



CERTSWARRIOR

GIAC GRID

GIAC Response and Industrial Defense (GRID)

Questions&AnswersPDF

ForMoreInformation:

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

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

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

Latest Version: 6.0

Question: 1

An ICS environment has experienced a ransomware attack affecting several critical systems. What should be the first step in the incident response process?

Response:

- A. Isolate the affected systems from the network to prevent further spread, and begin forensic analysis to identify the extent of the attack
- B. Increase system processing speed
- C. Restart all affected systems
- D. Reboot the entire network

Answer: A

Question: 2

Which of the following best describes an indicator of compromise (IOC) in threat hunting?

Response:

- A. An artifact observed on a network or device that indicates a potential breach
- B. A method for increasing system performance
- C. A hardware device used in ICS environments
- D. A network diagram

Answer: A

Question: 3

You are responsible for implementing active defense mechanisms in a critical infrastructure ICS environment. After reviewing traffic logs, you identify repeated attempts to access an ICS network segment from an external source. How should you proceed with mitigating this threat?

Response:

- A. Terminate all external connections to the ICS environment
- B. Ignore the attempts and continue regular operations
- C. Review firewall settings, block the IP addresses involved in the access attempts, and implement additional network segmentation to isolate critical systems
- D. Increase system capacity to handle more traffic

Answer: C

Question: 4

A manufacturing plant that relies on ICS systems for its production line receives an alert indicating that unauthorized access was attempted on one of its programmable logic controllers (PLCs). What should be the first steps in handling this situation using active defense principles?

Response:

- A. Ignore the alert and continue production
- B. Shut down the entire production line immediately
- C. Review the system logs, investigate the unauthorized access attempt, isolate the PLC from the network, and enhance access controls to prevent further attempts
- D. Reset all passwords for the entire ICS system without investigation

Answer: C

Question: 5

What is a common challenge in performing digital forensics in an ICS environment?

Response:

- A. ICS systems often have specialized hardware and software that require unique forensic tools and expertise
- B. ICS systems are designed for easy forensic analysis
- C. ICS systems are rarely targeted by cyber attacks
- D. ICS systems are compatible with standard IT forensics tools

Answer: A

Question: 6

Why is asset visibility crucial in an ICS environment?

Response:

- A. To track financial transactions
- B. To monitor employee performance
- C. To improve system power consumption
- D. To ensure that all devices and systems are accounted for and monitored for security vulnerabilities

Answer: D

Question: 7

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?
Response:

- 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: 8

How can centralized logging improve monitoring in ICS environments?
Response:

- A. By combining logs from multiple devices into a single system for easier analysis and detection of anomalies
- B. By reducing energy usage
- C. By eliminating the need for security protocols
- D. By automating backups

Answer: A

Question: 9

In ICS environments, what is the primary advantage of using anomaly-based detection systems?
Response:

- A. They improve system performance
- B. They require no configuration or monitoring
- C. They can detect unknown threats by identifying deviations from normal behavior
- D. They are cheaper than signature-based detection systems

Answer: C

Question: 10

Threat intelligence indicates that a known cyber espionage group has been targeting your ICS environment with sophisticated phishing campaigns. How should your organization respond to this intelligence?

Response:

- A. Educate employees on phishing awareness, implement stricter email security protocols, and closely monitor for signs of suspicious email activity
- B. Reduce employee work hours to minimize phishing attempts
- C. Ignore the intelligence and continue regular operations
- D. Increase system memory to prevent phishing attacks

Answer: A



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