350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

https://www.pass4itsure.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight.

Which type of compromise is indicated?

A. phishing

B. dumpster diving

C. social engineering

D. privilege escalation

Correct Answer: C

QUESTION 2

What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface

B. to create the logic that triggers alerts when anomalies occur

C. to identify vulnerabilities within an operating system

D. to analyze attacks to identify threat actors and points of entry

Correct Answer: A

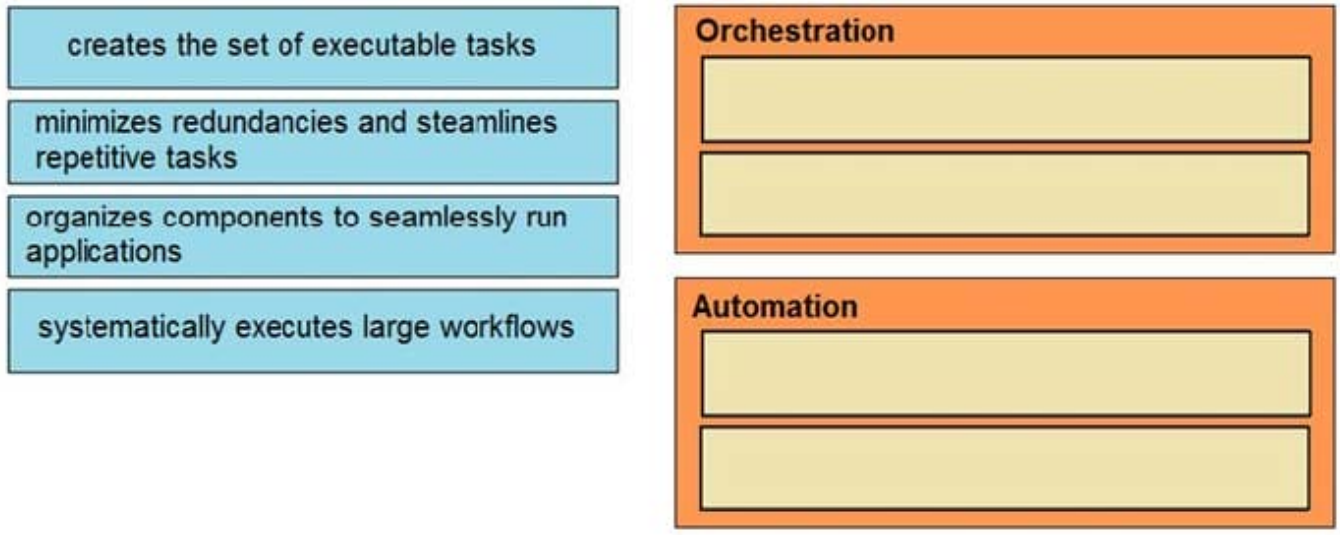
QUESTION 3

DRAG DROP

Drag and drop the function on the left onto the mechanism on the right.

