FEDInsider

# PARTNERING TO PROTECT OPERATIONAL TECHNOLOGY & CRITICAL INFRASTRUCTURE

***Government & industry must share information, streamline compliance & work together to protect critical environments from evolving cyber threats.***

**Featured Experts:**

- **Jonathan Feibus**
  *Chief Information Security Officer*, NRC

- **Marty Edwards**
  *Deputy CTO, OT/IoT*, Tenable

Safeguarding critical infrastructure is crucial to maintaining the stability and security of our society. Unfortunately, critical infrastructure is a desirable target for nation-state actors, hacktivists and other threat actors. Operational Technology (OT) is often targeted as an entry point in cyber-attacks against our nation's critical infrastructure due to gaps in visibility, outdated technology and pervasive security vulnerabilities. To counter these threats, government, industry and academia must work together to strengthen OT systems and eliminate gaps in visibility caused by the convergence of IT and OT environments.

To further discuss OT security, thought leaders from government and industry spoke at a recent FedInsider webinar to share the tools they need to tackle the increasing amount of OT threats and the role visibility plays in preventing attacks on IT systems through OT.

## WHAT'S AT STAKE

"OT are the black box computer devices that essentially underpin our entire infrastructure," said Marty Edwards, Deputy Chief Technology Officer, OT/IoT at Tenable. Yet when these devices were first integrated with IT systems, they weren't built with security in mind, creating vulnerabilities and gaps in protection.

Power grids, water filtration systems, medical devices, building control systems and more have all been under attack. "Anything that can be automated, anything that is put up on the internet, or anything that can be reached via a computer, is going to be vulnerable at some point," said Jonathan Feibus, Chief Information Security Officer with the Nuclear Regulatory Commission.

Confidentiality in the OT realm isn't entirely the concern, either. It's not about breaching the database to know how much water is available to a municipality, for instance. Rather, it's about not jeopardizing the integrity of that water and ensuring the breach can be dealt with, without needing to turn off the water supply. "It's a little bit of a different approach that needs to be taken to protect OT," Edwards said.

## SECURING OT ENVIRONMENTS STARTS WITH DATA

Advanced technologies can be used to secure OT and make it easier for IT teams to protect systems and networks. Artificial intelligence can help engineers identify network anomalies and analyze data for greater visibility.

"AI is going to be that attack mode that will look at every anomaly and bring my engineers' focus to it so that they can do what people are good at, focusing on that anomaly and fixing it," Feibus said.

AI can help teams detect where those anomalies are coming from and prioritize the remediation of vulnerable assets before they turn into a larger problem. As AI improves, it can even start to fix some of those routine problems autonomously.

Finding the right type of AI tools, however, starts with understanding the data. "When you are looking at layering AI solutions on your security automation, you really have to pay attention to the normalization and characterization of the data. And that is all about the underlying data," Edwards said.

AI won't solve all analytical problems, but it'll help with defense by filtering through hundreds of thousands of alerts and finding the anomalies and patterns that are concerning. "But you must have an extremely good asset inventory, threat detection and log correlation," Edwards said. "You must have all that underlying data in a format and in a structure that lends itself to the AI being able to learn what you need. Because if you put garbage in, you will get garbage back out."

## OT, IT & NATIONAL REQUIREMENTS

As OT and IT converge, agencies must understand how compliance and regulations impact their systems. The National Institute of Standards and Technology (NIST), for instance, has a cybersecurity framework that guides agencies through specific types of systems they may have, including OT. "You need to look at that suite of standards and try to marry those as best you can," Edwards

said, rather than creating more and more requirements for different sectors. "We should be trying to drive that common baseline across the board."

Agencies shouldn't look at a domain like OT in isolation. "If you are accountable and responsible for the security of the whole organization, you need to rack and stack all the risks no matter what network or what domain they are in," Edwards said. "But if you are not normalizing that and using the same sort of calculus to evaluate those risks, then you cannot compare them to each other."

Edwards and his team try to use a similar set of tools and analytics across the organization so that when risk pops up on the dashboard, everyone is looking at the same context. "Right now, I think we are looking at too many unicorns or specialized solutions, and we need to get to this point where we are evaluating that across the entire organization using the same cadre of tools in the same mechanisms."

Bringing the OT community together to form a standard set of OT requirements and regulations could help. Edwards said NIST, CISA and other agencies are collaborating to form a set of requirements that can be applied across the board. CISA's cybersecurity performance goals and NIST's cyber framework, for instance, are coordinated.

## THE RIGHT TOOLS, PROCESSES & PARTNERSHIPS

There is rarely a single security solution, and with OT systems, employing the right tech isn't enough. Network visibility and inventory tracking are key, and adopting AI, automation, and continuous diagnostics and mitigation programs can help. Having the proper security controls over assets – including cloud and on-premises environments – is also important.

Cross-sector collaboration and information sharing can also improve early warning systems and allow for proactive defense. Take the Colonial Pipeline cyberattack, for example. "That was not necessarily their OT production system that was infected. But out of an abundance of caution, they decided to voluntarily take down those systems because they didn't know how far the ransomware had spread," Edwards said. "If we can get better visibility into those environments, we will empower the boards of directors and chief executives in these organizations to say, We are pretty confident that we can keep running the operational stuff."

When it comes to collaboration and information sharing, venues like CISA's Joint Cyber Defense Collaborative are paramount. High-risk vulnerabilities found between agencies and their vendor partners are shared with federal partners so they can deploy the necessary defenses proactively. More of this is needed.

"If the government has some unique information they can share with industry, it helps us understand the threat landscape, and it helps us understand where the adversaries are pivoting to," Edwards said. "We have got a pretty solid technological community on the defense side that can build the defenses to help people like Jonathan at the NRC defend their environments."

There are also several community groups that the federal government participates in to help protect critical infrastructure sectors. Those professional communities have common infrastructure and security challenges that they share, as well as guidance to help others detect vulnerabilities and mitigate attacks made against either the public or private sector, Feibus said.

Those communities allow organizations to work together to figure out if they are experiencing the same things, "to make sure that if I see something, I can check with my neighbors and see if they are seeing it as well so that we can back each other up in a noncompetitive way," Feibus said.

There is great value in this collaboration, and while it is happening with CISA, the JCDC, FBI and NSA, Edwards said that more cooperation is always better. "There is always an opportunity to improve," he added, "And to work more closely together."