IT-OT Security Convergence Key to Optimizing Risk Management

Latest report reveals major visibility gaps in operational technology detection and response

DALLAS, June 27, 2023 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced a new study revealing that enterprise Security Operation Centers (SOCs) are expanding their capabilities to the OT domain, but major visibility and skills-related challenges are causing roadblocks.

To read a full copy of the SANS Institute report, *Breaking IT/OT Silos With ICS/OT Visibility*, please visit: https://resources.trendmicro.com/SANS-ICS-OT-Visibility-Survey.html

Bill Malik, vice president of infrastructure strategies at Trend Micro "IT-OT integration is already driving digital transformation for many industrial organizations, but to effectively manage risk in these environments, IT and OT security operations (SecOps) must also converge. OT security programs may be lagging, but there's a fantastic opportunity to close the visibility and skills gap by consolidating onto a single SecOps platform like Trend Vision One."

The study finds that half of the organizations now have an enterprise SOC that includes some level of ICS/OT visibility. However, even where respondents have a more "expansive" SOC, only half (53%) of their OT environments provided data for detection purposes.

This shortfall is also implicit in another finding: cyber event detection (63%) is the top capability that respondents want to integrate between IT and OT silos, followed by asset inventory (57%) and identity and access management (57%). Being able to detect events across IT and OT environments is the most critical to identifying root causes and preempting future threats that could potentially disrupt operations.

The report highlights endpoint detection and response (EDR) and internal network security monitoring (NSM) as crucial tools to help provide that root cause data. However, deployment of EDR on engineering and operator assets stands at less than a third (30%) of responding organizations.

NSM is rarely (<10%) deployed at a physical process and basic control level deep in OT environments.

Aside from visibility gaps, the study reveals major people and process challenges to expanding SecOps across IT and ICS/OT environments. Four out of the five top barriers highlighted by respondents are related to staff:

- Training IT staff in OT security (54%)
- Communication silos between relevant departments (39%)
- Hiring and retaining staff who understand cybersecurity (38%)
- Training OT staff in IT (38%)
- Insufficient risk visibility across IT and OT domains (38%)

Legacy technology is also cited as a top challenge for expanding OT SecOps visibility.

The limitations of legacy devices and networks (45%) and IT technologies not designed for OT environments (37%) are named among the top three challenges here, alongside a lack of OT knowledge among IT staff (40%).

Going forward, respondents are doubling down on efforts to converge IT-OT SecOps and drive greater visibility into OT threats.

Two-thirds (67%) plan to expand their SOC, and for those who have already deployed EDR, 76% are planning to expand these deployments in ICS/OT over the coming 24 months. Additionally, 70% of those who have already added NSM capabilities plan to expand these deployments in the same time frame.

**Trend Micro commissioned the SANS Institute to interview 350 SANS community members who are ICS/OT professionals working in critical infrastructure sectors across the US, Europe, and Asia.*

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for

environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

Media Contact:
Trend Micro Communications
817-522-7911
media_relations@trendmicro.com
