Symantec eLibrary course list - January, 2019

Advanced Threat Protection

Advanced Threat Protection 3.2: Differences
ATP 3.0: Analyzing Events and Incidents to Identify Indicators of Compromise
ATP 3.0: Endpoint Data Recorder and Advanced Searches
ATP 3.0: Introducing Advanced Threat Protection
ATP 3.0: Optimizing your ATP Environment
ATP 3.0: Recovering After an Incident
ATP 3.0: Remediating and Isolating Threats
ATP 3.0: Strengthening your Cybersecurity Framework
Advanced Threat Protection: Backup and Restore
Advanced Threat Protection: Installing and Managing SSL Certificates
Advanced Threat Protection: Network Overview
Advanced Threat Protection: Preparing your SEP 14 Environment for Incident Response
Advanced Threat Protection: SEP Connection Troubleshooting
Advanced Threat Protection: ServiceNow Integration
Advanced Threat Protection: Splunk Integration
Advanced Threat Protection: Troubleshooting
Advanced Threat Protection: Updating
ATP 2.x: Analyzing Events and Incidents to Identify Indicators of Compromise
ATP 2.x: Course Introduction: Attack at Solusell
ATP 2.x: Introducing Advanced Threat Protection
ATP 2.x: Optimizing your ATP Environment
ATP 2.x: Preparing your Endpoint Environment for Incident Response
ATP 2.x: Recovering After an Incident
ATP 2.x: Remediating and Isolating Threats
ATP 2.x: Strengthening your Cybersecurity Framework

BlueTouch Online Technical Webcasts

BTO Technical Webcast Series

CAS S400

Introduction to CAS S400

CloudSOC

Introduction to CloudSOC **NEW!**
CloudSOC R2.1.1: Differences (Sep 2018)

Cloud Web Security Services

Introduction to Web Isolation **NEW!**
WSS: SD Cloud Connector Solution Demo
WSS: Web Isolation Demo
WSS: Cloud Firewall
WSS: Traffic Redirection
WSS: SD Cloud Connector Solution
WSS: Web Isolation
Cloud WSS: Authentication
Cloud WSS: CASB CloudSOC Integration
Cloud WSS: Course Overview

Cloud WSS: DLP Integration
Cloud WSS: Explicit Proxy Access Method
Cloud WSS: Firewall/VPN Access Method Module
Cloud WSS: General Administration
Cloud WSS: Malware Analysis
Cloud WSS: Mobile Device Access Method
Cloud WSS: Policy
Cloud WSS: Proxy Forwarding Access Method
Cloud WSS: Remote Client Access Method
Cloud WSS: Reports
Cloud WSS: Selecting a Solution
Cloud WSS: SSL
Cloud WSS: Web Security Service Overview

Cloud Workload Protection

Introduction to Cloud Workload Protection **NEW!**

Content Analysis

Content Analysis 2.2 Administration

Control Compliance Suite

Introduction to Control Compliance Suite **NEW!**
Control Compliance Suite 11.0 Differences
Control Compliance Suite 11.x Administration
Control Compliance Suite 11.x Assessment Manager
Control Compliance Suite 11.x Policy Manager
Control Compliance Suite 11.x Risk Manager
Control Compliance Suite Advanced Check Writing: Standards Overview
Control Compliance Suite Vendor Risk Manager 11.0.2
CCS 11.x: Asset Schema Extensions
CCS 11.x: Reports and Dashboards around KPIs

Cyber Security Services

CSS Admin R1: Achieving 24x7 Global Threat Monitoring
CSS Admin R1: Cyber Security Services Overview
CSS Admin R1: DeepSight Datafeeds and Integration
CSS Admin R1: DeepSight Portal Demo
CSS Admin R1: Impact of Security Intelligence
CSS Admin R1: Introduction to the DeepSight API
CSS Admin R1: Managed Security Services Overview
CSS Admin R1: Managed Security Services Review
CSS Admin R1: MSS Platform and Architecture Overview
CSS Admin R1: Protecting Against Advanced Threats by Leveraging Threat Intelligence in MSS
CSS Admin R1: Provide for Timely Alerts and Custom Reporting
CSS Admin R1: Providing Relevant and Efficient Intelligence Using a Sophisticated Filter
CSS Admin R1: Security Monitoring and Managed IDS
CSS Admin R1: Timely Validation of Security Incidents

