ISMG EXECUTIVE ROUNDTABLE
Sponsored by Fortinet

Outmaneuvering Threat Actors in the Age of Industrial IoT

Agenda

6:00 – 6:30 p.m.
Registration, Networking

6:30 – 6:45 p.m.
Introductions & Opening Remarks

- **Nick Holland**, Senior Editor, Information Security Media Group
- **Christopher Blauvelt**, Global Enablement Engineer – Operational Technology, Fortinet

6:45 – 8:30 p.m.
Roundtable Discussion

8:30 p.m.
Program Concludes

ISMG INFORMATION SECURITY MEDIA GROUP

FORTINET® FAST. SECURE. GLOBAL.

Introduction

While much of the focus on connected devices has been consumer facing, there is a quiet revolution occurring as industrial controls evolve to embrace internet connectivity. Industrial IoT devices create a new threat landscape as IT converges with OT.

With an attack surface that is ever expanding and threat actors potentially causing critical harm, how can industries such as manufacturing, utilities and transportation ensure that they are secure? How can organizations avoid downtime? As demands for SCADA grow, how can organizations manage risk?

If you're looking for new answers to these questions, then welcome to this exclusive executive roundtable on **Outmaneuvering Threat Actors in the Age of Industrial IoT.**

Guided by insights from Christopher Blauvelt, global enablement engineer at this event sponsored by Fortinet, this invitation-only dinner will draw from the experiences of the attendees offering their views on how industrial controls can meet the demands of both security and efficiency in today's connected environment.

Among the discussion topics:

- What are the greatest challenges with the convergence of IT and OT?
- How can organizations take a more proactive approach to IT/OT threat management?
- What are the roadblocks and potential work arounds for gaining internal buy-in for mitigating what are, in many ways, threats without precedent?

You'll have the opportunity to discuss the topic with a handful of senior executives and market leaders in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- What are the biggest issues with the convergence of IT and OT?
- With so many channels of attack (GPS, internet, cellular networks) for industrial devices and an increasingly cloud-based environment, how do you keep abreast of cybersecurity threats?
- How can organizations take a more proactive approach to IT/OT threat management?
- What are the biggest challenges in getting internal buy-in for mitigating what are, in many ways, threats without precedent?
- Where do you perceive to have the greatest resistance when dealing with this type of change? How do you gain internal buy in?
- What would you advise companies investigating SCADA protection to consider when assessing vendors?

About the Expert

Joining our discussion today to share the latest insights and case studies is:

Christopher Blauvelt

Global Enablement Engineer – Operational Technology
Fortinet

Chris brings more than 10 years of cybersecurity and critical infrastructure experience working in the renewable energy industry. He was directly involved in the development, construction, and operations of wind and solar power plants and their high voltage systems. His work within the energy and utility industry has also afforded him experience in the development and maintenance of substation protection, automation, and control systems. Chris has a master's degree in electrical engineering from Clarkson University with thesis work in substation protection, automation, and control involving the IEC61850 family of protocols. When he is not working, Chris enjoys hobby electronics and spending time in the outdoors.

About Fortinet
Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network – today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide, and more than 300,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About the Moderator

Leading our discussion today is:

Nick Holland

Senior Editor,
Information Security Media Group

Holland, an experienced security analyst, has spent the last decade focusing on the intersection of digital banking, payments and security technologies. He has spoken at a variety of conferences and events, including Mobile World Congress, Money2020, Next Bank and SXSW, and has been quoted by The Wall Street Journal, CNN Money, MSNBC, NPR, Forbes, Fortune, BusinessWeek, Time Magazine, The Economist and the Financial Times. He holds an MSc degree in information systems management from the University of Stirling, Scotland.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

CONTEXT

Outmaneuvering Threat Actors in the Age of Industrial IoT

Q&A with Fortinet's Christopher Blauvelt

NOTE: In advance of this event, ISMG's Nick Holland spoke about the issue of IT and OT covergence with Fortinet's Christopher Blauvelt. Following is an excerpt of that conversation.


Christopher Blauvelt

Key Issues

NICK HOLLAND: What do you see as the biggest issues with the convergence of IT and OT?

CHRISTOPHER BLAUVELT: We have to realize that executives across the verticals that make up operational technology – manufacturing, energy and utilities, transportation or any of the Department of Homeland Security (DHS) 16 critical infrastructures for that matter – made the decision to pursue operational efficiency. That decision included the convergence of IT and OT systems. Airgap systems - the more primitive way of protecting those assets - are really absent as you look across the range of OT systems around the globe today.

Safety is still paramount. If you interview an OT system owner, they will always insist that safety and continuous operation are number one and number two on their list. However, there are consequences with convergence. That is what we're facing right now. Convergence is impacting systems where security was not often designed in.

So whether you're talking about endpoints or controllers or more primitive communication protocols that tend to be more exclusive to industrial control systems and SCADA systems, you really are dealing with legacy technology now colliding with modern options. You have to approach the sunset of the airgap with a strategy to design in security with consideration for the legacy systems.

Most operational technology systems are in place 10, 20, 30 years with very little change. That's driven by the motivation to keep things safe and continuously running. So there's a resistance to change. Now consider how quickly IT morphs. You have to assume that you're going to be tackling an environment where you will encounter a range of legacy systems that need security despite the fact that there are some inherent risks.

With convergence and the motivation to digitally transform, you lack visibility. And by that I mean your ability to understand the level of trust with any device or capability that's attached to the network – the infrastructure, regardless of what layer you're at. And, likewise, the need to be able to control – by that I simply mean be able to control the behavior, and the ability to affect any point of operation beyond that level for which you are approved.

