Industrial Control System Cybersecurity

Buyer's Top 10 Desktop Guide

The purpose of this guide is to provide you with high-level questions to ask of any prospective vendor looking to secure your industrial control systems (ICS).

It will provide you a path to determine critical information about the vendor's ability to offer a successful ICS security solution.

When looking to secure and maintain your control system it is essential to understand:

Why Answers to these Questions Matter:

Make an informed decision around the services and features required to properly secure your ICS

What to Look for in the Answers:

Comprehensive responses with details and examples of successful implementations

Potential Pitfalls:

Every vendor has strengths and weaknesses and these answers help you pinpoint the potential weaknesses

By asking the following 10 questions, you will better understand if the vendor offering meets your ICS security requirements.

Question 1:
How do you detect and protect against an ICS security threat?

Why it Matters
Monitoring, defending, and remediating against risks and threats throughout your network prevents downtime and loss of control – even against physical anomalies like squirrels, jellyfish, or birds.

What to Look For
A vendor that can baseline your environment by detecting and alerting you to anomalies that can cause system failure such as malicious security threats or human error, provide continuous monitoring for your ICS environment down to the control of physical processes, and offer robust forensic analysis after an attack to drive rapid remediation.

Potential Pitfalls
A vendor offering single, point-in-time security focused on a single type of threat, fragmented one-off security projects that create vulnerabilities in your system, and lacking an Intrusion Prevention System (IPS) for threat detection.

Question 2:
How do you participate in ICS standards creation, research and industry training?

Why it Matters
Adhering to ICS standards with up-to-date products, policies, and procedures ensures you won't implement an inefficient security solution that doesn't drive compliance.

What to Look For
A vendor that is involved in the security community and leads the development of new standards, is aware of new policies, procedures, system designs, training and threat reports, and is a member of the International Society for Automation (ISA).

Potential Pitfalls
A vendor that does not participate in the ISA or adhere to most current standards, leaves your team the burden of understanding and implementing standards, and offers a solution that won't drive compliance or adjust to frequently changing standards.

Question 3: How do you secure each boundary level of an ICS network?

Why it Matters

Applying a strategy to secure every level of your ICS network prevents disjointed solutions and insufficient levels of security.

What to Look For

A vendor with a portfolio of integrated physical security and cybersecurity solutions, the ability to apply passive and active security levels within a single environment, and solutions that address the specific security needs of each boundary level.

Potential Pitfalls

A vendor that provides unnecessary security levels for your system, lacks integration with your current architecture, and offers point security solutions that can't communicate with other systems.

Question 4: How is your industrial hardware manufactured and supported?

Why it Matters

Employing compatible, supportable, and flexible hardware from a vendor with design and support expertise is vital to avoid unnecessary network traffic and implementation issues from a poorly designed system.

What to Look For

A vendor with industrial design experience, support from design engineers who have extensive knowledge of the software, hardware components, and any impacts they may have on your system, and tested, lasting hardware.

Potential Pitfalls

A vendor with generic, original-device manufacturer (ODM) hardware, unintelligent hardware designs with excessive functions that cause latency, installed hardware with unusable features, and hardware without longevity or support options.

Question 5: How does your security help drive broader business outcomes?

Why it Matters

Maintaining the same standards of availability while securing your ICS is critical to achieve the increased connectivity required for an IoT network and drive the digital transformation of your architecture.

What to Look For

A vendor that offers industry-leading security and knowledge and has a broad services portfolio and partner ecosystem that can drive compliance, increase business visibility, create innovative business processes and policies, lower costs, reduce risk management on systems and the environment, decrease threat remediation time, and enable consistent management across physical and virtual environments.

Potential Pitfalls

A vendor that lacks the knowledge and tools to effectively manage risk across your environment, provides a superficial, non-holistic view of your security requirements, and increases operating costs and management resources.

Question 6: How does your solution integrate with other IT and OT products and services you offer?

Why it Matters

Integrating IT and OT security products and services decreases the likelihood of introducing vulnerabilities and gaps into your system.

What to Look For

A vendor committed to delivering fully integrated products and services, working closely with an integrated partner ecosystem to offer a robust security portfolio, and providing a single source for management and decision-making without introducing risk.

Potential Pitfalls

A vendor with multiple point solutions that create disjointed security policies and management layers, a lack of integration processes that leave you with additional costs, and poor system visibility for decision-making related to risk management and compliance.

Question 7: What types of visibility does your solution offer into an ICS?

Why it Matters

Gaining full visibility into every zone and segment of your ICS enables you to defend against risks and threats that go undetected through different layers.

What to Look For

A vendor that provides baseline asset discovery/inventory to determine the machines, network devices, and products that exist in different zones, offers passive discovery and inventory capabilities that quantify risk and residual risk, and who enables remediation against signatureless threats when they hit your system.

Potential Pitfalls

A vendor offering a "flat" network without zones and segments to differentiate your system, no firewalls or protection between different zones and segments, and manual asset discovery limited to the control system and manufacturing operations system layers.

Question 8: Can you describe the full range of security provided by your solutions at the IT and OT interconnect?

Why it Matters

Establishing network requirements and management processes through IT and OT convergence preserves the existing availability standards and improves your security.

What to Look For

A vendor that aligns IT and OT strategies and processes for visibility, enables secure communication between IT and OT systems, and helps you implement IEC-62443/ISA99 standards to secure your ICS.

Potential Pitfalls

A vendor unaware of key differences between IT and OT requirements, who provides limited communication between IT and OT organizations leading to vulnerabilities in your system, and increases latency from unnecessary features such as spam protection for a system without e-mail.

Question 9: What authentication and authorization protocols do you implement for network access?

Why it Matters

Utilizing a comprehensive set of authorization policies and protocols lowers your risk by keeping out unknown or unwanted entities, without impacting operations.

What to Look For

A vendor that provides context-aware identity management based on identity, location, and access history, allows you to streamline service operations by establishing specific standards throughout the network, and empowers you to make proactive governance decisions by tying identities to network elements.

Potential Pitfalls

A vendor offering limited network connectivity for access control, lack of an identity database and allowed protocols for your ICS, and inflexible rule definitions for granting access to segments of the network, applications, or services simply on authentication results.

© 2016 Cisco and/or its affiliates. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Question 10: How do you know that your security solution will successfully integrate with my network architecture?

Why it Matters

Implementing a solution that integrates seamlessly with your existing systems helps you avoid introducing unknowns and unintended consequences, or creating new vulnerabilities.

What to Look For

A vendor offering a tested and validated solution put through rigorous analysis and exposure to threats, comprehensive documentation around the implementation of security measures in your environment, multiple types of support and services for applying the security solution, and deep understanding of the ICS environment and what is required to secure it.

Potential Pitfalls

A vendor that doesn't know their solution will be successful in your environment before implementation, can't offer multiple levels of support and services to run the solution, and doesn't work with a robust partner ecosystem to secure an ICS.