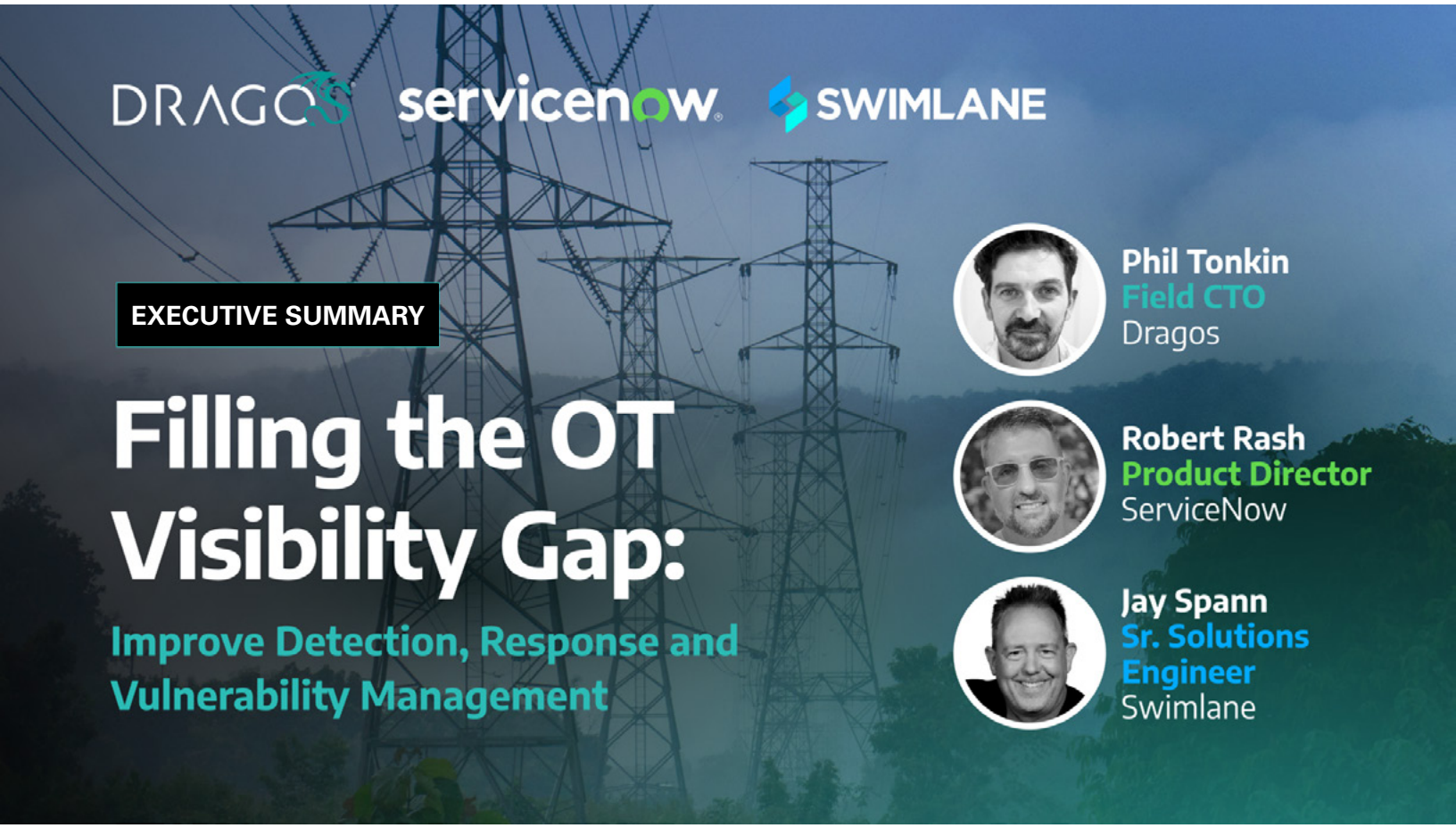
ENDEAVOR BUSINESS MEDIA



MAY 29, 2024

Filling the OT Visibility Gap: Improve Detection, Response and Vulnerability Management

OVERVIEW

The industrial infrastructure cybersecurity landscape is constantly evolving. Increasing threats and new legislation are driving organizations to find solutions to help manage the operational technology (OT) environment, including network monitoring, automated threat detection, and streamlined incident response workflows.

