browserhelp.exe every 5 minutes
- Browserhelp.exe checked for Spartacus, then creates funnygagwiper.exe and checks for a command from a C2 server
- Event logs are cleared
- Tries to stop Sense.exe (Defender for Endpoint service)
- Attacker tries to wipe the device with one final scheduled task
- SOC finds all this and stops it before the wiper could run



Let us know if you need help on Teams chat

For the next exercise please use your own demo tenant – instructions located at

Labs – Getting Started at
aka.ms/defendermasterclass-repo – lab
guide also available here!

If you can't create one – no problem! A link will be provided in the chat for you to access an account for a tenant I have made available.

aka.ms/defendermasterclass-repo

Thank you everyone!

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
- Launching December 2020

*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 header with the title 'Virtual Training Series' and a subtext 'Enhance your technical skills with interactive webinars for core customer technical scenarios.' Below this is a button labeled 'See the schedule >'. The main section is titled 'Featured trainings' and contains four cards, each with a thumbnail image, title, and date. The first card is for a live offering: 'Don't miss these new VTS opportunities' (Live VTS offerings - July 2020), dated 2020-06-12. The second card is for 'AZ-900: Microsoft Azure Fundamentals' (Recorded VTS - Beginner - 5 hrs 0 min), dated 2020-03-27. The third card is for 'MB-700: Microsoft Dynamics 365 Finance & Operations Apps Solution Architect' (Recorded VTS - Advanced - 5 hrs 0 min), dated 2020-06-26. The fourth card is for 'MS-900: Microsoft 365 Fundamentals' (Recorded VTS - Beginner - 4 hrs 0 min), dated 2020-05-22.

| Thumbnail | Title | Date |
|-----------|--|------------|
| | 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>

