Securing Cisco Networks with Open Source Snort (CPLL-SSFSNORT)

Duration: 180 days

The Securing Cisco Networks with Open Source Snort (SSFSNORT) training shows you how to deploy a network intrusion detection system based on Snort. Through a combination of expert instruction and hands-on practice, you will learn how to install, configure, operate, and manage a Snort system. You will also explore rules writing with an overview of basic options, advanced rules writing, how to configure PulledPork, and how to use OpenAppID to provide protection of your network from malware. You will learn techniques of tuning and performance monitoring, traffic flow through Snort rules, and more.
This training also earns you 32 Continuing Education (CE) credits toward recertification.

Skills You'll Learn

- Learn how to implement Snort, an open-source, rule-based, intrusion detection and prevention system
- Examine basic and advanced rules writing
- Discover how to protect your network from malware using PulledPork and OpenAppID
- Gain leading-edge skills for high-demand responsibilities focused on security

Learning Path Objectives

- Describe Snort technology and identify the resources available for maintaining a Snort deployment
- Install and configure a Snort deployment
- Configure the command-line options for starting a Snort as a sniffer, a logger, and an intrusion detector, and create a script to start Snort automatically
- Identify and configure available Snort intrusion detection outputs
- Describe rule sources, updates, and utilities for managing rules and updates
- Detail the components of the snort.lua file and determine how to configure it for your deployment
- Configure Snort for inline operation using the inline-only features
- Configure rules for Snort using basic rule syntax
- Describe how traffic flows through Snort and how to optimize rules for better performance
- Configure advanced-rule options for Snort rules
- Configure OpenAppID features and functionality
- Tune Snort for efficient operation and profile system performance