Data Loss Prevention

DLP 15: Installing Oracle and the Symantec DLP Enforce Server

DLP 15: Installing Symantec Data Loss Prevention Detection Servers
DLP 15: Installing a Symantec Data Loss Prevention OCR Server
DLP 15: Installing the Symantec Data Loss Prevention Endpoint Agent
DLP 15: Preparing to Install Symantec Data Loss Prevention
DLP 15: Symantec Data Loss Prevention Overview
DLP 15: Upgrading Symantec Data Loss Prevention
Data Loss Prevention 15.0: Differences
Data Loss Prevention 14.6: Differences
Data Loss Prevention 14.5: Differences
DLP 14.6 Install and Deploy: Differences Between 14.0 and 14.6
DLP 14.5: Data Loss Landscape
DLP 14.5: Educating Users to Adopt Data Protection Practices
DLP 14.5: Enhancing Data Loss Prevention through Third-Party Integrations
DLP 14.5: Identifying and Describing Confidential Data
DLP 14.5: Locating Confidential Data Stored on Premises and in the Cloud
DLP 14.5: Overview of Symantec Data Loss Prevention
DLP 14.5: Preventing Unauthorized Exposure of Confidential Data
DLP 14.5: Remediating Data Loss Incidents and Tracking Risk Reduction
DLP 14.5: Understanding How Confidential Data Is Being Used
Data Loss Prevention 14.0: Administration
Data Loss Prevention 14.0: Differences
Data Loss Prevention 12.5: Administration
Data Loss Prevention 12.0 Administration Training

Data Center Security

Introduction to Data Center Security **NEW!**
Data Center Security Server Advanced 6.7 Diagnostics and Troubleshooting
DCS:SA 6.7: Advanced Prevention
DCS:SA 6.7: Agent Management and Troubleshooting
DCS:SA 6.7: Configuring Agents
DCS:SA 6.7: Detection Policies
DCS:SA 6.7: Event Management
DCS:SA 6.7: Installation and Deployment
DCS:SA 6.7: Introduction to Security Risks
DCS:SA 6.7: Policy Overview
DCS:SA 6.7: SDCS: Server Advanced Overview
DCS:SA 6.7: System Management
DCS:SA 6.7: UNIX and Legacy Prevention Policies
DCS:SA 6.7: Windows Prevention Policies
Data Center Security: Server 6.0: Administration
Data Center Security: Server 6.5: Administration
Data Center Security: Server Advanced 6.0: Administration

Deepsight

DeepSight Technical Education Modules

Deployment Solution

DS 8.1: Building an Initial Reference Image (Advanced)
DS 8.1: Building an Initial Reference Image (Basic)

DS 8.1: Execution and Maintenance of a Migration Plan (Advanced)
DS 8.1: Execution and Maintenance of a Migration Plan (Basic)
DS 8.1: Ghost Explorer (Advanced)
DS 8.1: Ghost Explorer (Basic)
DS 8.1: Imaging MacOS (Advanced)
DS 8.1: Imaging MacOS (Basic)
DS 8.1: Overview of Endpoint Lifecycle Management (Advanced)
DS 8.1: Overview of Endpoint Lifecycle Management (Basic)
DS 8.1: Planning and Preparing for a Hardware / OS Migration (Advanced)
DS 8.1: Planning and Preparing for a Hardware / OS Migration (Basic)
DS 8.1: User Data Migration (Advanced)
DS 8.1: User Data Migration (Basic)

Diagnostic and Troubleshooting Methodology

Symantec Diagnostic and Troubleshooting Methodology

Email Security

Introduction to Email Security.cloud **NEW!**
ES.cloud R1: Help Meet Compliance and Privacy Requirements
ES.cloud R1: Overview of Email Security.cloud
ES.cloud R1: Prevent Accidental and Deliberate Data Breaches
ES.cloud R1: Protect Inboxes from Malware and Spam
ES.cloud R1: Protect from Advanced Persistent Threats
Email Security Service and Web Security Service: Administration
Email Security.cloud Supporting DMARC Validation
Email Security.cloud Technical Education Courses

