Sulabh Mishra
Arcsight Trainer
+91-9172620286

Arcsight Interview Questions

1. **What does ArcSight ESM stand for and what is its primary use?**

- So ArcSight ESM stands for Enterprise Security Manager.As the name itself implies the usage of this tool is that it adds value to your organization security policies. Using this tool, it will help the organizations to focus on the threat detection, analysis on the triages, compliance management. All of these are done on SIEM platform where it actually reduces the time taken to resolve a cybersecurity threat.

2. **What does SIEM stand for and what is it about?**

- SIEM stand for Security Information and Event management, So this is a platform where a holistic view of the security process implemented within the organization. The letter e is silent and it is addressed as "SIM" platform. Basically, in this process, the data is all gathered into one secure repository where the logs are used for future security analysis. This process is widely used in Payment Card Industry. It is actually classified as a data security standard in Payment Card industry.

3. **What are the key features of ArcSight Enterprise Security Manager?**

>The key features of ArcSight Enterprise Security Manager is as follows:

1. Enriched Security Event data
2. Powerful real-time data visualization and correlation
3. Automated workflows
4. Security process optimized
5. ArcSight Enterprise Security Manager tool is compatible with ArcSight Data Platform and ArcSight Investigate

4. **Explain how ArcSight ESM is protecting the businesses across the globe?**

- The following are the different ways that the business is actually protected by using ArcSight ESM tool, as follows:

1. It is capable of collecting data or information from any type of log source
2. It tremendously reduces the response time and also helps in reducing the damage as well
3. It can efficiently store information where the information can be retrieved as we generally do in enterprise-level databases.
4. It provides role relevant reports that are available within the enterprise
5. The architecture is scalable
6. Easily customizable and maintains high-performance system

5. **How does ArcSight ESM provide Powerful real-time data correlation?**

- Well, ArcSight ESM provides powerful real-time data correlation by processing number of events per second. Based on this analysis a more accurate outcome is proposed. So based

on this analysis, the threats that violate the internal rules are escalated within the platform. ESM actually processes 75,000 events per second basis.

6. What can be done using ArcSight ESM?

- ArcSight ESM actually helps the organizations and the individuals as below:
  All the event data is collected centrally and stored and monitor
  User-friendly compliance reporting in a single touch provides necessary data in an appropriate format.
  Has an ability to monitor and mitigate the risk.
  Eliminates manual process as much as possible
  Saves valuable hours of security analyst where they spend on false alarms
  Brings awareness to the team about the security process in place and the countermeasures implemented.

7. Why do organizations need Security Information and Event Management systems?

- Well, most of the small companies don't have enough manpower to make sure that their security process is intact. But they won't be able to be proactive and warn the team that there might be a possible threat attack, this is because they don't have any automatic mechanism which triggers a threat attack. So, to solve the real time issue and also make sure the security checks are monitored and analyzed, we have Security Information and Event Management system. Out of this system is ArcSight SEM. So basically, all the machine log data is analyzed and understands the patterns of normal behavior vs abnormal behavior. Thus, making it a perfect tool where it can understand the security logs so far and based on the analysis can trigger some information which might prevent a bigger threat to the entire organization.

8. How can ArcSight ESM help organizations in terms of security aspects?

- Well, ArcSight ESM can help the organizations building more enhanced use cases to improve the APT's (Advanced Persistent Threats)which will allow a faster and targeted response in a timely fashion.

9. What does ArcSight Logger do?

- So, ArcSight Logger is nothing but a log management solution that can be used widely in the security practices. So using solution, the users will be able to capture and analyze different type of log data and provide necessary inputs to all the individual's teams so their questions are answered. Eventually, this can be expanded into an enterprise level log management solution if needed.
  So using this solution, topics like compliance and risk management are taken into due consideration. Also, the data can be used for searching, indexing, reporting, analysis purposes and retention as well.

10. What is SIEM tool, explain briefly?

- In the field of Information technology and computer security, products which provide or offer services like real-time security generated alerts analysis can be categorized as SIEM tool.

11. What is a SOC team?

- The term SOC stands for "Security Operations Center".

Sulabh Mishra
Arcsight Trainer
+91-9172620286

So basically this is a center for all the websites, applications, databases, data centers and servers, networks are duly monitored and analyzed and well defended.

12. Explain what is the core offering of ArcSight ESM?

- The core offering of ArcSight ESM is:

1. Analyzes different threats to a database
2. Checks with the logs that were captured
3. Provide possible solutions or advice based on the risk level

13. What is the main purpose of ArcSight Express?

- Basically, ArcSight Express provides the same functionalities that they do at ArcSight ESM but at a very much smaller scale. ArcSight Express analyzes threats within a database and provides possible action item.

14. What is the main use of ArcSight Logger?

- The main use of ArcSight Logger is to capture or stream real-time data and categorize them into different buckets of specific logs.

