Vendor: EC-Council

Exam Code: 312-39

Exam Name: EC-Council Certified SOC Analyst (CSA)

Version: DEMO

QUESTION 1
Which of the following factors determine the choice of SIEM architecture?

A. SMTP Configuration
B. DHCP Configuration
C. DNS Configuration
D. Network Topology

Answer: C

QUESTION 2
What does HTTPS Status code 403 represents?

A. Unauthorized Error
B. Not Found Error
C. Internal Server Error
D. Forbidden Error

Answer: D
Explanation:
https://en.wikipedia.org/wiki/HTTP_403

QUESTION 3
Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

A. 4656
B. 4663
C. 4660
D. 4657

Answer: D
Explanation:
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4657

QUESTION 4
Which of the following are the responsibilities of SIEM Agents?

1. Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
2. Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.
3. Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4. Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

A. 1 and 2
B. 2 and 3
C. 1 and 4

D. 3 and 1

Answer: C

QUESTION 5
Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.

What does this event log indicate?

A. SQL Injection Attack
B. Parameter Tampering Attack
C. XSS Attack
D. Directory Traversal Attack

Answer: A

QUESTION 6
Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

A. COBIT
B. ITIL
C. SSE-CMM
D. SOC-CMM

Answer: C
Explanation:
https://www.iso.org/standard/44716.html

QUESTION 7
What does Windows event ID 4740 indicate?

A. A user account was locked out.
B. A user account was disabled.
C. A user account was enabled.
D. A user account was created.

Answer: A

QUESTION 8
Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS
B. TC Complete
C. Keepnote
D. Apility.io

Answer: A

Explanation:
https://www.esecurityplanet.com/products/threat-intelligence-platforms/

QUESTION 9
A type of threat intelligent that find out the information about the attacker by misleading them is known as _____.

A. Threat trending Intelligence
B. Detection Threat Intelligence
C. Operational Intelligence
D. Counter Intelligence

Answer: C
Explanation:
https://www.recordedfuture.com/threat-intelligence/

QUESTION 10
Chloe, a SOC analyst with Jake Tech, is checking Linux systems logs. She is investigating files at /var/log/ wtmp.

What Chloe is looking at?

A. Error log
B. System boot log
C. General message and system-related stuff
D. Login records

Answer: D
Explanation:
https://stackify.com/linux-logs/

QUESTION 11
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

Answer: A
Explanation:
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)

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**