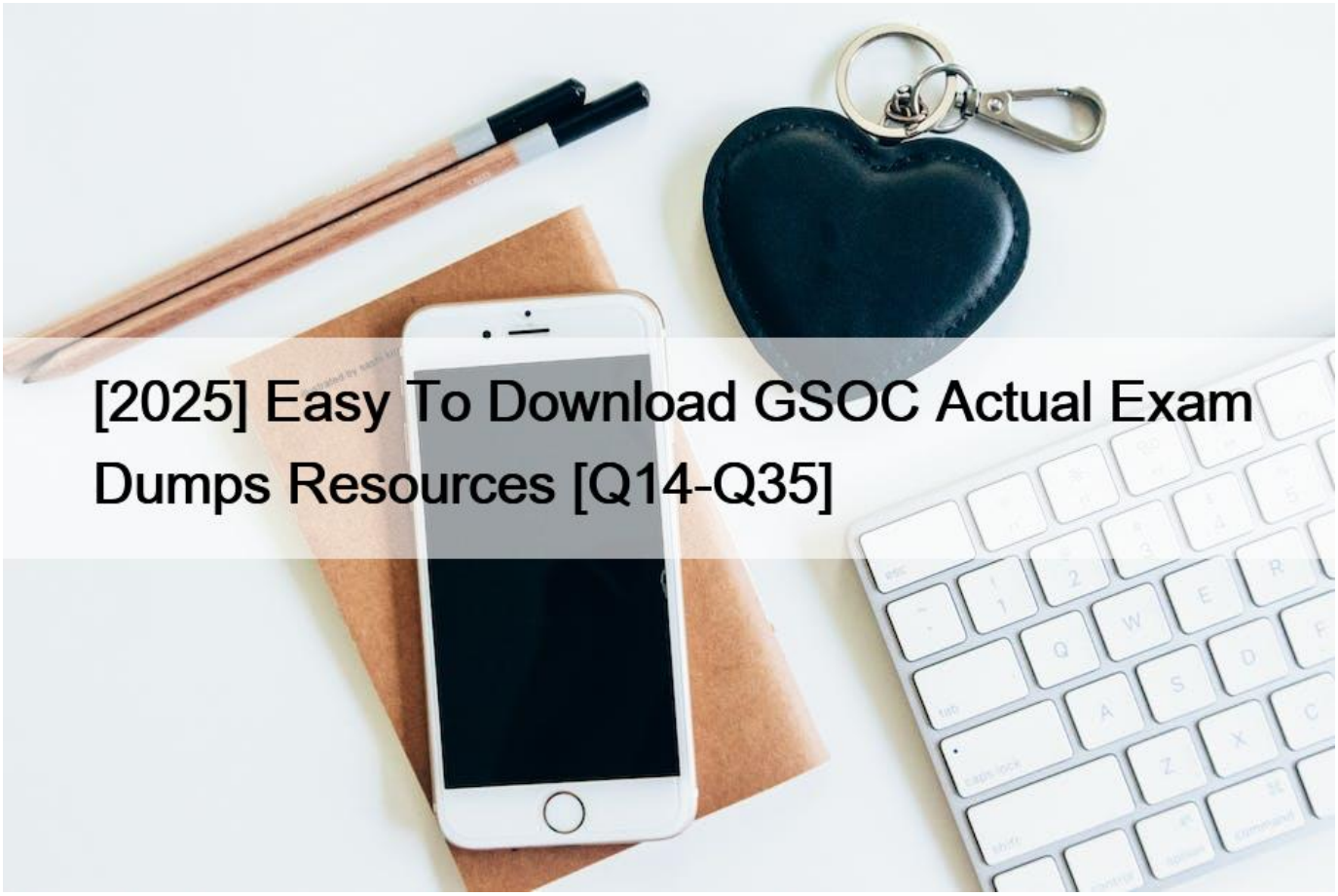
[2025 Easy To Download GSOC Actual Exam Dumps Resources [Q14-Q35



[2025] Easy To Download GSOC Actual Exam Dumps Resources
Uplift Your GSOC Exam Marks With The Help of GSOC Dumps

NEW QUESTION 14

Which of the following is an advanced technique for analytics design?

Response:
* Ignoring data privacy and security
* Design thinking approach
* Sticking strictly to initial design assumptions
* Avoiding iterative processes

NEW QUESTION 15

Which protocol is vulnerable to man-in-the-middle (MitM) attacks due to the lack of encryption?

Response:

* HTTPS
* SSH
* FTP
* DNSSEC

NEW QUESTION 16

Which actions help prevent DNS-based attacks?

(Choose Two)

Response:
* Implementing DNSSEC
* Allowing open DNS resolvers
* Using rate limiting on DNS queries
* Disabling DNS logging

NEW QUESTION 17

What is the purpose of DNSSEC in securing the DNS protocol?

Response:
* To encrypt all DNS traffic
* To authenticate DNS responses and protect against DNS spoofing
* To reduce DNS query times
* To block all DNS requests from external sources

NEW QUESTION 18

When testing analytics models, which of the following methods is crucial for assessing their performance?

(Choose Two)

Response:
* Testing only on the training dataset
* Cross-validation
* Evaluation on unseen data
* Consistent use of a single metric for all model types

NEW QUESTION 19

What is a crucial factor in a SOC’s success in improving an organization’s security posture?

