

Course Catalog 2012

Building a Successful ArcSight Team

ArcSight University prepares you for fast implementation and efficient operation

Learn from a full assortment of role-based, product oriented courses with delivery options designed to support the most demanding security needs.

Make training as unique as your organization

ArcSight University offers a variety of training options

- ▶ Including course customization and on-site delivery

Call us at: (888) 415-ARST for more details, or
Email: arst-education@hp.com



Table of Contents

ARCSIGHT ESM COURSES 3

ARCSIGHT ESM ESSENTIALS 4

INTRODUCTION TO ARCSIGHT ESM EVENT MANAGEMENT 5

ARCSIGHT ESM OPERATIONS..... 6

ARCSIGHT ESM SECURITY ANALYST..... 7

ARCSIGHT SKILLS ON-DEMAND: Incident Handling on Active Attacks 8

ARCSIGHT ESM USE CASE FOUNDATIONS 9

BUILDING ESM ADVANCED CONTENT FOR USE CASES 10

ARCSIGHT ESM ADMINISTRATOR 11

ARCSIGHT SKILLS ON-DEMAND: Security & Authentication 12

ARCSIGHT ESM ARCSIGHT ADVANCED ADMINISTRATION 13

ARCSIGHT CONNECTORS & CONNECTOR APPLIANCE COURSES .. 14

ARCSIGHT SMARTCONNECTOR FOUNDATIONS AND TOOL KITS..... 15

ARCSIGHT FLEXCONNECTOR CONFIGURATION..... 16

ARCSIGHT CONNECTOR APPLIANCE ADMINISTRATION & OPERATIONS 17

ARCSIGHT LOGGER COURSES 14

ARCSIGHT LOGGER SEARCH AND REPORTING 18

ARCSIGHT LOGGER ADMINISTRATION AND OPERATIONS 19

ARCSIGHT EXPRESS COURSES 14

ARCSIGHT EXPRESS ADMINISTRATION & OPERATIONS [Oracle]..... 20

ARCSIGHT EXPRESS ADMINISTRATION & OPERATIONS [CORR-Engine] 21

Did You Know?

In addition to traditional classroom training, you can take many of our courses on-line, as self-paced eLearning or instructor-led, Web-based, virtual classroom.

These symbols identify each delivery option. For complete course descriptions, latest schedule and registration instructions visit:

