312-39Q&As

Certified SOC Analyst (CSA)

Pass EC-COUNCIL 312-39 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/312-39.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.

What is the first step that the IRT will do to the incident escalated by Emmanuel?

A. Incident Analysis and Validation

B. Incident Recording

C. Incident Classification

D. Incident Prioritization

Correct Answer: C

QUESTION 2

Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

A. Windows Event Log

B. Web Server Logs

C. Router Logs

D. Switch Logs

Correct Answer: B

QUESTION 3

The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk. What kind of threat intelligence described above?

A. Tactical Threat Intelligence

B. Strategic Threat Intelligence

C. Functional Threat Intelligence

D. Operational Threat Intelligence

Correct Answer: B

Reference: https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/what-is-threat-intelligence/

QUESTION 4

Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

A. Failure Audit

B. Warning

C. Error

D. Information

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types

QUESTION 5

Which of the following formula represents the risk?

A. Risk = Likelihood × Severity × Asset Value

B. Risk = Likelihood × Consequence × Severity

C. Risk = Likelihood × Impact × Severity

D. Risk = Likelihood × Impact × Asset Value

Correct Answer: B

QUESTION 6

Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.

What would be her next action according to the SOC workflow?

A. She should immediately escalate this issue to the management

B. She should immediately contact the network administrator to solve the problem

C. She should communicate this incident to the media immediately

D. She should formally raise a ticket and forward it to the IRT

Correct Answer: B

QUESTION 7

Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

A. DoS Attack

B. Man-In-Middle Attack

C. Ransomware Attack

D. Reconnaissance Attack

Correct Answer: D

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf

QUESTION 8

Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.

What is Ray and his team doing?

A. Blocking the Attacks

B. Diverting the Traffic

C. Degrading the services

D. Absorbing the Attack

Correct Answer: D

QUESTION 9

Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

A. Slow DoS Attack

B. DHCP Starvation

C. Zero-Day Attack

D. DNS Poisoning Attack

Correct Answer: C

Reference: https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-are-zero-day-attacks.aspx

QUESTION 10

Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:
http://www.terabytes.com/process.php./../../../../etc/passwd

A. Directory Traversal Attack

B. SQL Injection Attack

C. Denial-of-Service Attack

D. Form Tampering Attack

Correct Answer: B

Reference: https://doc.lagout.org/security/SQL%20Injection%20Attacks%20and%20Defense.pdf

QUESTION 11

Which of the following Windows features is used to enable Security Auditing in Windows?

A. Bitlocker

B. Windows Firewall

C. Local Group Policy Editor

D. Windows Defender

Correct Answer: C

Reference: https://resources.infosecinstitute.com/topic/how-to-audit-windows-10-application-logs/

QUESTION 12

Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

A. Ransomware Attack

B. DoS Attack

C. DHCP starvation Attack

D. File Injection Attack

Correct Answer: A

Reference: https://www.netfort.com/category/ransomware-detection/

QUESTION 13

What is the process of monitoring and capturing all data packets passing through a given network using different tools?

A. Network Scanning

B. DNS Footprinting

C. Network Sniffing

D. Port Scanning

Correct Answer: C

Reference: https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types

QUESTION 14

Which of the following tool is used to recover from web application incident?

A. CrowdStrike FalconTM Orchestrator

B. Symantec Secure Web Gateway

C. Smoothwall SWG

D. Proxy Workbench

Correct Answer: B

QUESTION 15

The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?

A. Alert

B. Notification

C. Emergency

D. Debugging

Correct Answer: B