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://trellix-training.netexam.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://trellix-training.netexam.com.

This is a two-day instructor-led class designed for analysts and email administrators.

Day 1 introduces Trellix Email Security – Server and its key components, including detection of malicious files and URLs, email alerts and quarantine used for containment. This course is designed primarily for analysts who will derive meaningful, actionable information from Trellix alerts to assess and triage threats to their environment.

Day 2 is a workshop that introduces a framework for administration and diagnostics for Trellix Email Security – Server. It includes checklists, case studies, lab challenges and guidance for transitioning difficult cases to the Trellix Support team. This workshop is experiential, hands-on and will give learners experience in administering an appliance and diagnosing common issues.

Learning Objectives

After completing this course, learners should be able to:

Alert Analysis Course

- Recognize current malware threats and trends
- Understand the threat detection and prevention capabilities of your Trellix Email Security – Server
- Locate and use critical information in a Trellix alert to assess a potential threat
- Examine OS and file changes in alert details to identify malware behaviors
- Identify indicators of compromise (IOCs) in a Trellix alert and use them to identify compromised hosts

Diagnostics Workshop

- Identify common issues and steps for resolution with Email Security - Server deployment
- Perform administration tasks on the Email Security – Server appliance
- Recognize underlying technology and protocols of SMTP email transfer
- Using logs, determine status of email transfer and analysis
- Know when to escalate issues and obtain further assistance from Trellix

Who Should Attend?

Security professionals, incident responders, and email administrators responsible for the set up and management of Email Security – Server and who use Email Security – Server to detect, investigate, and prevent cyber threats.

Course Outline

Day 1: Alert Analysis

1. Trellix Core Technology
   - Malware infection lifecycle
   - MVX engine
   - Appliance analysis phases
2. Threats and Malware Trends
   - Malware overview and definition
   - Motivations of malware
   - MITRE ATT&CK framework
   - Types of malware
3. Threat Management
   - Features and functions of Email Security – Server
   - Appliance web UI
   - Alert overview
4. OS Changes
   - APIs
   - File and folder actions
   - Code injection
   - Processes
   - Mutexes
   - Windows Registry events
   - Network access
   - User Account Access (UAC)
5. Malware Objects
   - Malware object alerts
   - BOT communication details
   - OS change details for malware objects
   - Malware object origin analysis

Alert Analysis 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

Day 2: Diagnostics Workshop

1. Common Trellix Administration and Diagnostics
   - Troubleshooting process
   - Basic troubleshooting
   - Best practice
   - Common issues:
     - Licensing
     - Admin
     - Operation
     - Notifications
     - Boot
     - Performance
     - Upgrade
2. Email Security – Server Diagnostics
   - Health check
   - Server logs
3. Hardware Diagnostics
   - Troubleshooting PSU and HDD issues
   - Universal LED
4. Virtual Email Security Server Diagnostics
   - Licensing
   - DTI configuration
5. Diagnostics of Email Protocols
   - The process of email and the Email Security – Server SMTP/ESMTP
     - POP3 / IMAP
     - MTA
     - DNS
     - MX
     - Postfix
     - Email Security Server Modes
     - Reporting
     - Email Logs
6. Administration and Diagnostics of Email Security Appliances
   - Processing interface
   - Domains
   - Next-hop
   - Receiving mail
   - Analysis
   - Mail delivery
   - Delay and latency
   - Understanding queues
7. Transition
   - Transition a case to Trellix Customer Support
   - Using the Trellix Customer Portal

Trellix

Visit Trellix.com to learn more.

About Trellix
Trellix is a global company redefining the future of cybersecurity. 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's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.