Trellix

EDUCATION SERVICES

Investigations with Email Security Cloud

Instructor-Led Training

Highlights

Duration

1 day

Prerequisites

Students taking this course should have 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 course provides an overview of Trellix Email Security – Cloud core functionality and covers administration procedures and alert analysis.

Hands-on activities include rule/policy creation, alert generation and the breakdown and analysis of information found in a Trellix email alert that is used in incident reporting.

Learning Objectives

After completing this course, learners should be able to:

- Describe how Email Security detects and protects against malware
- Demonstrate knowledge of the email analysis process
- Configure Email Security settings, policies and notifications
- Describe the various queues used for email management and processing
- Identify alerts correlated with Trellix Network Security with and without Trellix Central Management
- Find critical alert information on the dashboard
- Access and manage alerts and quarantined emails
- Examine OS and file changes in alert details to identify malware behaviors and triage alerts

Who Should Attend

This course is intended for analysts (primary) and administrators responsible for the setup and management of Email Security – Cloud and use Email Security – Cloud to detect, investigate, and prevent cyber threats.

Course Outline

1. **Threats and Malware Trends**
   - Malware overview and definition
   - Attack motivations
   - Targeted attack lifecycle
   - Types of malware
   - Emerging threat actors
2. **Email Threats and Detection Engines**
   - Email Security internal flow
   - Malicious email campaigns
   - Email threats
   - Email hunting
3. **Email Security Cloud Alerts**
   - Email alerts summary and message details
   - Quarantine
   - Malware objects
   - Email trace
   - Email executive summary report
4. **MVX Alerts**
   - APIs
   - File and folder actions
   - Code injection
   - Processes
   - Mutexes
   - Windows registry events
   - Network access
   - User account access (UAC)
5. **Email Security – Cloud Administration**
   - Setting up and testing a new domain
   - Policy configuration
   - Remediation
   - Custom rules and YARA
   - End user reporting and notifications
   - Email analysis status
   - Advanced configurations
6. **YARA with Email Security – Cloud**
   - YARA hexadecimal
   - Regular expressions
   - Conditions
   - YARA rule resources
   - YARA in Trellix Email Security – Cloud

Trellix

Visit Trellix.com to learn more.

092023-20