DATA SHEET

FireEye Alert Analysis and Endpoint Investigations

Instructor-led training

HIGHLIGHTS

Duration
3 days

Prerequisites
A working understanding of networking and network security, the Windows operating system, file system, registry and regular expressions, and experience scripting in Python.

Recommended Pretraining
FireEye Network Security Deployment eLearning
*FireEye Endpoint Security Deployment eLearning

How to Register
Public sessions are listed on our course calendar.
https://www.fireeye.com/services/training/schedule/

Private sessions are available. Please contact your FireEye account representative for scheduling and pricing options.

This 3-day course examines how to triage alerts generated by FireEye Network Security, derive actionable information from those alerts, and apply the fundamentals of live analysis and investigation to investigate associated endpoints.

Hands-on activities span the entire analysis and live investigation process, beginning with a FireEye-generated alert, leading to discovery and analysis of the host for evidence of malware and other unwanted intrusion. Analysis will be performed using FireEye products and freely available tools.

For FireEye Endpoint Security customers, activities focus on investigation techniques using features such as the Triage Summary and Audit Viewer.

Learning Objectives

After completing this course, learners should be able to:

- Recognize current malware threats and trends
- Interpret alerts from FireEye Network and Endpoint Security products
- Locate and use critical information in FireEye alerts to assess a potential threat
- Define IOCs based on a FireEye alert and identify compromised hosts
- Describe methods of live analysis
- Create and request data acquisitions to conduct an investigation
- Define common characteristics of Windows processes and services
- Investigate a Redline® triage collection using a defined methodology
- Identify malicious activity hidden among common Windows events
- Validate and provide further context for alerts using Redline®

Who Should Attend

Network security professionals and incident responders who must use FireEye to detect, investigate, and prevent cyber threats.

Course Outline

Day 1

1. Threats and Malware Trends
   - Threat Landscape
   - Attack Motivations
   - Targeted Attack Lifecycle
   - Emerging Threat Actors
2. Initial Alerts
   - FireEye Endpoint Security Alerts
   - Triage with Triage Summary
   - FireEye Network Security Alerts
   - Mapping artifacts in an alert to host activity
3. MVX Alerts
   - FireEye alert types
   - Identifying forensic artifacts in the OS Change alert detail
   - Callbacks
   - SmartVision
   - Threat Assessment

Optional Content:

4. Custom Detection Rules
   - Yara Malware Framework
   - Snort Rules

Day 2

1. Using Audit Viewer and Redline
   - Access triage and data collections for hosts.
   - Navigate a triage collection or acquisition using Redline® or Audit Viewer
   - Apply tags and comments to a triage collection to identify key events
2. Windows Telemetry and Acquisitions
   - Live Forensic Overview
   - Windows Telemetry:
     - Memory Artifacts
     - System Information
     - Processes
     - File System
     - Configuration Files
     - Services
     - Scheduled Tasks
     - Logging
   - Acquiring Data

Optional Content:

3. Endpoint Security: Extended Capabilities
   - FireEye Market
   - Endpoint Security Modules*
   - HXTool*

Day 3

1. Investigation Methodology
   - Areas of Evidence
   - MITRE ATT&CK Framework
   - Mapping evidence to Attacker Activity

Optional Content

2. FireEye: Extended Capabilities
   - Open IOC Editor*
   - Endpoint Security REST API*

*Content only included for customers with FireEye Endpoint Security.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities.

For more details, or to view our full course catalog, please visit https://www.fireeye.com/services/training/

To learn more about FireEye, visit: **www.FireEye.com**

FireEye
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye
FireEye offers an innovative platform that eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.