خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره CCNP SECURITY-SESA سیسکو
Securing | Email with Cisco Email Security Appliance v۳.۰

شرح مختصر

دوره آمادگی شرکت در آزمون Concentration exam مدرک ۳۰۰-۷۲۰ SESA جهت اخذ مدرک CCNP Security

مروری بر دوره

مروری بر دوره

دوره امنیت v۳.۰ (SESA) Securing Email with Cisco Email Security Appliance پیاده سازی و راه اندازی راهکار تامین امنیت ایمیل ها در مقابل حملات phishing ، مخاطرات ایمیل های تجاری(Business Email Compromise)، باج افزارها(Ransomwares) و ارتقاء مدیریت policyهای امنیتی ایمیل ها، دانش و مهارت لازم شیوه استقرار ، عیب یابی و مدیریت قابلیت های مهم راهکار امنیتی Cisco Email Security Appliance سیسکو شامل محافظت در مقابل بدافزارهای پیشرفته ، بلاک کردن اسپم ها ، تامین امنیت در مقابل ویروسها توسط آنتی ویروس ، outbreak filtering (حفاظت در مقابل تهدیدات جدید و حمله های ترکیبی) ، رمزگذاری ایمیل ها، قرنطینه کردن و جلوگیری از از بین رفتن داده ها (data loss prevention) را به متقاضیان آموزش می دهد.

این دوره ، آمادگی لازم جهت شرکت در آزمون Securing Email with Cisco Email Security Appliance (SESA ۳۰۰-۷۲۰) برای اخذ مدارک CCNP Security و Certified Specialist - Email Content Security certifications را برای فراگیران فراهم می نماید.

مزایای دوره

توانایی استقرار راهکار محافظت از ایمیل ها با قابلیت دسترسی بالا به منظور مقابله با تهدیدات دینامیک و پویا با تغییرات سریع در سازمان ها

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

کسب مهارت های شغلی پیشرفته در حوزه امنیت اینترپرایز در سازمان ها

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- توصیف و مدیریت راهکار تامین امنیت ایمیل سیسکو (ESA)
- کنترل دامنه های فرستنده و گیرنده های ایمیل
- کنترل اسپم ها از طریق سیستم اعتبارسنجی Talos SenderBaseسیسکو و ابزارهای مقابله با اسپم(anti-spam)
- شیوه استفاده از آنتی ویروس و outbreak filters
- استفاده از policy های مربوط به ارسال و دریافت ایمیل ها
- استفاده از فیلترینگ های محتوای ایمیل ها
- اجرای policyهای فیلترینگ پیام ها
- پیشگیری از از بین رفتن داده ها(data loss)
- اجرای LDAP queries
- تایید session های پروتکل (SMTP)Simple Mail Transfer Protocol
- تأیید اعتبار ایمیل های ارسالی و دریافتی
- رمزگذاری ایمیل ها
- استفاده از سیستم قرنطینه پیام ها و متدهای تحویل به کاربر نهایی
- مدیریت متمرکز کلاسترها
- تست و عیب یابی

سرفصل ها (حضوری)

سرفصل ها

Outline

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- 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
    - Centralizing Services on a Cisco Content Security Management Appliance (SMA)
    - Release Notes for AsyncOS ۱۱.x
- 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
- 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

- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- 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

Lab outline

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Verify and Test Cisco ESA Configuration
Perform Basic Administration
Advanced Malware in Attachments (Macro Detection)
Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
Protect Against Malicious or Undesirable URLs Inside Attachments
Intelligently Handle Unscannable Messages
Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
Integrate Cisco ESA with AMP Console
Prevent Threats with Anti-Virus Protection
Applying Content and Outbreak Filters
Configure Attachment Scanning
Configure Outbound Data Loss Prevention
Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
Domain Keys Identified Mail (DKIM)
Sender Policy Framework (SPF)
Forged Email Detection
Configure the Cisco SMA for Tracking and Reporting

مخاطبان دوره

مخاطبان دوره

- مهندسان امنیت
- ادمین های امنیت
- معماران امنیتی
- مهندسان اجرایی
- مهندسان شبکه

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ادمین های شبکه
- تکنسین های امنیتی یا شبکه
- مدیران شبکه
- طراحان سیستم
- یکپارچه سازان و پارتنرهای سیسکو

پیش نیاز ها

پیش نیازها

- دارا بودن دانش کامل از سرویس های TCP / IP شامل Domain Name System (DNS)، Secure HTTP ، Simple Network Management Protocol (SNMP)، FTP، Shell (SSH) و HTTPS
- تجربه عملی IP routing
- دارابودن یک یا چند مورد از مدارک زیر یا دانش معادل آن:
- اخذ یکی از مدارک سیسکو (CCENT certification یا مدارک در سطوح بالاتر)
- اخذ مدارک مرتبط با حوزه کاری شامل Global Information Assurance Certification (GIAC)، EC-Council، CompTIA Security+ ، (ISC)۲ و ISACA
- اخذ مدرک ۱ CCNA® Cisco Networking Academy (CCNA و ۲ CCNA)
- اخذ مدارک تخصصی سیستم عامل ویندوز: Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA) ، Microsoft Certified Solutions Expert (MCSE) و CompTIA (A+, Network+, Server+)
- استفاده از منابع آموزشی سیسکو در حوزه امنیت ایمیل که از لینک زیر قابل دسترس می باشد:
- https://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html