www.arcsight.com/university

Mode of Delivery

Icon

Classroom



Virtual Classroom



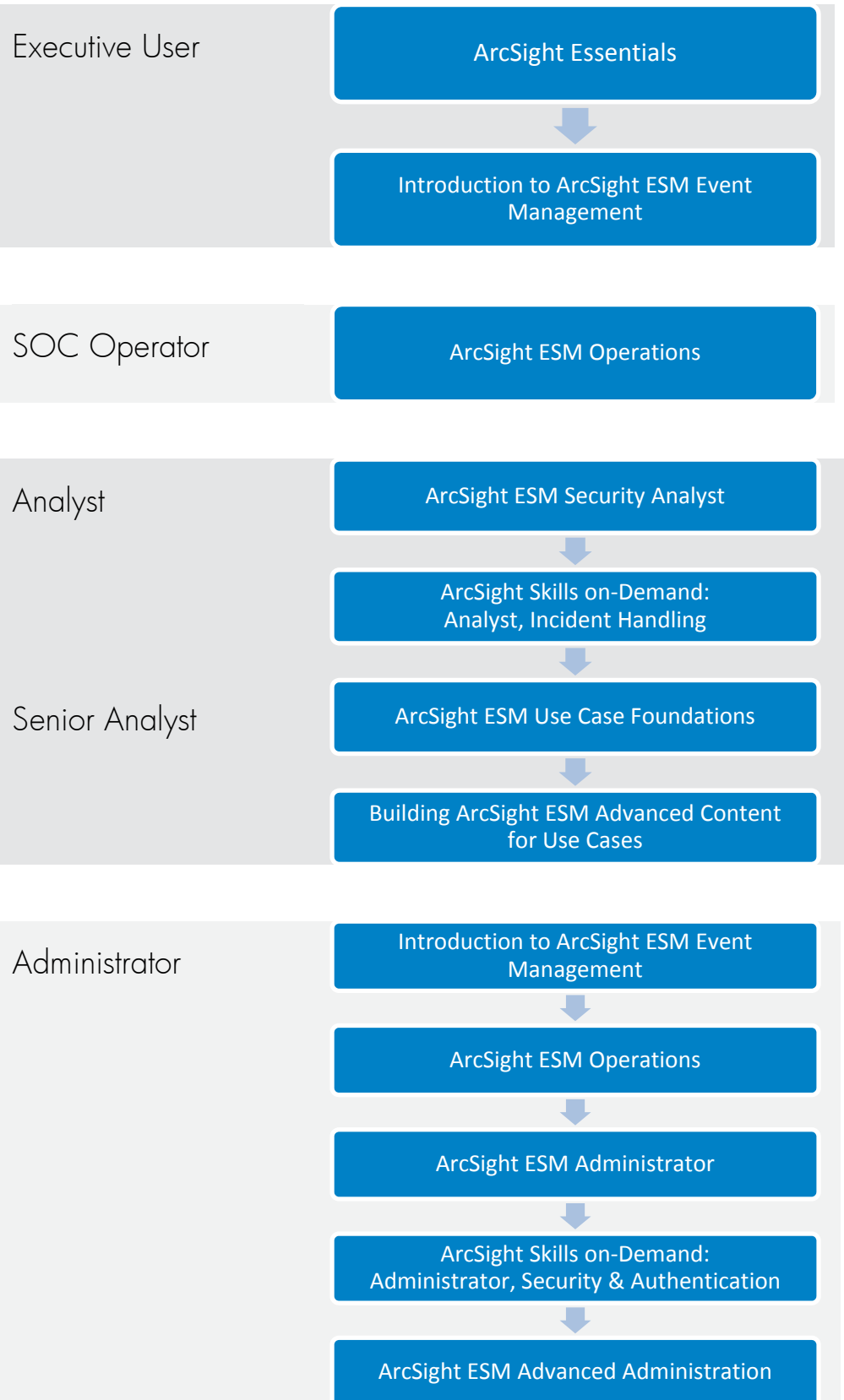
eLearning



Skills on-Demand



ArcSight ESM Courses



ArcSight Certification Exams

ArcSight Security Administrator
ArcSight Security Analyst

For more information, please visit www.arcsight.com/university and click on the **HP Certification** tab.

ArcSight ESM Essentials

Description:

ArcSight Essentials provides you with an introduction to the common security problems addressed by ArcSight's Security Information Event Management (SIEM) solution. Each module provides a high-level overview of each ArcSight product and describes how it solves the security risks experienced by digitally connected organizations.

Objectives:

At the end of this course, you will be able to:

- ▶ List the major security risks associated with a digital environment
- ▶ List and describe the functions of all ArcSight products
- ▶ Match the ArcSight solution to the security problem that is solved
- ▶ Using icons provided in a topic review, construct a simple SIEM solution using ArcSight products

Audience:

This introductory course is designed for newcomers and anyone interested in learning about ArcSight's SIEM solution.

Prerequisites:

To be successful in this course, you will have:

- ▶ Experience with common Information Security terms and concepts
- ▶ Experience with basic network computing concepts
- ▶ Familiarity with Windows and Unix operating systems

Delivery Method:



- ▶ Approximately 2 hours, self-paced, online, eLearning

Introduction to ArcSight ESM Event Management

Description:

The Introduction to ArcSight Event Management course provides the fundamental concepts of an ArcSight ESM implementation. Understanding these basic concepts is critical for anyone who needs to administer an ArcSight ESM implementation or perform analysis on security data within ArcSight ESM. This course is also a prerequisite to additional ArcSight ESM training.

Objectives:

At the end of this course, you will be able to:

- ▶ Identify roles of users who interact with ArcSight ESM
- ▶ Describe the components of an ArcSight ESM implementation
- ▶ Describe the structure of the ArcSight event schema
- ▶ Identify the phases of the ArcSight event life cycle

Audience:

This introductory course is intended for all ArcSight ESM users, who need to:

- ▶ Monitor security threats
- ▶ Assess risk exposure
- ▶ Enforce regulatory compliance requirements
- ▶ Manage Security Operations
- ▶ Administer an ArcSight ESM implementation

Prerequisites:

To be successful in this course, you will have:

- ▶ Experience with common Information Security terms and concepts
- ▶ Experience with basic network computing concepts
- ▶ Familiarity with Windows and Unix operating systems

Delivery Method:



Approximately 3 hours, self-paced, online, eLearning

NOTE:

This course is a subset of the *ArcSight ESM Security Analyst* eLearning course. If you have purchased, or plan to purchase, the *ArcSight ESM Security Analyst* eLearning course, **DO NOT purchase** this course.

ArcSight ESM Operations

Description:

The ESM Operations class provides you with comprehensive training on ESM operations. This course offers exercises for common functionality and procedures needed to quickly retrain or cross train a broader group of ESM operators. The modular format of this course enables you to select the topics and lessons applicable to your job tasks and allows you to return to lessons to refresh what you have previously learned.

