Securing Email with Cisco Email Security Appliance (SESA) v3.1

آنچه در این دوره خواهید آموخت :

دوره آموزشی Securing Email with Cisco Email Security Appliance (SESA) نسخه 3.1 به شما نشان می دهد که چگونه می توانید از Cisco Email Security Appliance استفاده کنید تا از سیستم های ایمیل خود در برابر فیشینگ، در معرض خطر قرار گرفتن ایمیل های تجاری و باج افزارها محافظت کنید و به ساده سازی امنیت ایمیل کمک کنید. این دوره عملی ، دانش و مهارت‌هایی را برای پیادسازی، عیب‌یابی و مدیریتCisco Email Security Appliance ، از جمله قابلیت‌های کلیدی مانند حفاظت پیشرفته بدافزار، مسدود کردن هرزنامه، محافظت از ضد ویروس، فیلتر شیوع، رمزگذاری، قرنطینه و داده‌ها در اختیار شما قرار می‌دهد و همه این موارد باعث پیشگیری از ضرر می شوند.

نحوه برگزاری دوره در سماتک :

- این دوره در سماتک ۳۰ ساعته برگزار خواهد شد .
- دارای لابراتوار خواهد بود .
- به صورت آنلاین برگزار خواهد شد .

پیش نیاز های دوره :

CCNA – MCSA

چه کسانی در این دوره میتوانند شرکت کنند :

- مهندسان امنیت
- ادمین های امنیت

- مهندسان شبکه
- ادمین های شبکه
- مدیران شبکه

اهداف دوره :

بعد از اتمام این دوره قابلیت انجام این فعالیت ها را خواهید داشت.

- Describe and administer the Cisco Email Security Appliance (ESA)
- Control sender and recipient domains
- Control spam with Talos SenderBase and anti-spam
- Use anti-virus and outbreak filters
- Use mail policies
- Use content filters
- Use message filters to enforce email policies
- Prevent data loss
- Perform LDAP queries
- Authenticate Simple Mail Transfer Protocol (SMTP) sessions
- Authenticate email
- Encrypt email
- Use system quarantines and delivery methods
- Perform centralized management using clusters
- Test and troubleshoot

سرفصل های دوره :

Module 1: Describing the Cisco Email Security Appliance

- Cisco Email Security Appliance Overview
- Technology Use Case
- Cisco Email Security Appliance Data Sheet
- SMTP Overview
- Email Pipeline Overview
- Installation Scenarios
- Initial Cisco Email Security Appliance Configuration
- Release Notes for AsyncOS 14.x

Module 2: Administering the Cisco Email Security Appliance

- Distributing Administrative Tasks
- System Administration
- Managing and Monitoring Using the Command Line Interface (CLI)
- Other Tasks in the GUI
- Advanced Network Configuration
- Using Email Security Monitor
- Tracking Messages
- Logging

Module 3 Controlling Sender and Recipient Domains

- Public and Private Listeners
- Configuring the Gateway to Receive Email
- Host Access Table Overview
- Recipient Access Table Overview
- Configuring Routing and Delivery Features

Module 4: Controlling Spam with Talos SenderBase and Anti-Spam

- SenderBase Overview
- Anti-Spam
- Managing Graymail
- Protecting Against Malicious or Undesirable URLs
- File Reputation Filtering and File Analysis
- Bounce Verification

Module 5: Using Anti-Virus and Outbreak Filters

- Anti-Virus Scanning Overview

- Sophos Anti-Virus Filtering
- McAfee Anti-Virus Filtering
- Configuring the Appliance to Scan for Viruses
- Outbreak Filters
- How the Outbreak Filters Feature Works
- Managing Outbreak Filters

Module 6: Using Mail Policies

- Email Security Manager Overview
- Mail Policies Overview
- Handling Incoming and Outgoing Messages Differently
- Matching Users to a Mail Policy
- Message Splintering
- Configuring Mail Policies

Module 7: Using Content Filters

- Content Filters Overview
- Content Filter Conditions
- Content Filter Actions
- Filter Messages Based on Content
- Text Resources Overview
- Using and Testing the Content Dictionaries Filter Rules
- Understanding Text Resources
- Text Resource Management
- Using Text Resources

Module 8: Using Message Filters to Enforce Email Policies

- Message Filters Overview
- Components of a Message Filter
- Message Filter Processing
- Message Filter Rules
- Message Filter Actions
- Attachment Scanning
- Examples of Attachment Scanning Message Filters
- Using the CLI to Manage Message Filters
- Message Filter Examples
- Configuring Scan Behavior

Module 9: Preventing Data Loss

- Overview of the Data Loss Prevention (DLP) Scanning Process
- Setting Up Data Loss Prevention
- Policies for Data Loss Prevention

- Message Actions
- Updating the DLP Engine and Content Matching Classifiers

Module 10: Using LDAP

- Overview of LDAP
- Working with LDAP
- Using LDAP Queries
- Authenticating End-Users of the Spam Quarantine
- Configuring External LDAP Authentication for Users
- Testing Servers and Queries
- Using LDAP for Directory Harvest Attack Prevention
- Spam Quarantine Alias Consolidation Queries
- Validating Recipients Using an SMTP Server

Module 11: SMTP Session Authentication

- Configuring AsyncOS for SMTP Authentication
- Authenticating SMTP Sessions Using Client Certificates
- Checking the Validity of a Client Certificate
- Authenticating User Using LDAP Directory
- Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
- Establishing a TLS Connection from the Appliance
- Updating a List of Revoked Certificates

Module 12: Email Authentication

- Email Authentication Overview
- Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing
- Verifying Incoming Messages Using DKIM
- Overview of Sender Policy Framework (SPF) and SIDF Verification
- Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
- Forged Email Detection

Module 13: Email Encryption

- Overview of Cisco Email Encryption
- Encrypting Messages
- Determining Which Messages to Encrypt
- Inserting Encryption Headers into Messages
- Encrypting Communication with Other Message Transfer Agents (MTAs)
- Working with Certificates
- Managing Lists of Certificate Authorities
- Enabling TLS on a Listener's Host Access Table (HAT)

- Enabling TLS and Certificate Verification on Delivery
- Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services

Module 14: Using System Quarantines and Delivery Methods

- Describing Quarantines
- Spam Quarantine
- Setting Up the Centralized Spam Quarantine
- Using Safelists and Blocklists to Control Email Delivery Based on Sender
- Configuring Spam Management Features for End Users
- Managing Messages in the Spam Quarantine
- Policy, Virus, and Outbreak Quarantines
- Managing Policy, Virus, and Outbreak Quarantines
- Working with Messages in Policy, Virus, or Outbreak Quarantines
- Delivery Methods

Module 15: Centralized Management Using Clusters

- Overview of Centralized Management Using Clusters
- Cluster Organization
- Creating and Joining a Cluster
- Managing Clusters
- Cluster Communication
- Loading a Configuration in Clustered Appliances
- Best Practices

Module 16: Testing and Troubleshooting

- Debugging Mail Flow Using Test Messages: Trace
- Using the Listener to Test the Appliance
- Troubleshooting the Network
- Troubleshooting the Listener
- Troubleshooting Email Delivery
- Troubleshooting Performance
- Web Interface Appearance and Rendering Issues
- Responding to Alerts
- Troubleshooting Hardware Issues
- Working with Technical Support

Module 17: References

- Model Specifications for Large Enterprises
- Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
- Cisco Email Security Appliance Model Specifications for Virtual Appliances
- Packages and Licenses