350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

QUESTION 1

How is a SIEM tool used?

A. To collect security data from authentication failures and cyber attacks and forward it for analysis

B. To search and compare security data against acceptance standards and generate reports for analysis

C. To compare security alerts against configured scenarios and trigger system responses

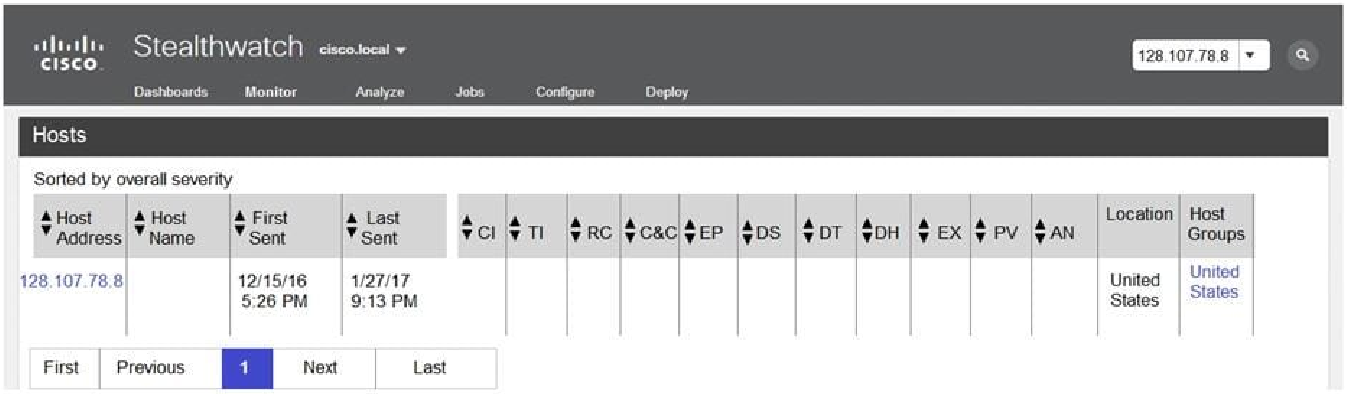
D. To collect and analyze security data from network devices and servers and produce alerts