Objectives:

At the end of this course, you will be able to:

- ▶ Using pre-configured ESM, identify and investigate events that appear as potential security risks
- ▶ Document the results of your investigation to enable others to pursue further analysis
- ▶ Using a predefined workflow, notify analysts and/or escalate investigations
- ▶ Print basic system health & incident investigation reports
- ▶ Use either the ArcSight Console or the ArcSight Web user interface

Audience:

This base-level training is intended for operators who use ArcSight ESM to monitor daily security events and investigate events of interest to a level where they are either dismissed or escalated to an Analyst or Administrator. Operator duties are assumed to be limited in scope, but may include using standardized, preconfigured resources, such as field sets, filters, queries, and reports.

Prerequisites:

To be successful in this course, you will have:

- ▶ TCP/IP networking, database concepts and enterprise security experience, which are highly advantageous
- ▶ Completed *Introduction to ArcSight ESM Event Management*

Delivery Method:



- ▶ Two days, instructor-led, virtual classroom
- ▶ Approximately 10 hours, self-paced, online, eLearning

ArcSight ESM Security Analyst

Description:

The ArcSight ESM Security Analyst course provides you with the knowledge required to use the ArcSight Console to monitor security events. You learn how to use ArcSight ESM workflow to escalate security incidents for further analysis and remediation. You also learn to use standard ArcSight ESM content to find and correlate event information, perform actions such as notifying stakeholders, analyze event data graphically, and report on security incidents within your security environment.

Objectives:

At the end of this course, you will be able to:

- ▶ Identify ArcSight ESM product components
- ▶ List the components of the ArcSight ESM Event Schema and how it is used to normalize base data
- ▶ Navigate ArcSight ESM Console and Web Components to correlate, investigate, analyze, and remediate both exposed and obscure threats
- ▶ Implement custom and stock Filters, Rules, Session Lists, etc. with the Integrated Case Management and Workflow, to identify, categorize, and escalate events of interest
- ▶ Either manually or using the Network Modeling Wizard, implement Network and Asset Models

Audience:

This basic course is intended for operators/analysts, who need to:

- ▶ Use the ESM Console to monitor, display and report on security incidents
- ▶ Use standard content to correlate, view and respond to security incidents
- ▶ Design, deploy and maintain the ArcSight network model to accurately build content, view and report on security incidents

Prerequisites:

To be successful in this course, you will have:

- ▶ Common security devices, such as IDS and firewalls
- ▶ Common network device functions and TCP/IP addressing
- ▶ Basic Windows operating system tasks & functions
- ▶ Possible attack activities, such as scans, man in the middle, sniffing, DoS, etc and possible abnormal activities, such as worms, Trojans, viruses, etc.
- ▶ SIEM terminology, such as threat, vulnerability, risk, asset, exposure, safeguards, etc.
- ▶ Security directives, such as Confidentiality, Integrity, Availability.

Delivery Method:



- ▶ Five days, instructor-led training at ArcSight or Customer on-site
- ▶ Approximately 14 hours, self-paced, online, eLearning AND approximately 16 hours, instructor-led, virtual classroom

ArcSight Skills on-Demand: Analyst Incident Handling on Active Attacks Module

Description:

Experience transforms competence to expertise. The training courses offered by ArcSight University provide the foundation knowledge and skills for the security professionals working with the ArcSight Technology and Solutions.

Skills on-Demand Provides:

Cloud based Labs

- ▶ Real-world experience of a configured ArcSight implementation
- ▶ Perform the activities at your own pace and from any convenient location via standard browser and high-speed internet connection
- ▶ Safe for experimenting, refresh to original state with “a push of a button”

Prescribed Activities for Analysts and Administrators

- ▶ Guides to ensure most important areas of expertise are covered
- ▶ Based upon Use Cases for Analysts to provide exposure to most demanding areas of daily work

eMentors

- ▶ Access to eMentors, experienced professionals and instructors, via email, with a committed turnaround time of 24 hours maximum
- ▶ eMentors are dedicated to providing support related to the Prescribed Activities of Skills on-Demand

Activities Included in this Module:

- ▶ Delivery of situational awareness
- ▶ Reduction of risk and downtime
- ▶ Threat control and prevention
- ▶ Path of Escalation
- ▶ Audit and compliance support
- ▶ Incident response and recovery
- ▶ Speed of aggregation and correlation
- ▶ Device and system coverage
- ▶ Ability to respond quickly through Real Time data and automation
- ▶ 24/7 uptime

Prerequisites:

To be successful in the activities in this Skills on-Demand, you will have:

