

KillTest

質量更高 服務更好



練習題

<https://www.killtest.net>

一年免費更新服務

Exam : GRID

**Title : GIAC Response and
Industrial Defense**

Version : DEMO

1.What is the main reason for documenting and maintaining a comprehensive asset inventory in an ICS environment?

- A. To track employee progress
- B. To improve system performance
- C. To increase the number of connected devices
- D. To ensure that all assets are accounted for and properly secured against potential threats

Answer: D

2.What is one of the benefits of using a centralized asset management system in an ICS environment?

- A. It increases system downtime
- B. It improves social media monitoring
- C. It decreases system performance
- D. It provides a single source of truth for tracking and managing all devices in the network

Answer: D

3.What makes detecting threats in ICS environments more challenging compared to traditional IT environments?

- A. ICS systems are rarely connected to the internet
- B. ICS systems typically operate with outdated hardware
- C. ICS systems require uninterrupted operations, limiting the use of traditional security measures
- D. ICS systems do not need security monitoring

Answer: C

4.What role does threat intelligence play in reducing the likelihood of future attacks in ICS environments?

- A. It helps organizations predict and prepare for emerging threats before they can exploit vulnerabilities
- B. It increases energy efficiency
- C. It reduces the cost of system hardware
- D. It improves employee training

Answer: A

5.Which of the following should be a priority when conducting threat hunting in an ICS environment?

- A. Investigating all anomalies, even if they seem benign
- B. Investigating only internal threats
- C. Disabling all security tools to reduce false positives
- D. Ignoring known threats and focusing solely on new ones

Answer: A