Vendor: Splunk

Exam Code: SPLK-5001

Exam Name: Splunk Certified Cybersecurity Defense Analyst

Version: DEMO

QUESTION 1
During their shift, an analyst receives an alert about an executable being run from C:\Windows\Temp. Why should this be investigated further?

A. Temp directories aren't owned by any particular user, making it difficult to track the process owner when files are executed.
B. Temp directories are flagged as non-executable, meaning that no files stored within can be executed, and this executable was run from that directory.
C. Temp directories contain the system page file and the virtual memory file, meaning the attacker can use their malware to read the in memory values of running programs.
D. Temp directories are world writable thus allowing attackers a place to drop, stage, and execute malware on a system without needing to worry about file permissions.

Answer: D

QUESTION 2
An analyst would like to visualize threat objects across their environment and chronological risk events for a Risk Object in Incident Review. Where would they find this?

A. Running the Risk Analysis Adaptive Response action within the Notable Event.
B. Via a workflow action for the Risk Investigation dashboard.
C. Via the Risk Analysis dashboard under the Security Intelligence tab in Enterprise Security.
D. Clicking the risk event count to open the Risk Event Timeline.

Answer: D

QUESTION 3
A Risk Rule generates events on Suspicious Cloud Share Activity and regularly contributes to confirmed incidents from Risk Notables. An analyst realizes the raw logs these events are generated from contain information which helps them determine what might be malicious.

What should they ask their engineer for to make their analysis easier?

A. Create a field extraction for this information.
B. Add this information to the risk message.
C. Create another detection for this information.
D. Allowlist more events based on this information.

Answer: A

QUESTION 4
What device typically sits at a network perimeter to detect command and control and other potentially suspicious traffic?

A. Host-based firewall
B. Web proxy
C. Endpoint Detection and Response
D. Intrusion Detection System

Answer: D

QUESTION 5
Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server's access log has the same log entry millions of times:

```
147.186.119.200 - - [28/Jul/2023:12:04:13 -0300] "GET /login/ HTTP/1.0"
200 3733
```

What kind of attack is occurring?

A. Denial of Service Attack
B. Distributed Denial of Service Attack
C. Cross-Site Scripting Attack
D. Database Injection Attack

Answer: B

QUESTION 6
According to David Bianco's Pyramid of Pain, which indicator type is least effective when used in continuous monitoring?

A. Domain names
B. TTPs
C. NetworM-lost artifacts
D. Hash values

Answer: D

QUESTION 7
An analysis of an organization's security posture determined that a particular asset is at risk and a new process or solution should be implemented to protect it. Typically, who would be in charge of implementing the new process or solution that was selected?

A. Security Architect
B. SOC Manager
C. Security Engineer
D. Security Analyst

Answer: C

QUESTION 8
Which of the following is a correct Splunk search that will return results in the most performant way?

A. index=foo host=i-478619733 | stats range(_time) as duration by src_ip | bin duration span=5min | stats count by duration, host
B. | stats range(_time) as duration by src_ip | index=foo host=i-478619733 | bin duration span=5min | stats count by duration, host
C. index=foo host=i-478619733 | transaction src_ip |stats count by host

D. index=foo | transaction src_ip |stats count by host | search host=i-478619733

Answer: A

QUESTION 9
There are many resources for assisting with SPL and configuration questions. Which of the following resources feature community-sourced answers?

A. Splunk Answers
B. Splunk Lantern
C. Splunk Guidebook
D. Splunk Documentation

Answer: A

QUESTION 10
A successful Continuous Monitoring initiative involves the entire organization. When an analyst discovers the need for more context or additional information, perhaps from additional data sources or altered correlation rules, to what role would this request generally escalate?

A. SOC Manager
B. Security Analyst
C. Security Engineer
D. Security Architect

Answer: C

QUESTION 11
Splunk Enterprise Security has numerous frameworks to create correlations, integrate threat intelligence, and provide a workflow for investigations. Which framework raises the threat profile of individuals or assets to allow identification of people or devices that perform an unusual amount of suspicious activities?

A. Threat Intelligence Framework
B. Risk Framework
C. Notable Event Framework
D. Asset and Identity Framework

Answer: B

QUESTION 12
While the top command is utilized to find the most common values contained within a field, a Cyber Defense Analyst hunts for anomalies. Which of the following Splunk commands returns the least common values?

A. least
B. uncommon
C. rare
D. base

Answer: C

QUESTION 13
The Lockheed Martin Cyber Kill Chain?breaks an attack lifecycle into several stages. A threat actor modified the registry on a compromised Windows system to ensure that their malware would automatically run at boot time. Into which phase of the Kill Chain would this fall?

A. Act on Objectives
B. Exploitation
C. Delivery
D. Installation

Answer: D

QUESTION 14
A Risk Notable Event has been triggered in Splunk Enterprise Security, an analyst investigates the alert, and determines it is a false positive. What metric would be used to define the time between alert creation and close of the event?

A. MTTR (Mean Time to Respond)
B. MTBF (Mean Time Between Failures)
C. MTTA (Mean Time to Acknowledge)
D. MTTD (Mean Time to Detect)

Answer: A

QUESTION 15
An analyst needs to create a new field at search time. Which Splunk command will dynamically extract additional fields as part of a Search pipeline?

A. rex
B. fields
C. regex
D. eval

Answer: A

QUESTION 16
Which of the following is considered Personal Data under GDPR?

A. The birth date of an unidentified user.
B. An individual's address including their first and last name.
C. The name of a deceased individual.
D. A company's registration number.

Answer: B

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**