312-39$^{\text{Q\&As}}$

Certified SOC Analyst (CSA)

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

QUESTION 1

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 2

An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP. Which SIEM deployment architecture will the organization adopt?

A. Cloud, MSSP Managed

B. Self-hosted, Jointly Managed

C. Self-hosted, MSSP Managed

D. Self-hosted, Self-Managed

Correct Answer: C

QUESTION 3

What type of event is recorded when an application driver loads successfully in Windows?

A. Error

B. Success Audit

C. Warning

D. Information

Correct Answer: D

Reference: https://www.manageengine.com/network-monitoring/Eventlog_Tutorial_Part_I.html

QUESTION 4

Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.

1.

Strategic threat intelligence

2.

Tactical threat intelligence

3.

Operational threat intelligence

4.

Technical threat intelligence

A. 2 and 3

B. 1 and 3

C. 3 and 4

D. 1 and 2

Correct Answer: A

Reference: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf (38)

QUESTION 5

Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

A. $ tailf /var/log/sys/kern.log

B. $ tailf /var/log/kern.log

C. # tailf /var/log/messages

D. # tailf /var/log/sys/messages

Correct Answer: B

Reference: https://tecadmin.net/enable-logging-in-iptables-on-linux/

QUESTION 6

According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

A. Create a Chain of Custody Document

B. Send it to the nearby police station

C. Set a Forensic lab

D. Call Organizational Disciplinary Team

Correct Answer: A

QUESTION 7

John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.

Which of the following types of threat intelligence did he use?

A. Strategic Threat Intelligence

B. Technical Threat Intelligence

C. Tactical Threat Intelligence

D. Operational Threat Intelligence

Correct Answer: D

QUESTION 8

John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming. Which of the following data source will he use to prepare the dashboard?

A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.

B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.

C. DNS/ Web Server logs with IP addresses.

D. Apache/ Web Server logs with IP addresses and Host Name.

Correct Answer: D

QUESTION 9

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?

A. High

B. Extreme

C. Low

D. Medium

Correct Answer: C

Reference: https://www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf (17)

QUESTION 10

Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?

A. Command Injection Attacks

B. SQL Injection Attacks

C. File Injection Attacks

D. LDAP Injection Attacks

Correct Answer: B

Reference: https://www.kiuwan.com/owasp-top-10-a1-injection/

QUESTION 11

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

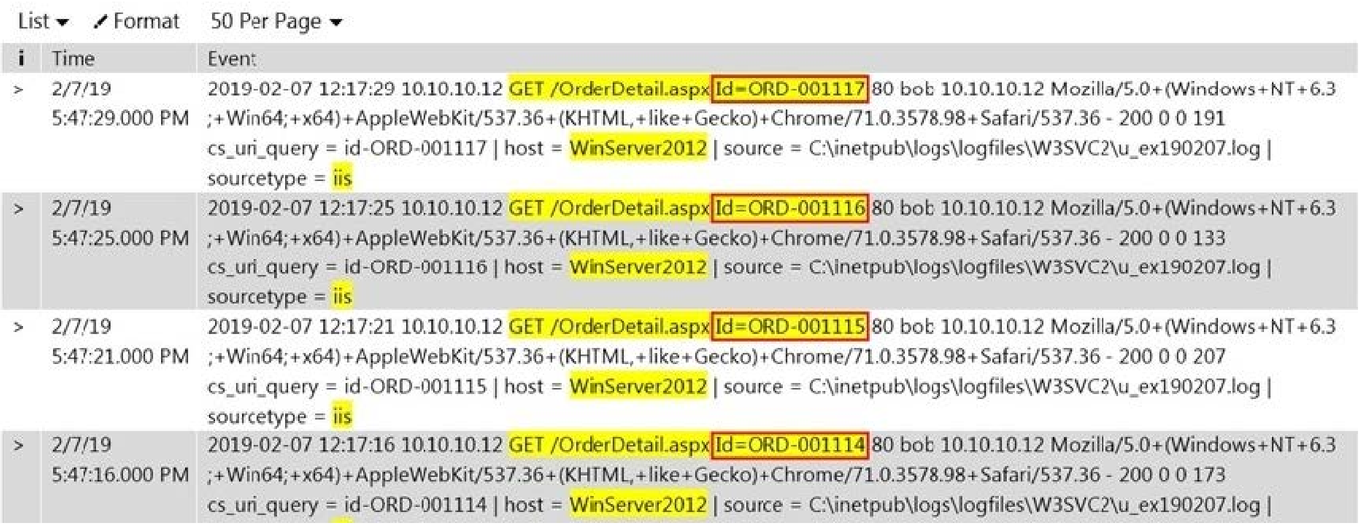
C. She should communicate this incident to the media immediately

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

Correct Answer: B

QUESTION 12

Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.



List ▾ Format 50 Per Page ▾

i	Time	Event

>	2/7/19
	5:47:29.000 PM
		2019-02-07 12:17:29 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001117 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 191
		cs_uri_query = id-ORD-001117 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
		sourcetype = iis

>	2/7/19
	5:47:25.000 PM
		2019-02-07 12:17:25 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001116 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 133
		cs_uri_query = id-ORD-001116 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
		sourcetype = iis

>	2/7/19
	5:47:21.000 PM
		2019-02-07 12:17:21 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001115 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 207
		cs_uri_query = id-ORD-001115 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
		sourcetype = iis

>	2/7/19 5:47:16.000 PM	2019-02-07 12:17:16 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001114 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3 ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 173 cs_uri_query = id-ORD-001114 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |

What does this event log indicate?

A. Directory Traversal Attack

B. XSS Attack

C. SQL Injection Attack

D. Parameter Tampering Attack

Correct Answer: D

Reference: https://infosecwriteups.com/what-is-parameter-tampering-5b1beb12c5ba

QUESTION 13

Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.

Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

A. Threat pivoting

B. Threat trending

C. Threat buy-in

D. Threat boosting

Correct Answer: C

QUESTION 14

What does the HTTP status codes 1XX represents?

A. Informational message

B. Client error

C. Success

D. Redirection

Correct Answer: A

Reference: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#:~:text=1xx%20informational%20response%20?20the%20request,syntax%20or%20cannot%20be%20fulfilled

QUESTION 15

Which of the following can help you eliminate the burden of investigating false positives?

A. Keeping default rules

B. Not trusting the security devices

C. Treating every alert as high level

D. Ingesting the context data

Correct Answer: A

Reference: https://stratozen.com/9-ways-eliminate-siem-false-positives/

312-39 PDF Dumps 312-39 Study Guide 312-39 Exam Questions