Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

PASS

killexams.com

GIAC

GICSP

Global Industrial Cyber Security Professional Certification

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/GICSP

Question: 1186

A team integrates operational intelligence into ICS threat modeling. This primarily helps with:

A. Compliance documentation exclusively
B. Identifying campaigns, TTPs, and high-value targets specific to their environment
C. Predicting exact future attack dates
D. Calculating precise monetary risk values only

Answer: B

Explanation: Operational intelligence refines models with current adversary behaviors, improving relevance and prioritization.

Question: 1187

A new PLC cabinet is installed next to a machine line. Management wants to document the layer and purpose of the devices inside the cabinet. Which classification is most accurate?

A. Level 3, because the cabinet stores production history
B. Level 0, because the cabinet is near the machine
C. Level 2, because the cabinet displays alarms
D. Level 1, because the PLC performs basic control

Answer: D

Explanation: The PLC is a Level 1 basic control device, even if it is physically mounted near machinery. Physical location alone does not determine Purdue level; the functional role does. PLCs perform logic and control actions for the process, which distinguishes them from supervisory interfaces and operations systems. Level assignment should be based on function and communication role.

Question: 1188

A power distribution company is implementing endpoint hardening on Windows-based engineering workstations. During a review, administrators discover that several users have the ability to install unsigned device drivers. Which action best reduces endpoint security risk?

A. Permit all users to install any driver because operational flexibility is more important than endpoint security
B. Configure policy to allow installation only of trusted and digitally signed drivers that have been validated for the ICS environment
C. Store unsigned driver packages on a shared network folder so operators can install them when necessary
D. Remove driver signature verification to simplify installation of third-party engineering utilities

Answer: B

Explanation:
Digitally signed drivers help verify software authenticity and integrity. Restricting driver installation to validated, trusted drivers prevents unauthorized kernel-level code from executing on industrial endpoints. Since drivers operate with elevated privileges, compromised or malicious drivers can completely undermine endpoint

security. Testing and validating drivers before deployment ensures compatibility with ICS applications while reducing operational risk.

Allowing unrestricted driver installation, disabling signature verification, or distributing unsigned drivers significantly increases the possibility of malware installation or system instability.

Question: 1189

A utility's security team is modeling threats to remote terminal units (RTUs) in a distributed ICS. Intelligence indicates nation-state interest in protocol abuse. Which high-level concept best guides identification of potential impacts?

A. Focusing only on data exfiltration risks
B. Prioritizing confidentiality over safety in all scenarios
C. Assessing effects on process availability and physical consequences using CIA adapted for OT
D. Assuming air-gapping eliminates all remote threats

Answer: C

Explanation: In ICS threat modeling, impacts are evaluated with emphasis on availability and safety due to physical processes. Intelligence on protocol abuse highlights risks like denial of view or command injection.

Question: 1190

A security analyst wants to detect tampering on an industrial communication channel. Which indicator would most strongly suggest an integrity issue?

A. The HMI desktop wallpaper is updated

B. Commands arrive but their contents or sequence no longer match expectations

C. The server room has changed paint color

D. The operator uses a different monitor brand

Answer: B

Explanation: A mismatch in contents, sequence, or expected values is a strong indicator of communication tampering or replay. In ICS, protocol integrity matters because a small modification can change process behavior. Visual or cosmetic changes to infrastructure are not indicators of channel integrity problems. The analyst should focus on the message semantics and consistency with expected process behavior.

Question: 1191

An industrial cybersecurity consultant recommends separating engineering workstations from operator HMIs into different security zones even though both systems reside within Purdue Level-2. Which explanation best justifies this recommendation?

A. Engineering workstations cannot communicate with HMIs under any industrial networking standard

B. Security zones may contain only one individual workstation according to Purdue guidelines

C. Purdue architecture requires engineering workstations to operate at Level 3 instead of Level 2

D. Engineering workstations generally present greater cyber risk because they modify controller configurations and often connect external devices

Answer: D

Explanation:
Engineering workstations perform high-privilege activities such as controller programming, firmware updates, and configuration changes. They frequently connect removable media and vendor laptops, increasing their exposure to cyber threats. Separating them into dedicated security zones enables stricter access controls and reduces the likelihood of attacks spreading to operator HMIs.

