



Industrial Control Systems Assessment

A partnership with Intel Security means more confidence that your end-to-end security posture can avoid risks before they strike.

The Foundstone Services Industrial Automation Security team is the premier partner for organizations in the ICS industry, drawing from the intelligence that secures the IP world and the talented professionals that have secured some of our nation's critical infrastructure.

Proven Methodology

We have a proven methodology for collaboration and customer success. This includes:

- Risk identification.
- Risk mitigation and elimination strategies.
- Industry best practices.

The Internet of Things (IoT) is exploding into thousands of smart, connected devices. As industrial facilities and their related infrastructure, manufacturing systems, and process controls get more complex, it's important to regularly identify and prioritize risks to supervisory control and data acquisition (SCADA) systems in order to analyze threats and resolve vulnerabilities in your critical infrastructure. Our Industrial Automation Security team works with you to maximize your existing investment in people, processes, and technology. By merging industry best practices with corporate risk and capability, we help you create and maintain a stronger security posture.

As a part of the Intel® Security Professional Services organization, Foundstone® Services takes what we learn from the real world and fuses it together with best practices for incident response and restoration, and creates courses in industrial control system (ICS) cybersecurity. Our ICS assessment evaluates your security posture and develops actionable recommendations to mitigate risks from external attackers, insider threats, and automated worms.

We combine our extensive history in incident response with ICS domain expertise to deliver an in-depth evaluation of how hardened your ICS network is in practice. Our evaluation includes:

- Common Vulnerability and Risk Mitigation Report.
- Assessment Services.
- Remediation Support.
- Incident Response.
- Education and Training.

Assessment Services

Our assessments take a deep look into your enterprise across the spectrum of people, processes, and technologies to analyze your current cyber posture.

Common Vulnerability and Risk Mitigation Report

This report is an introduction to industrial risk and is often a first step to understanding the cyber posture of your plant or location. It is a triage effort designed to take a quick look at identifying common areas of risk and includes findings and recommendations as well as an executive summary.

The report-generation process is quick and is meant to be a lightweight representational review of the security posture by looking at network endpoints and other common technical vulnerabilities.

Representational Assessment

Our most common assessment is a representational assessment that includes working with customer subject-matter experts to define the correct representation size, assets, personnel requirements, and locations. This assessment is intended to maximize tangible results while minimizing costs. The security posture, risks, threats, vulnerabilities, and risk strategies are all derived from the smaller set of assets reviewed. The methodology allows for flexibility to expand into areas that have a greater attack surface and contract from areas that are well contained.

Additionally, we can provide a full assessment or audit against any of the industry benchmarks such as NERC-CIP, NEI 09-09, API 1164, INGAA, NIST 800-82, ensuring your organization is meeting the necessary compliance requirements.

Remediation Support

The cornerstone of an industrial automation security assessment is the agility to adapt best practices and solutions to customer environments. We include strategic and tactical recommendations to harden your cyber posture, plus the expertise to make sure any improvements are implemented correctly.

Incident Response

There are two types of enterprises: those that have been breached and know it, and those that have been breached and don't know it. It is all too common to be breached and have a third party disclose the facts. Our Incident Response (IR) services start by examining both the corporate IR plan and the ICS IR plan, if available. Foundstone IR experts can assist in crafting an ICS-specific IR plan if there is not one available.

We understand that your systems must be available and restored, and we have considerable experience in government and other critical sectors. Our experts not only

add capacity to your overextended security personnel, but our threat intelligence expertise allows us to plan for known threats, understand their actions and consequences, and restore services faster than any other IR service provider.

Education

From both an offensive and defensive perspective, Foundstone Services has set the bar for teaching cybersecurity. Our industrial automation security team continues that tradition of excellence in the ICS space to provide greater understanding of problems and leading solutions to securing your ICS. The following courses can be adapted as needed. In addition, we frequently monitor the industrial control landscape to see if there are other courses that would be of value in securing the ICS space.

Course	Days	Audience	Skill Level
Introduction to ICS Security	1	General	Non-Technical
Securing the ICS	4	ICS Management	Some Technical
Attacking the ICS	4	CS Analysts	Technical
Assessment Development	2	Operational	Non-Technica

Table 1. Course offerings.

Learn More

Fill the gaps in your ICS security program with trusted advice from the Intel Security Professional Services organization. We provide security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about our services or email us at foundstone@intel.com.

Get more information at www.foundstone.com.

