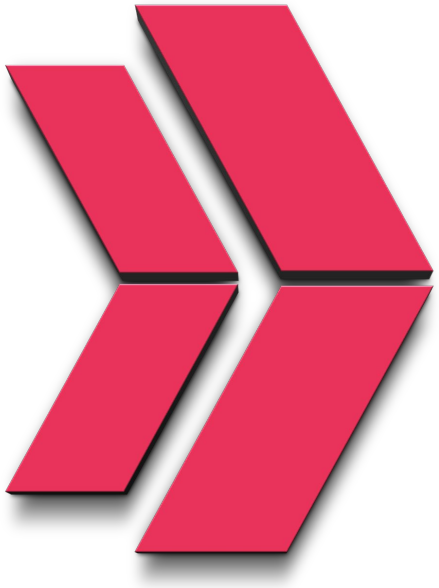


CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (12A-12B-12C-12D)

AGENDA

- 12A - Incident Response (12)
- 12B - Digital Forensics (5)
- 12C - Data Sources (5)
- 12D - Alerting and Monitoring Tools (7)
- TOTAL: 29

12A - Incident Response

12A - Incident Response

NO.1 A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

(A). Set the maximum data retention policy

(B). Securely store the documents on an air-gapped network

(C). Review the documents' data classification policy

(D). Conduct a tabletop exercise with the team

12A - Incident Response

NO.1 A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

(A). Set the maximum data retention policy

(B). Securely store the documents on an air-gapped network

(C). Review the documents' data classification policy

(D). Conduct a tabletop exercise with the team

12A - Incident Response

NO.2 Which of the following is required for an organization to properly manage its restore process in the event of system failure?

(A). IRP

(B). DRP

(C). RPO

(D). SDLC

12A - Incident Response

NO.2 Which of the following is required for an organization to properly manage its restore process in the event of system failure?

(A). IRP

(B). DRP

(C). RPO

(D). SDLC

12A - Incident Response

NO.3 A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

(A). Digital forensics

(B). E-discovery

(C). Incident response

(D). Threat hunting

12A - Incident Response

NO.3 A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

(A). Digital forensics

(B). E-discovery

(C). Incident response

(D). Threat hunting

12A - Incident Response

NO.4 Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

(A). Preparation

(B). Recovery

(C). Lessons learned

(D). Analysis

12A - Incident Response

NO.4 Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

(A). Preparation

(B). Recovery

(C). Lessons learned

(D). Analysis

12A - Incident Response

NO.5 Which of the following describes the reason root cause analysis should be conducted as part of incident response?

(A). To gather loCs for the investigation

(B). To discover which systems have been affected

(C). To eradicate any trace of malware on the network

(D). To prevent future incidents of the same nature

12A - Incident Response

NO.5 Which of the following describes the reason root cause analysis should be conducted as part of incident response?

(A). To gather loCs for the investigation

(B). To discover which systems have been affected

(C). To eradicate any trace of malware on the network

(D). To prevent future incidents of the same nature

12A - Incident Response

NO.6 Which of the following should a security operations center use to improve its incident response procedure?

A. Playbooks
B. Frameworks
C. Baselines
D. Benchmarks

12A - Incident Response

NO.6 Which of the following should a security operations center use to **improve its incident response procedure?**

A. Playbooks
B. Frameworks
C. Baselines
D. Benchmarks

12A - Incident Response

NO.7 Which of the following is the final step of the incident response process?

A. Lessons learned
B. Eradication
C. Containment
D. Recovery

12A - Incident Response

NO.7 Which of the following is the **final step of the incident response process?**

A. Lessons learned
B. Eradication
C. Containment
D. Recovery

12A - Incident Response

NO.8 A cybersecurity incident response team at a large company receives notification that malware is present on several corporate desktops. No known indicators of compromise have been found on the network.

Which of the following should the team do first to secure the environment?
A. Contain the impacted hosts
B. Add the malware to the application blocklist.
C. Segment the core database server.
D. Implement firewall rules to block outbound beaconing

12A - Incident Response

NO.8 A cybersecurity incident response team at a large company receives notification that malware is present on several corporate desktops. No known indicators of compromise have been found on the network.

Which of the following should the team **do first to secure the environment?**

A. Contain the impacted hosts

B. Add the malware to the application blocklist.

C. Segment the core database server.

D. Implement firewall rules to block outbound beaconing

12A - Incident Response

NO.9 Which of the following phases of an incident response involves generating reports?

