QUESTION 357
Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

A. An inability to monitor 100%, of every facility could expose the company to unnecessary risk.
B. The cameras could be compromised if not patched in a timely manner.
C. Physical security at the facility may not protect the cameras from theft.
D. Exported videos may take up excessive space on the file servers.

Answer: A

QUESTION 358
A financial institution would like to stare is customer data a could but still allow the data ta he accessed and manipulated while encrypted. Doing se would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concern about computational overheads and slow speeds, Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmatric
B. Symmetric
C. Homeomorphic
D. Ephemeral

Answer: B

QUESTION 359
A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers
B. State actors
C. Script kiddies
D. Advanced persistent threats

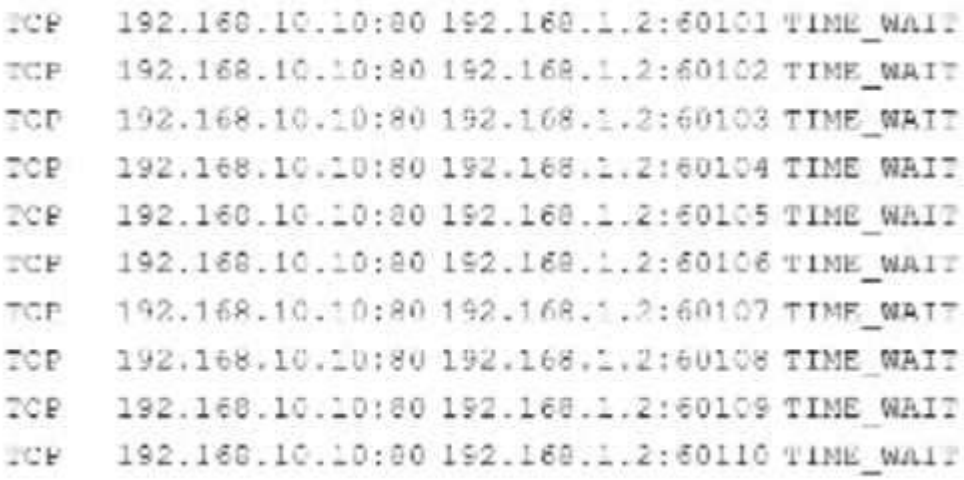
Answer: B

QUESTION 360
Which of the following often operates in a client-server architecture to act as a service repository. providing enterprise consumers access to structured threat intelligence data?

A. STIX
B. CIRT
C. OSINT
D. TAXII

Answer: B

QUESTION 361
A security analyst is reviewing the following output from a system:



Which of the following is MOST likely being observed?

A. ARP palsoning
B. Man in the middle
C. Denial of service
D. DNS poisoning

Answer: C

QUESTION 362
Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?

A. GOPR
B. CIS controls
C. ISO 27001
D. ISO 37000

Answer: A

QUESTION 363
A security researcher is attempting to gather data on the widespread use of a Zero-day exploit. Which of the following will the researcher MOST likely use to capture this data?

A. A DNS sinkhole
B. A honeypot
C. A vulnerability scan
D. cvss

Answer: B

QUESTION 364
An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops
B. Containers
C. Thin clients
D. Workstations

Answer: C

QUESTION 365
A security analyst is reviewing the following command-line output:

```
Internet address      Physical address      Type
192.168.1.1           aa-bb-cc-00-11-22     dynamic
192.168.1.2           aa-bb-cc-00-11-22     dynamic
192.168.1.3           aa-bb-cc-00-11-22     dynamic
192.168.1.4           aa-bb-cc-00-11-22     dynamic
192.168.1.5           aa-bb-cc-00-11-22     dynamic
---output omitted-
--
192.168.1.251         aa-bb-cc-00-11-22     dynamic
192.168.1.252         aa-bb-cc-00-11-22     dynamic
192.168.1.253         aa-bb-cc-00-11-22     dynamic
192.168.1.254         aa-bb-cc-00-11-22     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Which of the following Is the analyst observing?

A. IGMP spoofing
B. URL redirection
C. MAC address cloning
D. DNS poisoning

Answer: C

QUESTION 366
While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting

availability?

A. Conduct a ping sweep.
B. Physically check each system,
C. Deny Internet access to the "UNKNOWN" hostname.
D. Apply MAC filtering,

Answer: D

QUESTION 367
Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

A. An NDA
B. An AUP
C. An ISA
D. An MOU

Answer: D

QUESTION 368
A security administrator needs to inspect in-transit files on the enterprise network to search for Pll, credit card data, and classification words. Which of the following would be the BEST to use?

A. IDS solution
B. EDR solution
C. HIPS software solution
D. Network DLP solution

Answer: D

QUESTION 369
A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

A. logger
B. Metasploit
C. tcpdump
D. netstat

Answer: D

QUESTION 370
A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

A. Memory leak
B. Race conditions
C. SQL injection
D. Directory traversal

Answer: D

QUESTION 371
An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

A. Corrective
B. Deterrent
C. Preventive
D. Mandatory vacations
E. Job rotation
F. Separation of duties

Answer: DE

QUESTION 372
A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management. Which of the following tools can the analyst use to verify the permissions?

A. ssh
B. chmod
C. 1s
D. setuid
E. nessus
F. nc

Answer: B

QUESTION 373
A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations. Which of the following would address the CSO's concerns?

A. SPF
B. DMARC
C. SSL
D. DKIM
E. TLS

Answer: E

QUESTION 374
Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

A. Something you exhibit
B. Something you can do
C. Someone you know

D. Somewhere you are

Answer: D

QUESTION 375
A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

A. Payment Card Industry Data Security Standard
B. Cloud Security Alliance Best Practices
C. ISO/IEC 27032 Cybersecurity Guidelines
D. General Data Protection Regulation

Answer: A

QUESTION 376
A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO).

A. Due to foreign travel, the user's laptop was isolated from the network.
B. The user's laptop was quarantined because it missed the latest patch update.
C. The VPN client was blacklisted.
D. The user's account was put on a legal hold.
E. The laptop is still configured to connect to an international mobile network operator.
F. The user in unable to authenticate because they are outside of the organization's mobile geofencing configuration.

Answer: AB

QUESTION 377
The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

A. federation.
B. a remote access policy.
C. multifactor authentication.
D. single sign-on.

Answer: D

QUESTION 378
A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO. from sending email from a work account to a personal account. Which of the following types of service providers is being used?

A. Telecommunications service provider
B. Cloud service provider
C. Master managed service provider
D. Managed security service provider

Answer: B