Question: 1192

A BIA identifies critical OT functions with maximum tolerable downtime of 2 hours. How does this quantitative output integrate with risk-based IR?

A. Set RTO targets exceeding 2 hours for flexibility
B. Define IR escalation thresholds and recovery actions to meet or beat the MTD/RTO
C. Use MTD only for insurance claims processing
D. Ignore BIA for tactical incident handling

Answer: B

Explanation: BIA-derived MTD/RTOs are key risk metrics. IR plans incorporate time-bound actions, escalation, and parallel DR activities to ensure critical functions are restored within acceptable windows.

Question: 1193

An OT security engineer needs to analyze host audit logs on a Linux SCADA domain node to detect unauthorized file access attempts and privilege escalation commands. The system uses the native Linux Audit Framework (auditd). Which CLI command should the engineer execute to generate an interpreted, chronological audit report filtering for failed system calls across all monitored user sessions?

A. ausearch -m SYS_CALL -sv no
B. journalctl -u auditd --failed
C. auditctl -l -v
D. aureport -s -i

Answer: A

Explanation: The Linux Audit Framework includes utility tools such as ausearch and aureport. The command ausearch searches auditd log files for specific event types, system calls, or user IDs. Supplying -m SYS_CALL targets system call events, and -sv no filters specifically for unsuccessful (failed) executions, enabling security analysts to rapidly isolate privilege escalation attempts or unauthorized access violations on Linux control endpoints.

Question: 1194

Fenced perimeters and locked enclosures protect PLC cabinets at a manufacturing site. Why is this physical layer emphasized in ICS?

A. IT sites require stronger physical measures than ICS
B. Physical security is optional in networked environments
C. Unauthorized physical access can lead to direct process manipulation or introduction of threats with immediate safety or production impact
D. It primarily addresses data confidentiality concerns

Answer: C

Explanation: Physical controls are essential in ICS because access to controllers or wiring can bypass cyber protections and affect physical outcomes.

Question: 1195

A plant is building a defense plan against attacks on its control layer. Which combination best addresses Level 0 and Level 1 risks?

A. Social media monitoring and desktop themes
B. Shared passwords and open diagnostic ports
C. More office software updates and larger monitor sizes
D. Physical access control, engineering access restriction, and strong segmentation

Answer: D

Explanation: Level 0 and Level 1 defenses rely heavily on physical access control, tight restriction of engineering interfaces, and segmentation. These measures directly reduce the chances that an attacker can touch the process, reach the controller, or use trusted paths. Office-focused controls do not address the unique risks of field and control devices. In ICS, layered defenses near the process are essential.

Question: 1196

During an ICS architecture review, an auditor asks why Level 3 systems should not communicate freely with Level 1 controllers unless operationally required. Which

explanation is most appropriate?

A. Controllers automatically reject all network traffic originating from higher Purdue levels
B. Restricting unnecessary communication reduces the attack surface and limits opportunities for unauthorized access to real-time control systems
C. Level 3 systems are incapable of communicating using industrial protocols
D. Purdue architecture requires every Level 3 server to remain physically disconnected from industrial networks

Answer: B

Explanation:
One objective of the Purdue architecture is minimizing unnecessary communications between higher operational levels and real-time control systems. Restricting communication reduces attack paths, limits lateral movement, and protects deterministic control functions from unintended interactions. When communication is required, it should occur through controlled and well-defined pathways protected by appropriate security mechanisms.

Question: 1197

In a deployment of ISA100.11a, the security manager is compromised. What is the potential network-wide impact?

A. Ability to issue new keys or disrupt authentication for legitimate devices
B. Automatic network self-healing without intervention
C. None, as individual session keys are independent
D. Limited to data exfiltration from the manager only

Answer: A

Explanation: The security manager in ISA100.11a handles key distribution and authentication. Compromise allows broad control, including provisioning rogue devices or denying service.

Question: 1198

An oil refinery's Distributed Control System (DCS) uses multi-node redundancy. The system consists of primary and secondary redundant controller pairs executing identical process logic in lockstep at Level 1. What is the primary operational objective of placing redundant controllers at Purdue Level 1?

A. To convert analogue signals directly into Level 4 corporate financial reports.
B. To eliminate the need for Level 0 process instruments and physical actuators.
C. To provide continuous, uninterrupted real-time process control in the event of a primary controller hardware failure.
D. To host web-based public marketing dashboards directly from field nodes.