- ▶ Successfully completed *ArcSight ESM Security Analyst (AESA)* course [highly recommended] **or**
- ▶ 6 months experience with ArcSight ESM as a Security Analyst

Delivery Method:



- ▶ Eighteen hours web-based access to a virtual environment over a fourteen day period

ArcSight ESM Use Case Foundations

Description:

The ArcSight Use Cases Foundations provides you with detailed knowledge of the ArcSight security problem solving methodology, within the ESM context. In this course, you learn the methodologies to develop use cases for current business scenarios, derived from the top business drivers in the market. During the training, you learn to:

- ▶ Using ArcSight ESM, identify business drivers to develop Use Cases
- ▶ Identify Use Case problems and requirement statements associated with actual scenarios
- ▶ Using the Use Case worksheet, document a use case
- ▶ Develop ArcSight ESM content to accommodate Use Case discrete objectives

This course includes extensive hands-on exercises.

Objectives:

At the end of this course, you will be able to:

- ▶ In an ArcSight ESM context, define Use Case
- ▶ Using the Use Case worksheet from an initial problem statement, generate requirement statements and prioritize objectives
- ▶ Identify data sources and ESM resources required to fulfill the objectives of the use case
- ▶ Fulfill use case requirements by creating identified ESM content:
 - ◆ Construct ArcSight Active Channels to provide advanced analysis of the event stream
 - ◆ Develop ArcSight Rules to allow correlation activities
 - ◆ Build event-based data monitors to provide real time viewing of event traffic
- ▶ Package formulated ESM contents for the Use Case into ArcSight Resource Bundle

Audience:

This advanced course is intended for those whose primary responsibilities include:

- ▶ Defining organization's security objectives
- ▶ Building ArcSight ESM content to adhere to those objectives

Prerequisites:

To be successful in this course, you will have:

- ▶ Completed *ArcSight ESM Security Analyst (AESA)*
- ▶ Knowledge of:
 - ◆ Common network devices and their functions
 - ◆ TCP/IP functions
 - ◆ Windows operating system tasks
 - ◆ SIEM terminology and Security directives

Customization:

On-site, customized training is available for this course.

For more information, please email arst-edu-custom-training@hp.com

Delivery Method:



- ▶ Three days, instructor-led training at ArcSight or Customer on-site

Building ESM Advanced Content for Use Cases

Description:

This course covers ArcSight security problem solving methodology using advanced ArcSight ESM content to find, track and remediate security incidents, specifically identified in the course's use cases.

During the training, you will learn to:

- ▶ Use variables and correlation activities
- ▶ Customize report templates to use dynamic content
- ▶ Customize notification templates to send the appropriate notification based upon specific attributes of an event

Note: This course includes extensive hands-on exercises.

Objectives:

At the end of this course, you will be able to:

- ▶ In an ArcSight ESM context, define Use Case
- ▶ Using the Use Case worksheet from an initial problem statement, generate requirement statements and prioritize objectives
- ▶ Identify data sources and ESM resources required to fulfill the objectives of the use case
- ▶ To fulfill use case requirements, create identified ESM content:
 - ◆ Construct ArcSight Variables to provide advanced analysis of the event stream
 - ◆ Develop ArcSight Rules to allow advanced correlation activities
 - ◆ Build event-based data monitors to provide real time viewing of event traffic and anomalies
 - ◆ Implement custom velocity macros for notification
 - ◆ Create new report templates and functional reports using the statistics and dynamic values
 - ◆ Package formulated ESM contents for the Use Case

Audience:

This advanced course is intended for those whose primary responsibilities include:

- ▶ Defining organization's security objectives
- ▶ Building ArcSight ESM content to adhere to those objectives

Prerequisites:

To be successful in this course, you will have:

- ▶ Completed *ArcSight ESM Security Analyst (AESA)*
- ▶ Knowledge of:
 - ◆ Common network devices and their functions
 - ◆ TCP/IP functions and Windows operating system tasks
 - ◆ SIEM terminology and security directives

Delivery Method:



- ▶ Five days, instructor-led training at ArcSight or Customer on-site

ArcSight ESM Administrator

Description:

The ArcSight ESM Administrator course provides you with in-depth information about an ArcSight ESM installation. It includes instructions for performing administrative related tasks within ArcSight ESM. This course is designed for any System Administrator that performs routine administration tasks within ArcSight ESM, such as performing data backups and patch updates. You will be exposed to administrative and troubleshooting tools within ArcSight ESM and learn how to use them effectively.

