Introduction to Stealthwatch Implementation

COURSE OVERVIEW:

This 2-day Stealthwatch training course is designed to take a user through the initial introduction of flow in a network and introduces how Stealthwatch uses flows. Our online Stealthwatch training course then introduces users to the Stealthwatch product and its functionality, enabling you to proactively and reactively maintain network health. This course also specifically addresses the SMC client interface and SMC Web App Interface.

Basic Windows navigation skills, CCNA (or equivalent knowledge), and familiarity with standard network security concepts are all firm prerequisites in order to excel in this course. To get more details about Cisco Stealthwatch, read more information below from NterOne.

WHO WILL BENEFIT FROM THIS COURSE?

The knowledge and skills that a learner should have before attending this course are as follows:

- Customers whose role is to use the Stealthwatch System to monitor network performance.
- Channel partners responsible for completing the initial configuration of the Stealthwatch System into a customer network.
- Employees responsible for completing the initial configuration of the Stealthwatch System into a customer network.

PREREQUISITES:

This course is designed for network engineers who are interested in implementing Stormwatch in their network environment. To fully take advantage of this course and the topics covered therein, one must possess certain skills prior to attending. These skills include but are not limited to the following:

- CCNA or equivalent knowledge
- Familiarity with network security concepts
- Basic Windows navigation skills

COURSE OBJECTIVES:

After completing this course, you will be able to implement Stealthwatch in you network and collect forensic data. This course aims to do the following:

- Introduce learners to Flow concepts
- Introduce learners to Stealthwatch
- Teach learners how to proactively and reactively use Stealthwatch to maintain the health of their network

COURSE OUTLINE:

Module 1: Flow Basics

- Netflow Overview
- Flow Information
- Flow Collector
- Flow Stitching for bi-directional flow
- Deduplication

Module 2: Introduction to Stealthwatch

- What is Stealthwatch?
- Types of input
- Stealthwatch Management Console
- Flow Collector
- UDP Director
- Flow Sensor
- Cisco ISE
- Threat Intelligence License
- Visibility Through Netfow
- Conversational Flow Record
- Discovery
- IOC
- Response

Module 3: Introduction to Flow Collector

- Overview of Flow Collector
- Key Features of Flow Collector
- Baselining of all IP traffic
- Anomaly detection in traffic/host behavior
- Layer 7 anomaly detection
- Appliance or virtual deployment options
- NAT stitching
- P2P file sharing detection
- Host and service profiling
- Index-based prioritization technology OS fingerprinting
- Support for application-aware flows such as NBAR2
- Support for custom applications
- Closest interface determination and tracking
- Deduplication of flows
- Virtual environment monitoring
- Host Group tracking and reporting
- Router interface tracking and reporting
- Bandwidth accounting and reporting
- Packet-level performance metrics
- QoS (DSCP) monitoring
- Interface utilization alarming
- Unauthorized host access detection
- Unauthorized Web server detection
- Misconfigured firewall detection
- Combined internal and external monitoring
- Full flow logging

- Worm detection
- Botnet detection
- DoS/DDoS detection (SYN, ICMP, or UDP flood)
- Fragmentation attack detection
- Network scanning and reconnaissance detection
- Large file transfer detection
- Rogue server detection
- Long term flow retention

Module 4: Introduction to UDP Director

- UDP Director Overview
- Key Features of UDP Director
- Simplifies collection of network and security data
- Reduces points of failure on your network
- Provides a single destination for all UDP formats on the network including Netflow, SNMP, syslog, etc.
- Reduces network congestion for optimum network performance

Module 5: Introduction to Proxywatch

- Proxy watch overview
- Key Features
- Enhanced network visibility
- Additional context around converstions
- Follow the flow

Module 6: Introduction to StealthWatch Labs Intelligence Center (SLIC) Threat Feed

- SLIC High Level Overview

Module 7: Stealthwatch Installation

- This module introduces learners to the installation process of a Stealthwatch SMC VM and Flow Collector
- VM editions
- Recommended Resources
- Required Ports
- Example Deployment
- Deploying the OVA
- Logging into the SMC
- Initial Setup
- Adding Flow Collectors

Module 8: Stealthwatch Management Console

- Overview of SMC
- Key Features
- User identity tracking
- Appliance and virtual deployment options
- Root-cause analysis and troubleshooting
- Relational flow maps
- NAT stitching

- Custom dashboards
- Custom reporting
- Blocking, remediation or rate limiting
- Top N reports for applications, services, ports, protocols, hosts, peers and conversations
- Traffic composition breakdown
- Customizable user interface based on Point-of-View technology
- Advanced flow visualization
- Internal and external monitoring
- Capacity planning and historical traffic trending
- WAN optimization reporting
- DSCP bandwidth utilization
- Worm propagation visualization
- Internal security for high-speed networks
- Customizing Views

Module 9: Case Study

- Case Study 1
- Case Study 2

SUNSET LEARNING INSTITUTE (SLI) DIFFERENTIATORS:

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their cloud technology investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience.
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes at any of our established training facilities or from the convenience of your home or office with the use of our HD-ILT network (High Definition Instructor Led Training)
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- Dedicated account manager to suggest the optimal learning path for you and your team
- Enthusiastic Student Services team available to answer any questions and ensure a quality training experience