EDUCATION SERVICES

Alert Analysis and Diagnostics with Email Security - Server

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

A working understanding of networking, email security and email support.

How to Register

Public sessions are listed at https://training-catalog.trellix.com. Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://training-catalog.trellix.com.

This workshop introduces a framework for administration of the Email Security - Server. The course includes checklists, case studies, lab challenges and guidance for transitioning difficult cases to the Trellix Support team.

The course also introduces the key components and detection engines, including detection of malicious files and URLs, email alerts and quarantine used for containment.

This course is designed primarily for administrators or analysts who will derive meaningful, actionable information from Trellix alerts to assess and triage threats to their environment.

This hands-on workshop will give attendees experience administering the appliance, diagnosing common issues, and interpreting detection.

Learning Objectives

After completing this course, learners should be able to:

- Properly deploy Trellix Email Security - Server in the network
- Perform initial configuration of the appliance based on system requirements and user preferences
- Administer the appliance
- Recognize current malware threats and trends
- Understand the threat detection and prevention capabilities of Trellix Email Security –Server
- Locate and use critical information in a Trellix alert to assess a potential threat
- Identify Indicators of Compromise (IOCs) in a Trellix alert and use them to identify compromised hosts
- Troubleshoot common issues with the Email Security - Server and use logs to determine status
- Escalate issues to Trellix Support for further assistance

Who Should Attend

This course is intended for Security professionals, incident responders, and email administrators responsible for the setup and management of Email Security – Server and who use Email Security – Server to detect, investigate, and prevent cyber threats.

Course Outline

1. Appliance Administration
2. Email Threats
3. Email Security - Server Detection Features
4. Initial Alerts
5. MVX Alerts
6. Diagnostics

Elective Content

The following additional lessons are available at no extra fee. These lessons are not relevant for all audiences, and are provided upon customer request, if time permits. Please coordinate with your Trellix instructor.

Custom Detection Rules

- YARA malware framework file signatures
- YARA on Trellix appliances
- YARA hexadecimal
- Regular expressions
- Conditions
- Snort rule processing
- Enabling Snort rules
- Creating a Snort rule

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.