Correct Answer: D

Reference: https://www.varonis.com/blog/what-is-siem/

QUESTION 2

DRAG DROP



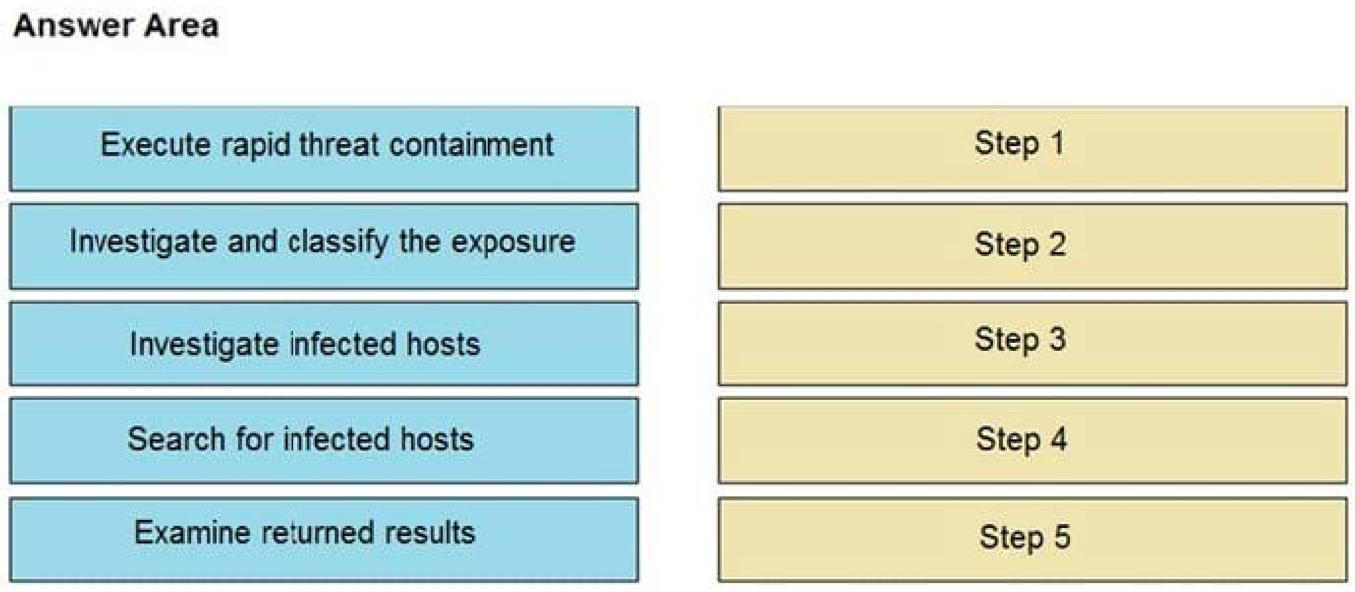
Hosts

Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States

Refer to the exhibit. The Cisco Secure Network Analytics (Stealthwatch) console alerted with “New Malware Server Discovered” and the IOC indicates communication from an end-user desktop to a Zeus CandC Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.

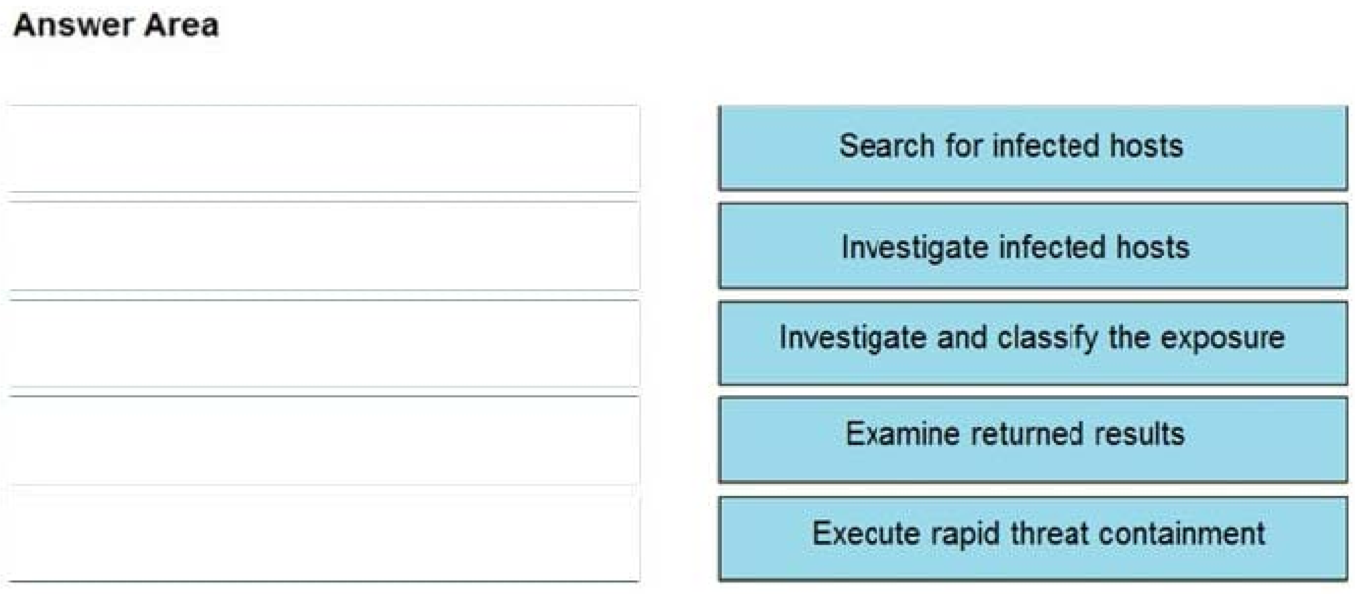
Select and Place:



Answer Area

Execute rapid threat containment	Step 1
Investigate and classify the exposure	Step 2
Investigate infected hosts	Step 3
Search for infected hosts	Step 4
Examine returned results	Step 5

Correct Answer:



Answer Area

	Search for infected hosts
	Investigate infected hosts
	Investigate and classify the exposure
	Examine returned results
	Execute rapid threat containment

QUESTION 3

An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering

B. data regression

C. data ingestion

D. data obfuscation

Correct Answer: A

QUESTION 4

A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

A. HIPAA

B. PCI-DSS

C. Sarbanes-Oxley

D. GDPR

Correct Answer: D

Reference: https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/

QUESTION 5

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

A. Host a discovery meeting and define configuration and policy updates

B. Update the IDS/IPS signatures and reimage the affected hosts

C. Identify the systems that have been affected and tools used to detect the attack

D. Identify the traffic with data capture using Wireshark and review email filters

Correct Answer: C