Objectives:

At the end of this course, you will be able to:

- ▶ Manage and install ArcSight ESM components
- ▶ Manage database space and retention policies
- ▶ Administer ArcSight ESM
- ▶ Back Up ArcSight ESM
- ▶ Upgrade ArcSight ESM
- ▶ Troubleshoot ArcSight ESM

Audience:

This course is intended for any system administrator that will be responsible administering some aspect of an ArcSight ESM implementation.

Prerequisites:

To be successful in this course, you will have:

- ▶ Completed *Introduction to ArcSight ESM Event Management*

Delivery Method:



- ▶ Four days, instructor-led training at ArcSight or Customer on-site
- ▶ Four days, instructor-led, virtual classroom
- ▶ Approximately 14 hours, self-paced, online, eLearning

ArcSight Skills on-Demand: Analyst Incident Handling on Active Attacks Module

Description:

Experience transforms competence to expertise. The training courses offered by ArcSight University provide the foundation knowledge and skills for the security professionals working with the ArcSight Technology and Solutions.

Skills on-Demand Provides:

Cloud based Labs

- ▶ Real-world experience of a configured ArcSight implementation
- ▶ Perform the activities at your own pace and from any convenient location via standard browser and high-speed internet connection
- ▶ Safe for experimenting, refresh to original state with “a push of a button”

Prescribed Activities for Analysts and Administrators

- ▶ Guides to ensure most important areas of expertise are covered
- ▶ Based upon Use Cases for Analysts to provide exposure to most demanding areas of daily work

eMentors

- ▶ Access to eMentors, experienced professionals and instructors, via email, with a committed turnaround time of 24 hours maximum
- ▶ eMentors are dedicated to providing support related to the Prescribed Activities of Skills on-Demand

Activities Included in this Module:

- ▶ Delivery of situational awareness
- ▶ Reduction of risk and downtime
- ▶ Threat control and prevention
- ▶ Path of Escalation
- ▶ Audit and compliance support
- ▶ Incident response and recovery
- ▶ Speed of aggregation and correlation
- ▶ Device and system coverage
- ▶ Ability to respond quickly through Real Time data and automation
- ▶ 24/7 uptime

Prerequisites:

To be successful in the activities in this Skills on-Demand, you will have:

- ▶ Successfully completed *ArcSight ESM Security Analyst (AESA)* course [highly recommended] **or**
- ▶ 6 months experience with ArcSight ESM as a Security Analyst

Delivery Method:



- ▶ Eighteen hours web-based access to a virtual environment over a fourteen day period

ArcSight ESM Advanced Administration

Description:

The ArcSight Advanced Administration course provides you with techniques to proactively analyze and troubleshoot the Oracle 11g database and ArcSight ESM manager to provide efficient services to your organization. This course teaches you to design and deploy hierarchical, fault tolerant manager implementations as well integration strategies between ArcSight ESM and other ArcSight appliances such as Logger, Connector Appliance, and the NSP products.

Objectives:

At the end of this course, you will be able to:

- ▶ Design, deploy and configure an ArcSight ESM multi-manager layout for high-availability and fail-over
- ▶ Assess and implement integration strategies for ArcSight ESM and ArcSight appliances
- ▶ Provide credentials for ArcSight ESM including RADIUS and LDAP/AD
- ▶ Use available ArcSight and Oracle tools to investigate the health of your installation
- ▶ Implement ArcSight best practices for backup and recovery for an Oracle 10g database

Audience:

This course is designed for users who need to:

- ▶ Install, administer, maintain and troubleshoot ArcSight ESM components
- ▶ Design and implement integrations between ArcSight ESM and other ArcSight appliances
- ▶ Proactively investigate the health of the ArcSight ESM environment including the Oracle 11g database

Prerequisites:

To be successful in this course, you will have an understanding of:

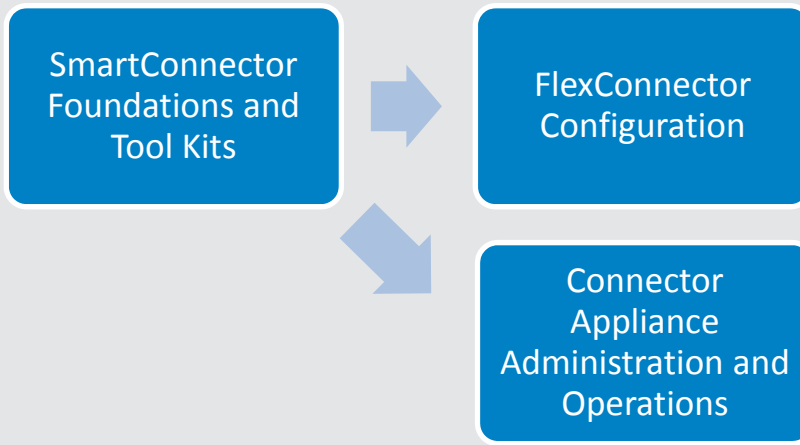
- ▶ Common security devices, such as IDS & firewalls
- ▶ Common network device functions, such as routers, switches, hubs, etc.
- ▶ TCP/IP functions, such as CIDR blocks, subnets, addressing, communications, etc.
- ▶ Basic Windows operating system tasks & functions
- ▶ Possible attack activities, such as scans, man in the middle, sniffing, DoS, etc., and possible abnormal activities, such as worms, Trojans, viruses, etc.
- ▶ SIEM terminology, such as threat, vulnerability, risk, asset, exposure, safeguards, etc.
- ▶ Oracle database structures
- ▶ 6 months experience administering ArcSight ESM
- ▶ Completed *ArcSight ESM Administrator*

