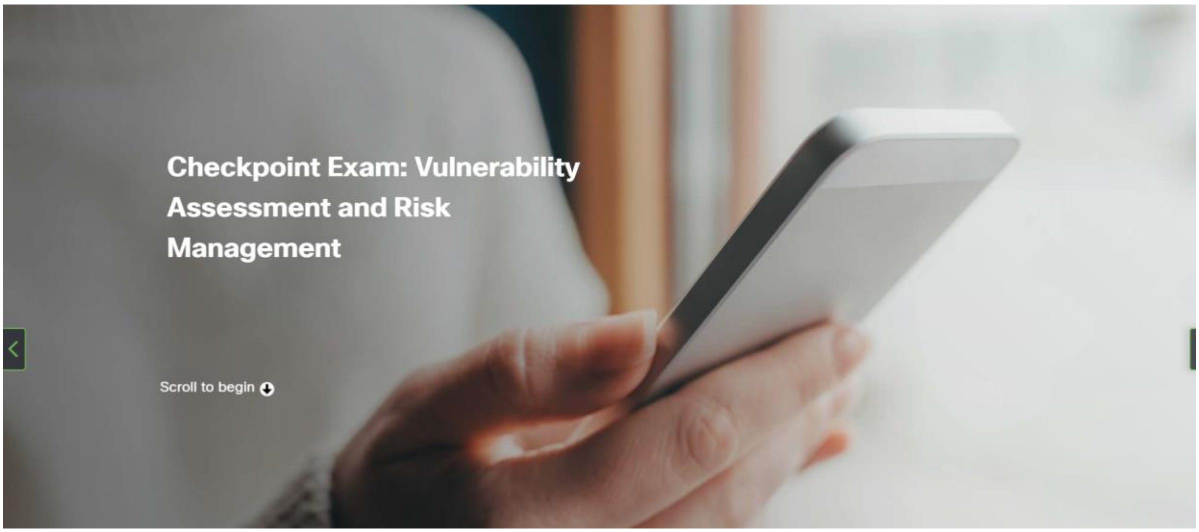
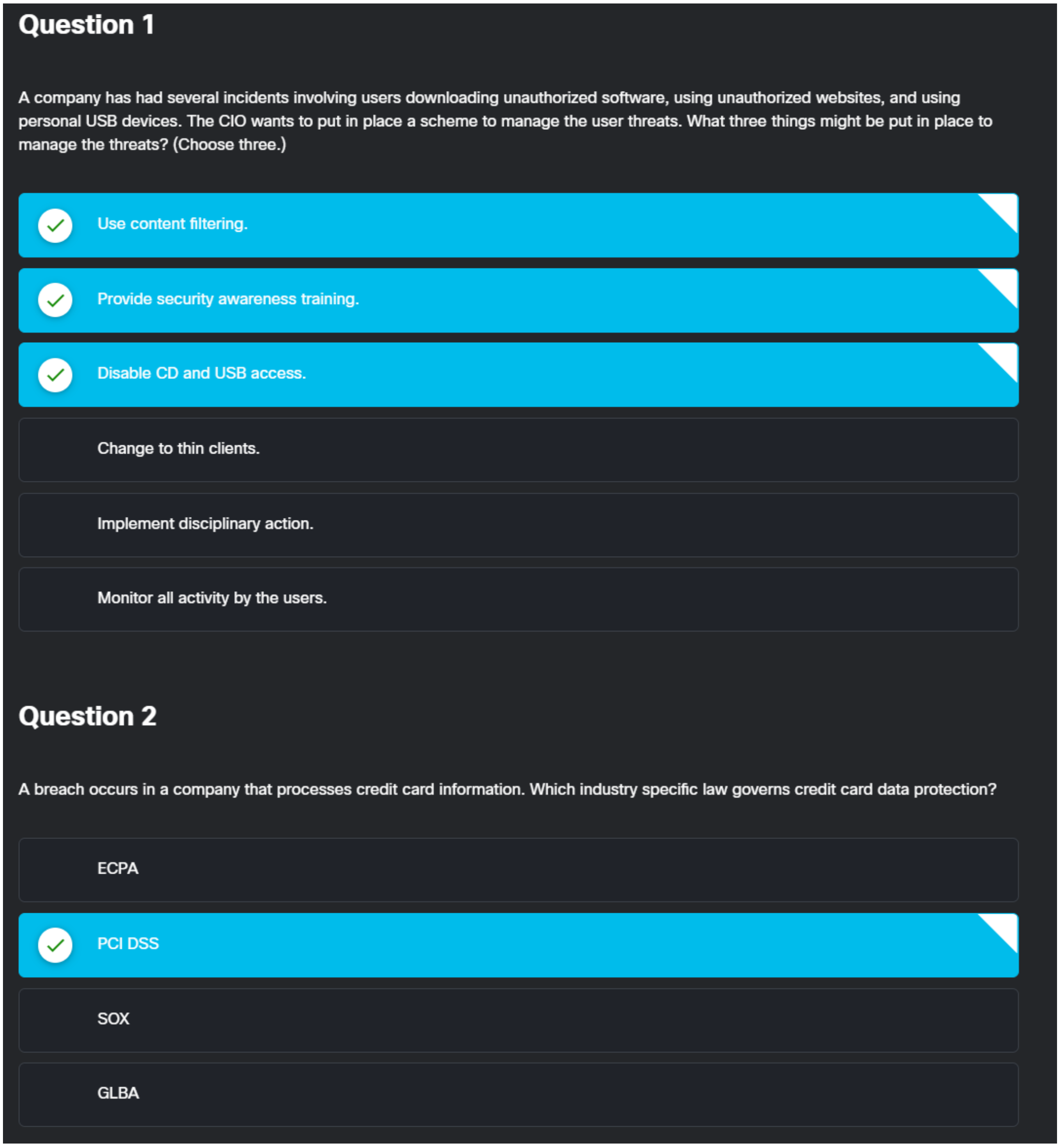
NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Checkpoint Exam: Vulnerability Assessment and Risk Management

Scroll to begin



Question 1

A company has had several incidents involving users downloading unauthorized software, using unauthorized websites, and using personal USB devices. The CIO wants to put in place a scheme to manage the user threats. What three things might be put in place to manage the threats? (Choose three.)

