CYBER DEFENSE MAGAZINE

eMAGAZINE

DECEMBER 2023

In This Edition

Bolstering IoT Cybersecurity Amid an Evolving Landscape: A CEO's Perspective

What’s The Role of Gaslighting in The Cyber Security Context of Social Engineering?

Generative Ai: The Future of Cloud Security

…and much more…

MORE INSIDE!

Key Differences in Securing OT & IT Environments

Critical cybersecurity components every security leader must know amid the convergence of IT & OT

By Joe O’Donnell, EVP of Corporate Development, Cyolo

The increasing cyberattacks against critical sectors, in addition to the growing convergence of operational technology (OT) and information technology (IT), spotlights the need for comprehensive ownership around OT security. Today, most organizations are looking to cybersecurity leaders, including Chief Information Security Officers (CISOs), to solve the problem.

Many leaders in the industry have shown great strength in securing IT environments and have successfully overcome highly disruptive events. However, IT security strategies and tools often do not translate to the OT environment. A comprehensive effort must be made to fully understand the OT landscape’s distinctive challenges and unique topography. To that end, let’s explore the key considerations for securing OT environments.

Systems Unavailable? Not an Option

In an IT environment, experiencing downtime for upgrades and patches, although inconvenient, is typically manageable. This is especially true in a Software-as-a-Service (SaaS) setting where new updates are continuously rolled out.

However, in the realm of OT environments, halting operations to implement a new operating system or apply a critical patch simply isn't an option. OT systems must maintain continuous operation for reasons of both safety and profitability. Any process that requires downtime is essentially a non-starter. For this reason, it's not unusual for CISOs to find that their infrastructure consists of decades-old systems that still serve as a critical piece of their operations.

The challenge for CISOs is identifying security controls that will seamlessly adapt to their current OT processes without interrupting them. The proper solutions will protect current infrastructure and critical processes without changing them or adding unnecessary complexity.

What Does Remote Access Mean for OT?

Typically, OT systems have been secured through isolation. As organizations increasingly connect OT and IT environments to allow easier access for third parties, or to capitalize on digitization, they must ensure that all access – regardless of who, where and how – is monitored, controlled and recorded.

Essentially, this means that any user trying to access an OT environment is considered an outsider until proven otherwise. Whether it is an employee, vendor or OT operator attempting to gain access to your data, any connection coming from the outside must not be trusted. It is no longer acceptable to only set up controls for what IT would consider to be remote.

Understanding the concept of 'never trust, always verify,' organizations need to continuously identify and authenticate every device, user and identity before providing them with access to network apps –securing all types of access scenarios and not just the standard and known ones.

Safety and Tools in OT & IT Environments

Though OT and IT security elements tend to operate differently, safety is always the common denominator.

In the OT world, safety refers to the reliability and responsiveness of cyber-physical systems. For instance, if an industrial boiler or blast furnace malfunctions, it could pose a threat to workers. On an enterprise level, system availability is crucial for maintaining precise and uninterrupted operations, ultimately driving profitability and productivity.

In IT, safety is defined as data protection. On an individual level, a compromise of data exposes them to substantial risks that can jeopardize their identity. On an organizational scale, protecting data helps avoid fines, data breaches and damage to reputation.

Given these distinctions, the tools tailored for IT seldom align with OT needs. One of the primary challenges comes from the disruptive nature of certain IT tools in OT environments. For instance, basic functions like vulnerability scanning, while essential in IT, can inadvertently interrupt critical OT processes and even render systems completely offline. This is exacerbated by the fact that most OT devices lack the necessary computational resources (CPU/RAM) to support endpoint security measures such as anti-virus software or other agents.

Another significant disparity lies in how data traffic is managed. IT tools are designed to route traffic through the cloud, which can be a serious detriment in OT environments. Unlike IT setups, OT systems often consist of numerous unconnected components that require a localized approach to data handling. Cloud-based routing compromises availability and simply cannot accommodate the unique architecture of OT environments.

IT tools and OT devices also differ in their lifecycles. IT solutions typically have much shorter lifespans compared to the robust, long-term endurance of OT equipment. The perpetual operation of OT environments leaves little room for tools that necessitate frequent patching, updates or downtime. The always-up nature of OT systems demands tools that can seamlessly integrate without causing operational disruptions.

Attempting to force-fit IT-designed tools into OT environments not only introduces unnecessary complexity but also fails to address the fundamental security needs of these distinct operational landscapes. Recognizing that OT systems require specialized security solutions tailored to their unique characteristics is paramount. By understanding these differences and embracing security tools designed specifically for OT, CISOs can enhance the security posture of their organizations, ensuring both safety and efficiency in today's interconnected world.

Converging OT & IT in a Digitally Advanced Era

It is critical for security leaders to fully comprehend the differences between OT and IT security. The many complexities across these environments could have a major impact on the business.

Learning and addressing the unique requirements of both systems will allow for a more effective security approach. CISO’s taking on this responsibility will benefit greatly by expanding “outside” of the systemic view and build relationships with plant managers and asset owners. Only then can the business successfully converge OT and IT environments. This approach will ensure that OT and IT practitioners help the business remain safe and competitive within ever evolving and advancing digital environments.

About the Author

Joe O'Donnell is a seasoned cyber security professional with over 30 years of experience in senior management roles. Throughout his career, he has made significant contributions to renowned companies such as Cisco Systems, Nortel, Palo Alto Networks, and currently, Cyolo. Joe's expertise lies in developing and leading successful programs, teams, and business lines. He has collaborated with exceptional colleagues to drive impactful new product launches and go-to-market strategies, including pioneering the first Industrial Cyber GTM. At Cyolo, Joe is at the forefront of the groundbreaking Industry 4.0 movement. Alongside his leadership in new product introductions, he is also recognized as a four-time CRN Channel Chief and a proud United States Coast Guard Veteran.

Joe can be reached online at https://www.linkedin.com/in/jodo/ and at https://cyolo.io/