CYLANCE CONSULTING

Industrial Control System Security Assessment

Identify and Mitigate Risks in ICS Environments

Benefits

- Increase comprehension of cybersecurity in industrial control systems, including best practices for securing ICS with integrated IT/OT systems
- Develop a systematic and repeatable approach to assessing and maintaining the security posture of ICS systems, including legacy architectures, legacy systems, and legacy devices, without replacement
- Support business objectives while maintaining safe and uninterrupted operations with security
- Create remediation strategies while balancing risk and return
- Implement a prevention-first methodology that removes the noise in environments and allows IT security professionals to focus on the activities that can be truly harmful

$8 Billion

Global financial loss due to the WannaCry attack in 2017.

Source: https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

Industrial Control Systems (ICS) manage an organization's risk, including security. While ICS were once stand-alone systems, they are now connected to an organization's IT infrastructure, yet contain fewer security controls. ICS now faces the same cybersecurity threats as corporate networks, but with cascading risk, physical damage, and bodily injury as potential impacts.

Additional challenges remain, such as applying patches vs. system downtime, an ICS system whose patches are at end of life, and dependencies on other systems with heterogeneous environments. All of these challenges make upgrades and updates challenging. Recent attacks, including NotPetya, Wannacry, Shamoon 2, BlackEnergy, Havex, and Clear Energy, demonstrate that attacks need not be targeted. A lot of work remains to protect vital systems and avoid business interruption and theft of data.

Further, it is also critical that organizations look into the security of their large, connected supply chains. Small companies providing critical components can also be targeted by threat actors and present cascading risks to the integrity of an organization's production process. With the OT team looking after the integrity of production process and the IT team after data protection, traditional trade-off between uptime/safety and security functionality (both perceived and real) continue.

Because of these unique challenges, ICS operators are left scrambling with IT and OT segmentation efforts, random uses of off-the-shelf security technologies such as antivirus, firewalls, etc., and some patching that is usually limited to Windows systems (servers and workstations). As significant production and financial losses are tied to any disruption in ICS, strengthening and securing an ICS environment has become more important than ever before.

While many considerations must be taken when addressing the fragile nature of ICS environments, an ICS Security Assessment can aid in **identifying and remediating vulnerabilities** that would allow an attacker to disrupt or take control of the system. Based on the results, the assessment can help **guide decisions on corporate best practices to enhance the organization's overall cybersecurity posture**.

Service Overview

Cylance® Consulting's globally-recognized ICS security experts will work closely with organizations to evaluate the security practices of the ICS environment and understand the challenges from their perspective. These security challenges are mapped on a timeline to illustrate key milestones and to identify any additional measures that need to be taken to improve the client's security over six to 24 months. Apart from these holistic assessments and project roadmap, Cylance's ICS experts also provide clients with metrics to report progress and a measured approach to improve capabilities to detect/respond to threats.

Cylance's approach is centered on providing context with regard to the potential business impact of cyber threats. By applying a structured and methodical approach to security, Cylance ICS experts will map out the different types of threat actors, their potential entry points, detection points, as well as prevention and containment opportunities within the network. This will help clients better understand the robust security tools they have in place and any countermeasures that need to be implemented.

Service Offerings

An ICS Assessment provides an effective means to identify the highest priority security concerns and recommendations for the control system environment. Information is collected about the organization's security practices, policies, and procedures through survey responses, staff interviews, tools, company documentation, and site walk downs. The primary categories for the assessment include:

ICS Security Assessment and Strategic Roadmap

A range of assessment activities focused on analyzing the effectiveness of an organization's security programs, this service looks into vulnerabilities and solutions to mitigate their critical risks/impacts. The strategic roadmap helps organizations build and prioritize the governance and remediation of critical vulnerabilities surrounding people, processes, and technologies.

ICS Risk Assessment

A high-level assessment focused on analyzing the overall posture and strategic direction of an organization, this service additionally supports a peer analysis across multiple owned assets.

ICS Security Testing

Designed to help organizations evaluate specifically implemented technologies or security controls, this service covers traditional IT, embedded devices, operations technology, control systems, and more.

ICS Security Response and Readiness

A range of assessment activities focused on analyzing an organization's readiness to respond to security incidents within their ICS, this service covers people, processes, and technology challenges in detection, response, and recovery around ICS assets.

The Cylance Difference

Holistic IT and OT Coverage

Cylance has ICS experts that have a wide range of expertise covering both IT and OT capabilities, allowing them to balance the concerns of both sides and ensure that they are aligned, integrated, and consistent. Cylance works closely with organizations to discuss ways to protect legacy architectures, legacy systems with outdated operating systems, and legacy devices, and ways to prevent malicious threat actors from shutting down your grid and halting your business operations.

No Business Interruption

Cylance performs any service activity without interruption to operations. From assessments to roadmap review to the execution of remediation efforts, Cylance's objective-based approach always looks at the protection of critical business operations and systems.