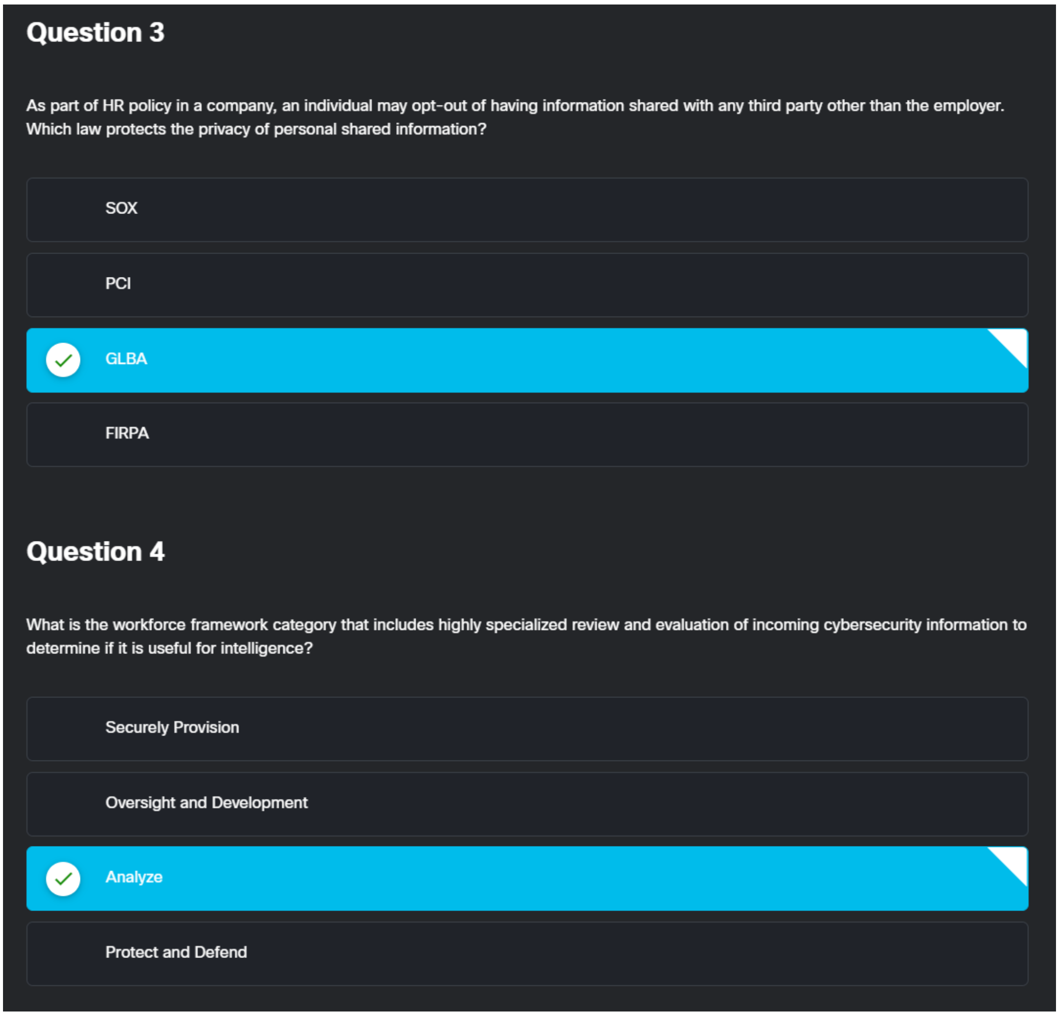
- ✓ Use content filtering.
- ✓ Provide security awareness training.
- ✓ Disable CD and USB access.
- Change to thin clients.
- Implement disciplinary action.
- Monitor all activity by the users.

Question 2

A breach occurs in a company that processes credit card information. Which industry specific law governs credit card data protection?

- ECPA
- ✓ PCI DSS
- SOX
- GLBA

NAMA	: Sasmita Rachmawati
NIM	: 2141762141
Kelas	: SIB-4C
Matkul	: Keamanan Sistem Informasi



Question 3

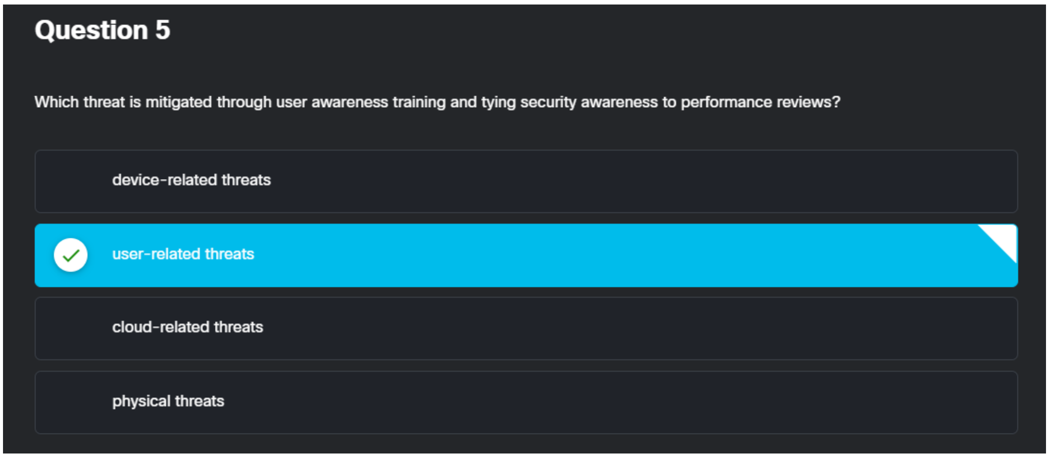
As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?

- SOX
- PCI
- [✓ GLBA]
- FIRPA

Question 4

What is the workforce framework category that includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence?