Delivery Method:

- ▶ Four days, instructor-led training at ArcSight or Customer on-site

ArcSight Connectors and Connector Appliance Courses

Administrators



ArcSight Logger Courses

Business User

ArcSight Logger Search and Reporting

Administrators

ArcSight Logger Administration and Operations

ArcSight Express Courses

All Users [CORR-Engine]

ArcSight Express 3.0 [CORR-Engine] Administration & Operations

All Users [Oracle]

ArcSight Express 4.5/5.0 [Oracle] Administration & Operations

ArcSight SmartConnector Foundations and Tool Kits

Description:

The ArcSight SmartConnector Foundations course provides you with detailed knowledge to install and configure ArcSight SmartConnectors.

Objectives:

At the end of this course, you will be able to:

- ▶ Install and configure SmartConnector software via CLI, GUI and the Connector Appliance
- ▶ Configure, enable, and disable automated startup
- ▶ Add, configure, and remove destinations and fail-over destinations
- ▶ Configure aggregation, filtering, batching and time correction functions
- ▶ Alter JVM settings, including those required to use more memory and support international locales
- ▶ SmartConnector Tool Kit includes:
 - ◆ JDBC Driver Installation
 - ◆ Windows Unified Connector
 - ◆ McAfee ePolicy Orchestrator Connector
 - ◆ CheckPoint OPSEC NG Connector
 - ◆ Sourcefire eStreamer Connector
 - ◆ Symantec Endpoint Protection Connector
 - ◆ Nessus Scanner Connector
- ▶ FlexConnector Tool Kit includes:
 - ◆ Delimited File FlexConnector
 - ◆ Syslog FlexConnector
 - ◆ RegEx FlexConnector
 - ◆ SNMP FlexConnector

Audience:

This course is intended for administrators, who need to:

- ▶ Deploy and manage ArcSight SmartConnectors

Prerequisites:

To be successful in this course, you will have a basic understanding of:

- ▶ Common network device functions
- ▶ TCP/IP functions, such as CIDR blocks, subnets, addressing, etc.
- ▶ Basic Windows operating system tasks
- ▶ SIEM terminology, such as threat, vulnerability, risk, asset, exposure, safeguards, etc.
- ▶ Security directives, such as Confidentiality, Integrity, Availability

Delivery Method:



- ▶ One-day instructor-led, virtual classroom AND approximately 5 hours, self-paced, online, eLearning [Tool Kits]
- ▶ Approximately 8 hours, self-paced, online, eLearning

ArcSight FlexConnector Configuration

Description:

ArcSight FlexConnector Configuration training provides you with an overview of the ArcSight SmartConnectors framework and explains the ArcSight ESM Schema. It teaches you how to construct and manipulate FlexConnector configuration, and property files and to use various parsing methods including fixed delimited, regular expressions, and database query. Examples from standard connectors are used to illustrate device-specific methodologies. Advanced configuration options such as multi-line Regex, parser linking and conditional mapping are also covered.

Objectives:

At the end of this course, you will be able to:

- ▶ Given a target event log file and configuration criteria, install ArcSight Connector software, configure a functional FlexConnector, and test with an ESM Active Channel
- ▶ Use the FlexConnector Wizard to create fixed delimited configuration files
- ▶ Use the Regex Tester tool to create common and sub-message parsing and token-to-event mapping
- ▶ Given ESM field set display criteria, create a tailored Categorization file for a parent FlexConnector and test its function in an active channel
- ▶ Navigate the connector configuration file hierarchy to locate, display and edit appropriate configuration properties files to perform advanced functions such as conditional mapping and parser linking

Audience:

This intermediate level course is intended primarily for security administrators, content authors/architects and IT integrators, who build and install custom connectors to provide critical event data feeds to ArcSight ESM or Logger. This can include senior analysts for networks, security systems, enterprise applications & databases.

