McAfee MVISION Endpoint Detection and Response Administration

McAfee® Education Services Instructor-Led Training

Adversaries maneuver in covert ways, camouflaging their actions within the most trusted components already in your environment. They don't always install something tangible like malware, but they always leave behind a behavioral trail. Endpoint detection and response (EDR) continuously monitor and gather data to provide the visibility and context needed to detect and respond to threats. But current approaches often burden already-stretched security teams with too much information. McAfee® MVISION EDR helps to manage the high volume of alerts, empowering analysts of all skill levels to do more and investigate more effectively. This course prepares security operations center (SOC) analysts to understand, communicate, and use the features of McAfee MVISION EDR. Through hands-on lab exercises, you will learn how to detect advanced device threats, fully investigate, and respond quickly.

Earn up to 16 CPEs after completing this course.*

* Student must self-report for CPE credits. We cannot guarantee any specific quantity, as it is up to the program or certification group to determine what they will or will not accept.

Audience

This course is intended for McAfee customers who serve as analysts and/or engineers, responsible for configuration, management, and monitoring activity on their systems, networks, databases, and applications using the MVISION EDR solution. They should have a working knowledge of networking, system administration, computer security concepts, and a general understanding of networking and application software.

Connect With Us

Agenda at a Glance

Day 1
- Welcome
- What Is EDR?
- Architecture
- Setup and Deployment
- Monitoring
- Alerting
- Historical Search
- Real-Time Search

Day 2
- Investigating
- Catalog
- Action History
- Performance Metrics
- Troubleshooting
- Use Cases
- Incident Response
- Threat Hunting

Recommended Pre-Work

It is recommended that students have a working knowledge of:
- Networking and system administration concepts
- Computer security concepts
- Network security concepts and practices
- Malware analysis, forensics, and tactics and techniques

Learning Objectives

What Is EDR?
- Review how MVISION EDR plays a part in the McAfee portfolio
- Define MVISION EDR components
- Distinguish how MVISION EDR helps the SOC mission
- Identify MVISION EDR capabilities
- Describe the MITRE ATT&CK Matrix

Architecture
- Describe the product/solution architecture
- Distinguish between deployment options
- Review common log and product files
- Identify product/solution communication paths and ports

Setup and Deployment
- Identify the supported platform, environment, or operating systems
- Review the first steps for adding MVISION EDR to your environment
- Install MVISION EDR on an on-premises (local) or MVISION ePO™ deployment
- Check in the required product extension(s)
- Deploy the MVISION EDR Client to endpoints

Monitoring
- View threat events in the Monitoring dashboard
- Review the MVISION EDR threat detection approach
- Take action from the Monitoring dashboard

COURSE DESCRIPTION

Alerting

- Leverage the Alerting dashboard to view the raw events from managed devices
- View how alert events match to the MITRE observed tactics and techniques

Historical Search

- Use historical data to assist with analyzing how a threat occurred in the system and what triggered it
- Review the Historical Search investigation capabilities

Real-Time Search

- Obtain information about processes currently running on managed endpoints using real-time search queries
- Leverage the query syntax to combine collectors and build powerful search expressions
- Take action on search results to execute reaction code onto managed endpoints

Investigating

- Analyze an investigation using the key findings and key artifacts discovered
- View details to investigated items, linked investigations, investigation guides, and similar cases in the investigation workspace

Catalog

- Navigate to the Catalog dashboard to view built-in collectors and reactions
- Use the Catalog dashboard to create or delete custom collectors and reactions

Action History

- View the details of actions performed through the Action History dashboard

Performance Metrics

- View the Performance Metrics page to analyze the amount of time spent on resolving investigations

Troubleshooting

- Walk through actions to take if no events are seen in the Monitoring dashboard
- View MVISION EDR tenancy status
- Perform troubleshooting steps for Investigations
- Troubleshoot Data Exchange Layer (DXL) connectivity

Use Cases

- Use the Monitoring dashboard to identify threats
- Create an investigation
- Quarantine a system or process
- Perform in-depth analysis using real-time search
- Increase familiarity and workflow with MVISION EDR

Related Courses

- McAfee® MVISION Endpoint
- McAfee® MVISION Cloud
- McAfee® MVISION ePO™
- McAfee® MVISION Mobile

Incident Response (IR)

- Review the definition of a cybersecurity incident
- Identify the different vectors of cyber incidents
- Describe IR and its importance
- Explain the IR lifecycle
- Identify the data sources which may be encountered during a digital forensic investigation
- List the order of volatility in relation to digital artifacts
- Explain the principles of evidence handling
- Maintain the chain of custody of evidence
- Identify tools needed for IR
- Acquire evidence

Threat Hunting

- Review the definition of threat hunting
- Describe why threat hunting is required
- Identify threat hunting platform drivers
- Identify different threat hunting styles
- Theories and models used in threat hunting
- Describe the threat hunting maturity model
- Describe advanced persistent threats
- Review threat hunting tips

Learn More

To order, or for further information, please email **SecurityEducation@mcafee.com**.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee, the McAfee logo, and ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2020 McAfee, LLC. 4442_0320
MARCH 2020