

ArcSight Advanced Administrators Workshop

Workshop Introduction – Workshop Objectives

Upon successful completion of this workshop, the participant will be able to:

- Describe ArcSight security deployment architecture advantages including integrations with ArcSight ESM 4.0, Logger, Connector Appliance and Threat Remediation Manager Products.
- Configure ArcSight ESM 4.0 multi manager layouts choosing appropriate ArcSight methodologies to provide high performance, high availability and fail over capabilities.
- Given specific site requirements, assess and implement integration strategies between ArcSight ESM 4.0 and ArcSight appliances such as Logger, Connector Appliance and Threat Remediation Manager.
- Utilize available authentication methods to provide credentials for ArcSight ESM 4.0 including RADIUS and LDAP/AD.
- Assess and optimize ArcSight ESM 4.0 components post installation, using setup commands, properties files and component log files.
- Utilize ArcSight's Logfu Utilities to aid in fine tuning ArcSight ESM Manager Statistics, Oracle Database Capacities and Event Throughput.
- Optimize ArcSight ESM 4.0 in order to maximize resource efficiency and operations productivity within your Security Operations Center.
- Employ available tools, utilities and associated configuration options in order to verify the health of your ArcSight installation.
- Utilize Oracle database tools to determine Oracle's explain plan for ArcSight queries in order to maximize throughput and efficiency.
- Assess and deploy ArcSight best practices for database backup and recovery.
- Evaluate and implement Oracle best practices for CPU Patchset Updating within the ArcSight ESM environment.

ArcSight Advanced Administrators Workshop

Workshop Introduction – Workshop Course Outline

▪ **Introductions**

(Instructor Lead Presentation)

▪ **Lesson I**

The ArcSight Enterprise

(Instructor Led Presentation)

- Technical Overview of ArcSight Enterprise
 - Logger Appliance
 - Connector Appliance
 - Threat Remediation Manager
- Using Multiple Managers
 - Hierarchical Layout
 - Peer to Peer
- High Availability and Fail Over Planning

▪ **Lesson II**

Integrating ArcSight Products

(Instructor Lead Presentations)

- Advanced Connector Setup and Configurations
- Integrations With ArcSight Appliances
 - Understanding CEF
 - Integrating the Logger Appliance
 - Using CounterAct Connectors to Integrate with TRM
 - Configuring the Forwarding Connector for Hierarchical Layouts
- Authenticating ArcSight Credentials
 - RADIUS Configurations
 - LDAP/AD Configurations

▪ **Lesson III**

Configuring ArcSight ESM

(Instructor Lead Presentations)

- Configuring ArcSight Components
 - CLI Configuration/Setup Commands per ArcSight Component
 - Discovering Component Properties Files
 - Understanding Log Files per ArcSight Component
 - Using Logfu to Monitor and Investigate Throughput and Capacity Conditions
- Configuring ArcSight for your Environment
 - Importing Assets Using the Asset Import Tool
 - Event Categorization and Map Files
 - Customizing ArcSight Case Management System
 - Customizing the ArcSight Web Interface
- Advanced ArcSight Network Modeling
 - Alternate Devices
 - Defining Multiple Zones
 - Dynamic Zones
 - Working With Customers Resource
 - Asset Categories
 - Building Content Using the ArcSight Network Model

ArcSight Advanced Administrators Workshop

▪ Lesson IV

Oracle Administration for ArcSight ESM

(Instructor Lead Presentations and Hands On Activity)

- ArcSight Oracle Administration
 - Using Manage.jsp
 - Understanding ArcSight ESM 4.0 Database Checks
 - Using the ArcSight DB Check Utility
 - Using the ArcSight Health Check Utility
 - Using ArcSight Manager Inventory Tool
 - Modifying Oracle Data Files
 - Troubleshooting Oracle JDBC Sessions
 - ArcSight Report Query Optimizer
 - ArcSight Event Integrity Component
- Basic Oracle Administration
 - Using the Remote Diagnostic Agent
 - Logging Oracle Explain Plans
 - Oracle Backup Strategies
 - Understanding Oracle CPU Patchset Updating