Answer: C

Explanation: Redundancy at Purdue Level 1 is implemented to ensure high availability and operational fault tolerance. If a primary logic solver fails, the redundant secondary controller seamlessly takes over deterministic process execution without interrupting physical operations or compromising safety parameters.

Question: 1199

Sudo configuration on Linux OT servers used for engineering tasks must balance usability with security and auditability. What settings achieve this?

A. Distribute the root account password to the entire operations team for shared use
B. Define granular sudoers rules permitting specific commands per user or group while enabling comprehensive command logging
C. Grant all operational users unrestricted root privileges through sudo
D. Disable the sudo utility completely across all Linux systems in the environment

Answer: B

Explanation: Properly configured sudo limits privilege escalation to necessary commands and provides detailed logging essential for accountability in ICS environments.

Question: 1200

A plant manager asks why external threat intelligence matters if the facility has not experienced an incident. What is the best answer?

A. It makes physical security unnecessary
B. It is only useful for consumer apps
C. It replaces the need for local risk analysis
D. It helps identify threats before they are observed locally

Answer: D

Explanation: External threat intelligence helps organizations understand techniques, targets, and attacker behaviors before they appear locally. In ICS, this can reveal

emerging tactics against similar plants, devices, or vendors. It does not replace local analysis, but it improves awareness of the broader threat landscape. Combining intelligence with site-specific modeling produces better decisions.

Question: 1201

\(

An adversary taps into an unencrypted PROFIBUS DP serial network (1.5 Mbps) connecting a master controller to several Remote I/O nodes. The attacker injects malicious payload frames to alter the state of output modules. The plant engineer attempts to mitigate this vulnerability by deploying an inline industrial firewall. What physical limitation prevents a standard IP-based Ethernet firewall from directly securing a legacy PROFIBUS DP bus?

A. Ethernet firewalls operate strictly on optical wireless laser frequencies.
B. PROFIBUS DP uses a legacy RS-485 differential voltage physical layer with token-passing protocol framing, requiring dedicated serial-aware hardware security appliances rather than standard RJ-45 Ethernet interfaces.
C. PROFIBUS DP mandates 4096-bit RSA encryption on all physical copper wires, which disables standard network routing.
D. Ethernet firewalls cannot process nuclear radiation shielding signals.

Answer: B

Explanation: Legacy fieldbus protocols like PROFIBUS DP operate on the RS-485 physical layer (using two-wire differential voltage signaling) with master-slave / token-passing Data Link framing, completely separate from IEEE 802.3 Ethernet and IP stacks. Standard IT or OT Ethernet firewalls feature RJ-45/SFP interfaces and process Ethernet/IP frames, making them physically and logically incapable of connecting to or filtering native RS-485 serial fieldbuses without specialized serial-aware security hardware.
\)

Question: 1202

A scenario at a power substation involves IEDs at Level 1. Attackers exploit unauthenticated GOOSE messages. What impact results?

A. Automatic patching of known protocol vulnerabilities
B. Improved synchronization across protective relays
C. Enhanced visibility into substation status for operators
D. Unauthorized tripping or blocking of protective actions on circuit breakers

Answer: D

Explanation: GOOSE (Generic Object Oriented Substation Event) messages in Level 1 IEDs are often unauthenticated, allowing injection that can disrupt protection schemes for Level 0 equipment like breakers.

Question: 1203

An industrial organization is analyzing historical ICS malware families to understand evolving threat capabilities. The team reviews the 2010 Stuxnet attack against uranium enrichment facilities. What unique capability did Stuxnet demonstrate that fundamentally changed the threat landscape for industrial control systems?

A. It encrypted desktop background wallpapers on corporate IT computers demanding cryptocurrency payments.
B. It relied entirely on unauthenticated public Wi-Fi networks to flood field sensors with ICMP echo requests.
C. It was a highly sophisticated, multi-stage cyber weapon specifically engineered to

target Siemens PLCs, secretly alter frequency drive motor speeds, and manipulate process feedback signals to conceal physical damage.
D. It was a simple macro virus that deleted PDF files on corporate administrative desktop systems.

Answer: C

Explanation: Stuxnet demonstrated a landmark evolution in ICS threats. It targeted Siemens Step 7 software and S7-300 PLCs controlling frequency converter drives. Stuxnet secretly altered motor speeds to destroy physical centrifuges while simultaneously spoofing normal sensor telemetry back to operator HMI screens to mask ongoing physical destruction.

