5 CRITICAL CONTROLS
FOR WORLD-CLASS OT CYBERSECURITY

HOW TO ALIGN YOUR LEADERSHIP AND IMPLEMENT A SUCCESSFUL OPERATIONAL TECHNOLOGY (OT) SECURITY POSTURE

OT CYBERSECURITY HAS NEVER BEEN MORE IMPORTANT.

As operational technology (OT) cybersecurity becomes a top priority from boardrooms to the manufacturing floor, CISOs and their teams must implement proven strategies to protect the business.

OT, however, has long been underrepresented, leading to communication challenges, a cultural gap with IT, and uncertainty about how to move forward.

The good news? OT cybersecurity is now getting the attention it deserves. Read on to discover the key components of a world-class OT cybersecurity program.

BUILD THE FOUNDATION WITH EXECUTIVE ALIGNMENT

Before industrial control systems (ICS) teams can build a set of controls to support OT cybersecurity, they must get buy-in from the top. Executive and board-level alignment creates the foundation for a successful program. **How can ICS teams help executives understand the risks and rewards of OT security?**

Use real-world scenarios. Extrapolate the impact of a potential attack using actual numbers from specific plants. Leaders know how much it would cost for a plant to go down for X days or weeks; emphasize those numbers.

Research previous attacks. To demonstrate the consequences of OT security failures, look into the SEC filings of companies that were hit. See how long each plant was down and how much it cost.

Explain the difference between IT and OT. Help them understand that the organization has been focused on reducing IT cyber risk while under-serving OT – the side of the house that actually generates revenue – and that it's now time to course correct.

You've got the buy-in, now what? Once the C-suite and Board are educated and aligned on the risks and necessity of OT security, consider your package of controls.

THE RIGHT CONTROLS

The SANS Institute identified five critical controls for ICS/OT cybersecurity. We offer additional insight on how to implement these controls in your OT environments.

ICS incident response plan

OT's incident and response plan is distinct from IT's. OT involves different device types, communication protocols, different types of tactics, techniques, and procedures (TTPs) specific to the industrial threat groups. Investigation requires a different set of tools and languages. Managing the potential impact of an incident is different for pipelines, electrical grids, and manufacturing plants.

Create a dedicated plan that includes the right points of contact, such as which employees have which skills inside which plant, as well as thought-out next steps for specific scenarios at specific locations. Consider table top simulation exercises to test and improve response plans.

A defensible architecture

OT security strategies often start with hardening the environment - removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points, and mitigating high risk vulnerabilities. Perhaps even more important than a secure architecture are the people and processes to maintain it. The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.

Visibility and monitoring

You can't protect what you can't see. A successful OT security posture maintains an inventory of assets, maps vulnerabilities against those assets (and mitigation plans), and actively monitors traffic for potential threats.

Visibility gained from monitoring your industrial assets validates the security controls implemented in a defensible architecture. Threat detection from monitoring allows for scaling and automation for large and complex networks. Additionally, monitoring can also identify vulnerabilities easily for action.

Secure remote access

Secure remote access is critical to OT environments. A key method, multi-factor authentication (MFA) is a rare case of a classic IT control that can be appropriately applied to OT. Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment.

Where MFA is not possible, consider alternate controls such as jumphosts with focused monitoring. The focus should be placed on connections in and out of the OT network and not on connections inside the network.

Risk-based vulnerability management

Knowing your vulnerabilities – and having a plan to manage them – is a critical component to a defensible architecture. While patching an IT system like a worker's laptop is relatively easy, shutting down a plant has huge costs.

An effective OT vulnerability management program requires timely awareness of key vulnerabilities that apply to the environment, with correct information and risk ratings, as well as alternative mitigation strategies to minimize exposure while continuing to operate.

Dragos: Your partner for world-class OT cybersecurity

Implementing and adopting these OT cybersecurity controls requires technology and people. As the industry's most advanced ICS/OT cybersecurity platform, Dragos helps you visualize, detect, and respond to cyber threats. Plus, our network of renowned ICS/OT cybersecurity practitioners give you the insight and expertise to combat today's most sophisticated threats.

With Dragos, you get the technology and the team to put a world-class OT security posture in place.

Learn more and connect with us at dragos.com

DRAGOS