Trellix

DATASHEET

MVISION Endpoint Detection and Response (EDR) Administration

Education Services Instructor-led Training

Introduction

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 dump too much information on already stretched security teams. 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 SOC Analysts to understand, communicate, and use the features provided by Endpoint Detection and Response. Through hands-on lab exercises, you will learn how to detect advanced device threats, fully investigate, and quickly respond.

This course prepares SOC Analysts to understand, communicate, and use the features provided by Endpoint Detection and Response.

Audience

This course is intended for customers, acting as either or both Analysts and Engineers, responsible for configuration, management, and monitoring activity on their systems, networks, databases and applications using the MVISION EDR solution. A working knowledge of networking, system administration, computer security concepts, and a general understanding of networking and application software.

Agenda At A Glance

Day 1

- Welcome
- What is EDR?
- Architecture
- Setup and Deployment
- Monitoring
- Alerting
- Device Search
- Historical Search

Day 2

- Real-time Search
- Investigating
- Catalog
- Action History
- Performance Metrics
- Troubleshooting
- Use Cases
- Incident Response
- Threat Hunting

Course Learning Objectives

What is EDR?

- Recall how MVISION EDR plays a part in the company portfolio
- Define MVISION EDR components
- Distinguish how MVISION EDR helps the SOC Mission
- Identify MVISION EDR capabilities
- Describe the MITRE ATT&CK Matrix

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, tactics and techniques

Architecture:

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

Setup and Deployment:

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

Monitoring:

- Recall what Cyber Threat Hunting is.
- Identify different Threat Hunting styles.
- Describe why Threat Hunting is required.
- Recall Threat Hunting tips.
- View threat events in the Monitoring dashboard.
- Recall the MVISION EDR threat detection approach.
- Recall how to take action from the Monitoring dashboard.

Alerting:

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

Device Search:

- Use device data to assist with analyzing how a threat occurred in the system and what triggered it.
- Recall the Device Search investigation capabilities.

Historical Search:

- Use historical data to assist with analyzing how a threat occurred in the system and what triggered it
- Recall 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, i nvestigation guides, and similar cases in the investigation workspace.
- Recall what is a cyber security incident.
- Identify the different vectors of cyber incidents.
- Describe what is Incident Response (IR) and its importance.

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.

Related Courses

- MVISION Endpoint
- MVISION Cloud
- MVISION ePO
- MVISION Mobile

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 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

.