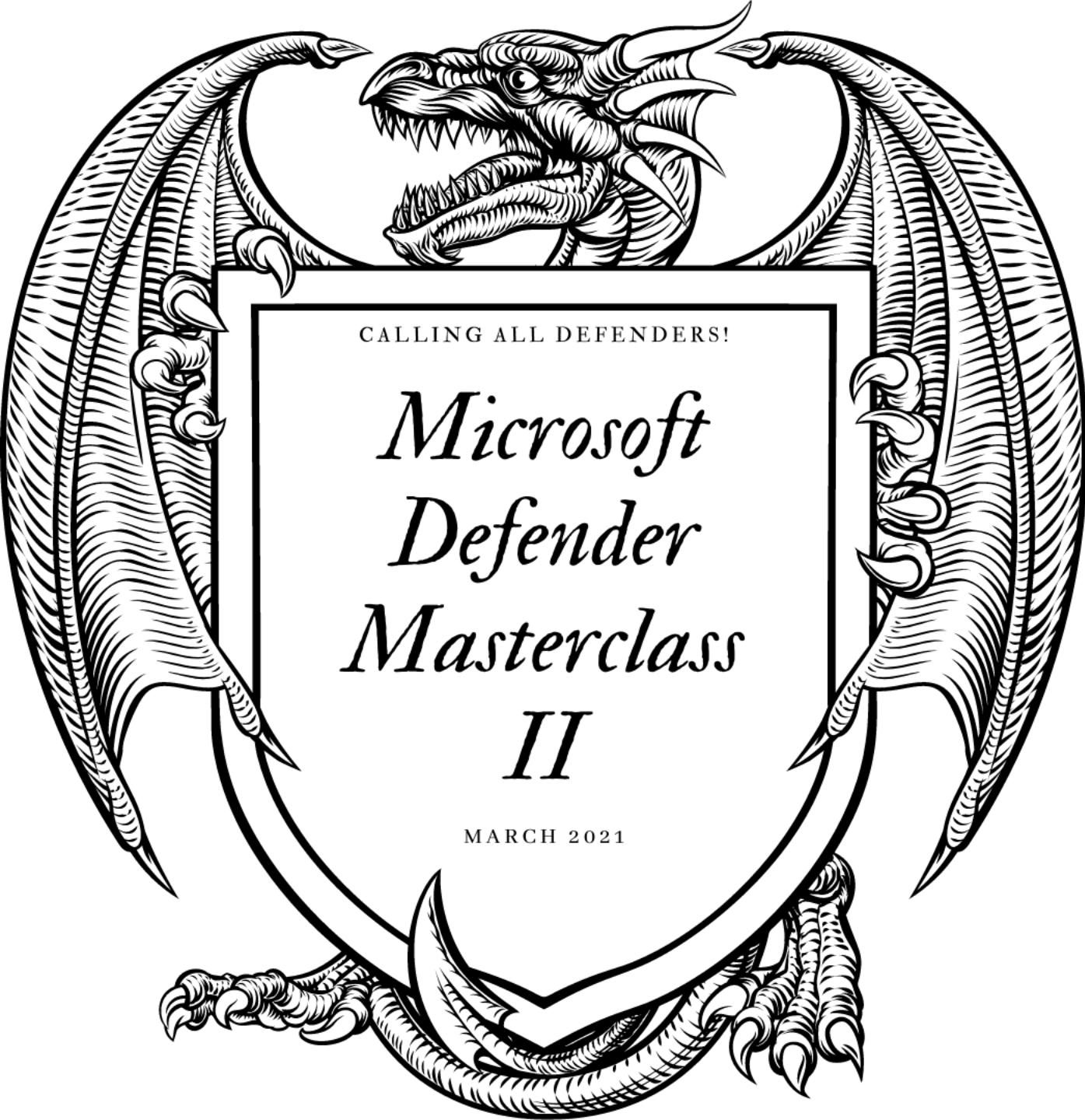
Ninja Self paced training

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



aka.ms/defendermasterclass-feedback

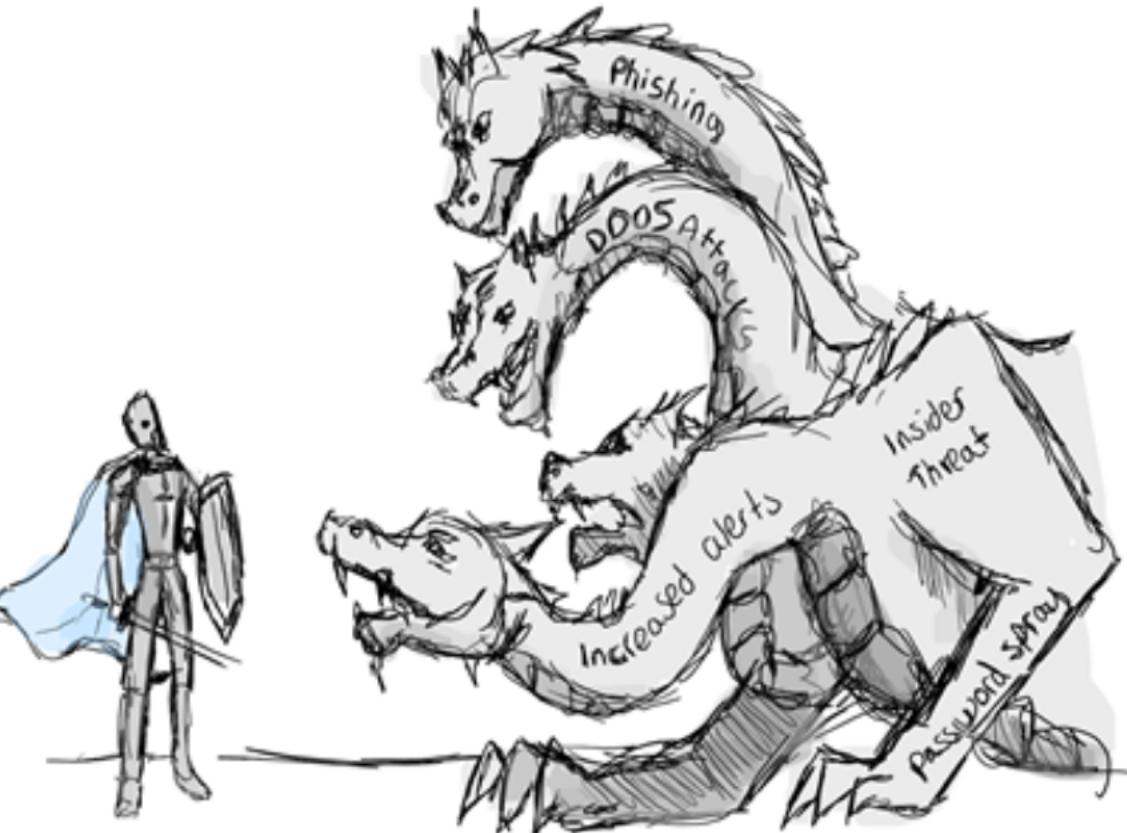
Thank you everyone!

