Hewlett Packard Enterprise

ArcSight ESM 6.5 Advanced Administrator - ASE H0DW3S

This course provides you with the knowledge required to use advanced HP 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. You will familiarize and/or reinforce your understanding of the advanced correlation capabilities within ArcSight ESM that provide a significant edge in detecting active attacks.

This course covers HP ArcSight security problem solving methodology using advanced HP ArcSight ESM content to find, track and remediate security incidents. During the training, you will learn to use variables and correlation activities, customize report templates for dynamic content, and customize notification templates to send the appropriate notification based upon specific attributes of an event.

ArcSight ESM 6.5 Advanced Administrator - ASE	
Price	USD $4,000
Links to local schedules, pricing and registration	**US/Canada**
HP course #	H0DW3S
Category	Security
Duration	5 days

Audience

This basic course is intended for operators\analysts, who need to:
- Define their organization's security objectives
- Build or use advanced content to correlate, view and respond to those security objectives

Prerequisites

To be successful in this course, you must have:
- Completed the HP ArcSight ESM 6.5c SP1 Admin & Analyst training
- Knowledge of:
  - Common security device functions, such as IDS/IPS, Network and Host-based firewalls, etc.
  - Common network device functions, such as routers, switches, hubs, etc.
  - TCP/IP functions, such as CIDR blocks, subnets, addressing, communications, etc.
  - Windows operating system tasks, such as installations, services, sharing, navigation, etc.

- Possible attack activities, such as scans, man in the middle, sniffing, DoS, DDoS, 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

Course objectives

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

- Navigate HP ArcSight ESM Console and Command Center to correlate, investigate, analyze, and remediate both exposed and obscure threats
- Construct HP ArcSight Variables to provide advanced analysis of the event stream
- Develop HP ArcSight Lists and Rules to allow advanced correlation activities
- Optimize event-based data monitors to provide real time viewing of event traffic and anomalies
- Design new report templates and create functional reports
- Find events through the search tools

Certifications/exams

- ArcSight ESM 6.5c SP1 Advanced Administrator

Course outline

Topics Covered

Module 1 – ArcSight ESM Overview

- ESM Components
- ArcSight Event Schema
- Normalization Process
- Seven Phases of Event Lifecycle

Module 2 – ArcSight Console

- Toolbar Commands
- Navigator Panel
- Viewer Panel Views
- ESM Console Help

Module 3 – ESM Active Channels

- Active Channels
- Field Sets

Module 4 – ESM Filters

- Working with Filters

Module 5 – Data Monitors and Dashboards

- Event Monitoring

Module 6 – Variable Customization

- Benefits of Using Variables
- Creating Variables
- Promoting Local Variables
- Use Cases with Variables

Module 7 – ESM Lists

- Active and Session Lists

Module 8 – ESM Rules
- Rules Overview
- Conditions, aggregation, actions, and triggers
- Lightweight and Per-persistence Rules

Module 9 – Query Viewers Authoring
- Query Viewer Functions
- Building a Trend

Module 10 – ESM Reports
- Reports Overview
- Report Workflow
- Defining Data Sources
- Best Practices Using Trends
- Creating a Report
- Special Types of Reports

Module 11 – Unified Event Search Tools
- ArcSight Command Center Search Interface
- Event Search Input
- Search Results Display
- Search Facilities

Learn more at

hpe.com/us/training/security

H0DW3S Ver A.00

c04762984 August 2015

Hewlett Packard Enterprise