A. Recovery
B. Preparation
C. Lessons learned
D. Containment

12A - Incident Response

NO.9 Which of the following phases of an incident response involves **generating reports?**

A. Recovery
B. Preparation
C. Lessons learned
D. Containment

12A - Incident Response

NO.10 Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation
B. Recovery
C. Lessons learned
D. Analysis

12A - Incident Response

NO.10 Which of the following is the phase in the incident response process when a security analyst **reviews roles and responsibilities?**

A. Preparation
B. Recovery
C. Lessons learned
D. Analysis

12A - Incident Response

NO.11 Which of the following is the most effective way to protect an application server running software that is no longer supported from network threats?

A. Air gap
B. Barricade
C. Port security
D. Screen subnet

12A - Incident Response

NO.11 Which of the following is the most effective way to protect an application server running software that is **no longer supported from network threats?**

A. Air gap
B. Barricade
C. Port security
D. Screen subnet

12A - Incident Response

NO.12 Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

A. SLA
B. MOU
C. MOA
D. BPA

12A - Incident Response

NO.12 Which of the following describes the understanding between a company and a client about what will be provided and the **accepted time needed to provide the company with the resources?**

A. SLA
B. MOU
C. MOA
D. BPA

12B - Digital Forensics

12B - Digital Forensics

NO.1 Which of the following allows for the attribution of messages to individuals?

(A). Adaptive identity

(B). Non-repudiation

(C). Authentication

(D). Access logs

12B - Digital Forensics

NO.1 Which of the following allows for the attribution of messages to individuals?

(A). Adaptive identity

(B). Non-repudiation

(C). Authentication

(D). Access logs

12B - Digital Forensics

NO.2 During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

(A). Analysis

(B). Lessons learned

(C). Detection

(D). Containment

12B - Digital Forensics

NO.2 During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

(A). Analysis

(B). Lessons learned

(C). Detection

(D). Containment

12B - Digital Forensics

NO.3 Which of the following incident response activities ensures evidence is properly handied?

(A). E-discovery

(B). Chain of custody

(C). Legal hold

(D). Preservation

12B - Digital Forensics

NO.3 Which of the following incident response activities ensures evidence is properly handied?

(A). E-discovery

(B). Chain of custody

(C). Legal hold

(D). Preservation

12B - Digital Forensics

NO.4 After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

(A). Retain the emails between the security team and affected customers for 30 days
(B). Retain any communications related to the security breach until further notice
(C). Retain any communications between security members during the breach response
(D). Retain all emails from the company to affected customers for an indefinite period of time

12B - Digital Forensics

NO.4 After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

(A). Retain the emails between the security team and affected customers for 30 days

(B). Retain any communications related to the security breach until further notice

(C). Retain any communications between security members during the breach response

(D). Retain all emails from the company to affected customers for an indefinite period of time

12B - Digital Forensics

NO.5 Which of the following is a reason why a forensic specialist would create a plan to preserve data after an incident and prioritize the sequence for performing forensic analysis?

A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold

12B - Digital Forensics

NO.5 Which of the following is a reason why a forensic specialist would create a plan to **preserve data after an incident and prioritize the sequence** for performing forensic analysis?

A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold

12C - Data Sources

12C - Data Sources

NO.1 A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

(A). Obtain the file's SHA-256 hash

(B). Use hexdump on the file's contents

(C). Check endpoint logs

(D). Query the file's metadata

12C - Data Sources

NO.1 A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

(A). Obtain the file's SHA-256 hash

(B). Use hexdump on the file's contents

(C). Check endpoint logs

(D). Query the file's metadata

12C - Data Sources

NO.2 A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

(A). Logging all NetFlow traffic into a SIEM

(B). Deploying network traffic sensors on the same subnet as the servers

(C). Logging endpoint and OS-specific security logs

(D). Enabling full packet capture for traffic entering and exiting the servers

12C - Data Sources

NO.2 A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

(A). Logging all NetFlow traffic into a SIEM

(B). Deploying network traffic sensors on the same subnet as the servers

(C). Logging endpoint and OS-specific security logs

(D). Enabling full packet capture for traffic entering and exiting the servers

12C - Data Sources

NO.3 A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

(A). Packet captures

(B). Vulnerability scans

(C). Metadata

(D). Dashboard

12C - Data Sources

NO.3 A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

(A). Packet captures

(B). Vulnerability scans

(C). Metadata

(D). Dashboard

12C - Data Sources

NO.4 A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation.

Which of the following logs should the analyst use as a data source?

(A). Application

(B). IPS/IDS

(C). Network

(D). Endpoint

12C - Data Sources

NO.4 A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation.

