Industrial Control Systems/Operational Technology Healthcheck

Highlights

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

Identify exposed ICS/OT vulnerabilities so you can establish an achievable plan to reduce your system's cyber security risk

Mandiant is a trusted advisor to organizations globally with decades of cumulative 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)/Operational Technology (OT) Healthcheck combines Mandiant's knowledge of threat actors and experience responding to security incidents with our ICS/OT consultants' domain expertise to deliver an in-depth evaluation of how well-segmented, protected and monitored your ICS/OT deployment is in practice.

Overview

The ICS/OT Healthcheck is a minimally invasive assessment of a system or 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 Healthcheck combines a workshop-based ICS/OT architecture review with detailed technical analysis of firewall configurations and live ICS/OT network traffic.

Mandiant's ICS/OT specialists speak the language of process and control, and work directly with the ICS/OT engineers to adapt cyber security best practices appropriately for the environment. We also work with IT security leaders to equip them with the domain knowledge and credibility required to engage their ICS/OT teams in effective cyber security discussions.

Our approach

Architectural risk analysis and threat modeling

Document current network understanding

- Review existing architecture diagrams, dataflow and designs.
- Inventory and evaluate industrial/operational 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/OT 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 network packet captures from your ICS/OT network. The packet capture is reviewed for security risks such as:

- Unintended connectivity from the ICS/OT to the Internet or business network
- Dual-homed devices
- ICS/OT protocols traversing the ICS/OT 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/OT network should always be routed through a DMZ.
- ICS/OT networks should not be allowed to directly access, and should never be directly connected to the Internet

What You Get

- **ICS/OT Healthcheck report**
  A detailed technical report describing Mandiant's observations, including any security vulnerabilities, misconfigurations, architectural weaknesses, suspicious network traffic or anomalous activity. The report will provide actionable and prioritized technical recommendations for each observation, along with a summary of the key themes emerging from the assessment.
- **Threat model diagram**
  A representative diagram of your ICS/OT 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.
- **Presentation of strategic and technical recommendations**
  A summary of our observations and recommendations to the technical and management-level stakeholders.