

SIEM McAfee – Security Information & Event Management Administration

Course Content –

Module 1: SIEM Overview

- What is SIEM?
 - Security Information and Event Management (SIEM)
- Event Analysis and Workflow
- Event Normalization
- Event Aggregation
- Event Correlation
- Log Management and Retention
- Security Information Management
- Security Event Management
- How SIEM is Used
- Compliance Obligations
- Elusive Security Events
- SIEM Components Overview
 - McAfee® Enterprise Security Manager (ESM)
- McAfee® Enterprise Log Manager (ELM)
- McAfee® Event Receiver (ERC)
- McAfee® Application Data Monitor (ADM)
- McAfee® Database Event Monitor (DEM)
- McAfee® Advanced Correlation Engine (ACE)
- McAfee SIEM Architecture – “Combo Boxes”
- Enterprise Security Manager(ESM)
- Receiver (ERC)
- Database Event Monitor (DEM)
- Application Data Monitor (ADM)
- Advanced Correlation Engine (ACE)
- Risk Correlation
- Correlation
- The Big Picture
 - Identifying Business Needs and Stakeholders

- Deployment Scenarios
- Large Centralized Deployment Example
- Large Distributed Deployment Example
- First-Time ESM Setup
 - Navigating the ESMI
 - Configure the Properties for the ESMI System
- Add the Devices to the System
- Configure the Device Properties
- FIPS Compliant Mode
- Implementation Process Checklist
 - Back-up and recovery plans
 - Consider integration with existing products
- Ensure end-user communications
- Apply Software Updates
- Do Validation Testing
- Follow Testing Procedures
- Change Control

Module 2: ESM and Receiver Overview

- McAfee Enterprise Security Manager
 - McAfee ESM Properties
 - ESM System Information
 - Content Packs
 - ESM Custom Settings
 - Login and Print Settings
 - Custom Device Event Links
 - Remedy Email Server Settings
 - Cyber Threat Feeds
 - ESM Email Settings
 - ESM – Configuration, Key Management and Maintenance
- ESM Settings – File Maintenance
- ESM – Login Security
- ESM – Profile Management

- ESM – Reports
- ESM – System Logs
- ESM – Users and Groups
- ESM – Add User
- ESM – Add Group
- ESM – Add Privileges
- ESM – Watchlists
- McAfee Receiver
 - Receiver Properties
 - Receiver Name and Description
 - Receiver Connection
 - Receiver Configuration
 - Receiver Management
 - Receiver Key Management
 - Receiver Device Log
 - Receiver Asset Sources
- Receiver HA
- Practice 2: SIEM Users and Groups

Module 3: ESMI Views

- The Data Problem
 - Increased Incidents
 - Filtering Issues
 - Event Management Challenges
 - The Solution
- McAfee ESMI
 - McAfee User Interface
 - ESMI Desktop
 - Views Toolbar
 - Views Toolbar
 - Out-of-Box Views
 - Use-Case Scenarios Using ESMI Dashboards

- Key Dashboards
 - Summarize By
 - Normalized Dashboard
 - Asset Vulnerability Summary
 - Geolocation Map
 - Source User Summary
 - Host Summary
 - Default Flow Summary
 - Incident Dashboard
 - Incidents Dashboard – Event Drilldown
 - Custom Views
 - Data Binding
 - SIEM Workflow Demonstration
 - Identify Slow and Low Data Exfiltration
 - Key take-aways from this demonstration
- Configure User-specific ESM Settings
 - Configure User Time Zone
 - Configure User Default Views
 - Practice 3: Creating a Custom View

Module 4: Filtering, Watchlists, and Variables

- Filters
 - Filter a view
 - Filter Sets
 - Default Filters
 - Using Multiple Filter Sets
 - Description of contains and regex Filters
- Syntax for contains and regex
- Points to consider when using contains or regex:
- String Normalization
- String Normalization File
- Watchlists and Variables
 - Watchlists

- Creating a Watchlist
- Adding a Watchlist
- Static and Dynamic Watchlists
- GTI Watchlist
- Create a watchlist of threat or IOC feeds from the Internet
- Rule Variables
- Common list of Variables
- Configure Variables
- Practice 4: Watchlists

Module 5: Receiver Data Source Configuration

- Receiver Data Sources
 - Data Sources Screen
 - Add Data Source Definitions
 - Client Data Sources
 - Adding Client Data Sources: Match on Type vs. IP
- Child Data Sources
- Data Source Grouping
- Data Source Profiles
- Data Sources – Auto Learn
- Data Sources – WMI
- Data Sources – WMI Event Logs
- Data Sources – Syslog
- Data Sources – Generic Net Flow
- Data Sources – Correlation Engine
- McAfee ePO
- Importing and Exporting Data Sources
- Data Source Time Problems
- Time Delta Page
- Discovered Assets
 - Asset Manager
 - Vulnerability Assessment Data Sources
 - Vulnerability Assessments

- Enable VA
- Real Time Data Enrichment
- Case Management
 - Remedy (Ticketing System) Interface
- Practice 5: Data Sources

Module 6: Aggregation

- Aggregation Overview
 - SIEM Architecture
- How Aggregation Works
 - Simplified Aggregation Example
 - Raw Events
 - Aggregated Events
 - Event Aggregation
 - Dynamic Aggregation
 - Automatic Retrieval
 - Manual Retrieval
 - Changing Settings
 - Sample Aggregated Event Count
 - Event Aggregation
 - Start at Level Aggregation
 - Level Aggregation
 - Level Aggregation
 - Event Aggregation – Custom
 - Custom Field Aggregation Example
- Modify Event Aggregation Settings
- Flow Aggregation
- Flow Aggregation Levels
- Start at Level Aggregation
- Level Aggregation
- Level Aggregation
- Flow Aggregation – Custom