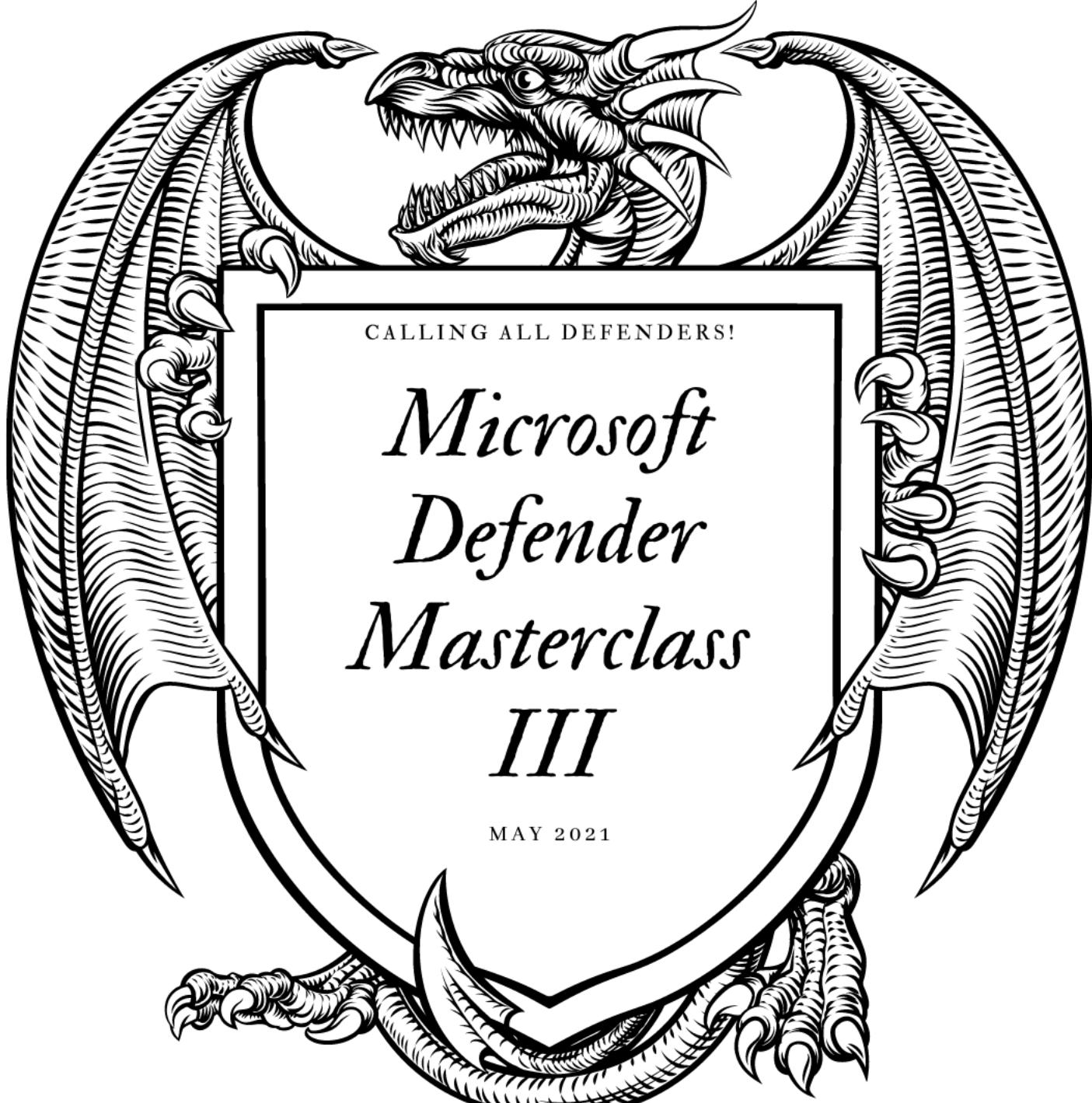


CALLING ALL DEFENDERS!

Microsoft *Defender* *Masterclass* II

MARCH 2021





Capture the Flag – June 2021

