Hewlett Packard Enterprise

ArcSight ESM 6.5 Administrator and Analyst - ATP H0DW2S

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.

ArcSight ESM 6.5 Administrator and Analyst - ATP	
Price	USD $3,200
Links to local schedules, pricing and registration	**US/Canada**
HP course #	H0DW2S
Category	Security
Duration	4 days

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

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

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

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

Learn more at

hpe.com/us/training/security

H0DW2S Ver A.00

c04762980 August 2015

Hewlett Packard Enterprise