



Course Overview

ArcSight ESM 6.5 Administrator and Analyst

HP ArcSight ESM 6.5 Administrator and Analyst training is a hands-on, four day instructor-led course detailing Enterprise Security Manager (ESM) product facilities while performing related tasks on a live ArcSight ESM. Learners use the ArcSight Console, ArcSight Command Center, and ArcSight Web user interfaces to monitor security events, configure ESM, and manage users and ESM network intelligence resources. Using ArcSight ESM workflow, participants isolate, document, escalate, and resolve security incidents. This course enables tailoring standard ArcSight ESM content to acquire, search, and correlate actionable event data; and perform remedial activities such as incident analysis, stakeholder notification, and reporting security conditions within your network environment.

Audience

This course is intended for any system administrator and/or analyst, who needs to:

- Monitor, remediate, and report on security incidents using ArcSight ESM facilities
- Use standard content to correlate, display and respond to identified issues in real time
- Design, deploy and maintain ArcSight network, asset and user modeling for your cyber-infrastructure

Course title:	ArcSight ESM 6.5 Administrator and Analyst
HP product number:	AS3C0066
Category/Subcategory:	Application Security
Course Length:	4 days
Level:	Advances
Delivery language:	English
To order visit:	www.aramatech.com/about

Prerequisites

Recommended:

- Computer desktop and network browser skills
- TCP/IP networking, file system and database concepts
- Enterprise security, event and log management experience is highly advantageous

Certifications and Related Examinations

- ArcSight Security Solutions ATP

Course Objectives

Upon completion of this course, students will be able to:

- Make ArcSight ESM operational upon initial installation, creating user accounts and implementing built-in solutions content
- Implement Network and Asset Modeling facilities to enable site-specific business-oriented views within your ArcSight ESM environment
- Investigate, identify, analyze, and remediate exposed security issues using ArcSight ESM monitoring and detection features
- Use workflow management to provide real-time incident response and escalation tracking
- Modify and run standard reports to provide situational awareness and network status to enterprise stakeholders
- Establish ESM peering to perform distributed event search and content management across multiple ESM instances

Detailed course outline

Topics Covered

Module 1 – Introduction to ArcSight ESM

- User roles
- ESM components, resources, and communications

Module 2 – ArcSight Event Schema and Lifecycle

- Event schema groups
- Event LifeCycle phases

Module 3 – ESM Installation and Configuration

- Requirements and system preparations
- First Boot and Network Model wizards
- Enable bundled content

Module 4 – ESM Console

- Installing, logging on and navigation

Module 5 – ArcSight Command Center

- Utilizing the ArcSight Command Center

Module 6 – ArcSight Web Interface

- Access the content and functionality available

Module 7 – Active Channels, Filters and Field Sets

- View live events
- Create an active channel and add field sets

Module 8 – Rules and Lists

- Create and validate rules and lists

Module 9 – Dashboards and Data Monitors

- Event monitoring using dashboards

Module 10 – Query Viewers

- Overview of query viewers

Module 11 – ESM Reports

- Defining, running and archiving reports

Module 12 – Workflow Cases

- Define, access, and manage cases

Module 13 – User Administration

- Administration of users

Module 14 – User Notifications

- Functions, templates, and configuring
- ArcSight Whine Daemon

Module 15 – Use Case Resources

- Create or modify resource content to fulfill solution objectives

Module 16 – ArcSight Content Management

- Features, requirements, and configuration
- Configuring ArcSight host peers

Module 17 – Event Search

- Search interface, expressions, and filters
- Search results display

Module 18 – HP ArcSight Support Resources

- Access resources
- Locate component logs to obtain status
- Perform support activities

Why education services from HP?

- Comprehensive curriculum of job-specific training leading to vendor certification
- Unmatched technical expertise and support for HP products and technologies
- Award winning Virtual classrooms (SmallBiz Windows Collaboration Product of the Year 2010) and Virtual Labs for a real hands-on experience
- Training you need, when and where you need it with our Remotely Assisted Instructional Learning (RAIL)
- Top 20 training provider and content development - www.TrainingIndustry.com
- Streamlined purchase and management of training with HP Care Pack Services for Education
- Global training with more than 90 training locations world-wide
- Recognized as an IDC MarketScape leader for IT education (IDC MarketScape: Worldwide IT Education and Training 2012 Vendor Analysis, doc #232870, February 2012)
- More than 30 years of Education Consulting

[For more information
ESP-EduOps@hp.com](mailto:ESP-EduOps@hp.com)

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

HP Education services are governed by the HP Education Services Terms and Conditions