- Flow Aggregation – Ports
- Port Values
- Practice 6: Aggregation

Module 7: Policy Editor

- Policy Editor Overview
 - Policy Editor Screen
 - Default Policy
 - Policy Tree
 - Policy Tree icons
 - Policy Tree Menu Items
 - Copy or Copy and Replace a Policy
- To copy a policy, follow the steps
- Import a Policy
- Export a Policy
- Policy Change History
- Policy Status
- Policy Rollout
- Rollout Policy Correlation
- Tags
- Operations Menu
- Tools Menu
- Normalization Categories
- Severity Weights
- Rule Types
- Rules Display Pane
- Rule Inheritance
 - The Inheritance Icons
- Rule Properties – Settings
 - Action
 - Severity
 - Blacklisting
 - Aggregation
 - Copy packet
- Advanced Syslog Parser Rules

- Parsing Tab
- Field Assignment Tab
- Mapping
- Data Source Rules – Auto Learned
- Practice 1: Using the Syslog Parser – Part 1
- Practice 2: Using the Syslog Parser – Part 2

Module 8: Correlation

- Optimized Risk Management
 - SIEM Technology Adoption Curve
- Event Normalization
- Event Correlation
- Event Correlation Engine
 - Understanding Correlation
 - Multiple Attackers Example
- Scanning Single Server (Distributed Dictionary Attack)
 - Receiver-based Correlation
 - Advanced Correlation Engine
 - Advanced Correlation Engine Risk
 - Content, Context and Risk Correlation
 - Add a Correlation Data Source
 - Correlation Rule Editor
 - Component of a rule
 - Correlation Rule Editor – Filters
 - Simple Example: Creating a Custom Correlation Rule
- Criteria
- System penetration scenario
- Rollout Correlation Policy
- Scenarios
- Rollout Correlation Policy
- Practice 8.1: Correlation Rules
- Practice 2: Adding an ACE Appliance
- Practice 8.3: Historical Correlation

Module 9: Notifications and Reporting

- Alarms
 - Create an Alarm
 - Alarm Settings
 - Alarm Settings – Condition Types
- Deviation from Baseline
- Device Failure
- Device Status Change
- Event Delta
- FIPS Failure
- HA Failure
- Field Match
- Internal Event Match
- Specified Event Rate
- Alarm Settings – Devices
- Alarm Settings – Actions
- Alarm Settings – Escalation
- Alarm Settings Additional Notes
- Additional Alarm Options
- Alarms Log
- Alarm Details
- Triggered Alarms View
- Reporting Overview
 - Out of Box Reports
 - Create Reports
 - System Properties – Reports
 - Add Report
 - Sections 1, 2, and 3
 - Section 4
- Section 5
- Section 6
- New Report Layout
- Designing Report Layout
- Document Properties
- Report Conditions

- Query Wizard
- UCF Report Filter
- Email Report Recipients
- Email Report Groups
- SMS Report Recipients
- SNMP Reports Recipients
- Syslog Report Recipients
- Add a Syslog Recipient
- Remove a Syslog Recipient
- View Running Reports
- View Report Files
- Export views and reports
- Practice 9.1: Creating Alarms
- Practice 9.2: Reporting

Module 10: Working with ELM

- ELM Overview
 - Important Terms
 - Adding an ELM
 - ELM Properties
 - ELM Information
 - ELM Configuration
 - ELM Management
 - ELM Redundancy
 - Device Log
 - ELM Data
 - Enhanced ELM Search View
- Configuring the ELM for Storage
 - ELM Storage
 - Estimating ELM Storage Example
 - ELM Storage Pools
 - Add, Edit, or Delete a Storage Device
 - Add, Edit, Delete a Storage Pool

- Mapping data sources to ELM storage Pools
- ELM MigrateDB
- ELM Mirrored Data Storage
- Creating an Integrity Check Job

Module 11: Troubleshooting and System Management

- McAfee Technical Support
 - ServicePortal (<http://m.mcafee.com>)
 - Web Gateway Extranet (<https://contentsecurity.mcafee.com>)
 - McAfee Customer Service (<http://service.mcafee.com>) 1-866-622-3911 261
 - Login Troubleshooting
 - ESM Fails to Communicate with the Client
 - Client Fails Version Validation Test
 - ESM is Rebuilding
 - ESM is Backing Up or Restoring the Database
- Unable to SSH or login to the ESM
- The NGCP password for the ESMI desktop has been lost
- User can log in to ESMI but they have no rights
- Operating System and Browser- specific Issues
- ESM Login Screen Does Not Come Up on Linux Browser
- Login – unable to get the certificate using Firefox using IPv6 address
- Export/Download Troubleshooting When Using Windows 7
- Hardware Issues
- How to obtain the serial number from a device
- Beeping during initial startup
- Update and Upgrade Issues
- Software Upgrade Process
- How to ensure that the update file is not corrupt
- Manual rules updates
- Troubleshooting Upgrade to Version 9.5.0
- Reasons for Flags
- Device Status Alerts
- Device Status Window
- ESM and ESMI Troubleshooting
- How to initiate a callhome

- How to access the terminal via the GUI
- ESM Settings – Database
- How to export the ESMI login history
- How to manually set the time if no NTP server is available
- Unable to download rules from the McAfee servers
- How to determine if you are getting data from your data source
- McAfee SIEM Sizing Overview