PHARMACEUTICAL MANUFACTURING:

5 CRITICAL CONTROLS FOR WORLD-CLASS OT CYBERSECURITY

How to Align Your Leadership and Implement a Successful Operational Technology (OT) Security Posture

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

DRAGOS®

contents

- OT Cybersecurity Has Never Been More Important 3
- Build the Foundation with Executive Alignment..... 4
- Three Ways to Speak Your Board's Language 5
- Next Step: Prioritization 6
- Collaboration Between IT and OT 7
- Five Critical Controls For Effective OT Cybersecurity 9
  - One: ICS Incident Response Plan 10
  - Two: Defensible Architecture 11
  - Three: Visibility and Monitoring 12
  - Four: Secure Remote Access 13
  - Five: Risk-Based Vulnerability Management 14
- Your Partner for World-Class OT Cybersecurity 15

OT CYBERSECURITY HAS NEVER BEEN MORE IMPORTANT FOR PHARMACEUTICAL MANUFACTURING.

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 for pharmaceutical manufacturers.

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.

Why is top-down alignment so crucial? When cybersecurity strategies come from the bottom up, teams tend to address them with the resources that they have. As a result, many efforts aren't resourced correctly, which opens the organization to unnecessary risk.

It's also difficult to scale. Getting every plant manager or outsourcing partner educated and on board is rarely realistic, while putting the responsibility on leadership enables a bias for action.

3 Ways to speak your Board's language

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. Help the executive team understand how critical it is to maintain the integrity of the batch -- and remind them of the regulatory consequences of cybersecurity incidents.
- **Research previous attacks.** To demonstrate the consequences of OT security failures, look into the SEC filings of pharmaceutical companies that were hit. See how long each plant was down and how much it cost.
- **Explain the difference between IT and OT.** Communicate to the Board how IT and OT are different. 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.

Next step: Prioritization

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.

Start by asking executives for a top-to-bottom list of the most important sites in the company. That list will act as a prioritization tool, enabling IT and OT to work together to decide what systems and locations to focus on first.

Use the scenarios from the initial conversations to establish how much priority each site should receive and how to balance operations across prevention, detection, and response. What you learn from the "A" sites, you can then apply to the "B" and "C" sites.

Collaboration between IT and OT

Many successful OT attacks originate in IT systems like remote access VPNs. To protect the business as a whole, IT and OT must work together. This includes sharing technology – asset management is a great place to start. Done right, collaboration between IT and OT eliminates duplication of effort, adds consistency, eliminates gaps in OT/IT interface points, and reduces complexity in the overall enterprise environment.

CAN OT BORROW FROM IT?

You can't copy and paste your OT security program from IT. While IT focuses on system and data security, OT must account for systems of systems and physics. Some overlap will happen – and even be desirable – but don't simply duplicate everything that IT does when OT requires a different approach.

Critical controls for effective OT cybersecurity

Leadership is on board. Sites are prioritized. Up next: the right controls to ensure world-class OT cybersecurity for pharmaceutical manufacturing.

01

An ICS incident response plan

02

A defensible architecture

03

OT visibility: asset inventory, vulnerability mapping, & monitoring

04

Secure remote access

05

Risk-based vulnerability management

CONTROL #1:

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 handled differently depending on your industry — pharmaceutical manufacturing environments have unique challenges and need specific incident response plans.

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. Remember, if you're outsourcing part of your manufacturing, your partners need to have ICS-specific incident response plans in place. Evaluate their plans based on these recommendations.

CONTROL #2:

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. Partners, contractors, and temporary labor forces also need to be well trained in cybersecurity fundamentals specifically for the OT environment.

CONTROL #3:

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.

CONTROL #4:

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.

