HP ArcSight Security Solutions

Exam description

This exam tests your skills on the ArcSight security solution, including addressing major security risks associated with a digital environment and designing a security solution, using ArcSight products, to combat those risks. Additionally, exam will test your ability to gather business requirements for the ArcSight solution.

This certification exam is designed for candidates with "on the job" experience. The associated training courses, which usually include labs, provide a foundation, but you are expected to have experience in the real world as well.

Who should take this exam?

New candidates who want to acquire the *HP ATP - ArcSight Security V1* certification.

Exam contents

This exam has 60 questions. Here are the types of questions to expect:
- Multiple choice

- Multiple choice (multiple responses)

Objectives

This exam validates that you can successfully perform the following:

HP0-A100	Sections/Objectives
6.8%	ArcSight Technology Overview • List common Business risks faced by organizations • Describe How ArcSight Technologies address these risks • List ESM Resources
10%	ArcSight Event Schema • List ArcSight Event Schema Group • Describe ArcSight Event Schema Definitions
20%	ArcSight Event Lifecycle • Lifecycle Overview • Describe Data Collection and Event Processing • Describe Priority Evaluation and Network Model Lookup • Describe Correlation of the Event Stream • Describe Monitoring and Investigation process

Exam ID	HP0-A100
Exam type	Proctored
Exam time	90 minutes
Exam length	60 questions
Passing score	65%
Delivery languages	English
Related certifications	• HP ATP - ArcSight Security V1
Supporting courses	These recommended courses help you prepare for the exam: • ArcSight Security Solutions ATP Training
Additional study materials	

Register for this exam

You will need an HP Learner ID.

During the exam, you can make specific comments about the exam and items. HP welcomes these comments as part of our continuous improvement process.

No online or hard copy reference material will be allowed at the testing site. This exam may contain beta test items for experimental purposes.

	• Describe Workflow • Describe Reporting and Incident Analysis
15%	What is Enterprise Security Manager (ESM)? • List problems solved by ESM • List the benefits of using ESM
8.3%	What is ArcSight Express? • List problems solved by ArcSight Express • List The benefits of using ArcSight Express
13.3%	What are SmartConnectors and the Connector Appliance? • List problems solved by SmartConnectors • List the benefits of using SmartConnectors • List the benefits of using a Connector Appliance
5%	What is Logger? • List problems solved by Logger • List the benefits of using Logger
11.6%	What are Compliance Insight Packages (CIPs)? • Describe CIPs • List the benefits of using CIPs
10%	What is IdentityView? • Describe IdentityView • Describe the benefits of using IdentityView

Tips for taking this exam

This exam assesses whether you have the knowledge and skills to navigate and utilize ArcSight Security products as a security solution in a business development and production environment.

Take the time to read the entire question and consider all of the options carefully *before* you answer. If the question indicates that it features an exhibit, study the exhibit and reread the question. Make sure to select the answer that correctly responds to the question that is asked, not simply an answer that includes some correct information.

If the question asks for more than one answer, remember to select each correct answer. You will not receive partial credit for a partially correct answer.

Sample questions

Use the following questions to help assess whether you are ready to take the exam. Answers to these sample questions are provided at the end of this guide.

1. What is the purpose of the ArcSight Enterprise Security Manager (ESM)?
    a.   A. enables situational awareness and visibility of the security risks across an organization
    b.   B. enables a security bus such that devices may communicate
    c.   C. enables security integration between disparate devices
    d.   D. enables security device management using a common browser-based Management Console

Answers
This section provides answers to and references for the sample questions.

1. What is the purpose of the ArcSight Enterprise Security Manager (ESM)?
    a.   A. enables situational awareness and visibility of the security risks across an organization
    b.   B. enables a security bus such that devices may communicate
    c.   C. enables security integration between disparate devices
    d.   D. enables security device management using a common browser-based Management Console
    References:
    HP ArcSight Security Solutions Training Course (HPAS-SS.v1)
    ArcSight Security Solutions ATP Student Guide.pdf
        —   Module 1 – ArcSight Technology Overview

For more information

HP ExpertOne: www.hp.com/go/ExpertOne-ContactUs