Prevention-first Methodology

Cylance leverages AI and a prevention-first methodology to secure endpoints from both known and unknown attacks. Cylance's prevention-first strategy utilizes an adversarial-based approach for hygiene to quickly identify threats from commodity malware to sophisticated threat capabilities. Removing the noise from environments allows IT security professionals to focus on the activities that can be truly harmful.

Flexible Planning

Cylance Consulting works with cyber insurance carriers, law firms, OT, security teams, and risk managers to identify the highest priority concerns and provide the recommended order for improvement. While not all organizations will be able to implement security best practices all at once, Cylance balances projects against budget to help clients achieve their roadmap goals.

Deliverables

The information obtained from the assessment is used to provide the organization with:

- A risk profile that addresses impact, threat, vulnerability, probability, and countermeasures
- A prioritized road map for remediating security concerns

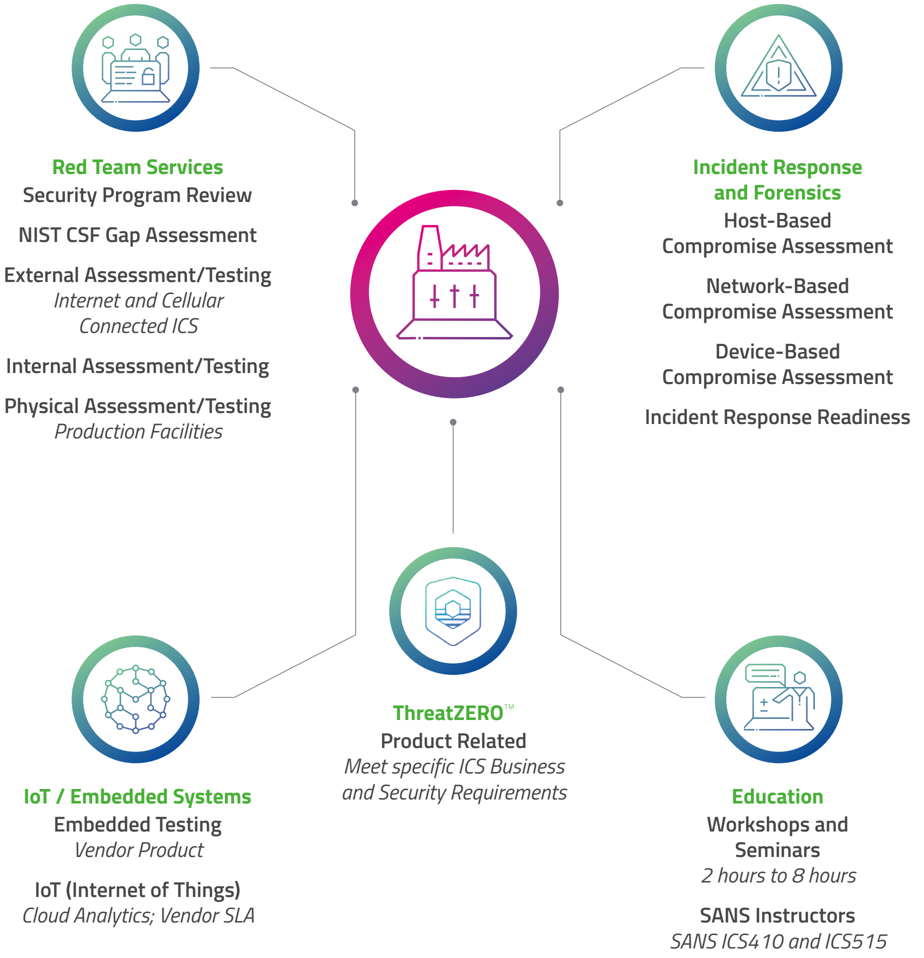
Identify weaknesses and develop actionable recommendations to mitigate the risks in your ICS environment. Contact Cylance Consulting or your technology provider to discuss your needs.

About Cylance Consulting

- World-renowned experts work synergistically across practice areas to deliver consistent, fast, and effective services around the world
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to prevent attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Compromise Assessments, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, Strategic Services, and Education

Other Related Services

Cylance's experts are world-renowned and have vast experience in working synergistically across various practice areas. They deliver consistent, fast, and effective services across the globe. Cylance's ICS Assessment can be integrated with other Cylance services around Incident Containment and Compromise Assessments, Red Team Services, IoT and Embedded Systems, and ThreatZERO™ Services.



Red Team Services

Security Program Review

NIST CSF Gap Assessment

External Assessment/Testing
Internet and Cellular Connected ICS

Internal Assessment/Testing

Physical Assessment/Testing
Production Facilities

Incident Response and Forensics

Host-Based Compromise Assessment

Network-Based Compromise Assessment

Device-Based Compromise Assessment

Incident Response Readiness

ThreatZERO™

Product Related
Meet specific ICS Business and Security Requirements

IoT / Embedded Systems

Embedded Testing
Vendor Product

IoT (Internet of Things)
Cloud Analytics; Vendor SLA

Education

Workshops and Seminars
2 hours to 8 hours

SANS Instructors
SANS ICS410 and ICS515

+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting