# Cyber Security Services Administration

## COURSE DESCRIPTION

The Cyber Security Services Administration 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**
2 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**

- Current Threat Landscape and the need for CSS
- Symantec Information Protection Strategy
- Introduction to Cyber Security Services

Lesson 2: **Managed Security Services Overview**

- Introduction to Symantec Managed Security Services
- 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 Overview

Lesson 3: **Achieving 24x7 Global Threat Monitoring**

- Managed Security Services Architecture
- 24x7 Global Threat Monitoring by trained security analysts
- Managed Security Services Portal Overview

Lesson 4: **MSS Platform and Architecture Overview**

- Leveraging Existing SIEMs
- MSS Log Collection Platform (LCP) Architecture and Transport Methods
- Providing for Log Aggregation with Symantec Event Agent and Collectors
- Implementing a Solution Design Onsite
- Comprehensive Support of Device Types and Log Collection Categories

Lesson 5: **Timely Validation of Security Incidents**

- What is the SOC Technology Platform?
- Provide for Timely Log Collection and Storage to meet Business Requirements
- STP Automated Validation Process Decreases Time for Incident Validation
- Timely Identification, Analysis, and Notification of Security Incidents

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

- The Evolution of Threats
- Solving the Advanced Threat Problem
- Leveraging the capabilities of ATP with MSS

Lesson 7: **Security Monitoring and Managed IDS**

- MSS Security Monitoring Solution
- MSS Managed IDS Solution

Lesson 8: **Managed Security Services Review**

- Review of Symantec Managed Security Services Architecture
- 24x7 Global Threat Monitoring by trained security analysts
- Timely validation and remediation of security incidents
- Protect Against Evolving Complexity and Advanced Threats in Cybersecurity
- Security Monitoring and Managed IDS Solutions

Lesson 9: **Impact of Security Intelligence**

- The Evolving Threat Landscape
- On the Nature of Security Intelligence
- The Value of Security Intelligence Across the Enterprise
- Intelligence as a Proactive Solution

Lesson 10: **Symantec Deepsight Intelligence Overview**

- Introduction to the Global Intelligence Network
- Sources of Information in the GIN
- Managed Adversary Threat Intelligence
- Additional Sources

Lesson 11: **Provide for Context Aware Threat Intelligence Portal with Delegate Authority based on User and Group Roles**

- DeepSight Portal Access and Layout
- DeepSight Portal Contents and Navigation
- Licensing and Portal Levels
- Configuring the Organization Profile and Licenses
- Account Management, Users, Roles, and Groups

Lesson 12: **Provide for More Targeted Intelligence and Minimizing Noise by Utilizing Technology Lists**

- Technology List purpose and theory
- Creating a Technology List
- Publishing and Sharing Technology Lists
- Uploading Lists

Lesson 13: **Provide for Timely Alerts and Access to Custom Reporting Based on Customer Policies and Practices**

- Alerts and Monitors Overview
- Creating an Alert
- Alert Delivery Methods
- Mining DeepSight for Custom Reporting
- Scheduled Reports and Report Delivery

Lesson 14: **Leveraging Threat Intelligence with Existing SIEM Investment in Support of Customer Policies and Practices**

- Datafeed Types and Value
- The Security Risk Datafeed
- The Vulnerabilty Datafeed
- Basic and Advanced IP Reputation Datafeeds
- Basic and Advanced URL/Domain Reputation Datafeeds
- Methods of Integration and Tools
- Datafeed Integration with ArcSight
- Datafeed Integration with SPLUNK
- Datafeed Integration with Risk Fabric

Lesson 15: **Integrating DeepSight Threat Intelligence into Custom Applications with the DeepSight API**

- A New Access Method
- DeepSight API Details
- DeepSight API Entitlements

Lesson 16: **Deepsight Intelligence Review**