MANDIANT®
A FireEye® Company

Industrial Control Systems Security Gap Assessment

Engage Mandiant to evaluate the cyber security posture of your industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems.

DATA SHEET

SECURITY CONSULTING

BENEFITS

- **Align operational and information technology security strategies**
  Mandiant's ICS specialists speak the language of operational technology (OT) and work directly with the engineers responsible for OT to adapt cyber security best practices appropriately for the ICS environment. We also work with IT security leaders to equip them with the domain knowledge and credibility required to approach their OT teams in security discussions.
- **Establish visibility into industrial control systems security risks**
  Enhance your understanding of your industrial control systems security posture and establish the appropriate metrics to monitor progress.
- **Reduce the impact of ICS-related security incidents**
  Ensure your ICS assets are protected by deploying the appropriate people, process and technology to minimize risk to your system.
- **Prioritize budget and resources**
  Allocate security spending and effort on the controls that matter most and address real-world threats and risks.

The ICS Security Gap Assessment draws on Mandiant's knowledge of advanced threat actors, experience responding to security breaches and ICS domain expertise to deliver an in-depth evaluation of your industrial control systems security program and a technical review of your ICS architecture. We incorporate the results, along with an assessment of your incident response readiness, into a strategic roadmap for improving the security of your ICS and SCADA systems.

Overview

Our Industrial Control Systems Security Gap Assessment is designed to identify existing gaps, provide recommendations on how to address vulnerabilities and enhance visibility into the security posture of your ICS assets. Mandiant's approach goes beyond regulatory compliance and standards conformance to help organizations make an immediate and sustained improvement in their ability to resist compromise and respond to targeted attacks.

Our consultants evaluate three key domain areas during this assessment. We review your ICS cyber security program to ensure appropriate policies and procedures are in place so you can efficiently meet or exceed cyber security regulations and industry standards. We evaluate your ICS architecture to identify technical gaps and propose both short-term risk mitigation strategies and long-term changes to address architectural, software and hardware design flaws. Finally, we identify the most valuable logs and ICS security information to enhance the security operation center's visibility into the ICS technology and recommend tools and processes to improve your organization's ability to respond to an incident.

ICS cyber security program

- Strategy and mission
- Standards and policies
- Change management
- Threat intelligence
- Vulnerability and patch management
- Training

Defensibility of ICS architecture

- Network design
- Access control
- Security infrastructure
- Software and hardware asset inventory and diagrams
- ICS communications protocols

Incident response readiness

- Event and incident management
- Instrumentation and network visibility
- Log management
- Security operations center integration

Improve your ICS security program by identifying key areas of improvement to strengthen your defense posture against advanced threats.

Unique challenges for industrial control systems

CHALLENGE	BARRIERS TO IMPROVING ICS	OUR SOLUTION
Change-averse culture	• Limited change windows (e.g. quarterly and annually) • Vendor approval required for 3rd party software • Fragile systems • Skeptical engineering workforce	We help you avoid major configuration changes with a passive network monitoring strategy, using techniques such as log collection and network packet capture.
Domain-specific technology	• Requires specialized knowledge of industrial control systems technology and communications • Many enterprise IT security technologies are not ICS-aware	Our ICS experts will work to identify any gaps in the coverage of your Enterprise IT strategy and recommend ways to extend or complement it to cover ICS.
Significant deficiencies in products and standards	• Bugs and flaws in vendor implementations • Flawed designs (e.g. lack of authentication, non-standard logging, lack of security/identity features) • Product vulnerabilities are not always addressed by vendor, limited support policies, slow adoption of new protocols	We inventory the hardware, software, and communications protocols in your environment to identify these flaws and make technical and process improvement recommendations.

Our approach

Over the course of the assessment, we will provide an in-depth evaluation of your industrial control systems security program, architecture, and incident response readiness. At the end of the engagement you receive a defined roadmap of short-, medium- and long-term improvement initiatives.

Step 1: Documentation collection and analysis

Mandiant experts will review existing polices, standards and procedures to gain an understanding of the industrial control systems environment and associated security policies and procedures.

Step 2: Interactive workshops and architectural threat model

Based on the information we gather, our experts will assess your organization's maturity levels against best practices and industry standards. We perform an in-depth technical analysis of security threats to your ICS architecture and explain how to protect against them. We will work with you to identify your organization's goals and desired end state.

Step 3: Recommendations and roadmap

We evaluate all the data collected during the assessment and provide recommendations and an implementation roadmap to achieve the organization's desired immediate and future goals. Improve your ICS security program by identifying key areas of improvement to strengthen your defense posture against advanced threats.

WHAT YOU GET

- **Cyber threat briefing:** We provide an overview of the latest threats that Mandiant has seen and include recommendations on how to protect your industrial control systems against these threats.
- **ICS security gap analysis:** A detailed report is provided that includes observations from the assessment and recommendations on how to further develop and strengthen the three key domains assessed.
- **Threat model diagram:** Mandiant works with your team to build a representative diagram of your industrial control system, map the various threat vectors that could be used to disrupt or degrade your operations and discuss how to prioritize the appropriate security controls.
- **Improvement roadmap:** At the end of the assessment we deliver a roadmap highlighting strategic and tactical improvement along with sequence and prioritized recommendations.

Mandiant, a FireEye company, has driven threat actors out of the computer networks and endpoints of hundreds of clients across every major industry. We are the go-to organization for the Fortune 500 and government agencies that want to defend against and respond to critical security incidents of all kinds.

Mandiant, a FireEye Company | 703.683.3141 | 800.647.7020 | info@mandiant.com | **www.mandiant.com** | **www.fireeye.com**

MANDIANT
A FireEye® Company