Securing OT assets requires a collaborative effort, bringing together internal stakeholders with OEMs, vendors, and service providers to prioritize vulnerabilities and identify critical processes that inform best-fit security solutions.

Industry-leading companies Dragos, ServiceNow, and Swimlane leveraged their collective expertise to develop a holistic solution that works against cyber threats targeting both IT and OT environments, by providing well-established workflows that equate to improved business efficiencies and a more effective response program when performing incident response across both networks.

CONTEXT

The presenters discussed strategies to enhance operational technology protection.

KEY TAKEAWAYS

Mission-critical industrial infrastructure is facing constantly-evolving cybersecurity threats.

The threat landscape has long presented significant challenges for security professionals—and is constantly evolving. As infrastructure and OT assets have become increasingly connected, new trends have emerged in threat attacks, including:

- **Growing capabilities of state actors,** particularly in targeting critical infrastructure to carry out both active, disruptive attacks and intelligence-gathering stealth attacks.
- **The rise of ransomware,** specifically attacks that target OT operators. The year-over-year increase in manufacturing sector ransomware attacks is significant, as attackers have realized the criticality of timely restoration of OT systems and thus an increased likelihood of receiving ransom payouts.
- **Activist (also: Hactivist) group attacks** motivated by the behaviors and the geopolitical environment, which have grown in number and frequency.

To combat these rising threats and keep pace with the ever-evolving threat landscape, governments are further bolstering legislation to drive required coverage further down into organizational operations. Pending regulations (e.g., NIS 2 in the EU, NERC CIP 15-1 in the US) are focused on filling the OT visibility gap, but the requirements present new challenges for assets owners and operators. Gaining the visibility necessary to understand the risk landscape within a company is a significant undertaking.

> "To solve these problems, you've got to be able to picture what's out there, and that's a big challenge."
>
> *Phil Tonkin, Dragos*

Filling the OT Visibility Gap: Improve Detection, Response and Vulnerability Management

Collaboration is key to a successful security strategy.

Recognizing security-critical processes and being able to integrate them into a comprehensive automated solution depends on having a strong understanding of the entire OT environment. Investing resources both in identifying all OT assets and in defining the processes that will achieve desired results (rather than poorly designed processes that do not solve actual problems) will bolster security and improve compliance.

A useful way to understand the most likely risks to any given organization is to identify who would be targeted and why, and then determining how attackers would go about executing those threats. Considering capability and motivation in the context of the specific organization helps prioritize vulnerability management.

Good asset management offers benefits beyond thwarting threat actors. It also contributes to improved risk management and resilience outside of intentional attacks, such as weather-related events or unexpected equipment failures.

To gain asset visibility, automate processes, and manage compliance requirements, there is no single solution that will make sense for every company, and no single solution that will solve all issues within one company. Instead, for companies looking to make improvements in OT compliance and cybersecurity, the best way to manage risk is with a combined set of tools (i.e., best-of-breed solutions) that integrate well with each other and provide complementary functionality to manage OT cybersecurity risk and achieve all aspects of the company's security goals.

> "To solve anything in security today, collaboration is the name of the game."
>
> *Jay Spann, Swimlane*

As part of an effective OT security journey, there are important steps to take to avoid potential implementation pitfalls:

- **Supply chain assessment.** Before building out a vulnerability management strategy, organizations should have a good understanding of **what their supply chain looks like**. Identifying the OEMs supplying components into the environment is a better-informed approach for developing a more effective security strategy.
- **Multi-stakeholder collaboration.** Involving all stakeholders and **fostering a collaborative environment** helps ensures that critical information is not missed when determining the best strategy and solutions. When there are good relationships between the engineering workforce, partners, system integrators, and OEMs, the more detailed and complete the knowledge gathered and documented is, the more effective the prioritization and remediation of vulnerabilities will be.
- **Leverage partnerships.** During the discovery process and beyond, draw on the experience of the partners that are already in place at the company. **Leveraging the expertise of existing partners** can help guide a more comprehensive, powerful security approach. Partners can access a wide range of automation best practices and recommended tools that have been proven at other engagements, that can contribute to a better solution.

Filling the OT Visibility Gap: Improve Detection, Response and Vulnerability Management

Dragos, ServiceNow, and Swimlane work together to provide comprehensive OT security.

Securing distributed assets across potentially hundreds of sites, each with thousands of connected devices that are designed and codified to a specific operation, is an enormous challenge for humans to manage without codified knowledge, digitalized data, and tools that enable automation workflows.

