Become a Microsoft Defender for Endpoint Ninja

techcommunity.microsoft.com/t5/microsoft-defender-atp/become-a-microsoft-defender-atp-ninja/ba-p/1515647

July 13, 2020

Jul 13 2020 09:59 AM

Last updated: May 18th 2022

Do you want to become a ninja for Microsoft Defender for Endpoint? We can help you get there! We collected content for two roles: “Security Operations (SecOps)” and “Security Administrator (SecAdmin)”. The content is structured into three different knowledge levels, with multiple modules: Fundamentals, Intermediate, and Expert. Some topics can be relevant for SecOps as well as for SecAdmins and are listed for both roles. We will keep updating this training on a regular basis and highlight new resources.

In addition, after each level, we offer you a **knowledge check** based on the training material you have just finished! Since there’s a lot of content, the goal of the knowledge checks is to help ensure understanding of the key concepts that were covered. Lastly, there’ll be a fun **certificate** issued at the end of the training: Disclaimer: **This is not an official Microsoft certification and only acts as a way of recognizing your participation in this training content**.

`If you already did the training, you can focus on the latest updates (August 2021 update)`

Table of Contents

Module 2. Getting started

Module 3. Threat and vulnerability management

Module 4. Attack surface reduction

Module 5. Next generation protection

Module 6. Investigation – Incident

Module 7. Alert handling

Module 8. Automated investigation and remediation

Module 9. Microsoft Threat Experts

Module 10. Reporting

Module 11. Evaluation Lab

Security Operations Intermediate

Module 1. Architecture

Module 2. Threat and vulnerability management

Module 3. Next generation protection.

Module 4. Advanced hunting

Module 5. Automated investigation and remediation

Module 6. Threat analytics

Module 7. Unified indicators of compromise (IOCs)

Module 8. Evaluation lab

Module 9. Community (blogs, webinars, GitHub)

Security Operations Expert

Module 1. Responding to threats

Module 2. Alert handling

Module 3. File analysis

Module 4. Advanced hunting

Module 5. Unified indicators of compromise IOCs

Module 6. Custom reporting

Module 7. Community (blogs, webinars, GitHub)

Security Administrator Fundamentals

Module 1. Architecture

Module 2. Onboarding

Module 3. Grant and control access

Module 4. Security configuration

Module 5. Reporting

Module 6. SIEM Integration

Security Administrator Intermediate

Module 1. Threat and vulnerability management (TVM)

Module 2. Attack surface reduction

Module 3. Next generation protection

Module 4. Advanced hunting

Module 5. Conditional access

Module 6. Microsoft Cloud App Security (MCAS)

Module 7. Community (blogs, webinars, GitHub)

Module 8. Migration

Security Administrator Expert

Module 1. Custom reporting (PowerBI)

Module 2. Advanced hunting

Module 3. Custom Integrations, APIs

Learn about our partner integrations

Legend:

🎥 Product videos	🎬 Webcast recordings	🗣️ Tech Community
📖 Docs on Microsoft	📝 Blogs on Microsoft	GitHub
⤴ External	💻 Interactive guides	

Security Operations Fundamentals

Module 1. Technical overview

- 🎥 Short overview “What is Microsoft Defender for Endpoint"
- 🎬 End-to-end security for your endpoints

Module 2. Getting started

- 📖 Portal overview
- 📝 Welcome to Microsoft 365 Defender!
- 📖 Use basic permissions to access the portal
- 🎥 How to use RBAC
- 📝 Device Inventory

Module 3. Threat and vulnerability management

- 🎥 What is threat and vulnerability management
- 🎬 "Bringing IT & security together: How Microsoft is reinventing threat and vulnerability management"
- 💻 Reduce organizational risk with threat and vulnerability management

Module 4. Attack surface reduction

- 🎥 Learn about all the features to help you reduce the attack surface
- 📝 Understand attack surface reduction rules
- 📝 Track and regulate access to websites with web content filtering

Module 5. Next generation protection

- 📖 Microsoft Defender Antivirus: Your next generation protection

Module 6. Investigation – Incident

- 🎥 Learn about the rich investigation experience
- 📖 Work with incidents

- 📝 MITRE ATT&CK Techniques available in the device timeline
- 💻 Investigate and remediate threats with Microsoft Defender for Endpoint

Module 7. Alert handling

- 🎥 Get the most out of an alert page
- 📝 Working with alerts
- 📝 Alert categories aligned with MITRE ATT&CK
- 📝 How alerts are enhanced to include MITRE ATT&CK technique information

Module 8. Automated investigation and remediation

- 🎥 How automation works
- 📝 Defining metrics for successful security operations

Module 9. Microsoft Threat Experts

- 🎥 What is Microsoft Threat Experts
- 📖 Getting started with Microsoft Threat Experts

Module 10. Reporting

- 📖 Out of the box reports

Module 11. Evaluation Lab

- 📖 Get started with the evaluation lab
- 🎥Short walk-through the evaluation lab

> Ready for the Fundamentals Knowledge Check?