- Securely Provision
- Oversight and Development
- [✓ Analyze]
- Protect and Defend

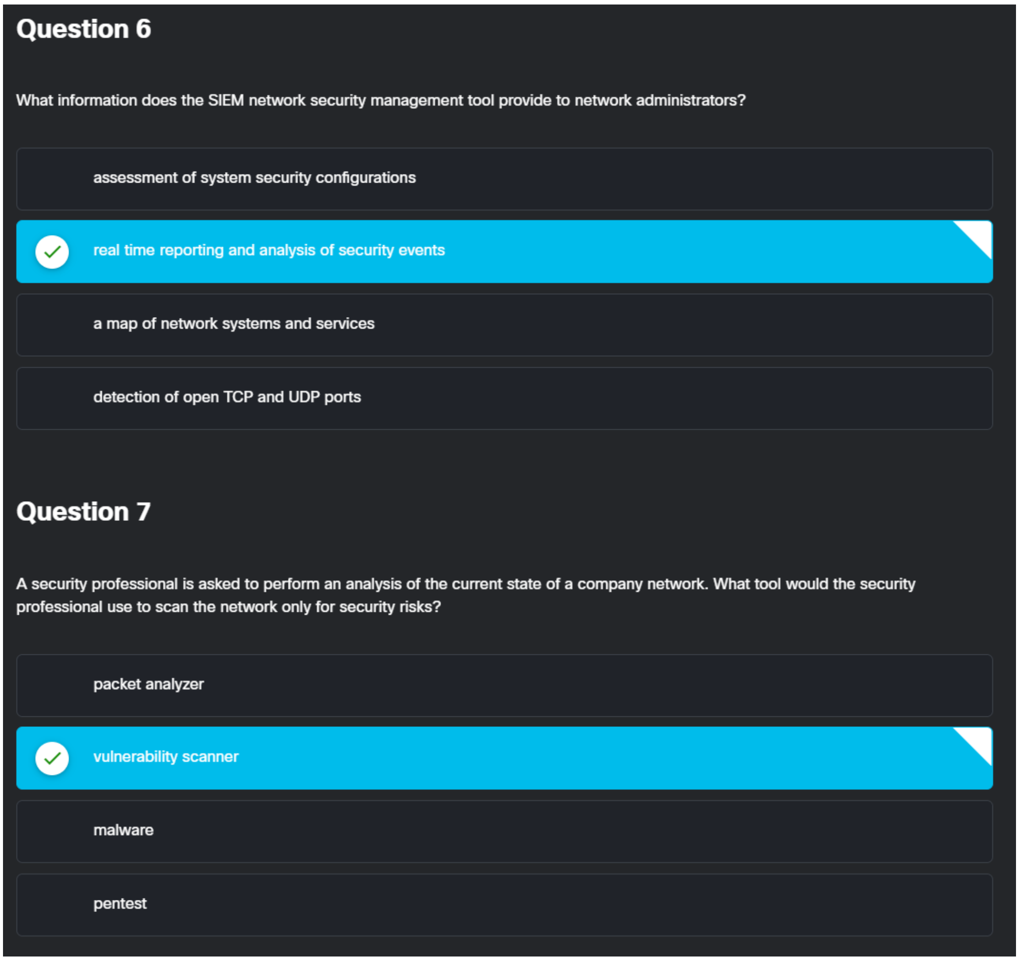


Question 5

Which threat is mitigated through user awareness training and tying security awareness to performance reviews?

- device-related threats
- [✓ user-related threats]
- cloud-related threats
- physical threats

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 6

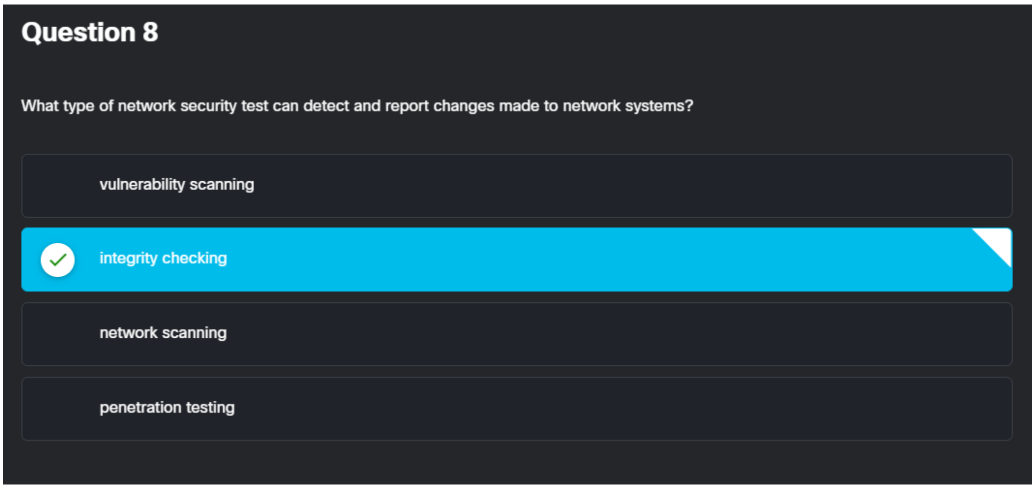
What information does the SIEM network security management tool provide to network administrators?

- assessment of system security configurations
- [✓ real time reporting and analysis of security events]
- a map of network systems and services
- detection of open TCP and UDP ports

Question 7

A security professional is asked to perform an analysis of the current state of a company network. What tool would the security professional use to scan the network only for security risks?

- packet analyzer
- [✓ vulnerability scanner]
- malware
- pentest

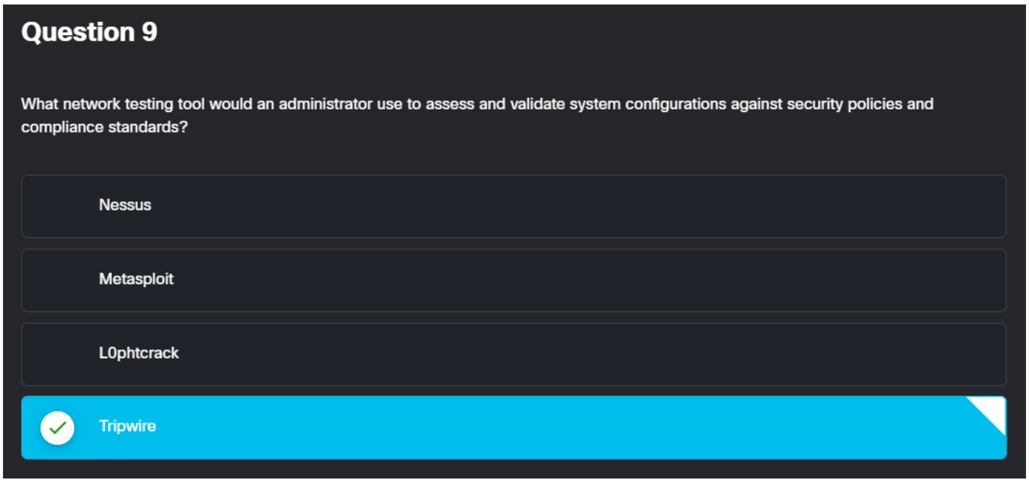


Question 8

What type of network security test can detect and report changes made to network systems?