Encryption and Encryption Management Server

Introduction to Symantec Encryption **NEW!**
Encryption Management Server 3.4.1 Diagnostics and Troubleshooting
SEMS 3.3: Administrative Keys
SEMS 3.3: Clustering
SEMS 3.3: Configuring Client Enrollment
SEMS 3.3: Configuring General Policy Settings
SEMS 3.3: Configuring Symantec Drive Encryption
SEMS 3.3: Configuring Symantec File Share Encryption
SEMS 3.3: Consumers and Groups
SEMS 3.3: Course Introduction
SEMS 3.3: Cryptography Essentials
SEMS 3.3: Installing Symantec Encryption Desktop
SEMS 3.3: Installing Symantec Encryption Management Server
SEMS 3.3: Key Not Found
SEMS 3.3: Keys
SEMS 3.3: Mail Policy
SEMS 3.3: Monitoring and Reporting
SEMS 3.3: Other Symantec Encryption Desktop Features
SEMS 3.3: Preparing Symantec Encryption Management Server for Symantec Desktop Clients
SEMS 3.3: Server Messaging
SEMS 3.3: Symantec Drive Encryption Management Recovery

SEMS 3.3: Symantec Encryption Desktop Messaging
SEMS 3.3: Symantec Encryption Introduction
SEMS 3.3: Web Email Protection
Endpoint Encryption 11.x Technical Education Course
PGP Universal Server 3.2 and PGP Desktop 10.2: Administration

Endpoint Detection and Response

Introduction to Endpoint Detection and Response **NEW!**
Endpoint Detection and Response 4.0 Differences

Endpoint Protection

Introduction to Endpoint Application Isolation and Control **NEW!**
Introduction to Endpoint Protection **NEW!**
Introduction to Endpoint Protection Cloud **NEW!**
Introduction to Endpoint Protection Mobile **NEW!**
Endpoint Protection 15.0: Differences (Nov 2018)
Endpoint Protection Cloud R2.0.1: Differences
SEP Hardening App Control: Differences
SEP Hardening App Center: Differences
What's New in Symantec Endpoint Protection 14.2
What's New in Symantec Endpoint Protection 14.1
What's New in Symantec Endpoint Protection 14
Endpoint Protection 14: Differences
Migrating to Symantec Endpoint Protection 14
SEP 14: Client Communication Issues
SEP 14: Content Distribution Issues
SEP 14: Controlling Endpoint Integrity and Compliance
SEP 14: Discovering Endpoint Client Implementation Methods and Strategies
SEP 14: Enforcing Adaptive Security Posture
SEP 14: Enforcing Content Updates on Endpoints using the Best Method
SEP 14: Extending the SEP Infrastructure
SEP 14: Installation and Migration Issues
SEP 14: Monitoring and Managing Endpoints
SEP 14: Performance Issues
SEP 14: Preparing and Delivering a Successful SEP Implementation
SEP 14: Responding to a Security Incident
SEP 14: Securing Endpoints Against File-Based Threats
SEP 14: Securing Endpoints Against Network-Based Attacks
SEP 14: Troubleshooting Techniques and Tools
SEP 14: Troubleshooting the Console
SEP Mobile Self Service Training
Endpoint Protection 12.1.5 Technical Education Course
Endpoint Protection 12.1.6 Differences
Endpoint Protection 12.x: Administration
Endpoint Protection 12.x: Maintain and Troubleshoot

Ghost Solution Suite

Introduction to Ghost Solution Suite **NEW!**
Ghost Solution Suite 3.0: Administration

Information Centric Analytics (ICA)

Introduction to Information Centric Security **NEW!**
ICE R1: Architecture and Implementation **NEW!**
ICT 15.1: Architecture and Implementation **NEW!**
ICA 6.5: Architecture and Implementation
ICA 6.5: Introduction
ICA 6.5: Manage and Administer
Information Centric Encryption R1.0: Introduction
Information Centric Security Module 15.1: Introduction
Information Centric Tagging 15.1: Introduction
Information Centric Analytics (ICA): Dashboards
Information Centric Analytics 6.5: Differences