15. What are the key capabilities of ArcSight Logger?

- The key capabilities of ArcSight Logger is:

1. It collects logs from any sort of log generating source
2. After collecting the data, it categorizes and registers as Common Event Format (CEF)
3. These events can be searched with the use of a simple interface
4. It can handle and store years worth of logs information
5. It is perfect for automation analysis which can be later used for reporting, the intelligence of logs or events for IT Security purposes and logs analytics.

16. What does ArcSight Connectors mean?

- The main use of ArcSight Connectors is listed below:

** With the use of ArcSight connectors, the user can actually automate the process of collecting and managing the logs irrespective of the device. All the data can be normalized into a CEF, i.e. Common Event Format
** ArcSight connectors provide a bunch of universal data collections from different unique devices.

17. What does ArcSight Manager do, explain in brief?

- The use of ArcSight manager is to simply put in place robust security parameters within the organization.So it is one of the high-performance service engines which actually filters, manages, correlates all security-related events that are collected by the IT system.

The main parts that are essential for the ArcSight manager to work appropriately is:

** ArcSight Console
** ACC
** CORR Engine

Sulabh Mishra
Arcsight Trainer
+91-9172620286

** ArcSight SmartConnectors

The operational environment for ArcSight Manager is nothing but the underlying OS and the file system that are in place.

18. **Architecture and placement of hardware of HP Arcsight**

19. **What is EPS in Arcsight? what do you know about licenses of EPS**

20. **What is smart and flex connectors? functions of these connectors? difference between them**?

- connector used to fetch/read logs from unsupported devices adding to it and is a customized connector flex

21. **SQL injection explain this concept? SQL injection is a technique to add (or inject) malicious SQL code to a website**

22. **What's an example of three factor authentication? Password (something you know),finger print (something you are) and RSA Token (something you have)**

23. **What is malware?**

24. **What port should be open at the time of implementing SIEM?**

25. **How to check an event is false positive or its threat?**

26. **What alert you usually monitor? e.g. example of types of alert of all devices**

27. **How would you choose which license you buy for SIEM? depend on the no. of device and EPS**
28. **What will check if a device is not sending logs?**

29. **What will u do if collector stops functioning?**

30. **what are Component of ARCSIGHT?**

31. **What are the reports you send on daily basis?**

32. **What are latest vulnerability found? Ghost, Heartbleed , Shellshock & IE vulnerability**

33. **What is the difference between Local collector and Remote collector?**

34. **What are the things you check for Testing the Security Architecture of your organization?**

35. **Network scanning,Vulnerability scanning,Penetration testing,Password cracking,Social engineering attempts.**

Sulabh Mishra
Arcsight Trainer
+91-9172620286

36. What is false positive and negative?

37. What is true positive and negative?

38. what will do if you saw a Zero-day attack??

39. what is logger and its use in arcsight ?

40. what is the difference between simple and join co-relation?

41. what is trend & active list in arcsight ?

42. what is the difference between ESM & LOGGER in arcsight??

43. what is the difference between CORR and Database?

44. What are common risks at ArcSight? And how to face?

45. What does IDS stand for?

- IDS stands for “Intrusion Detection System”. This is the main component when it comes to ArcSight ESM.

Q: Few bullet points on ArcSight ESM?
The following are the important points about ArcSight ESM tool:

1. With this tool, administrators and analyst can actually detect more incidents
2. Operate more efficiently
3. The same data set can be used for real-time correlation of the data and log management application can use the same dataset.

46. What are the system requirements for implementing ArcSight ESM?

- Supported Operating systems are:

1. Red Hat Enterprise Linux Version 6.2, 64 bit CPU
2. Memory 16-36GB
3. Disk space for 2-4 TB
4. Average Compression of 10:1 SAS 15K RPM

47. SQL injection explain this concept

> SQL injection is a technique to add (or inject) malicious SQL code to a website for example that has a vulnerability in it's entry field
-The attacker can have the entry field dump the contents of a database to the attackers service.
-One method to fix the server would be to patch the vulnerability.

Sulabh Mishra
Arcsight Trainer
+91-9172620286

48. What port does ICMP use?

- Trick question: ICMP does not use a port since it does not have a place for a port. It is encapsulated with an IP datagram only.

49. What is a SYN Flood?

- A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

50. What is a slow Denial of Service (DOS) attack?

- In a slow DOS is that the attack tools sends an HTTP request that never finishes. As a result, each listener process never finishes its quota of MaxRequestsPerChild so that it can die. By sending a small amount of never-complete requests, Apache gladly spawns new processes/threads up to MaxClients at which point it fails to answer requests and the site is DOS'ed.

51. Give an example of something you discovered and what did you do to handle it
52. What is a TCP handshake, describe how SSL works, Whats difference between TCP/UDP
53. Describe how heartbleed works or describe the POODLE attack
54. Describe how the TCP handshake works
55. What's the difference between and IDS and an IPS? Give examples of each.
56. What is the OSI model and how might it be used in your position in this role?
57. Name four types of DNS records and what they signify.
58. Explain what is the role of information security analyst?
59. Mention what is data leakage? What are the factors that can cause data leakage?
60. List out the steps to successful data loss prevention controls?
61. Mention what are personal traits you should consider protecting data?
62. Have you ever created SIEM content?