Which of the following would be MOST effective to contain a rapidly attack that is affecting a large number of organizations?

A. Machine learning
B. DNS sinkhole
C. Blocklist
D. Honeypot

Correct Answer: D

QUESTION 435
If a current private key is compromised, which of the following would ensure it cannot be used to decrypt all historical data?

A. Perfect forward secrecy
B. Elliptic-curve cryptography
C. Key stretching
D. Homomorphic encryption
Correct Answer: B

QUESTION 436
A systems administrator is looking for a solution that will help prevent OAuth applications from being leveraged by hackers to trick users into authorizing the use of their corporate credentials. Which of the following BEST describes this solution?

A. CASB
B. UEM
C. WAF
D. VPC

Correct Answer: C

QUESTION 437
As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

A. User behavior analysis
B. Packet captures
C. Configuration reviews
D. Log analysis

Correct Answer: D

QUESTION 438
Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers' accounts. Which of the following should be implemented to prevent similar situations in the future?

A. Ensure input validation is in place to prevent the use of invalid characters and values.
B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.

C. Configure the web application firewall to look for and block session replay attacks.
D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

Correct Answer: A

QUESTION 439
A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

A. Hoaxes
B. SPIMs
C. Identity fraud
D. Credential harvesting
Correct Answer: D
Explanation:
Hoax
A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.

Identity theft
Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit .

Credential Harvesting
Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse .

QUESTION 440
A desktop support technician recently installed a new document-scanning software program on a computer However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software.

Correct Answer: C

QUESTION 441
The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

A. Requiring all new, on-site visitors to configure their devices to use WPS
B. Implementing a new SSID for every event hosted by the college that has visitors

C. Creating a unique PSK for every visitor when they arrive at the reception area
D. Deploying a captive portal to capture visitors' MAC addresses and names

Correct Answer: D

QUESTION 442
Which of the following would detect intrusions at the perimeter of an airport?

A. Signage
B. Fencing
C. Motion sensors
D. Lighting
E. Bollards
Correct Answer: B
Explanation:
Fibre optic cable is designed to detect and pinpoint the location of intrusion anywhere on the airport perimeter fence, providing real-time reporting of intrusion

QUESTION 443
While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method. Which of the following would BEST detect a malicious actor?

A. Utilizing SIEM correlation engines
B. Deploying Netflow at the network border
C. Disabling session tokens for all sites
D. Deploying a WAF for the web server

Correct Answer: D

QUESTION 444
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor

Correct Answer: C

QUESTION 445
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

Correct Answer: D

QUESTION 446
Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

A. Common Weakness Enumeration
B. OSINT
C. Dark web
D. Vulnerability databases
Correct Answer: D

QUESTION 447
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

Correct Answer: C

QUESTION 448
An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

A. Web log files
B. Browser cache
C. DNS query logs
D. Antivirus

Correct Answer: C

QUESTION 449
A SOC is implementing an in sider-threat-detection program. The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

A. A honeyfile
B. ADMZ
C. DLP
D. File integrity monitoring

Correct Answer: A

QUESTION 450
An organization is planning to open other datacenters to sustain operations in the event of a natural disaster. Which of the following considerations would BEST support the organization's resiliency?

A. Geographic dispersal
B. Generator power
C. Fire suppression
D. Facility automation

Correct Answer: D

QUESTION 451
A company is receiving emails with links to phishing sites that look very similar to the company's own website address and content. Which of the following is the BEST way for the company to mitigate this attack?

A. Create a honeynet to trap attackers who access the VPN with credentials obtained by phishing.
B. Generate a list of domains similar to the company's own and implement a DNS sinkhole for each.
C. Disable POP and IMAP on all Internet-facing email servers and implement SMTPS.
D. Use an automated tool to flood the phishing websites with fake usernames and passwords.

Correct Answer: C

QUESTION 452
Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

A. Development
B. Staging