Prerequisites:

To be successful in this course, you will have:

- ▶ Completed *ArcSight ESM Security Analyst (AESA)* - highly recommended
- ▶ Completed *ArcSight ESM Administrator* - highly recommended
- ▶ A working knowledge of Regular Expressions

Delivery Method:



- ▶ Three days, instructor-led training at ArcSight or Customer on-site

ArcSight Connector Appliance Administration and Operations

Description:

The ArcSight Connector Appliance Administration and Operations course provides you with the knowledge to administer, configure, and effectively manage an ArcSight Connector Appliance.

Objectives:

At the end of this course, you will be able to:

- ▶ Identify and differentiate the various ArcSight Connector Appliance models and their capabilities
- ▶ Install and configure Connector Appliance
- ▶ List the components that make up a Connector Appliance and describe how they interoperate
- ▶ Mount remote file systems with a Connector Appliance
- ▶ Configure a SmartConnector on Connector Appliance
- ▶ Configure a software SmartConnector for remote management by Connector Appliance
- ▶ Perform complex tasks like batch configuration changes on Connectors
- ▶ Upgrade individual SmartConnectors
- ▶ Upgrade, Backup and Restore SmartConnectors
- ▶ Upgrade, Backup and Restore a Connector Appliance

Audience:

This course is intended for administrators, who need to:

- ▶ Deploy and maintain ArcSight Connector Appliances

Prerequisites:

To be successful in this course, you will have a basic understanding of:

- ▶ Common network device functions, such as routers, switches, hubs, etc.
- ▶ TCP/IP features and functions, such as CIDR blocks, subnets, addressing, communications, etc.
- ▶ Windows operating system tasks, such as installations, services, sharing, navigation, etc.
- ▶ SIEM terminology, such as threat, vulnerability, risk, asset, exposure, safeguards, etc.
- ▶ Security directives, such as Confidentiality, Integrity, Availability.

Delivery Method:



- ▶ Two days, instructor-led, virtual classroom
- ▶ Approximately 6 hours, self-paced, online, eLearning

ArcSight Logger Search and Reporting

Description:

ArcSight Logger Search and Reporting provides you with task-focused training to quickly configure and use your Logger's event search and reporting capabilities. Learning content is specifically intended for team members of security operations, network operations, auditing and compliance. This course includes exercises on common functionality and procedures to leverage built-in product content as well as custom tailoring techniques to fulfill event search and reporting demands in enterprise security and operations log management environments.

Objectives:

At the end of this course, you will be able to:

- ▶ Explain and implement event indexing and use the Logger search builder to access field-based, full-text and regex-based event search facilities
- ▶ Access and customize search field set display controls and search constraint criteria to refine and tune event search results
- ▶ Use Logger search builder to access unified event search facilities, save search queries as filters, saved searches, shared or search group filters
- ▶ Access reporting resources to use pre-built reports, copy and customize reports, and manage report groups and categories to control distribution and access to report information
- ▶ Run reports as scheduled jobs, ad hoc, or as a background task, publish and archive results according to given distribution and retention criteria

Audience:

This is a base-level course that provides you with specific end-user event search and reporting topics intended for team members of security operations, network operations, as well as personnel responsible for auditing and compliance.

Prerequisites:

To be successful in this course, you will have:

- ▶ Computer desktop, browser, and file system navigation skills
- ▶ TCP/IP networking, database concepts and enterprise security experience, which are highly advantageous

Delivery Method:



- ▶ Approximately 3 hours, self-paced, online, eLearning

NOTE:

This course is a subset of the *ArcSight Logger Administration & Operations* eLearning course. If you have purchased, or plan to purchase, the *ArcSight Logger Administration & Operations* eLearning course, **DO NOT purchase** this course.

ArcSight Logger Administration and Operations

Description:

ArcSight Logger Administration and Operations provides you with comprehensive training to quickly configure your Logger Appliance or Downloadable Software Logger and bring it into an operational state. Learning content is specifically intended for team members of security operations, network operations, auditing and compliance. This course includes hands-on training exercises on common functionality and procedures to tailor and maintain ArcSight Logger.

Objectives:

At the end of this course, you will be able to:

- ▶ Initialize Logger Appliance or install Software Logger, establish network connection, implement initial Logger storage, retention policy, and event indexing
- ▶ Configure event source devices/device groups, such as event Receivers, Forwarders, etc. and optional connector management facilities
- ▶ Establish and manage Logger user/group controls
- ▶ Use the Logger search builder to access unified event search facilities, save search queries as filters, saved searches, scheduled alerts, shared or search group filters
- ▶ Access reporting resources to view pre-built reports, copy and customize reports, and manage report groups and categories to control distribution and access to report information

Audience:

This is a base-level course that provides specific content to perform system administrative and IT integration initial setup tasks for ArcSight Logger Appliance or Software form factors, version 5.0. Additional end-user topics are intended for team members of security operations, network operations, as well as personnel responsible for security auditing and compliance.