- vulnerability scanning
- [✓ integrity checking]
- network scanning
- penetration testing

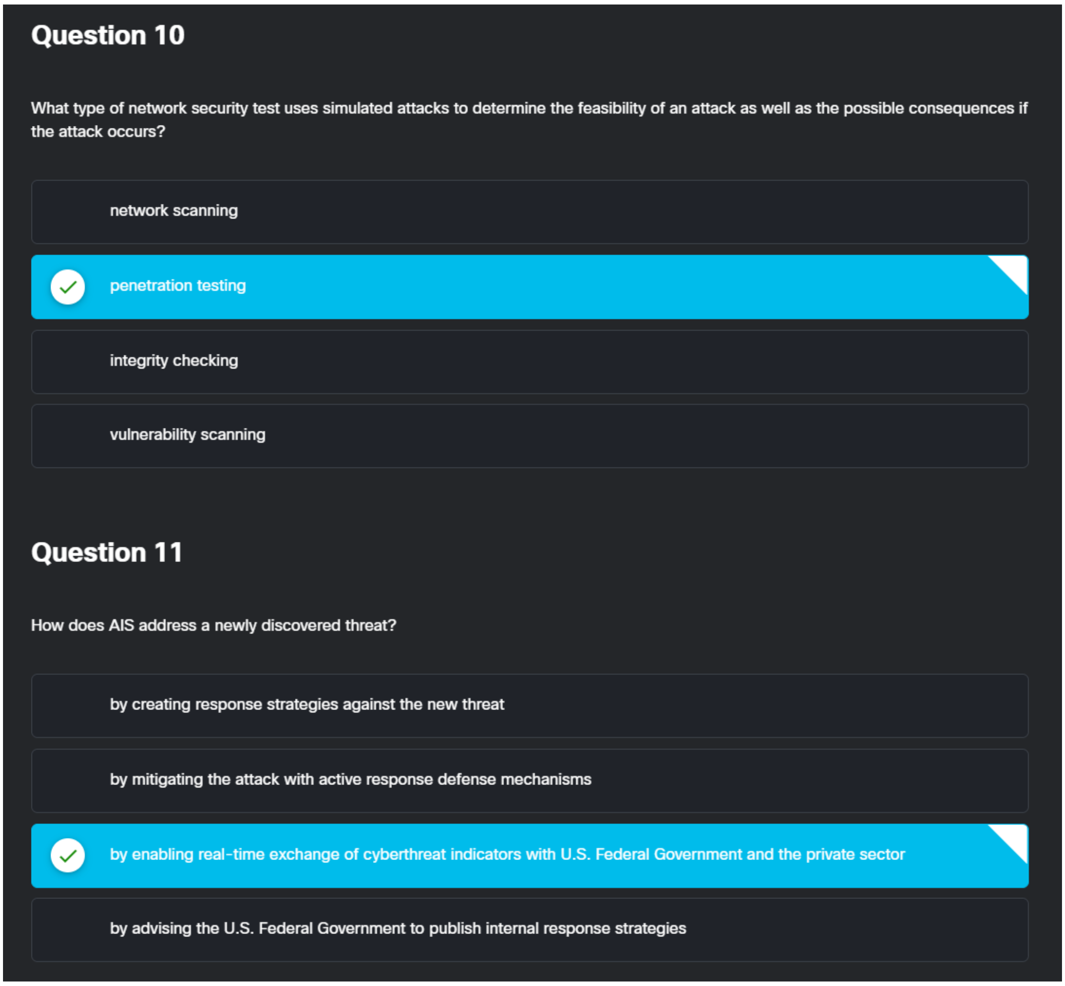
NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 9

What network testing tool would an administrator use to assess and validate system configurations against security policies and compliance standards?

- Nessus
- Metasploit
- L0phtcrack
- ✓ Tripwire



Question 10

What type of network security test uses simulated attacks to determine the feasibility of an attack as well as the possible consequences if the attack occurs?

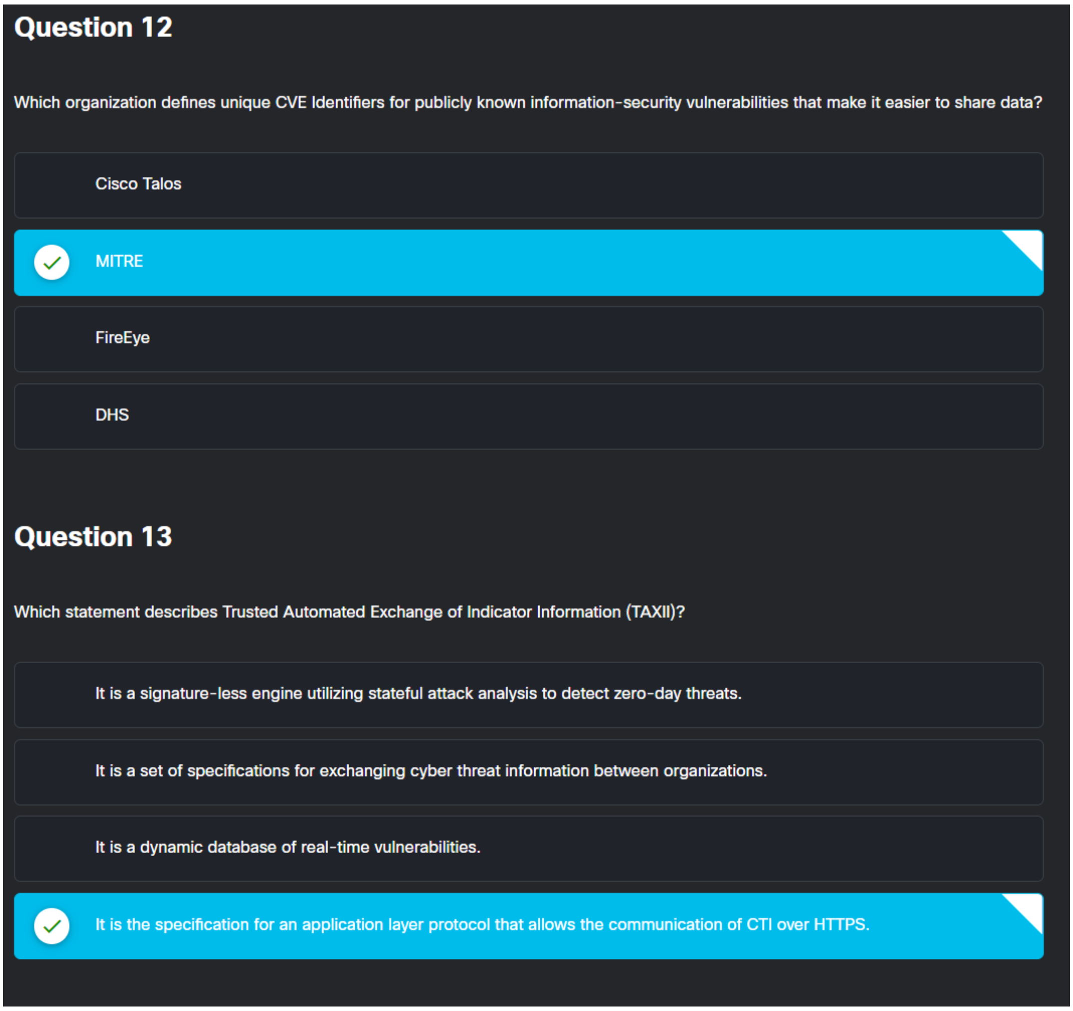
- network scanning
- ✓ penetration testing
- integrity checking
- vulnerability scanning

