HP TRAINING

Hp Arcsight Esm 6 5 Security Administrator And Analyst Training Course

Master HP ArcSight ESM 6.5 to effectively administer security operations and analyze threats.

DURATION
Flexible

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

The HP ArcSight ESM 6.5 Security Administrator and Analyst Training Course provides a comprehensive deep dive into leveraging HP's Enterprise Security Manager (ESM) platform for robust cybersecurity operations. This intermediate-level course is meticulously designed for IT professionals aiming to master the intricacies of ArcSight ESM 6.5, a leading Security Information and Event Management (SIEM) solution. Participants will gain practical expertise in real-time security monitoring, advanced threat detection, incident correlation, and effective incident response, equipping them with the skills to defend against sophisticated cyber threats.

Throughout this training, you will explore the core functionalities of ArcSight ESM 6.5, including its architecture, data collection mechanisms (Connectors), event processing, rule engine, and reporting capabilities. The curriculum bridges the gap between administrative tasks, such as platform configuration, maintenance, and optimization, and analytical responsibilities, like investigating security incidents, threat hunting, and generating compliance reports. By completing this course, you will not only enhance your organization's security posture but also significantly boost your career prospects as a skilled cybersecurity professional capable of operating and managing a critical SIEM platform.

Level	Intermediate
Vendor	HP

COURSE CURRICULUM

01 Module 1: Introduction to ArcSight ESM 6.5 Architecture

- Overview of SIEM and ArcSight ESM
- ArcSight ESM components: Logger, Manager, Console, Connectors, SmartConnectors
- Understanding event flow and data processing
- Installation and initial configuration considerations

02 Module 2: ArcSight ESM Data Collection and Normalization

- SmartConnectors deployment and configuration
- Parsing and normalization of security events
- Managing data sources and log collection policies
- Introduction to ArcSight FlexConnectors

03 Module 3: Security Monitoring and Event Analysis

- Using the ArcSight Console for real-time monitoring
- Creating and managing Dashboards and Active Channels
- Filtering, grouping, and searching for security events
- Understanding ArcSight event categories and severities

04 Module 4: Rule Creation, Correlation, and Reporting

- Developing correlation rules for threat detection
- Building use cases and managing triggered alerts
- Creating and scheduling compliance and operational reports
- Customizing report templates and data visualization

05 Module 5: Incident Management and Response with ArcSight

- Leveraging ArcSight for incident investigation
- Workflow management and case tracking

- Integration with incident response playbooks
- Best practices for security incident handling

06 Module 6: Advanced Administration and Optimization

- User and group management, access control
- Platform health monitoring and performance tuning
- Backup and recovery strategies for ArcSight ESM
- Introduction to ArcSight content development and best practices

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Senior Security Operations Center (SOC) Analyst**

> **SIEM Platform Administrator (ArcSight Specialist)**

> **Cybersecurity Incident Response Team Lead**

FREQUENTLY ASKED QUESTIONS

Q: What foundational cybersecurity knowledge or IT experience is recommended before enrolling in this ArcSight ESM 6.5 training?

This intermediate-level course assumes participants have a basic understanding of networking concepts (TCP/IP, firewalls, proxies), operating systems (Windows Server, Linux), and fundamental cybersecurity principles. Prior exposure to security event logs or other SIEM platforms would be beneficial but is not strictly required, as the course covers ArcSight fundamentals comprehensively.

Q: How will mastering ArcSight ESM 6.5 benefit my ability to detect and respond to advanced persistent threats (APTs) or zero-day attacks?

This course equips you with the skills to configure and leverage ArcSight ESM's powerful correlation engine, enabling you to build sophisticated rules that detect patterns indicative of APTs or unusual activities that could signify zero-day exploits. You'll learn to analyze aggregated security events, identify anomalous behavior, and effectively utilize the platform's investigative tools to proactively pinpoint and respond to advanced threats before they escalate.

Q: What is the primary distinction between the 'Administrator' and 'Analyst' roles taught in this course, and how will the training prepare me for both?

The course provides dual-track expertise. As an 'Administrator,' you'll learn to install, configure, maintain, and optimize the ArcSight ESM platform, including managing connectors, users, and system health. As an 'Analyst,' you'll focus on utilizing the configured platform for real-time threat monitoring, incident investigation, rule creation for threat detection, and generating compliance reports. The curriculum is structured to provide hands-on experience in both aspects, ensuring you are proficient in both managing and operating ArcSight ESM for comprehensive security operations.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke