Symantec Advanced Threat Protection 2.*x*: Incident Response

(Symantec Advanced Threat Protection 2.0)

COURSE DESCRIPTION

The *Symantec Advanced Threat Protection 2.x: Incident Response* course is designed for the network, IT security, and systems administration professional in a Security Operations position. This class covers how to detect, 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 Symantec Endpoint Protection endpoints 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 suspicious activity.
- Recover from an outbreak using Symantec best practices and update your Cybersecurity plan.

Who Should Attend

This course is for network managers, resellers, systems administrators, client security administrators, systems professionals, and consultants who are charged with the configuration, and day-to-day management of Advanced Threat Protection and Symantec Endpoint Protection in a variety of network environments.

Prerequisites

You must have working knowledge of advanced computer terminology, including TCP/IP networking terms and Internet terms, and an administrator-level knowledge of Microsoft Windows operating systems.

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

How ATP Fits Inside The Cybersecurity Framework

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

Introducing ATP

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

Configuring Global Settings and SEPM Integration

- Configuring Global Settings
- Configuring ATP:Email correlation
- Configuring Symantec Endpoint Protection correlation
- Configuring ATP and SEP detection and response

Working with Events and Incidents

- ATP detection overview
- Viewing events
- Analyzing Incidents
- Analyzing the dashboard
- Searching for indicators of compromise (IOC)

Preparing your SEP Endpoint Environment for Response

- Configure Host Integrity and Quarantine Firewall policies for ATP quarantine
- Configuring the SEP endpoints to communicate with ATP (Insight)
- Operational and Alert Mode

Acting on 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