Prerequisites:

To be successful in this course, you will have:

- ▶ Computer desktop, browser, and file system navigation skills
- ▶ TCP/IP networking, database concepts and enterprise security experience

Delivery Method:



- ▶ Three days, instructor-led training at ArcSight or Customer on-site
- ▶ Three days, instructor-led, virtual classroom
- ▶ Approximately 14 hours, self-paced, online, eLearning

ArcSight Express

Administration and Operations [Oracle]

Description:

The *ArcSight Express Administration and Operations* course provides you with comprehensive training for ArcSight Express. This course includes hands-on training exercises on packaged content and functionality for you to bring the ArcSight Express appliance into production environments.

Objectives:

At the end of this course, you will be able to:

- ▶ Use ArcSight Express built-in content, such as standard Channels, Filters, Rules, Active Lists and Reports, to make ArcSight Express ready to use upon initial installation.
- ▶ Configure Network and Asset Modeling to build custom business-oriented views within the ArcSight Express environment
- ▶ Utilize ArcSight Express monitoring and detection features to isolate, investigate, analyze, and remediate exposed security issues to provide situational awareness and real time incident response
- ▶ Given Storage Appliance network and business access requirements, configure global, platform, and system settings for both appliance and user resources
- ▶ Utilize Search and Report Query facilities to define and locate matching events from the Storage Appliance and deploy high usage queries as filters, saved searches, or scheduled reports

Audience:

This course is intended for all users of the ArcSight Express appliance, including members of security operations, network operations, as well as those responsible for auditing and compliance. It is designed for users who need to:

- ▶ Administer the ArcSight Express appliance
- ▶ Perform IT integration tasks for both the ArcSight Express and Logger Storage Appliances
- ▶ Utilize the Search and Report Query facilities

Prerequisites:

To be successful in this course, you will have:

- ▶ Computer desktop, browser, and file system navigation skills
- ▶ TCP/IP networking, database concepts and enterprise security experience are highly advantageous



Delivery Method:

- ▶ Five days, instructor-led training at ArcSight or Customer on-site
- ▶ Five days, instructor-led, virtual classroom
- ▶ Approximately 32 hours, self-paced, online, eLearning

NOTE:

This course is intended for AE 4.5/5.0 with Oracle, not AE 3.0 with the CORR-Engine

This course **only** covers the following deployment model:



ArcSight Express Administration and Operations [CORR-Engine]

Description:

The ArcSight Express Administration and Operations course provides you with comprehensive training for ArcSight Express. This course includes hands-on training exercises on packaged content and functionality for you to bring the ArcSight Express appliance into production environments.

Objectives:

At the end of this course, you will be able to:

- ▶ Use ArcSight Express built-in content, such as standard Channels, Filters, Rules, Active Lists and Reports, to make ArcSight Express ready to use upon initial installation
- ▶ Configure Network and Asset Modeling to build custom business oriented views within the ArcSight Express environment
- ▶ Utilize ArcSight Express monitoring and detection features to isolate, investigate, analyze, and remediate exposed security issues to provide situational awareness and real time incident response
- ▶ Configure ArcSight settings, system settings, and user resources appropriately
- ▶ Create custom content
- ▶ Access reporting resources to use pre-built reports, copy and customize reports, create report dashboards, and manage report groups and categories to control distribution and access to report objects and published information

Audience:

This course is intended for all users of the ArcSight Express appliance, including members of security operations, network operations, as well as those responsible for auditing and compliance. It is designed for users who need to:

- ▶ Administer the ArcSight Express appliance
- ▶ Perform IT integration tasks for both the ArcSight Express Appliances
- ▶ Utilize the Search and Report Query facilities

Prerequisites:

To be successful in this course, you will have:

- ▶ Computer desktop, browser, and file system navigation skills
- ▶ TCP/IP networking, database concepts and enterprise security experience are highly advantageous



Delivery Method:

- ▶ Five days, instructor-led training at ArcSight or Customer on-site
- ▶ Five days, instructor-led, virtual classroom
- ▶ Approximately 32 hours, self-paced, online, eLearning

NOTE:

This course is intended for AE 3.0 with the CORR-Engine, not AE 4.5/5.0 Oracle.

This course **only** covers the following deployment model:

