

GIAC GRID

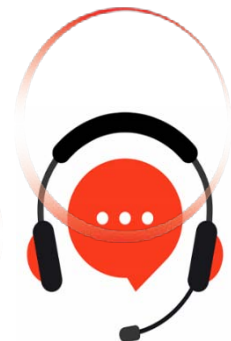
GIAC Response and Industrial Defense (GRID)

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/grid>

Latest Version: 6.0

Question: 1

Why is it important to maintain real-time visibility into ICS assets?

- A. To increase system uptime
- B. To monitor employee productivity
- C. To reduce system latency
- D. To quickly identify and respond to any changes or anomalies in the network

Answer: D

Question: 2

Which of the following best describes the importance of network segmentation in ICS environments for asset visibility?

- A. It reduces the need for regular updates
- B. It improves system performance
- C. It helps identify and isolate devices within specific network segments for better security monitoring
- D. It increases network traffic

Answer: C

Question: 3

Which of the following is a key objective of the recovery phase in incident response for ICS environments?

- A. To restore affected systems to normal operation
- B. To disable all network connections
- C. To monitor billing usage
- D. To update firewall rules

Answer: A

Question: 4

Which of the following should be included in the post-incident review phase of incident response in ICS environments?

- A. Identifying lessons learned and improving future incident response efforts
- B. Replacing all hardware systems
- C. Reducing security monitoring
- D. Ignoring the incident to save time

Answer: A

Question: 5

Why is it difficult to deploy detection tools that perform full system scans in ICS environments?

- A. ICS systems are already fully secured
- B. Full system scans can disrupt the critical operations of ICS systems, causing downtime or performance issues
- C. Detection tools are not compatible with ICS devices
- D. ICS systems do not store any critical data

Answer: B

Question: 6

What is a common method used during threat hunting in ICS environments to identify abnormal behavior?

- A. Reviewing daily email reports
- B. Analyzing baseline behavior to detect anomalies
- C. Rebooting ICS systems
- D. Monitoring employee attendance

Answer: B

Question: 7

Your organization has deployed an IDS in an ICS environment, and the system has generated an alert indicating unusual communication between a remote workstation and a programmable logic controller (PLC).

How should you proceed with investigating this issue?

- A. Disable the IDS system

- B. Review the logs to identify the nature of the communication, verify if the workstation should have access to the PLC, and investigate the user's activity
- C. Ignore the alert, as it could be a false positive
- D. Restart the PLC to reset its communication logs

Answer: B

Question: 8

What is a common challenge when implementing continuous monitoring in ICS environments?

- A. High bandwidth requirements
- B. Difficulty in updating software
- C. The need to maintain system uptime without disruptions
- D. Lack of network devices

Answer: C

Question: 9

During a threat hunting exercise, you identify suspicious communication between a third-party vendor system and one of your ICS control servers.

What actions should you take to investigate this further?

- A. Ignore the communication as it is likely a legitimate interaction
- B. Review the logs from both the vendor system and control server, contact the vendor to verify the legitimacy of the traffic, and temporarily disable communication until the issue is resolved
- C. Reboot the ICS control server
- D. Increase network traffic to monitor the communication

Answer: B

Question: 10

How can threat intelligence help prioritize security efforts in ICS environments?

- A. By identifying the most critical threats and focusing resources on addressing them
- B. By increasing the frequency of backups
- C. By reducing system storage
- D. By minimizing employee interactions

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>