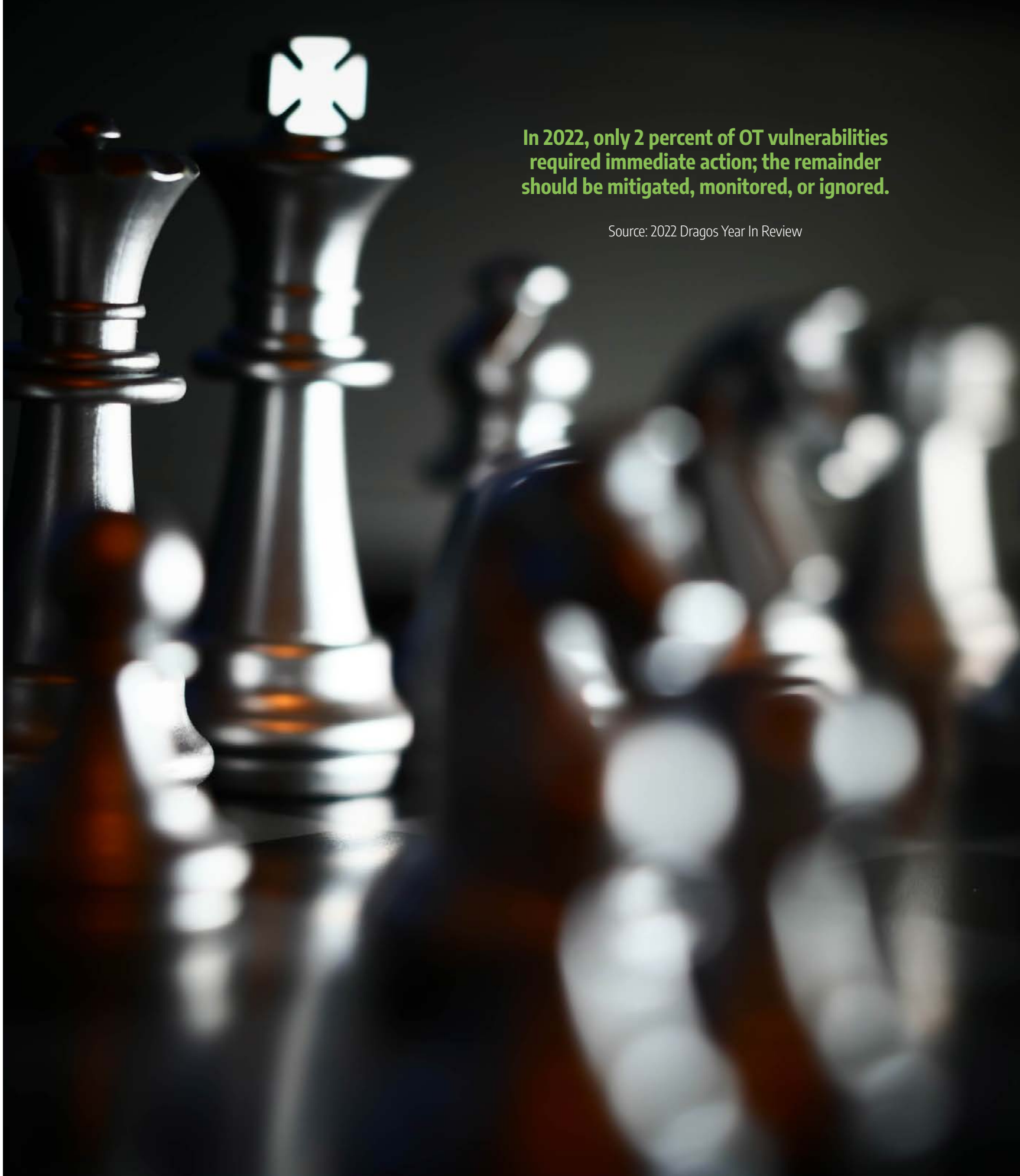
Where MFA is not possible, consider alternate controls such as jumphosts with focused monitoring. The focus should be placed on connections in and out of the OT network and not on connections inside the network.

CONTROL #5:

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.



In 2022, only 2 percent of OT vulnerabilities required immediate action; the remainder should be mitigated, monitored, or ignored.

Source: 2022 Dragos Year In Review

Dragos: Your partner for world-class pharmaceutical manufacturing 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.

Our key offerings include:

- **Dragos Platform** – combines ICS/OT network sensors, a scalable data architecture, and expert analysis modules for asset inventories, vulnerabilities, threats, and streamlined response
- **Dragos Intelligence** – ICS/OT specific news, research, and analysis on industrial cyber threats, industry targeting, vulnerabilities, and actionable defense recommendations
- **Dragos Services** – experienced professionals delivering OT security assessments, risk management, threat hunting, and incident response services

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

Dragos is an industrial (OT/ICS/IIoT) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Dragos.com