Course Description

# McAfee SIEM Advanced Administration 201

**Customer Instructor-Led Training**

McAfee ® SIEM appliances provide near real-time visibility into the activity on all your systems, networks, databases, and applications. This enables you to detect, correlate, and remedy threats in minutes across your entire IT infrastructure. This course is a continuation of the SIEM Administration 101 course, that takes the student through a deeper dive into analysis techniques using the features provided by SIEM. Through hands-on lab exercises, the student will learn how to optimize the SIEM by upgrading, tuning and instituting a workflow analysis using McAfee recommended best practices and methodologies.

## Recommended Pre-Work

It is recommended that students complete the SIEM Administration 101 course available on the Netexam website and have at least 1-year experience using McAfee SIEM appliances.

## Course Goals

- Install and configure SIEM appliances to suit the enterprise environment
- Employ enterprise assets to provide context to SIEM events
- Tune and customize policy rules
- Write effective correlation rules
- Build workflow views incorporating third party feeds

## Agenda At A Glance

**Day 1**

- Class Introduction
- Lecture - Chapter 1: SIEM Installation and Configuration
- Lab: Upgrading SIEM Devices
- Lab: Configure the ESM and Receiver
- Lecture - Chapter 2: Establishing Context in SIEM

**Day2**

- Lab: Defining Zones
- Lab: Importing Assets
- Lab: Implementing Data Enrichment

## Audience

- Enterprise customers who have a working knowledge of networking and system administration concepts, a good understanding of computer security concepts, and a general understanding and experience of networking and application software.

**Register Now for Training**

intel Security

## Course Description

- Lecture - Chapter 3: Operating and Tuning the SIEM
- Lab: Filtering on Erroneous Events
- Lab: Configuring Variables
- Lab: Modifying Correlation rules
- Lecture - Chapter 4: Correlation Rules

**Day 3**

- Lab: Creating a Custom Correlation Rule
- Lecture - Chapter 5: Workflow and Analysis
- Lab: Using Content Packs
- Lab: Implementing URL Actions
- Lab: Importing Threat Feeds
- Lab: Using Cyber Threat Feeds
- Begin Lab: Final Exam Break-out and Discussion

**Day 4**

- Continue Lab: Final Exam Presentations and Discussion

## Course Outline

**SIEM Installation and Configuration**

- Device Overvies
- Upgrade SIEM Software
- Perform a Manual Rules Update.....
- Suggested Methodology for Adding Data Sources for the First Time
- Verify That All Data Sources Are Logging
- Connect to AD for Login Authentication
- Configure Variables

**Establishing Context in SIEM**

- Define Zones and Tags
- Connect the SIEM to a Windows Domain Controller for Asset Import
- Implement Data Enrichment

**Operating and Tuning the SIEM**

- Rule Tuning
- Customize Parsing

**Correlation Rules**

- Rule Correlation
  - Event Flow
  - Writing Rules

**Workflow and Analysis**

- SIEM Technology Adoption Curve Review
- Content Packs
- Baselines
- Implement URL Actions
- Threat Management
- Threat Feeds
- Situational Awareness Use-Case



**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com