Symantec Advanced Threat Protection 3.*x*: Incident Response

(Symantec Advanced Threat Protection 3.0)

COURSE DESCRIPTION

The *Symantec Advanced Threat Protection 3.x: Incident Response* course is designed for the IT security professional in a Security Operations position. This class covers how to detect, investigate, remediate, and recover from an incident using Advanced Threat Protection.

Delivery Method
Instructor-led training (ILT)

Duration
Two days

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

- Describe Advanced Threat Protection products, components, dependencies, and system hierarchy.
- Configure Advanced Threat Protection to prepare your environment for responding to incidents.
- Detect events and incidents in the ATP Manager and search for indicators of compromise (IOC).
- Remediate threats by isolating breached endpoints and blacklisting suspicious files and addresses.
- Recover from an outbreak using Symantec best practices and update your Cybersecurity plan.

Who Should Attend
This course is for anyone who is charged with the configuration, day-to-day management, and incident response using Advanced Threat Protection and Symantec Endpoint Protection in a variety of network environments.

Prerequisites
You must have a working knowledge of Symantec Endpoint Protection, Windows operating systems, endpoint and network security concepts.

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

Introduction

- Course overview
- The classroom lab environment

Strengthening your Cybersecurity Framework

- Advanced Persistent Threat (APTs) review
- Stages of an Attack
- Preventative steps as defined by STAR/Security Response
- Cybersecurity core functions

Introducing Advanced Threat Protection

- Introduction
- Shared technologies
- Examining the ATP architecture and sizing guide
- Becoming familiar with Symantec ATP
- Creating ATP accounts
- Describing views and data analysis per incident response role

Optimizing your ATP Environment

- Configuring Global Settings
- Configuring ATP: Email correlation
- Configuring ATP: Roaming correlation
- Configuring Symantec Endpoint Protection correlation
- Configuring ATP and SEP Detection and Response configuration

Analyzing Events and Incidents to Identify Indicators of Compromise

- ATP detection overview
- Viewing events that occur in your environment
- Analyzing Incidents
- Analyzing the dashboard
- Searching for indicators of compromise (IOC)

Preparing your Endpoint Environment for Incident Response

- Configure Host Integrity and Quarantine Firewall policies for ATP's Isolate and Rejoin feature
- Configure the Virus and Spyware policy for High Security mode

Remediating and Isolating threats

- Isolating breached endpoints
- Remediating malicious files and reducing false positives
- Responding to threats by blacklisting suspicious addresses
- Examining case studies

Recovering After an Incident

- Recovery best practices
- Gathering information for reporting
- Creating a Lessons Learned report