Cyber Security Services Administration R1

COURSE DESCRIPTION

The Cyber Security Services Administration R1 course will provide a technical deep dive and hands on experience with Symantec's Cyber Security Services.

Delivery Method
Instructor Led Training and Virtual Academy

Duration
3 days

Course Objectives
By the completion of this course, you will be able to:

- Have a solid understanding of the current cyber security market conditions and the need for Cyber Security Services
- Identify the components of the technical architecture of Symantec's CSS Services and understand how it integrates with the customer's environment
- Understand the Business Objectives achieved by CSS Services
- Identify the competitive differentiators of Symantec's CSS Services

Who Should Attend
This course is for partners and Symantec staff that are charged with the configuration, integration, and day-to-day management of Managed Security Services and Deepsight Intelligence.

Prerequisites
It is recommended that the student has 1-3 months experience working with the Managed Security Services SOC and Log Collection Platform plus Symantec Managed Security Services Portals (Both DeepSight Intelligence portal and MSS Portal), including performing integration projects with DeepSight Application Programming Interface (APIs).

Hands-On
This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Lesson 1: Overview of Cyber Security Services

- Provides an overview of Symantec's Cyber Security Services product strategy and where CSS fits into this strategy
- Introduces the Symantec Cyber Security Services Administration Course
- Reviewing the business objectives that correspond with the mission of CSS

Lesson 2: Managed Security Services Overview

- Introduction to Symantec Managed Security Services
- Overview of the following business objectives and how CSS can customers meet those goals:
    - 24x7 Global Threat Monitoring by trained security analysts
    - Timely validation and remediation of security incidents
    - Protect against evolving complexity and advanced threats in cybersecurity
- Managed Security Services Portal login

Lesson 3: Achieving 24x7 Global Threat Monitoring

- Discuss the Managed Security Services Architecture and how it facilitates 24x7 global threat monitoring for customers
- Managed Security Services portal overview

Lesson 4: MSS Platform and Architecture Overview

- Discuss leveraging existing SIEMs in the customer's environment
- Introduce the MSS Log Collection Platform (LCP) architecture and transport methods
- Examine how CSS provides for log aggregation with Symantec Event Agent and Collectors
- Implementing a solution design onsite
- Provide a comprehensive overview of the support of various device types and log collection categories

Lesson 5: Timely Validation and Remediation of Security Incidents

- What is the SOC Technology Platform?
- Provide for timely log collection and storage to meet business requirements
- Discuss how the STP automated validation process decreases the time required for incident validation
- Examine how MSS facilitates the timely identification, analysis, and notification of security incidents

Lesson 6: Protecting Against Advanced Threats by Leveraging Threat Intelligence in MSS

- Discuss the evolution of threats and how to solve the advanced threat problem
- Introduce how to leverage the capabilities of ATP with MSS

Lesson 7: Security Monitoring and Managed IDS

- Discuss the MSS security monitoring solution
- Introduce the MSS Managed IDS solution

Lesson 8: Managed Security Services Review

- Review the Symantec Managed Security Services architecture, 24x7 Global Threat Monitoring by trained security analysts, timely validation and remediation of security incidents, how to protect against evolving complexity and advanced threats in cybersecurity, and Security Monitoring and Managed IDS Solutions

Lesson 9: The Impact of Security Intelligence

- Discuss the need for and the nature of Security Intelligence in the Enterprise
- Examine how Security Intelligence is of use across the Enterprise, and how Security Intelligence can function as a proactive solution.
- Cover the basics of Symantec DeepSight, to include where the intelligence comes from for DeepSight
- Detail the functions of the MATI team

Lesson 10: The DeepSight Portal Demo

- Cover the basic functions and features of the DeepSight Intelligence Portal
- Provide a walkthrough of each of the Portal's major features

Lesson 11: Providing Relevant and Efficient Intelligence Using a Sophisticated Filter

- Discuss an overview of the value of Technology lists in providing relevant, low-noise intelligence
- Cover Technology List purpose and theory.
- Examines the core criteria of a Technology List and strategies for List management
- Provide a walkthrough of Technology List creation

Lesson 12: Provide for Timely Alerts and Custom Reporting

- Cover all basic requirements for creating new and custom Alerts in DeepSight, and includes a detailed walkthrough of the process of Alert creation
- Examines controlling Intelligence delivery through the use of Alert Delivery Methods
- Provide an overview of Custom Reports in DeepSight and a walkthrough of Custom Report Creation.

Lesson 13: DeepSight Datafeeds and Integration

- Describe extending Security Intelligence usability by integrating DeepSight Intelligence with in-place software products.
- Provide an overview of the Datafeed types, and a walkthrough of using the Datafeed Client Tool as a means of describing functionality of DeepSight Datafeeds.

Lesson 14: Introduction to the DeepSight API

- Cover an introduction to the new DeepSight API feature, together with the API's general characteristics, usability, and need in an enterprise
- Discuss the entitlements and use restrictions of the DeepSight API