Question 11

How does AIS address a newly discovered threat?

- by creating response strategies against the new threat
- by mitigating the attack with active response defense mechanisms
- ✓ by enabling real-time exchange of cyberthreat indicators with U.S. Federal Government and the private sector
- by advising the U.S. Federal Government to publish internal response strategies

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 12

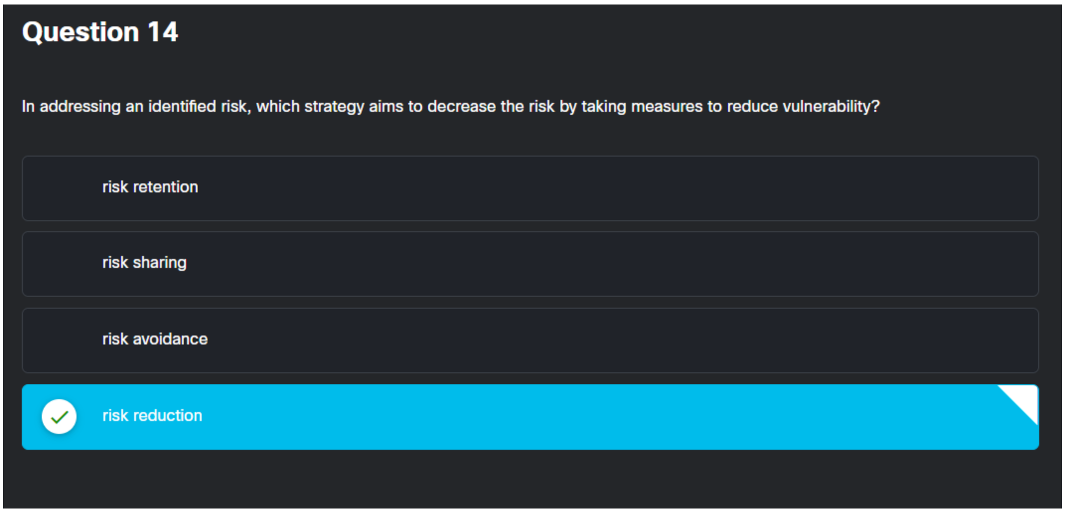
Which organization defines unique CVE Identifiers for publicly known information-security vulnerabilities that make it easier to share data?

- Cisco Talos
- ✓ MITRE
- FireEye
- DHS

Question 13

Which statement describes Trusted Automated Exchange of Indicator Information (TAXII)?

- It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.
- It is a set of specifications for exchanging cyber threat information between organizations.
- It is a dynamic database of real-time vulnerabilities.
- ✓ It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.

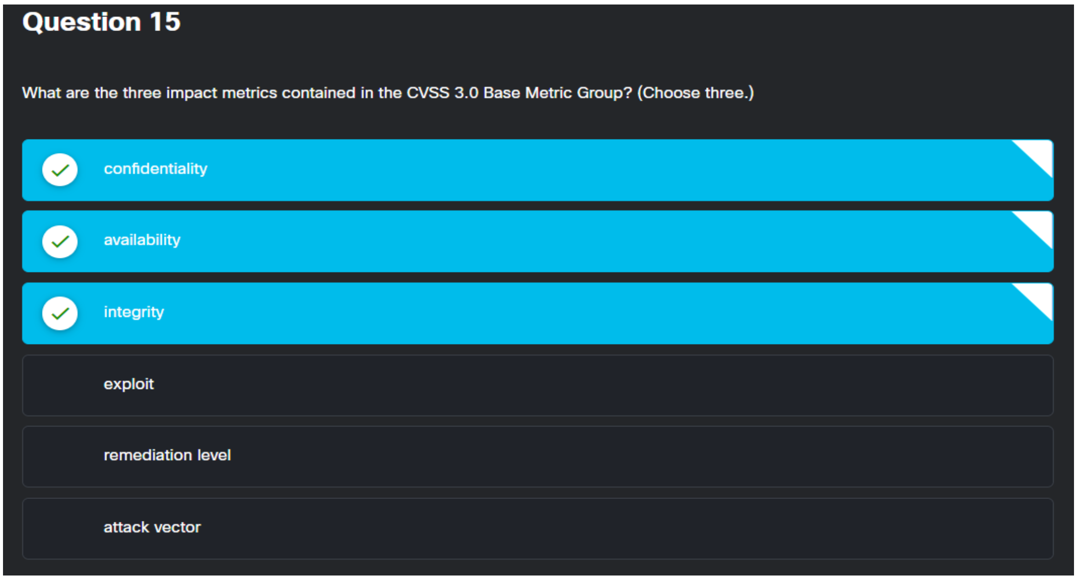


Question 14

In addressing an identified risk, which strategy aims to decrease the risk by taking measures to reduce vulnerability?