Which of the following logs should the analyst use as a data source?

(A). Application

(B). IPS/IDS

(C). Network

(D). Endpoint

12C - Data Sources

NO.5 An analyst is reviewing an incident in which a user clicked on a link in a phishing email.

Which of the following log sources would the analyst utilize to determine whether the connection was successful?

A. Network
B. System
C. Application
D. Authentication

12C - Data Sources

NO.5 An analyst is reviewing an incident in which a **user clicked on a link in a phishing email.**

Which of the following log sources would the analyst utilize to determine whether the connection was successful?

A. Network
B. System
C. Application
D. Authentication

12D - Alerting and Monitoring Tools

12D - Alerting and Monitoring Tools

NO.1 A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

(A). Tuning

(B). Aggregating

(C). Quarantining

(D). Archiving

12D - Alerting and Monitoring Tools

NO.1 A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

(A). Tuning

(B). Aggregating

(C). Quarantining

(D). Archiving

12D - Alerting and Monitoring Tools

NO.2 Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

(A). SIEM

(B). DLP

(C). IDS

(D). SNMP

12D - Alerting and Monitoring Tools

NO.2 Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

(A). SIEM

(B). DLP

(C). IDS

(D). SNMP

12D - Alerting and Monitoring Tools

NO.3 Which of the following best describes configuring devices to log to an off-site location for possible future reference?

A. Log aggregation
B. DLP
C. Archiving
D. SCAP

12D - Alerting and Monitoring Tools

NO.3 Which of the following best describes configuring devices to **log to an off-site location** for possible future reference?

A. Log aggregation
B. DLP
C. Archiving
D. SCAP

12D - Alerting and Monitoring Tools

NO.4 An organization is required to maintain financial data records for three years and customer data for five years.

Which of the following data management policies should the organization implement?

A. Retention
B. Destruction
C. Inventory
D. Certification

12D - Alerting and Monitoring Tools

NO.4 An organization is required to **maintain financial data records for three years** and **customer data for five years.**

Which of the following data management policies should the organization implement?

A. Retention
B. Destruction
C. Inventory
D. Certification

12D - Alerting and Monitoring Tools

NO.5 The Chief Information Security Officer wants to put security measures in place to protect PII. The organization needs to use its existing labeling and classification system to accomplish this goal.

Which of the following would most likely be configured to meet the requirements?
A. Tokenization
B. S/MIME
C. DLP
D. MFA

12D - Alerting and Monitoring Tools

NO.5 The Chief Information Security Officer wants to put security measures in place to **protect PII**. The organization needs to use its existing labeling and classification system to accomplish this goal.

Which of the following would most likely be configured to meet the requirements?
A. Tokenization
B. S/MIME
C. DLP
D. MFA

12D - Alerting and Monitoring Tools

NO.6 An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment.

Which of the following solutions would mitigate the risk?
A. XDR
B. SPF
C. DLP
D. DMARC

12D - Alerting and Monitoring Tools

NO.6 An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that **sensitive data could be exfiltrated** from the environment.

Which of the following solutions would mitigate the risk?

A. XDR

B. SPF

C. DLP

D. DMARC

12D - Alerting and Monitoring Tools

NO.7 A growing company would like to enhance the ability of its security operations center to detect threats but **reduce the amount of manual work** required to the security analysts.

Which of the following would best enable the reduction in manual work?

A. SOAR

B. SIEM

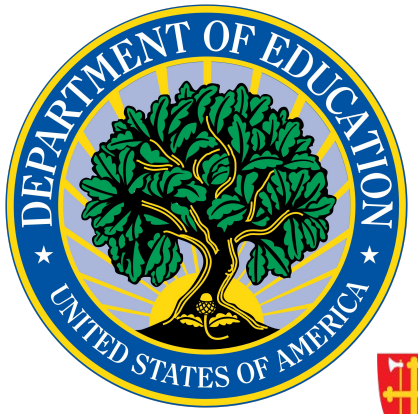
C. MDM

D. DLP

THANKS!

Any questions?

Our Graduates are Hired By



Google

Deloitte.

AT&T

ally
do it right.

DEN NORSKE KIRKE
Kirkepartner

Robinhood

VIZNET

COMCAST

INSPARK

ING BANK

proValus

SOCRadar®
Extension to Your SOC Team!

AGILIS
TECHNOLOGIES

Humana
Wellness

EQUANS

BBS

BGA
SECURITY

gravity
IT RESOURCES

GetMoneyGlobal

proximus

northramp

ease
LEARNING