Operational Technology Risk Assessment

Get a clear picture of your plant's cybersecurity risk posture.

As industrial control systems (ICS) become more connected and complex, it is important to regularly identify and prioritize the risks of severe, damaging attacks. Proper identification and prioritization of risks can help secure critical assets and assure reliability, business continuity, and regulatory compliance.

Proven Methodology

OTRA is a four-week engagement, offering a fixed scope and price to analyze:

- Strengths of current risk posture.
- Weaknesses of current risk posture.
- Tactical and strategic recommendations to increase the strength of your risk posture.

Project Deliverables

Final report

- Executive Summary.
- Cybersecurity Posture Profile.
- Risk Assessment.
- Cybersecurity Solution Roadmap with Recommended Risk Mitigations.

Executive briefing

- Face-to-face meeting with all stakeholders to review the final report

As industrial facilities and their related manufacturing, process control, and infrastructure get more complex, it's important to regularly identify and prioritize risks to supervisory control and data acquisition (SCADA) systems, analyze threats, and resolve vulnerabilities in your critical infrastructure.

Based on a combination of several industry leading methodologies, our Operational Technology Risk Assessment (OTRA) is designed to provide a clear picture of your plant's cybersecurity risk posture. We take a comprehensive look across your enterprise—including the people, processes, and technologies—to determine your current risk posture. We not only show you the security vulnerabilities in your plant, we also give you a roadmap to follow to improve your cybersecurity risk posture.

Assessment Methodology

Our assessment takes a deep look across your industrial enterprise at the spectrum of people, processes, and technologies. We analyze your current cybersecurity posture and provide a customer-based strategy to close identified gaps. We break down our assessment into four components: kickoff, plan delivery, assessment, and final delivery. Each step is designed to allow constant communication and feedback to maximize your investment in Intel Security.

Information Gathering

Information gathering is the first step of the assessment and helps us become familiar with your environment. This phase will also help you understand what is required for a successful engagement. We will request certain documentation as outlined below. The Information gathering phase usually begins before we come on site.

Analysis

We start this phase with an on-site meeting to review the assessment process, time requirements for your personnel, and our understanding of the previously provided information.

While on site, we will work with your extended teams to collect additional information, both electronically and physically.

Report Generation

We provide a report that outlines your current cybersecurity risk posture and provides a detailed roadmap on areas you can improve. Report generation usually takes place off site on Intel Security's premises.

Executive Presentation

An executive presentation will be made to all relevant stakeholders on the findings contained in the report.

The Intel Security Difference

The Intel Security Professional Services team has a long history of working with clients across the globe as strategic advisor with product-agnostic program-level engagements. Our teams of security experts assess network vulnerabilities, evaluate gaps in information security programs, offer strategies that meet compliance goals, and even help develop programs to prepare for security emergencies.

Customer Requirements

We find that our customers understand their industrial control system (ICS) environment far more than we can, which is why we ask that our customers help us arrange interviews with employees who are familiar with the current plant environment. For example, we often need to interview site managers, process control engineers, and operators. You will need to provide any additional requested documentation. Our experience is that it is best to receive this documentation prior to having Intel Security personnel arrive on site.

Focus Areas

Our comprehensive approach recommends the analysis of a representative sample of systems in your environment—rather than all systems in your environment. This approach reduces your cost while allowing us to accurately determine your cybersecurity risk posture.

We take a representational sampling approach to analyzing customer data, building the assessment and posture based on the representative sample, and applying it to the enterprise. Our OT Risk Assessment is broken into three core focus areas: people, processes, and technologies.

People

People are the most important aspect of any process. They are the cornerstone of industrial security. We take the time to understand your operational personnel and their cybersecurity capabilities, operational needs, cybersecurity operational impacts, and process operations. Through targeted discussions with your subject matter experts, we work to fully understand the personnel impact on cybersecurity.

Processes

Processes form the boundaries for good cybersecurity operations. We inspect the core plant technology and cybersecurity processes, including how technology is procured, deployed, secured, and operated. Reviewing these processes allows us to gain insight into your cybersecurity practices and your ability to prevent interruptions in production processes.

Technologies

We review all of the traditional IT technology with our industry-leading methodologies, ensuring context in the industrial application. We also review all of the industrial assets and their related protocols to understand and define end-to-end gaps and deficiencies in application, configuration, or efficiency. This unique Intel Security offering ensures that your investment in technology is used optimally in both cybersecurity and operations and that a balance of operational efficiency and cybersecurity is maintained.

Learn More

Fill the gaps in your ICS security program with trusted advice from the Intel Security global 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 you 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**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com