QUESTION 215

A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?

A. Hacktivist
B. Organized crime
C. Insider threat
D. Nation-state

Correct Answer: D

QUESTION 216

The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network. Which of the following would work BEST to prevent the issue?

A. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
B. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.

Correct Answer: A

QUESTION 217

A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

A. Implement a virtual machine alternative.
B. Develop a new secured browser.
C. Configure a personal business VLAN.
D. Install kiosks throughout the building.

Correct Answer: C

QUESTION 218

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

A. Pyramid of Pain
B. MITRE ATT&CK

C. Diamond Model of Intrusion Analysts
D. CVSS v3.0

Correct Answer: B

QUESTION 219
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds. Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating datA.

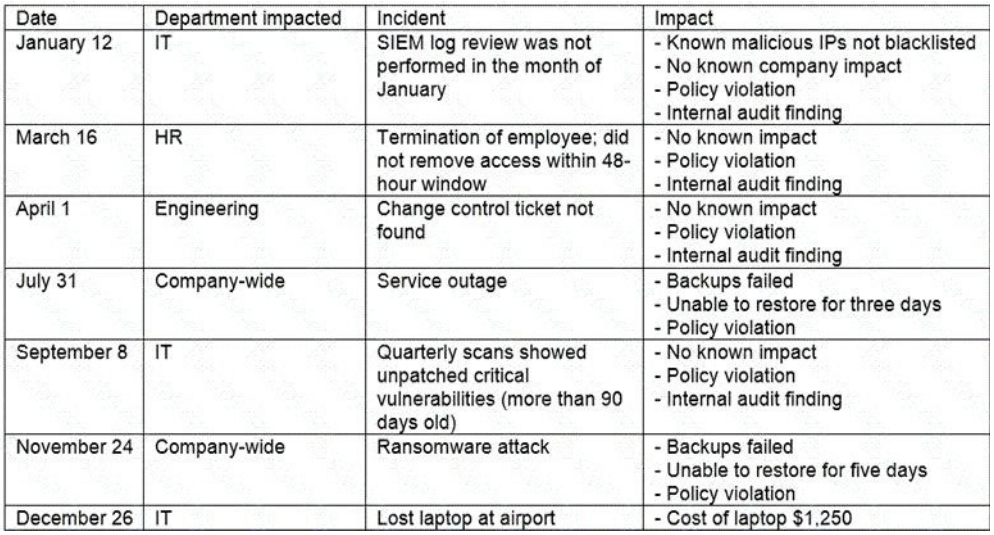
Correct Answer: D

QUESTION 220
A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

A. Dissemination
B. Analysis
C. Feedback
D. Requirements
E. Collection

Correct Answer: E

QUESTION 221
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues. The steering committee wants to rank the risks based on past incidents to improve the security program for next year. Below is the incident register for the organization.



Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop $1,250

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?

A. Hire a managed service provider to help with vulnerability management
B. Build a warm site in case of system outages
C. Invest in a failover and redundant system, as necessary
D. Hire additional staff for the IT department to assist with vulnerability management and log review

Correct Answer: C
Explanation:
Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

QUESTION 222
Understanding attack vectors and integrating intelligence sources are important components of:

A. proactive threat hunting
B. risk management compliance.
C. a vulnerability management plan.
D. an incident response plan.
Correct Answer: C

QUESTION 223
A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?

A. Change management
B. Application whitelisting
C. Asset management
D. Privilege management

Correct Answer: A

QUESTION 224
A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

A. Data masking
B. Data loss prevention
C. Data minimization
D. Data sovereignty

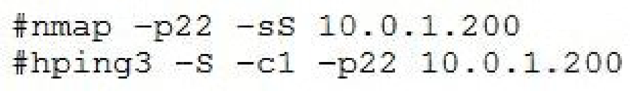
Correct Answer: A

QUESTION 225
Which of the following is MOST closely related to the concept of privacy?

A. An individual's control over personal information
B. A policy implementing strong identity management processes
C. A system's ability to protect the confidentiality of sensitive information
D. The implementation of confidentiality, integrity, and availability

Correct Answer: A

QUESTION 226
A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:



```
#nmap -p22 -sS 10.0.1.200
#hping3 -S -c1 -p22 10.0.1.200
```

The analyst then compares the following results for port 22:

nmap returns "Closed"

hping3 returns "flags=RA"

Which of the following BEST describes the firewall rule?

A. DNAT -to-destination 1.1.1.1:3000
B. REJECT with -tcp-reset
C. LOG -log-tcp-sequence
D. DROP

Correct Answer: B
Explanation:
No doubt does the nmap result mean its being rejected as it returns closed. However, what threw me for a loop was the hping3 response. After further web surfing I found that the "flag=RA" means actually means "flag= RST, ACK" which means that it too was rejected.

QUESTION 227
An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by public users accessing the server. The results should be written to a text file and should include the date, time, and IP address associated with any spreadsheet downloads. The web server's log file is named webserver.log, and the report file name should be accessreport.txt. Following is a sample of the web server's log file:

```
2017-0-12 21:01:12 GET /index.htlm - 84.102.33.7 - return=200 1622
```

Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

A. more webserver.log | grep * xls > accessreport.txt
B. more webserver.log > grep "xls > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E "return=200 | accessreport.txt
D. more webserver.log | grep -A *.xls < accessreport.txt

Correct Answer: C

QUESTION 228
To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

A. The workstation of a developer who is installing software on a web server
B. A new test web server that is in the process of initial installation
C. The laptop of the vice president that is on the corporate LAN
D. An accounting supervisor's laptop that is connected to the VPN

Correct Answer: C

QUESTION 229
Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

A. SSO
B. DLP
C. WAF
D. VDI

Correct Answer: B

QUESTION 230
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

A. Input validation
B. Output encoding
C. Parameterized queries