IT Management Suite

Introduction to IT Management Suite **NEW!**
IT Management Suite 8.5: Differences
IT Management Suite 8.1 Diagnostics and Troubleshooting
ITMS 8.1: Business Analytics & Reporting
ITMS 8.1: Discovering Resources within the Environment
ITMS 8.1: Effective Software Management
ITMS 8.1: Identifying Relationships Between Assets
ITMS 8.1: Improved Security Through Automated Patch Management
ITMS 8.1: Managing the Contract and Procurement Process
ITMS 8.1: Reducing Desk-side Visits with Remote Support
ITMS 8.1: Understanding Software License Compliance
ITMS 8.0 Webinar: Exploring Symantec ITMS 8.0 SCS Exam (250-423) Objectives and Use Cases
ITMS 8.0: Business Analytics and Reporting
ITMS 8.0: Discovering Resources
ITMS 8.0: Effective Software Management
ITMS 8.0: Identifying Relationships between Assets
ITMS 8.0: Improved Security Through Automated Patch Management
ITMS 8.0: Managing the Contract and Procurement Process
ITMS 8.0: Reducing Desk-side Visits Through Remote Support
ITMS 8.0: Understanding Software License Compliance
IT Management Suite 7.5: Administration
ITMS Fundamentals: Basic Architecture Overview
ITMS Fundamentals: Installing and Configuring
ITMS Fundamentals: Managing Policies, Jobs, and Tasks
ITMS Fundamentals: Managing Targets and Filters
ITMS Fundamentals: Organizational Views and Groups
ITMS Fundamentals: Securely Managing Remote Computers
ITMS Fundamentals: SMP Overview
Client Management Suite 7.6: Administration
Asset Management Suite 7.5: Administration
ServiceDesk 7.5: Administration
Managing Software Licenses with Symantec IT Management Suite 7.5
Workflow Solution 7.6: Administration

Workspace Streaming 7.5
Workspace Virtualization 7.5

Managed Security Services

Managed Security Services Portal FAQ

Management Center

Introduction to Management Center and Reporter **NEW!**
Management Center Essentials
Migration from BlueCoat Director to Symantec Management Center

Messaging Gateway

Introduction to Messaging Gateway **NEW!**
SMG 10.6: Adaptive Reputation Management
SMG 10.6: Anti-Malware
SMG 10.6: Anti-Spam
SMG 10.6: Content Filtering
SMG 10.6: Control Center
SMG 10.6: Installation
SMG 10.6: Introduction
SMG 10.6: Introduction to Network Prevent for Email and Content Analysis
SMG 10.6: Users and Host Configuration
Messaging Gateway 10.0: Administration
Messaging Gateway Differences

Mail Threat Defense

MTD Configuring Email Security Policies

PacketShaper

Introduction to PacketShaper
PacketShaper 11.9.1: Classifying Traffic
PacketShaper 11.9.1: Fault Tolerance, Deployments and Platform Health
PacketShaper 11.9.1: Initial Configuration and Understanding Applications
PacketShaper 11.9.1: Management and Identifying Network Issues
PacketShaper 11.9.1: Prioritizing Traffic in the Network
PacketShaper 11.9.1: Responding to Network Issues
PacketShaper 11.9.1: Welcome to PacketShaper
PacketShaper Essentials 11.9.1

Protection Engine

Protection Engine 7.5 Administration and Deployment

ProxySG

Introduction to ProxySG Secure Web Gateway **NEW!**
ProxySG 6.6 Diagnostics and Troubleshooting
ProxySG: Access Logging on the ProxySG
ProxySG: Advanced Authentication Concepts on the ProxySG
ProxySG: Advanced Encrypted Traffic Management on the ProxySG
ProxySG: Authenticating Users on the ProxySG
ProxySG: Exceptions and Notifications on the ProxySG
ProxySG: Hypertext Transfer Protocol
ProxySG: Intro to Content Filtering