- risk retention
- risk sharing
- risk avoidance
- ✓ risk reduction

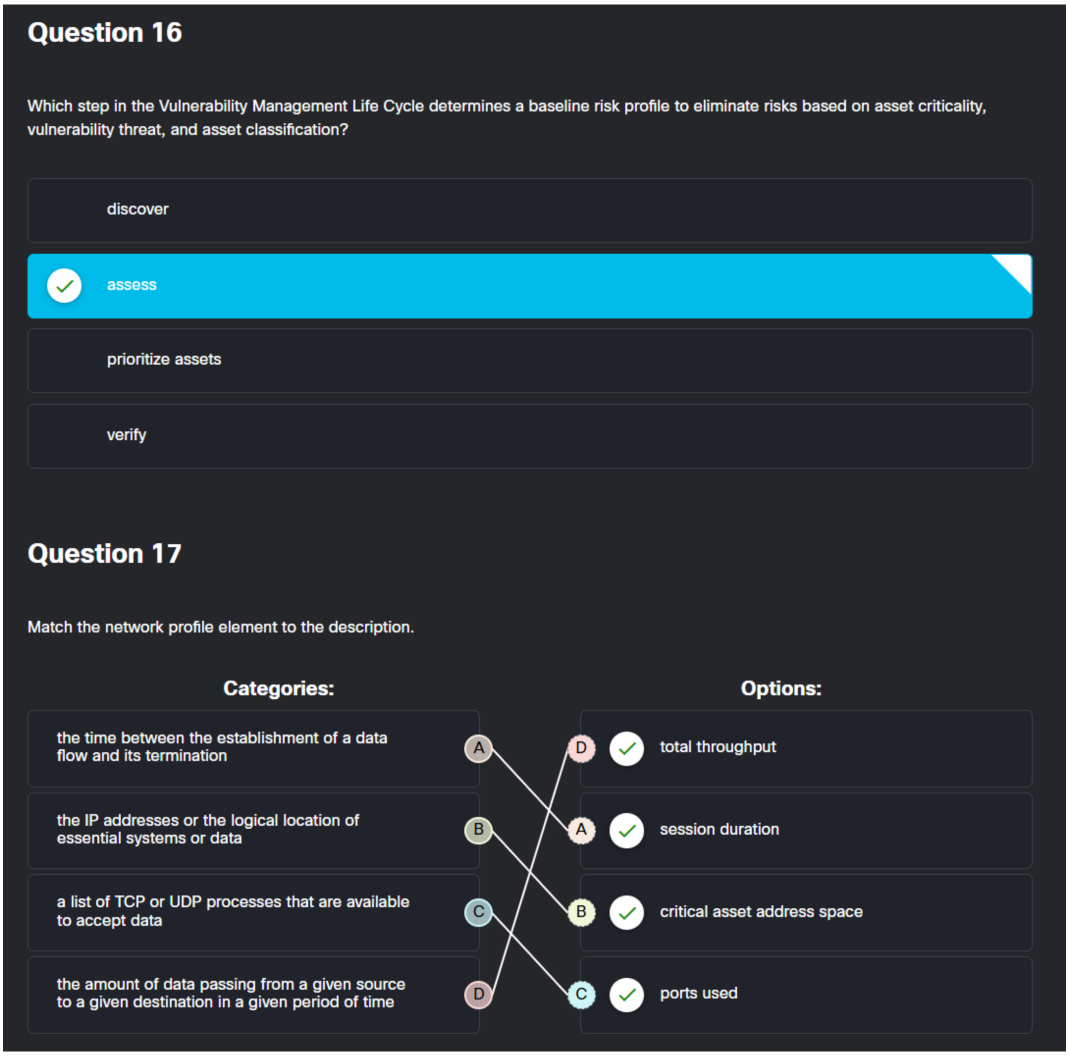
NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 15

What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)

- ✓ confidentiality
- ✓ availability
- ✓ integrity
- exploit
- remediation level
- attack vector



Question 16

Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

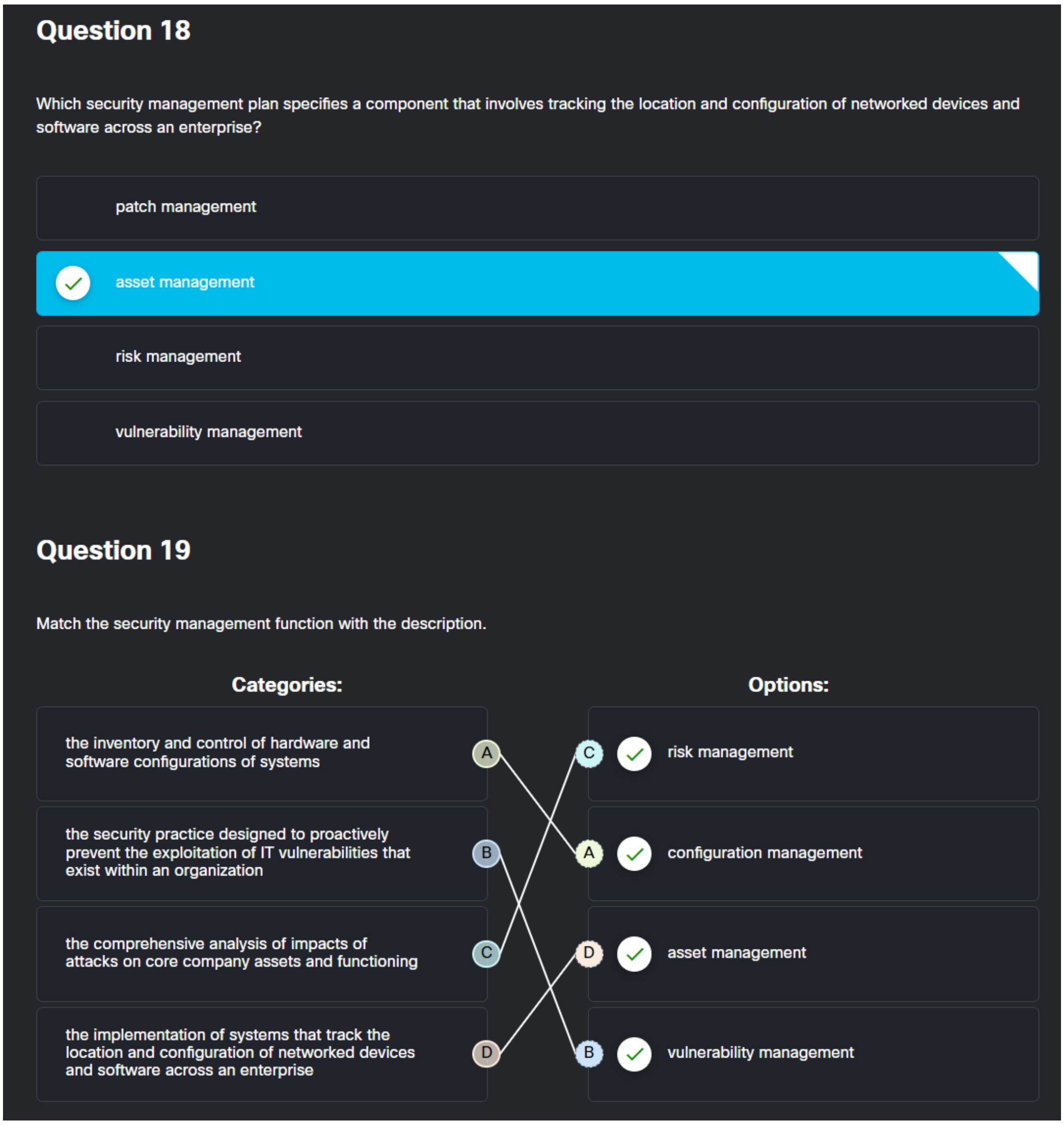
- discover
- ✓ assess
- prioritize assets
- verify

Question 17

Match the network profile element to the description.

