
Exam : GICSP

Title : Global Industrial Cyber
Security Professional
(GICSP)

Version : DEMO

1. An organization wants to use Active Directory to manage systems within its Business and Control system networks.

Which of the following is the recommended security practice?

- A. Shared Active Directory domain with separate domain controllers for the Business and Control system networks
- B. An Active Directory domain for the Business network and a Windows workgroup with a domain controller for the Control system network
- C. Separate Active Directory domains for the Business and Control system networks
- D. Shared Active Directory domain with fully functional domain controllers for the Business network and a Read-Only Domain Controller for the Control system network

Answer: D

Explanation:

The recommended best practice is to use a shared Active Directory domain while deploying a Read-Only Domain Controller (RODC) within the Control system network (D).

This approach:

Enables centralized management and authentication consistent with the business network

Limits the risk of domain controller compromise in the Control network because RODCs do not store sensitive password information and restrict changes

Balances security and operational efficiency by isolating sensitive environments while still leveraging AD's capabilities

Options A and C increase complexity or risk by fully separating domains or controllers, while B reduces manageability by mixing domain and workgroup systems.

GICSP highlights RODCs as a means to secure domain services in ICS environments where full domain controllers pose a security risk.

Reference: GICSP Official Study Guide, Domain: ICS Security Governance & Compliance

Microsoft Active Directory Best Practices (Referenced in GICSP)

GICSP Training on Identity Management and Network Segmentation

2. Which type of device is the following configuration setting from?

deny modbus function write-multiple-holding registers

- A. Network firewall
- B. NIDS
- C. SIEM
- D. Application firewall

Answer: D

Explanation:

The configuration line denies a specific Modbus function code, which is a command-level filter for industrial protocols.

This type of control is typical of an application firewall (D) designed to understand and filter industrial control system protocols at the application layer.

A network firewall (A) typically filters traffic based on IP addresses, ports, and protocols, but not protocol function codes.

NIDS (B) detects and alerts on suspicious traffic but does not usually enforce blocking rules.

SIEM (C) collects and analyzes logs, not real-time blocking.

GICSP emphasizes the role of application-layer firewalls in protecting ICS protocols like Modbus.
Reference: GICSP Official Study Guide, Domain: ICS Security Architecture & Design NIST SP 800-82 Rev 2, Section 5.5 (Application Layer Security) GICSP Training on ICS Protocol Security Controls

3.Which of the following devices is most likely to be in the same level as an HMI workstation that interfaces with a PLC?

- A. Variable speed drive
- B. Programmable logic controller
- C. Data historian
- D. Remote terminal unit

Answer: D

Explanation:

In the Purdue model, HMIs typically reside at Level 2 (Supervisory Control), providing interfaces for operators to monitor and control devices. Remote Terminal Units (RTUs) (D) also commonly reside at this level, interfacing between controllers and supervisory systems.

Variable speed drives (A) and PLCs (B) are usually located at Level 1 (Control Devices LAN).

Data historians (C) typically reside at Level 3 or higher in the Operations Support DMZ or enterprise network.

GICSP materials emphasize proper classification of devices by Purdue levels for effective network segmentation and security.

Reference: GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture

Purdue Model and Network Segmentation, IEC 62443

GICSP Training on ICS Network Architecture

4.What is a characteristic of Windows Server Update Services (WSUS) in an ICS environment?

- A. Requires the clients to connect to the Internet to download patches
- B. Inventories both hardware and software within an Active Directory domain
- C. Allows the administrator to create custom groups of computers

Answer: C

Explanation:

WSUS enables centralized patch management and allows administrators to create custom groups of computers (C) to target updates and schedules appropriately, which is useful in segmented ICS environments.

WSUS clients do not require direct Internet access (A) as WSUS servers can download updates centrally.

WSUS does not perform hardware or software inventory (B); that functionality is provided by other tools like MECM.

GICSP highlights WSUS as a practical tool for managing patches in ICS with fine-grained control.

Reference: GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response

Microsoft WSUS Documentation

GICSP Training on Patch Management in ICS

5.What is a characteristic of the Ladder Diagram approach for programming controllers?

- A. Is similar to a low level programming language like assembly

-
- B. May be similar to high level computer programming languages like C
 - C. Uses steps to execute commands and transitions to wait for conditions to move forward
 - D. Based on circuit diagrams of relay logic hardware and operates on rules rather than procedures

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Ladder Diagram (LD) programming is a graphical language used for PLC programming that visually resembles circuit diagrams of relay logic hardware (D). It is rule-based and designed to be intuitive for electricians and engineers familiar with relay control systems.

It is not similar to low-level assembly (A) or high-level languages like C (B).

Option (C) describes Sequential Function Charts (SFC), which use steps and transitions.

GICSP emphasizes Ladder Diagrams as a foundational method in industrial control logic design.

Reference: GICSP Official Study Guide, Domain: ICS Fundamentals & Architecture IEC 61131-3

Standard on PLC Programming Languages GICSP Training on PLC Programming Methods