ProxySG: Intro to CPL
ProxySG: Intro to Encrypted Traffic Management
ProxySG: Intro to ProxySG S200
ProxySG: Intro to ProxySG S500
ProxySG: Introduction to Content Policy Language (CPL)
ProxySG: Introduction to Encrypted Traffic Management on the ProxySG
ProxySG: Introduction to HTTPS
ProxySG: Introduction to PSG S400
ProxySG: Introduction to the ProxySG Management Console
ProxySG: Introduction to the Symantec Blue Coat ProxySG Secure Web Gateway
ProxySG: Introduction to the Visual Policy Manager
ProxySG: Introduction to the Visual Policy Manager (Pre)
ProxySG: Managing Downloads on the ProxySG
ProxySG: Policy Tracing on the ProxySG
ProxySG: ProxyAV Essentials
ProxySG: ProxySG Integration
ProxySG: PSG Performance Monitoring
ProxySG: SG Migration 510, 810, 900, 9000
ProxySG: SGOS Architecture
ProxySG: SGOS Architecture Fundamentals
ProxySG: Symantec Blue Coat ProxySG Initial Configuration
ProxySG: Symantec Blue Coat ProxySG Proxy Services
ProxySG: Symantec Blue Coat ProxySG Security Deployment Options
ProxySG: System Diagnostics on the ProxySG
ProxySG: Troubleshooting Policies with Policy Tracing
ProxySG: Using SNMP
ProxySG: Using Stunnels and Encrypted Tap on the ProxySG
ProxySG: WebFilter, WebPulse, and the Global Intelligence Network

Reporter

Reporter Essentials

SSL Visibility Appliance

Introduction to SSLV
SSL Visibility 4.4: Differences
SSLV 4.3: Deploying the SSLV
SSLV 4.3: Expose Encrypted Inbound Traffic
SSLV 4.3: Expose Encrypted Outbound Traffic
SSLV 4.3: Expose Encrypted Threats for Forensic Analysis While Maintaining Compliance Regulations
SSLV 4.3: Introduction to Encrypted Traffic Management
SSLV 4.3: Introduction to Encrypted Traffic Management with Symantec SSLV
SSLV 4.3: Migrate and Upgrade SSLV
SSLV 4.3: Offloading SSL Decryption for ProxySG Efficiency
SSLV 4.3: Simplify Management of Multiple SSLV Appliances with Management Center
SSLV 4.3 Administration (Basic)
SSL Visibility 4.x Deployment
SSLV 4.x Differences
SSLV Essentials 3.0.1: Course Opening

SSLV Essentials 3.0.1: Deployment Modes
SSLV Essentials 3.0.1: Integration
SSLV Essentials 3.0.1: Introduction to the SSL Visibility Appliance
SSLV Essentials 3.0.1: Monitoring and Troubleshooting
SSLV Essentials 3.0.1: PKI Management
SSLV Essentials 3.0.1: Platform Management
SSLV Essentials 3.0.1: Policies
SSLV Essentials 3.0.1: SSL Visibility Appliance Initial Configuration
SSLV Essentials 3.0.1: Working with SSL

Validation and Identity Protection

Introduction to Validation and ID Protection **NEW!**
VIP Diagnostics and Troubleshooting R1
IAS Intro R1: Introduction to Identity and Authentication
IAS Intro R1: Introduction to Symantec Identity and Authentication Services
VIP Service R1: Improve Web Application Security with Multi-Factor Authentication
VIP Service R1: Plan and Implement the Symantec VIP Service
VIP Service R1: Review of the Symantec VIP Service
VIP Service R1: Secure VPN and Remote Access Using RADIUS and VIP Strong Authentication
VIP Service R1: Select the Appropriate VIP Strong Authentication Method
VIPAM R1: Control Access to Web Applications Based Upon Organization Requirements
VIPAM R1: Enable Multi-factor Authentication Based Upon Business Requirements
VIPAM R1: Enhance Security and Improve User Experience Through Single Sign-on
VIPAM R1: Introduction to Symantec VIP Access Manager
Validation and ID Protection Services VIP 9.X
VIP General Modules

X-Series

X-Series: Flow Processing
X-Series: High Availability
X-Series: Installation and Configuration Fundamental
X-Series: Monitoring & Troubleshooting
X-Series: Platform Hardware Overview
X-Series: System Maintenance
X-Series: System Management