Categories:			Options:
the time between the establishment of a data flow and its termination	A	D	✓ total throughput
the IP addresses or the logical location of essential systems or data	B	A	✓ session duration
a list of TCP or UDP processes that are available to accept data	C	B	✓ critical asset address space
the amount of data passing from a given source to a given destination in a given period of time	D	C	✓ ports used

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 18

Which security management plan specifies a component that involves tracking the location and configuration of networked devices and software across an enterprise?

patch management

[✓ asset management]

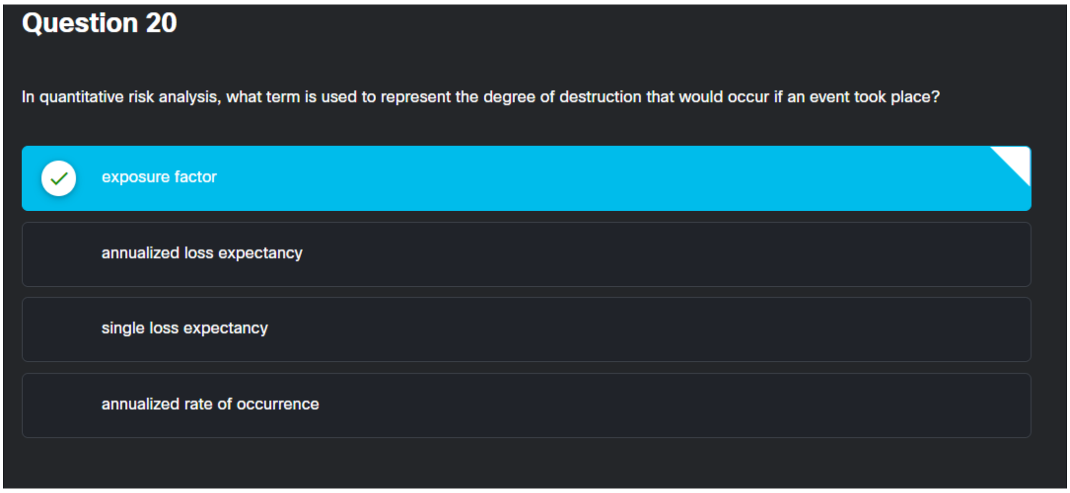
risk management

vulnerability management

Question 19

Match the security management function with the description.

Categories:			Options:
the inventory and control of hardware and software configurations of systems	A	C	✓ risk management
the security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization	B	A	✓ configuration management
the comprehensive analysis of impacts of attacks on core company assets and functioning	C	D	✓ asset management
the implementation of systems that track the location and configuration of networked devices and software across an enterprise	D	B	✓ vulnerability management



Question 20

In quantitative risk analysis, what term is used to represent the degree of destruction that would occur if an event took place?

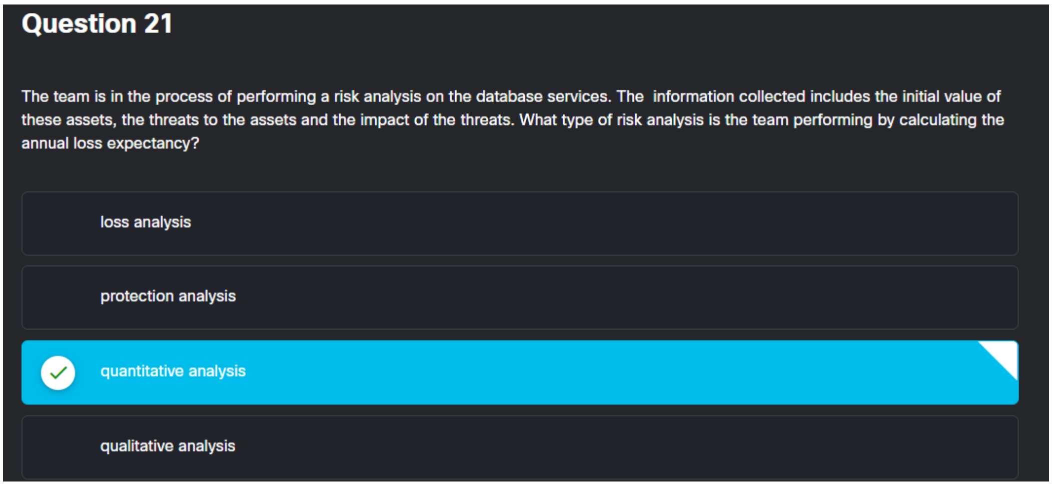
[✓ exposure factor]