So, if you think north, south, east, west in a large enterprise infrastructure, the goal ought to be to contain any issue that might surface. Convergence brings all those ideas and those challenges to bear.

Tracking Threats

HOLLAND: With so many channels of attack for industrial devices, how do you keep abreast of all the cybersecurity threats?

BLAUVELT: We have to acknowledge first that the attack surface has expanded. The convergence that we talked about previously, the idea of drawing together what has historically been air gapped, has

introduced the need to share intelligence. By that I mean gaining real-time situational awareness.

For quite some time, we've had shared intelligence services for the IT world in real time. There's an appetite for it in operational technology, and I'm aware of cybersecurity alliances coming together now.

But the real goal of all of this is getting to actionable intelligence and to be able to thread situational awareness into a designed-in OT security solution. The fabric approaches you're starting to hear about now are enabling intelligence sharing services so that you have speedy awareness within your environment. Without shared intelligence, you're always going to be chasing the adversary, and the adversary is sophisticated today and has the ability to leverage whatever vulnerabilities are available to them to get on the target. Your ability to share and be aware, at speed within your environment, allows you then to build an actionable defense.

Threat Management

HOLLAND: How can organizations take a more proactive approach to IT and OT threat management?

BLAUVELT: We need to depart from the motive of trying to react to what we see. We need to pursue an approach where we're designing in a comprehensive security solution. "Designing in" is really the key here.

We're dealing with a more primitive culture within operational technology. We have to be able to show how we can design in security without interrupting operations. Latency in the world of OT is devastating. It's costly, and the attitude is, "I need security, but I have to be able to run safely and at my continuous speed 24/7."

We bring that understanding and consider ways to design in a solution that delivers the imperatives, including visibility, which is complete knowledge of every device and every capability that is attached to the network regardless of what layer. If we're talking about the intersection where IT and OT come together, we need to have complete visibility for safe and secure operations.

Likewise, we need to have the same imperative in designing in control. As we look at each layer, we start to determine ways to design in micro segmentation to cleverly control access and disable any adversary capability that surfaces. If I'm the adversary, I'm going to remain very stealthy on the target until such time as I want to achieve the effects that I'm after. If I can control the domains, I can detect and then quarantine, detonate, disable or neutralize the threat before it goes live. And that requires at speed behavioral analytics.

By combining things like visibility, control and behavioral analytics, and taking an approach where I design that in, I achieve a more comprehensive solution with great transparency because it's running within the environment. I'm providing the OT system owner the confidence necessary to ensure there are no behaviors – whether it's an adversary-driven one or a sequence of errors – that are going to cause issues on the live plant floor.

"But the real goal of all of this is getting to actionable intelligence and to be able to thread situational awareness into a designed–in solution."

Gaining Buy-In

HOLLAND: It strikes me listening to you that in many ways we're dealing with threats that don't have precedence in our organizations. What do you find to be the biggest challenges in getting internal buy-in to tackle these threats?

BLAUVELT: Yes, that's always the big challenge – to convince investors that what you can't see, in fact, could cause great disruption, financial loss, challenge to trade craft, challenge to your reputation in a competitive world, and naturally across the operational technology and critical structure verticals.

Looking at what the adversary can accomplish and then correlating that to a specific environment is a great first step because it brings reality into the equation. If we understand the intent of the adversary, we're taking the right first step. You have to recognize there's a plethora of real-world examples out there. You can read all about it.

You have to take a step back and look at your own environment, and understand that the adversary may be attempting to run an extortion attack – simply applying ransomware to achieve some financial gain. WannaCry is a perfect example of this. More likely, and data suggests, it's an espionage intent where they're seeking to exfiltrate data to gain your company's secrets. They can then gain an equivalent advantage by leveraging that which is exclusive to your business domain.

And, of course, you can also think about industrial sabotage. That can be subtle – the slight maneuvering or changing of a process within the system that causes an effect on the production line, which then causes an issue down the line when you're producing and delivering consumer goods. Now your issue multiplies because your reputation's at stake. Or the sabotage could extend all the way to the kinetic, where I'm able to disrupt your safety instrumentation system. And if I can accomplish that, I can preclude your ability to stop a process that's run afoul and could actually cause physical harm – not just to the plant, but to the people within the plant as well.

You must know that the adversary is going to accomplish penetration of the environment in multiple points. The first order of battle is to get on the target in multiple places so that I have more than one way to achieve success. Of course, the designing in leveraging a security fabric says, "Hey, I'm going to counter that by recognizing behaviors and neutralizing them at real speed but in a way that never allows them to affect live operations."

"If we understand the intent of the adversary, we're taking the right first step."

Assessing Vendors

HOLLAND: What would you advise organizations that are investigating SCADA, industrial controls protection, to consider when they're assessing vendors?

BLAUVELT: We're talking about an approach that is about designing in security to get scalability of a solution that runs at speed. It really is about being able to work and partner with the SCADA or ICS system owner and take them on a journey. The first step is about understanding the system environment and then being able to design in a complete solution.

The operational technology system owner is not willing to disrupt their operation. Change can be difficult. They want to take an approach where they can get from where they are today to the end point of a complete designed-in solution that gives them the situational awareness and the confidence that their operations, and the integrity of those operations, are preserved.

The journey begins with understanding followed by aligning the imperatives of the OT system owner with the security priorities of the business. By taking an approach that allows you to design in a range of capabilities for a complete solution – considering visibility, control and behavioral analytics – you will enable an agile organization the has an its eye on safety, availability and security across this new IT / OT converged environment. ■

Notes

Notes

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY® Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io