INDUSTRIAL CONTROL SYSTEMS HEALTHCHECK

UNDERSTAND YOUR INDUSTRIAL CONTROL SYSTEM'S EXPOSED VULNERABILITIES AND ESTABLISH AN ACHIEVABLE PLAN TO REDUCE YOUR SYSTEM'S CYBER SECURITY RISK

Mandiant is a trusted advisor to organizations globally with over 10 years of experience dealing with advanced threat actors from around the world. We support organizations during the most critical times after a security breach has been identified and proactively help them improve their detection, response and containment capabilities. The Industrial Control Systems (ICS) HealthCheck combines Mandiant's knowledge of threat actors and experience responding to security incidents with our ICS consultants' domain expertise to deliver an in-depth evaluation of how well-segmented, protected and monitored your ICS network is in practice.

Overview

The ICS HealthCheck is a minimally invasive assessment of an industrial facility's overall cyber security posture. This assessment is specifically designed to meet the needs of organizations concerned about the operational risk associated with software-based agents, network scanning or other more aggressive security evaluation techniques. The ICS HealthCheck combines a workshop-based ICS architecture review with detailed technical analysis of firewall configurations and live ICS network traffic.

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 engage their OT teams in effective cyber security discussions.

MANDIANT®
A FireEye® Company

Proactively identify and mitigate complex security vulnerabilities that can lead to the compromise of critical systems.

KEY BENEFITS

- Minimally invasive assessment approach avoids the operational risks associated with software agents and network scanning in an ICS environment
- Identifies ICS security vulnerabilities, misconfigurations and flaws
- Human analysis of anomalous and suspicious activity, performed by ICS experts using ICS-aware tools
- Actionable recommendations prioritized, customized and placed into appropriate context based on the risks and concerns specific to your industrial process

FireEye®
SECURITY REIMAGINED

Our approach

Architectural Risk Analysis & Threat Modeling

Document Current Network Understanding

- Review existing architecture diagrams, dataflow and designs.
- Inventory and evaluate industrial communications protocols that are in use.
- Review any existing security standards for hardware and software deployment.

Develop Threat Model

- Take the resulting architecture diagrams and create the basis for a threat model during an interactive workshop with the customer's IT and operations/engineering staff.
- Build visual representation of the possible attacks on the control system, based on our extensive knowledge of real-world attacker tactics.
- Aid the prioritization of security control implementation for ICS, identifying the attack vectors representing the most exposure and risk.

Prioritize Controls

- Facilitate a discussion with your technical team to identify security controls that appropriately address the identified threats.
- Provide a value-based prioritization of the potential controls, considering factors such as risk reduction, cost/effort and speed of implementation.

Technical Data Analysis

Network Segmentation Review – We analyze a network packet capture file from a FireEye PX device deployed to the customer's ICS network. The packet capture is reviewed for security risks such as:

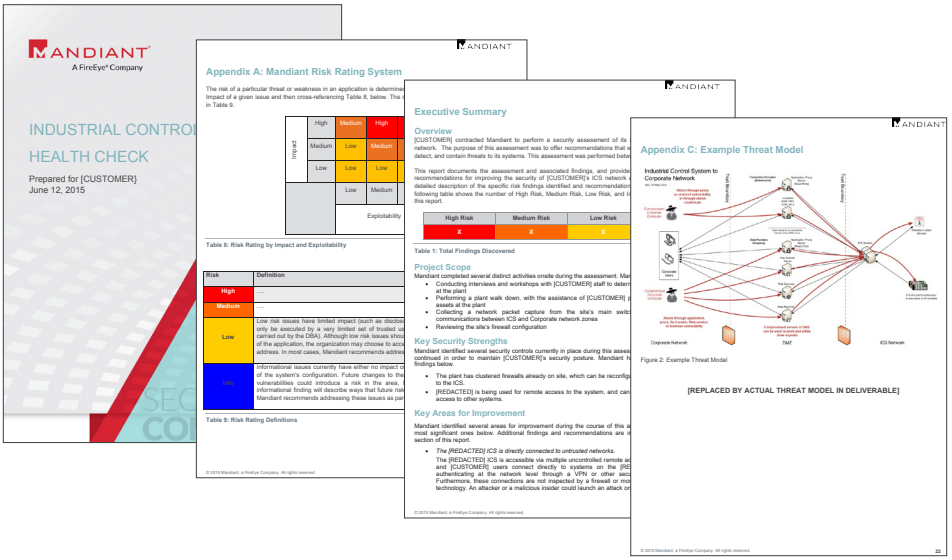
- Unintended connectivity from the ICS to the Internet or business network
- Dual-homed devices
- ICS protocols traversing the ICS firewall
- Anomalous computer-to-computer connections

Security Device Configuration Review – We review the efficacy of the configuration and rule-sets of network security devices, such as firewalls. For example:

- Inbound traffic to the ICS network should always be routed through a DMZ.
- ICS networks should not be allowed to directly access, and should never be directly connected, to the Internet.

WHAT YOU GET

- **Threat Model Diagram:** A representative diagram of your ICS that maps the various threat vectors that could be used by attackers to disrupt or degrade your operations, and a discussion of how to prioritize the appropriate security controls.
- **ICS HealthCheck report:** A detailed technical report describing Mandiant's observations, including any security vulnerabilities, misconfigurations, architectural weaknesses, suspicious network traffic or anomalous activity with actionable and prioritized technical recommendations for each observation, along with a summary of the key themes emerging from the assessment.
- **Presentation of Strategic and Technical Recommendations:** A summary of our observations and recommendations to the technical and management-level stakeholders.



For more information on Mandiant consulting services, visit:
www.FireEye.com/Mandiant.html

Mandiant, a FireEye Company
1440 McCarthy Blvd. Milpitas, CA 95035
(703) 935 1701 | 800.647.7020 | info@mandiant.com

www.Mandiant.com