

Secure Configuration Manager Essentials

Introduction

The Secure Configuration Manager Essentials course is a lecture and lab style, three-day course designed to help students understand, deploy, and successfully use NetIQ® Secure Configuration Manager™. NetIQ training designed this course with real-world content and with an emphasis on hands-on exercises. You will learn to install and use Secure Configuration Manager to examine the weaknesses in Windows, UNIX, web-server, and database systems. You will learn how to:

- Manage and inventory IT Assets and determine the vulnerabilities present on managed systems
- Apply industry standard baselines and criteria such as the SANS / FBI Top 20, HIPPA, and Sarbanes-Oxley to determine weaknesses
- Develop your own customized checks for specific vulnerabilities

In this class, you will practice using features within Secure Configuration Manager to remove these vulnerabilities and lock down Windows and UNIX computers systems, IIS web-servers, and Microsoft SQL-Server database servers. Additionally, you will also learn how to:

- Keep your security content up to date
- Use Secure Configuration Manager to be automatically informed when new vulnerabilities are discovered by the computer security industry
- Interface Secure Configuration Manager with NetIQ Security Manager

Training Agenda for Secure Configuration Manager Essentials

The following table lists the agenda for the Secure Configuration Manager Essentials class. Changes to the training agenda outlined may constitute a change of scope.

Day 1 Topics

Architecture

- Architecture Overview
- Components
- Process flow
- Communications

Installation

- Planning for installation
- Prerequisite check
- Install
- Configuration
- Hands-On Labs
 - Install Secure Configuration Manager
 - Configure the Core Services Computer

Installing Secure Configuration Manager Agent

- Windows Agent Installation
- UNIX Agent Installation
- Post Agent Installation
- Hands-On Labs
 - Windows Agent installation
 - UNIX Agent Installation

Using the Web Server Console

- Install and use the Web Console
- How to create an SSL Certificate
- Hands-On Labs
 - Install the Web Console
 - Use the Web Console

Asset Management

- How to use the Secure Configuration Manager Console
- Build the Asset Map
- Create and Manage Groups
- Hands-On Labs
 - Create and populate New Groups
 - Use the Star Tree View
 - Use the Flex Grid View
 - Admin Reports Wizard

Console Security

- Console Users
- Authentication Sources
- User Roles & Permissions
- Password Policy
- Hands-On Labs
 - Set the Password Policy
 - Create Secure Configuration Manager Console Users
 - Create and Use Secure Configuration Manager Console Roles

Day 2 Topics

Vulnerability Assessment

- Key Terms
- Security Checks
- Tasks
- Task Suites
- Policy Templates
- Report Viewer
- Hands-On Labs
 - Select Platform Security Checks
 - Run Tasks to Check Your Agents
 - Run Standard Platform Security Tasks
 - Run a Policy Template
 - Use a Policy Template to Reduce Vulnerabilities
 - Create a Policy Template
 - Run a Task Suite
 - Create a Task Suite

Using the Web Console

- Web Server Console Install
- SSL Keys
- Use Browser to Access Reports
- Hands-On Labs
 - Install the Web Console Server
 - Use the Web Console

Customization

- Creating Custom Checks
- Creating Custom Policy Templates
- Hands-On Labs
 - Create Custom Checks
 - Port 80 Open
 - HTTPD Daemon Running
 - Create a Custom Template
 - Custom Check for Registry Key Value
 - Policy Template with Registry Value Custom Check
 - Advanced Custom Checks Lab
 - Specific Registry Key / Value set
 - Specific User-ID exists on Windows computers
 - Specific directory exists on Windows computers and has executable files in it
 - Specific software package installed on UNIX computers
 - Change the Endpoint Importance Values
 - Export and Import

Custom Tasks and Active Audit

- Custom Tasks
- Active Audit
- Hands-On Labs
 - Create Custom Tasks and use Custom Tasks with Active Audit
 - Create a Custom Task Suite That Uses Custom Tasks

Correcting Windows Vulnerabilities

- Principles for Correcting Windows Vulnerabilities
- Hands-On Labs
 - Lock Down Windows with Templates and Task Suites

Day 3 Topics

Using the UNIX Manager

- Manage Agents
- Baseline File Systems
- Run Expert (UNIX) System Checker
- Scan for Network Services
- Lockdown (baseline) File System
- Manage Resource Access
- Hands-On Labs
 - Run the Expert Checker
 - Baseline a File System
 - Monitor Open Ports

Correcting UNIX Vulnerabilities

- Principles for Correcting UNIX Vulnerabilities
- Hands-On Labs
 - Lock Down UNIX with Templates, Task Suites, and with the UNIX Manager

Updating Security Knowledge

- AutoSync Wizard
- Hands-On Labs
 - Download new Templates and Patch Databases
 - Use the new Templates and new Patch Databases
 - Archive Updates

Virtual Classroom Setup Guide

NetIQ training conducts classes in a lecture with labs format. The requirements listed in this section are in place to ensure that the trainer can conduct effective discussions and demonstrations and that the students can perform all of the lab exercises. Failure to meet these requirements may compromise the value of the training. Please contact trainingadmin@netiq.com if you are unable to meet any of these requirements.

Basic Requirements

- A whiteboard or flip chart with markers
- A projector (or TV) capable of displaying at least 800x600 resolution
- Public Internet access. Students must be able to reach <https://training.netiq.com>
- One computer for the instructor
- One computer for each student

Minimum Computer Hardware Requirements

- Intel® Pentium® 1.3 GHz
- 1 GB of RAM

Software Requirements

- Microsoft® Windows XP or later operating system
- Citrix® Presentation Server Client (lightweight Citrix Client available for download at <https://training.netiq.com>)

Customized NetIQ Virtual Machines

- As the class begins, the instructor will guide the students to access the NetIQ Virtual Training environment at <https://training.netiq.com> with a student-specific logon.
- These customized virtual machines will provide all the configurations required for installing and running NetIQ software.
- NetIQ software will NOT be installed directly onto any of the student computers. Instead, NetIQ software will be leveraged within the virtual machines provided in the NetIQ Virtual Training Environment.