Question: 1204

An administrator at a water treatment plant is configuring an IEEE 802.11ac Wi-Fi network for Level 2 operator HMIs. The administrator chooses WPA3-Enterprise using 192-bit Security Mode instead of WPA2-Personal. Which cryptographic algorithm suite is enforced by WPA3-Enterprise 192-bit mode to protect wireless frame confidentiality and integrity?

A. DES 56-bit block ciphers with MD5 hashing algorithms.
B. Unencrypted ASCII text wrappers operating over static Telnet transport ports.
C. RC4 stream ciphers with 40-bit static initialization vectors and CRC-32 integrity checks.
D. GCMP-256 (Galois/Counter Mode Protocol) for encryption and HMAC-SHA-384 for key derivation and integrity checks.

Answer: D

Explanation: WPA3-Enterprise 192-bit Mode is aligned with CNSA (Commercial National Security Algorithm) suite requirements. It mandates robust cryptographic primitives: GCMP-256 (Galois/Counter Mode) for authenticated symmetric encryption, HMAC-SHA-384 for key derivation and Message Authentication Codes, ECDSA using 384-bit prime curves or RSA-3084 for digital signatures, and ECDHE for key exchange, offering superior protection against frame interception and manipulation compared to legacy standards.

Question: 1205

WirelessHART join process uses a join key. What risk arises if the same key is used network-wide without rotation?

A. Compromise of one device or key exposure allows unauthorized joining of rogue nodes
B. Built-in resistance to offline dictionary attacks
C. Automatic enforcement of unique per-device keys by design
D. No risk as keys are never transmitted

Answer: A

Explanation: Shared join keys in WirelessHART increase risk. Best practice involves secure provisioning and rotation to limit the impact of key compromise.

Question: 1206

A remote site uses wireless backhaul to connect to the main control center. The link must stay up for safe operations. Which availability risk is most important?

A. Office printer toner shortages

B. Desktop icon arrangement changes

C. File naming inconsistencies

D. Jamming, congestion, and link instability

Answer: D

Explanation: For a wireless backhaul that supports safe operations, availability is often the top concern. Jamming can block the channel, congestion can degrade performance, and link instability can interrupt telemetry or control. In ICS, losing a wireless backhaul may mean losing visibility or command capability at a remote site. Availability planning should include redundancy, monitoring, and interference resilience.

Question: 1207

An engineer discovers unauthorized changes to PLC logic at Level 1 after a USB incident. What best describes the compromise path?

A. Firmware downgrade using official vendor tools only

B. SQL injection into the connected historian database

C. Malicious project file or logic upload via engineering tools on compromised workstations

D. Direct internet exposure of the PLC web interface

Answer: C

Explanation: Level 1 PLCs are commonly compromised by loading altered control programs or projects through engineering workstations or removable media, allowing logic manipulation.

Question: 1208

A site has a batch system that coordinates production steps and tracks manufacturing status. The team is deciding where to place it in the Purdue hierarchy. Which answer is correct?

A. Level 2, because it is only an operator screen
B. Level 3, because it supports plant-level operations
C. Level 0, because it drives physical actuators
D. Level 1, because it replaces PLC logic

Answer: B

Explanation: Batch systems belong at Level 3 because they manage plant-level production workflows rather than directly controlling the process. They are part of site operations and often interface with historians and other reporting systems. They may depend on data from lower layers but should not command field devices directly. Correct placement helps reduce unnecessary trust paths.

Question: 1209

A food processing company is implementing defense-in-depth using both Purdue levels and security zones. Which statement best describes the relationship between these two concepts?

A. Security zones replace Purdue levels because network segmentation provides complete architectural guidance

B. Security zones require each Purdue level to contain only one device type

C. Purdue levels organize assets according to operational function, while security zones organize assets according to trust boundaries and security requirements

D. Purdue levels determine firewall configurations, while security zones determine controller scan times

Answer: C

Explanation:

Purdue levels describe the functional hierarchy of industrial systems, while security zones group assets according to trust, risk, and communication requirements. Organizations often implement multiple security zones within a single Purdue level to achieve finer-grained security controls and stronger defense-in-depth.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.