annualized loss expectancy

single loss expectancy

annualized rate of occurrence

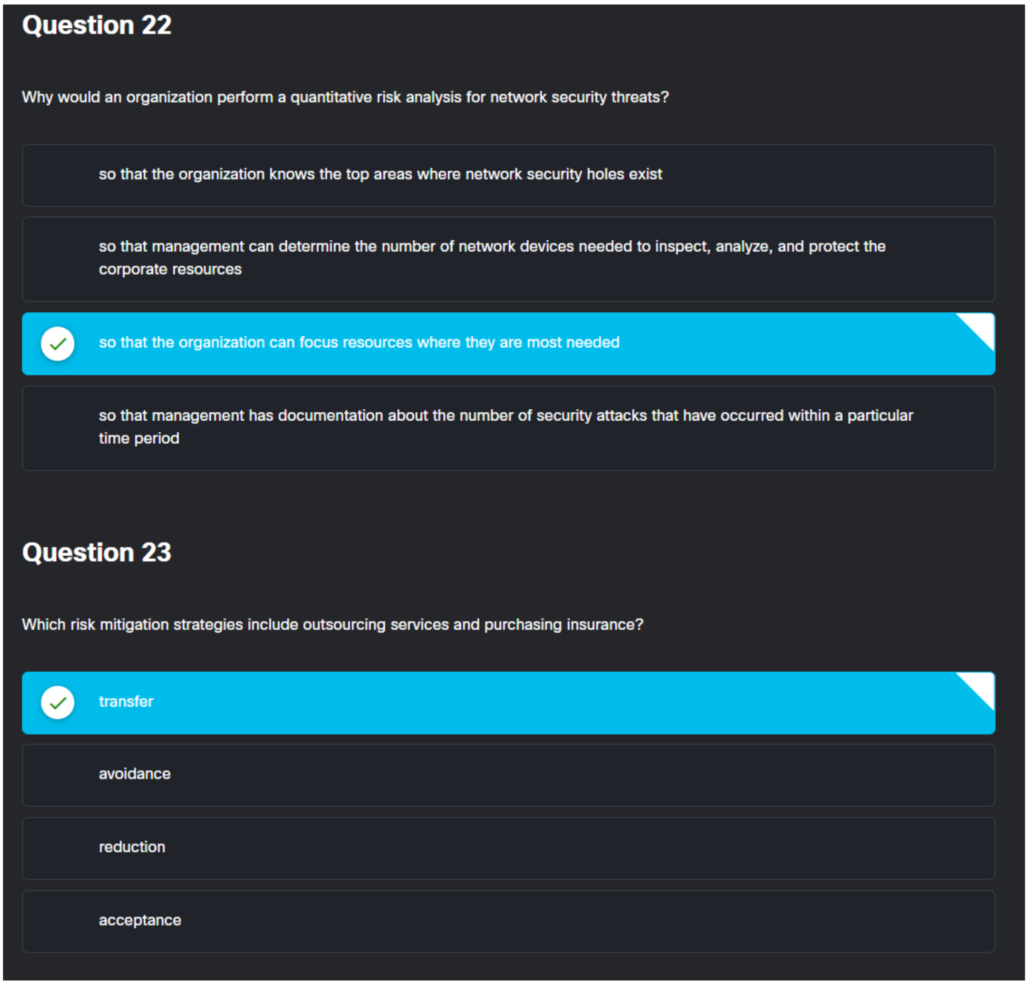
NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 21

The team is in the process of performing a risk analysis on the database services. The information collected includes the initial value of these assets, the threats to the assets and the impact of the threats. What type of risk analysis is the team performing by calculating the annual loss expectancy?

- loss analysis
- protection analysis
- ✓ quantitative analysis
- qualitative analysis



Question 22

Why would an organization perform a quantitative risk analysis for network security threats?

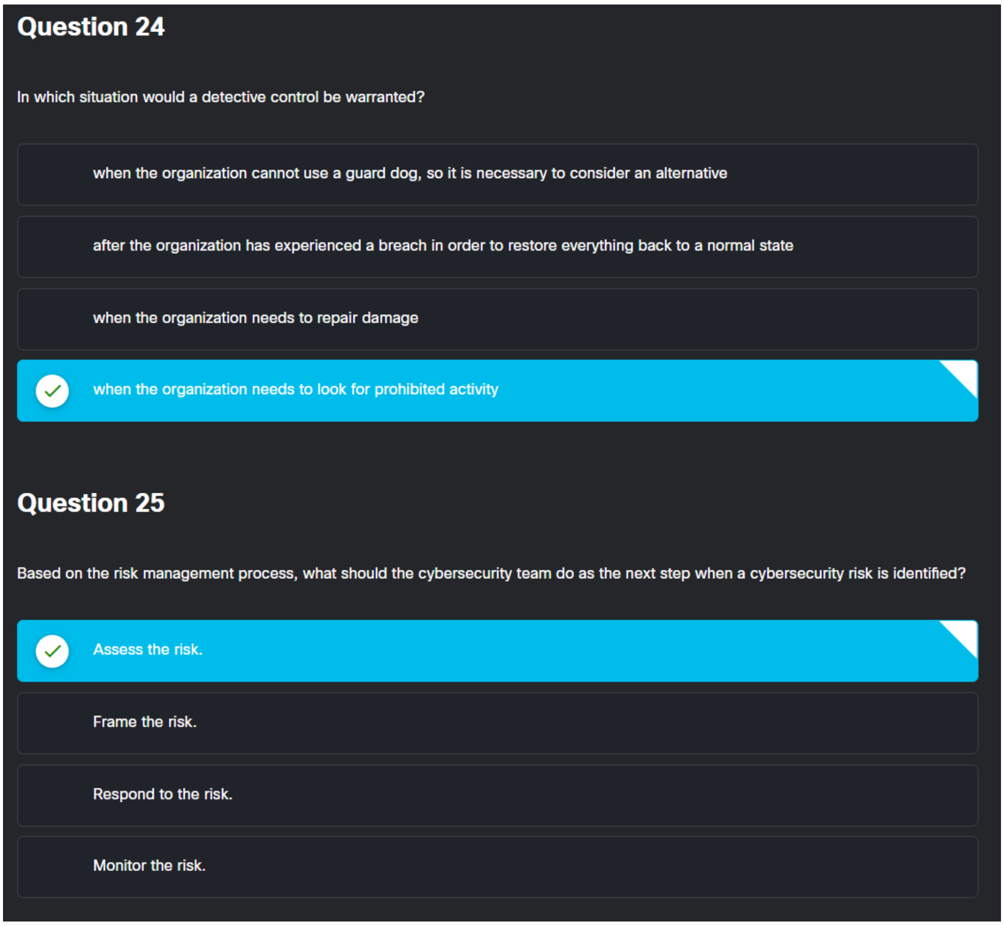
- so that the organization knows the top areas where network security holes exist
- so that management can determine the number of network devices needed to inspect, analyze, and protect the corporate resources
- ✓ so that the organization can focus resources where they are most needed
- so that management has documentation about the number of security attacks that have occurred within a particular time period

Question 23

Which risk mitigation strategies include outsourcing services and purchasing insurance?

- ✓ transfer
- avoidance
- reduction
- acceptance

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 24

In which situation would a detective control be warranted?

- when the organization cannot use a guard dog, so it is necessary to consider an alternative
- after the organization has experienced a breach in order to restore everything back to a normal state
- when the organization needs to repair damage
- ✓ when the organization needs to look for prohibited activity

Question 25

Based on the risk management process, what should the cybersecurity team do as the next step when a cybersecurity risk is identified?

- ✓ Assess the risk.
- Frame the risk.
- Respond to the risk.
- Monitor the risk.