Response:
* Isolating the SOC team from the rest of the IT department to avoid biases
* Conducting regular and comprehensive training for SOC staff
* Limiting the SOC’s access to essential systems only
* Focusing exclusively on external threat intelligence

NEW QUESTION 20

In the process of analytics enrichment, which of the following is a recommended best practice?

Response:
* Relying solely on internal data sources
* Enriching data using random intervals
* Incorporating external data sources to enhance analysis
* Ignoring data reliability to focus on speed

NEW QUESTION 21

What are essential practices when analyzing HTTP(S) traffic to identify attacks?

(Choose Three)

Response:
* Checking for inconsistent IP addresses in the traffic logs
* Ignoring encrypted traffic as it is always secure
* Monitoring for unexpected status codes like 500 Internal Server Error
* Inspecting the payload for malicious content
* Assuming all GET requests are safe

NEW QUESTION 22

What is the primary method to defend against cross-site scripting (XSS) attacks on web applications?

Response:
* Disabling HTTPS
* Input validation and output encoding
* Blocking IP addresses from unknown locations
* Increasing the number of web servers

NEW QUESTION 23

Which of the following is a fundamental practice for defending endpoints against malware?

Response:
* Disabling all endpoint security tools to improve system performance
* Allowing users to approve their security exceptions
* Regularly updating antivirus signatures and software patches
* Using the same standard user account on all endpoints

NEW QUESTION 24

In the context of Linux, what is the significance of the ‘/var/log/dmesg’ file?

Response:
* It logs user authentication events exclusively.
* It contains kernel ring buffer messages.
* It records all the user-level messages.

* It details the package management system logs.

NEW QUESTION 25

Which of the following are key benefits of continuous monitoring by the Blue Team?

(Choose Two)

Response:
* Identifying and mitigating threats in real time
* Disabling all network traffic during business hours
* Reducing the attack surface by addressing vulnerabilities promptly
* Replacing the need for periodic security audits

NEW QUESTION 26

Which practices are essential for maintaining endpoint security in an organization?

(Choose Two)

Response:
* Implementing endpoint patch management to address vulnerabilities
* Disabling antivirus software to reduce resource consumption
* Regularly backing up important data to mitigate the impact of ransomware attacks
* Allowing users to install software without restrictions

NEW QUESTION 27

What is one of the primary roles of a Security Operations Center (SOC)?

Response:
* Developing marketing strategies for cybersecurity products
* Performing offensive cybersecurity operations
* Monitoring and analyzing organization’s security posture on an ongoing basis
* Focusing solely on physical security measures

NEW QUESTION 28

During the sharing phase of analytics, what is an effective practice for fostering understanding and engagement among stakeholders?

(Choose Three)

Response:
* Utilizing interactive visualizations
* Providing detailed technical documentation to all stakeholders regardless of their background
* Tailoring the presentation to the audience’s level of expertise
* Offering actionable insights based on the data
* Limiting access to data to prevent information overload

NEW QUESTION 29

Which protocol is commonly targeted by attackers to move laterally within a network?

Response:
* DHCP
* ICMP
* SMB
* FTP

NEW QUESTION 30

Why is it important for Blue Teams to continuously update and refine their automation workflows?

Response:
* To keep pace with the rapidly changing threat landscape
* To ensure that workflows become increasingly complex and harder to understand
* To reduce their reliance on technology in favor of manual processes
* To increase the time spent on each incident for thorough investigation

NEW QUESTION 31

Your organization has deployed endpoint security tools across all user devices. Recently, one of the senior executives noticed a significant slowdown in their device’s performance. Upon investigation, you discover that a resource-intensive application was installed without proper authorization. This behavior seems unusual, and you suspect a potential security incident.

What steps should your team take to mitigate this issue and prevent future incidents?

(Choose Three)

Response:
* Isolate the device from the network to prevent further spread of potential malware
* Re-image the device to restore it to its original state
* Conduct a full forensic analysis to determine the source and impact of the unauthorized application
* Ignore the incident since it only affected one device
* Review and strengthen endpoint application control policies to prevent unauthorized software installation

NEW QUESTION 32

Your team has detected a significant increase in traffic to a DNS server, leading to degraded network performance. Upon investigation, you identify the traffic as part of a DNS amplification attack.

Which of the following steps should your team take to mitigate the attack and secure the DNS infrastructure?

(Choose Three)

Response:
* Enable rate limiting on DNS queries to reduce malicious traffic
* Disable DNS logging to improve performance
* Implement DNSSEC to improve the integrity of DNS responses
* Block traffic from suspicious IP addresses

* Set up a single open DNS resolver to handle external traffic

NEW QUESTION 33

Which of the following factors should be considered when triaging security incidents?

(Choose Two)

Response:
* The potential impact on business-critical systems
* The geographical location of the incident responder
* The severity of the threat or attack
* The number of users online at the time of the incident

NEW QUESTION 34

In the context of SSH, what is a common attack method?

(Choose Three)

Response:
* Brute force attacks to guess passwords
* ICMP tunneling to hide communications
* Man-in-the-middle attacks to intercept data
* Exploiting vulnerabilities in older SSH versions
* Using SMTP to intercept SSH keys

NEW QUESTION 35

In Linux systems, where can you commonly find security event logs?

Response:
* /etc/security
* /var/log/auth.log
* /home/logs/
* /sys/log/security/