Security Operations Intermediate

Module 1.Architecture

- 🎥 Understand the architecture of the service

Module 2. Threat and vulnerability management

- 🎥 Discovery and remediation
- 📝 Endpoint Discovery - Navigating your way through unmanaged devices
- 💻 Reduce organizational risk with threat and vulnerability management

- 📝 Tag your high value assets for better prioritization

Module 3. Next generation protection

- 📖 Learn about our approach to fileless threats
- 🎬 Stopping attacks in their tracks through behavioral blocking and containment
- 📝 EDR in block mode
- 📝 Firmware level protection with a new Unified Extensible Firmware Interface (UEFI) scanner
- 📝 Enhanced antimalware engine capabilities for Linux and macOS
- 📝 Enhanced Antimalware Protection for Android

Module 4. Advanced hunting

- 🎥 Quick overview & a short tutorial that will get you started fast

Module 5. Automated investigation and remediation

- 📝Automate the boring for your SOC with automatic investigation and remediation!
- 📝 Default settings
- 📖 Configure automated investigation and remediation capabilities
- 📖 Manage automation file uploads
- 📖 Manage automation folder exclusions

Module 6. Threat analytics

- 🎥 Get familiar with threat analytics
- 📖 Understand the analyst report section in threat analytics
- 📖 Track and respond to emerging threats

Module 7. Unified indicators of compromise (IOCs)

- 🎥 Working with IOCs

Module 8. Evaluation lab

- 🎥 Short walk-through the evaluation lab
- 📝 Breach & attack simulators for the evaluation lab
- 📝 Expanded OS support & Atomic Red Team simulations
- 📖 Request more devices

Module 9. Community (blogs, webinars, GitHub)

- 📑 Various repositories

> Ready for the Intermediate Knowledge Check?

Security Operations Expert

Module 1. Responding to threats

- 🎥 Overview of live response
- 📖 Investigate entities on devices using live response
- 📖 Response actions on machines
- 📖 Response actions on a file

Module 2. Alert handling

- 📖 Manage alert suppression rules

Module 3. File analysis

- 🎥 Use the built-in sandbox to detonate files
- 📝 Submit items to Microsoft for review

Module 4. Advanced hunting

- 📖 Learn the query language
- 📖 Advanced hunting schema reference
- 🎬 Webinar series, episode 1: KQL fundamentals (MP4, YouTube)
- 🎬 Webinar series, episode 2: Joins (MP4, YouTube)
- 🎬 Webinar series, episode 3: Summarizing, pivoting, and visualizing Data (MP4, YouTube)
- 🎬 Webinar series, episode 4: Let's hunt! Applying KQL to incident tracking (MP4, YouTube)
- 📝 Hunting for reconnaissance activities using LDAP search filters
- ⤴ Plural sight KQL training

- 📝 Updates to threat and vulnerability management tables
- 📖 Details about DeviceTvmSoftwareInventory
- 📖 Details about DeviceTvmSoftwareVulnerabilities
- 📝 How to migrate advanced hunting to Microsoft 365 Defender

Module 5. Unified indicators of compromise IOCs

Module 6. Custom reporting

- 📖 Create custom reports using Power BI
- 📑 Custom reports on GitHub

Module 7. Community (blogs, webinars, GitHub)

> Ready for the Expert Knowledge Check?

Security Administrator Fundamentals

Module 1. Architecture

- 🎥 Understand the architecture of the service

Module 2. Onboarding

Module 3. Grant and control access

- 📖 Use basic permissions to access the portal
- 🎥 How to use RBAC
- 📝 How to use tagging effectively (Part 1)
- 📝 How to use tagging effectively (Part 2)
- 📝 How to use tagging effectively (Part 3)
- 🎥 Multi-tenant access for Managed Security Service Providers
- 📝 Step-by-step: Multi-tenant access for Managed Security Service Providers

Module 4. Security configuration

Module 5. Reporting

Module 6. SIEM Integration

- 📖 Management APIs

> Ready for the Fundamentals Knowledge Check?

Security Administrator Intermediate

Module 1. Threat and vulnerability management (TVM)

Module 2. Attack surface reduction

- 🎥 Learn about all the features to help you reduce the attack surface
- 📖 Learn about attack surface reduction rules
- 📝 Track and regulate access to websites with web content filtering
- 🎥 Learn more about Application control
- 🎥 Get a better understanding of Network protection

- 📝 Understand attack surface reduction rules
- 📝 How to configure attack surface reduction rules and how to use exclusions
- 📖 Details about using Microsoft Endpoint Manager MEM OMA-URI to configure ASR rules
- 📝 How to report and troubleshoot Microsoft Defender for Endpoint ASR Rules
- 📝 USB device control on Mac
- 📖 Device control for MacOS
- 📝 Migrate from a 3rd party HIPS solution into ASR rules
- 🎥 Reputation analysis - Microsoft Defender SmartScreen

Module 3. Next generation protection

Module 4. Advanced hunting

- 🎥 Quick overview & a short tutorial that will get you started fast

Module 5. Conditional access

- 🎥 How to configure conditional access

Module 6. Microsoft Defender for Cloud Apps

Module 7. Community (blogs, webinars, GitHub)

- 📑 Advanced hunting queries on GitHub

Module 8. Migration

> Ready for the Intermediate Knowledge Check?

Security Administrator Expert

Module 1. Custom reporting (PowerBI)

Module 2. Advanced hunting

Module 3. Custom Integrations, APIs

- 🎥 Use Microsoft Defender for Endpoint APIs
- 📖 Available APIs
- 📝 API Explorer and Connected applications
- 📖 Microsoft Defender for Endpoint API Explorer

- 📝 Customized views with APIs
- 📖 Use the official Power Automate Connector
- 📝 Raw data export
- 🎥 Streaming API
- 📖 Threat and vulnerability management API collection Export Assessment API
- 📖 Threat and vulnerability management API collection Remediation Activity

Learn about our partner integrations

> Ready for the Expert Knowledge Check?

Once you've finished the training and the knowledge checks, please **click here** to request your certificate (you'll see it in your inbox within 3-5 business days.)