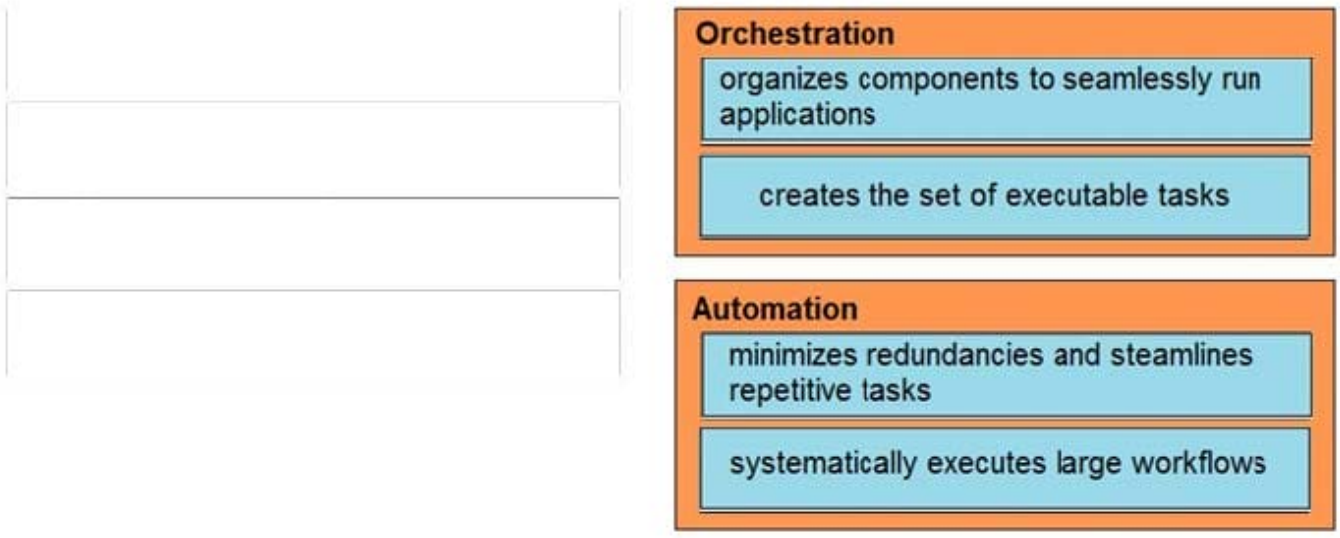
Select and Place:

Answer Area



Correct Answer:

Answer Area



QUESTION 4

What is a benefit of key risk indicators?

A. clear perspective into the risk position of an organization

B. improved visibility on quantifiable information

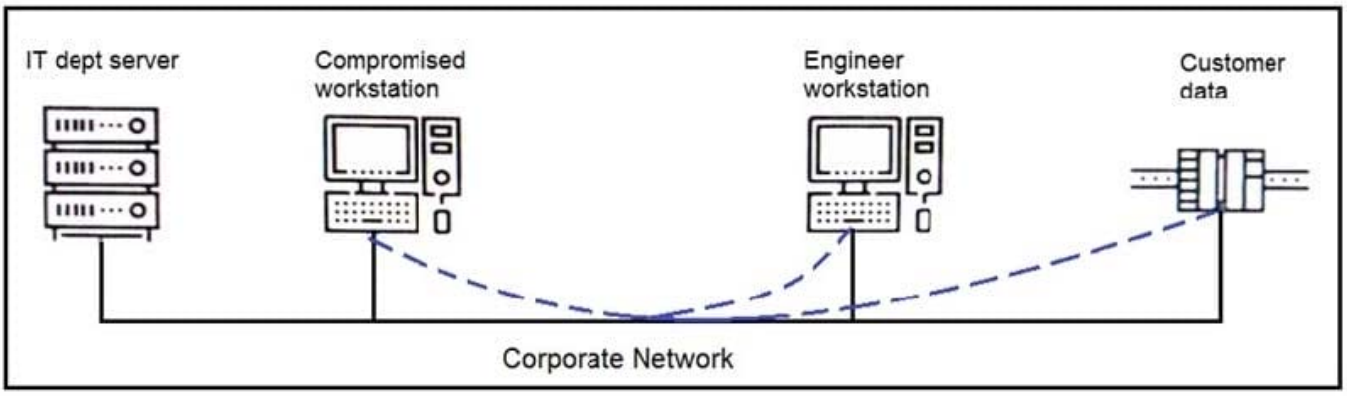
C. improved mitigation techniques for unknown threats

D. clear procedures and processes for organizational risk

Correct Answer: C

Reference: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.

QUESTION 5



Refer to the exhibit. An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols

B. Deploy a SOAR solution and correlate log alerts from customer zones

C. Deploy IDS within sensitive areas and continuously update signatures

D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Correct Answer: A