> "To identify what is truly critical, from a threatened vulnerability standpoint, but also what doesn't apply—that's the most critical piece."
>
> *Robert Rash, ServiceNow*

To secure the radically different environment of OT versus more traditional IT protection, Dragos, ServiceNow, and Swimlane took a collaborative approach, leveraging their individual expertise in an integrated solution to provide improved potential incident detection, response, and vulnerability management.

These three solutions are best-of-breed in distinct but complementary focus areas:

- **Dragos** offers OT intelligence-driven threat detection, vulnerability management, and actionable mitigation guidance.
- **ServiceNow** streamlines OT asset and ticket management.
- **Swimlane** provides integration and automation to tie together any and all tools needed to address security use cases.

Adversaries evolve their Tactics, Techniques, and Procedures (TTPs) with subtle behaviors lost in the noise. Traditional threat detection systems struggle in OT environments because they depend too much on IT-focused intelligence and broad anomaly detection, leading to too many alerts without clear action steps. This situation overwhelms security teams, complicating the identification and response to OT-specific threats.

The Dragos Platform's Threat Detection module is a precise, OT-specific threat detection engine with actionable insights, minimizing false positives and providing clear prioritization to safeguard ICS/OT environments efficiently. It utilizes proprietary OT-specific intelligence, delivering actionable insights for operational technologies. It addresses alert fatigue by clarifying alert reasons, highlighting relevant threats, and suggesting guided responses, uniquely catering to the sophisticated needs of OT environments.

OT cyber teams are often overwhelmed by the sheer volume of potential vulnerabilities that require remediation. Without simple, OT-accurate, and prioritized guidance, it is challenging to address the most critical vulnerabilities effectively, leading to operational risks and non-compliance with regulatory standards and best practices such as The SANS 5 Critical Controls.

The Dragos Platform's Vulnerability Management provides comprehensive vulnerability information with prioritization and enriched risk scoring specified for the complications of OT environments. It gives Platform users the information needed to focus on the highest priority issues to mitigate risk, minimize downtime, and allocate cybersecurity resources where they are most needed. It does this by leveraging a robust vulnerability database, defined threat levels, and enriched risk scoring, which together provide prioritized 'Now, Next, Never' guidance for strategic responses.

Filling the OT Visibility Gap: Improve Detection, Response and Vulnerability Management

By working together, the solution combines monitoring and management of the physical components in an OT environment, vulnerability prioritization rules based on organization-specific processes and device roles, and automated workflows for alerting and remediation. Integration with multiple sources offers detailed visibility into the OT environment, which can be filtered by department, owner, or other business-centered role to focus discussions, support better decision making, and develop more effective, targeted strategies.

ADDITIONAL INFORMATION

To learn more, visit:

- **Dragos.** dragos.com
- **ServiceNow.** dragos.com/partner/servicenow/
- **Swimlane.** dragos.com/partner/swimlane/

Filling the OT Visibility Gap: Improve Detection, Response and Vulnerability Management

BIOGRAPHIES

Phil Tonkin
Field Chief Technology Officer, Dragos

Phil Tonkin is Field Chief Technology Officer at Dragos, Inc. where he uses his experience in the energy sector to provide technical insight and strategic guidance in securing industrial operations. His career has included roles in electricity transmission, distribution, and generation; gas transmission, distribution, and storage; and IT. Prior to joining Dragos, he led the OT security program at one of the world's largest investor-owned utilities for five years.

Robert Rash
Outbound Product Management Director, ServiceNow

Robert Rash is the Outbound Product Management Director responsible for responsible for the success and market strategy of our Operational Technology Management solution. Robert provides product strategies and roadmap for the OTM products to deliver a world-class solution for managing operational technology assets. Robert has more than 20 years of OT industrial automation, engineering, programming, and manufacturing experience. Before joining ServiceNow in 2022, Robert provided process improvement and OT security solutions to the manufacturing and utility industries.

Jay Spann
Senior Solutions Engineer, Swimlane

Jay Spann is the Security Automation Evangelist for Swimlane. With over 28 years of experience and a master's degree in computer science, Jay has led technology initiatives for major organizations like Raytheon and the Department of Defense. He's renowned for his expertise in IT and OT Security. With a keen focus on leveraging low-code solutions, he continues to drive innovation and efficiency in the OT industry's security landscape, ensuring robust protection and streamlined operations for critical infrastructure.