Beyond the Report: How OT Threat Intelligence Drives Safer Operations

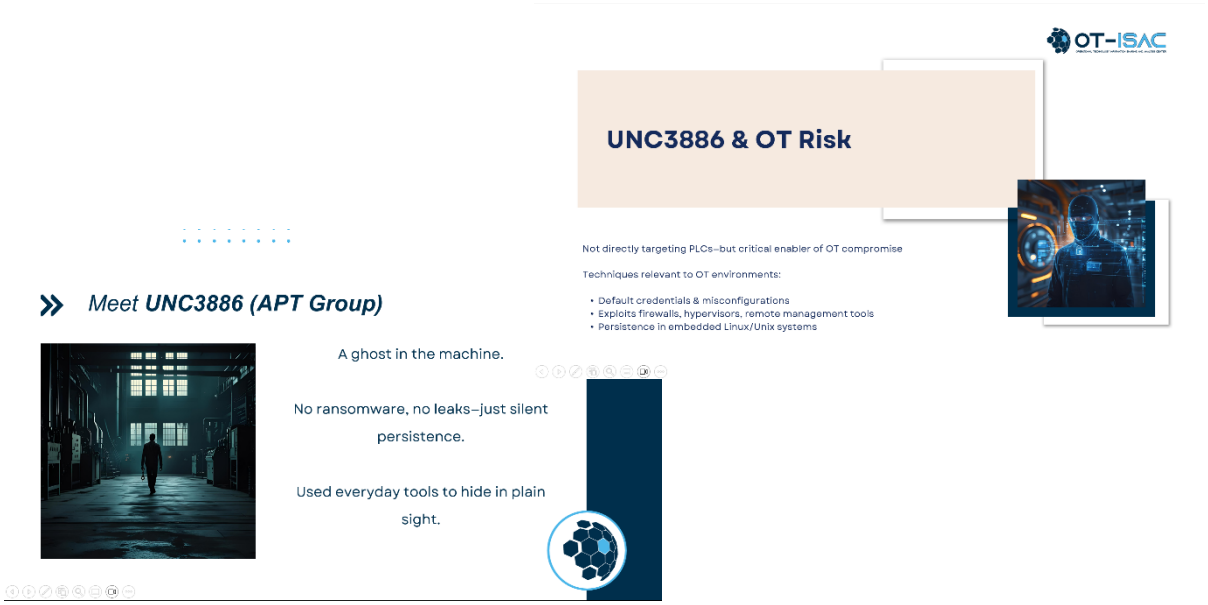
SINGAPORE—The future of industrial automation was a central theme at the 2nd ARC Singapore Industry Forum, held on August 7, 2025, in Singapore. Dedicated to **"Winning in the Industrial AI Era,"** the event brought together experts from technology users, suppliers, and industry associations. The forum showcased how open standards, AI, 5G, robotics, and cybersecurity are converging to shape the next generation of industrial operations.

Among the invaluable perspectives shared, AJ Eserjose, Regional Director of OT-ISAC, delivered a presentation that reframed the discussion on OT cybersecurity. Titled **"Beyond the Report: How OT Threat Intelligence Drives Safer Operations,"** the talk highlighted the critical shift from passive threat reporting to proactive, actionable intelligence in operational technology (OT) environments.

The session began by explaining that traditional, generalized threat reports are often ineffective for OT systems, which control physical processes in critical sectors like energy and manufacturing. The unique nature of these environments demands a different, more focused approach to security.

A key part of the presentation involved a real-world case study of the advanced persistent threat (APT) group known as UNC3886. This example served to illustrate a crucial point: attackers are not always using well-known ransomware or malware. The UNC3886 group, for instance, compromised critical infrastructure by leveraging

legitimate tools and misconfigurations, making their actions difficult to detect with traditional, signature-based security tools. This case underscores the importance of shifting the focus from known threats to detecting attacker behavior patterns.



The session highlighted that, through collaborative efforts, effective OT threat intelligence must be built on several key elements:

- Attacker behavior patterns: Understanding how adversaries operate is more valuable than simply knowing what tools they use.
- Protocol misuse: Focusing on how attackers might exploit protocols within the unique context of OT systems.
- Threat mapping: Utilizing frameworks like the MITRE ATT&CK for ICS to map threats and understand an attacker's tactics and techniques.
- Vulnerability advisories: Providing information on vulnerabilities along with practical, compensating controls to mitigate risks.
- Post-incident learnings: Sharing lessons learned from past incidents to strengthen the entire community's defenses.

The presentation concluded with a call to action for the OT community. OT-ISAC emphasized the need for organizations to move beyond a passive defensive stance and become active cybersecurity contributors in the industry. The OT sector are encouraged to build internal processes for threat intelligence and viewing

cybersecurity not just as a technical problem but as a "team sport" that requires close collaboration between both IT and OT teams.

This topic was a testament to the forum's goal of fostering a deeper understanding of the technologies driving industrial change. The collective expertise of all 22 speakers provided pillars to build upon to help shape the future of industrial automation.

You can watch the full presentation here:
https://www.youtube.com/watch?v=3guOJlVve8E&feature=youtu.be

About OT-ISAC

Operational Technology Information Sharing and Analysis Center (OT-ISAC) is a secure threat information sharing community for Operational Technology-using companies headquartered in Asia Pacific.

A member company can securely and anonymously share threat information with OT-ISAC analysts who further enrich and disseminate actionable alerts, intelligence and best practices for all community members to defend themselves and take mitigating action against malicious actors, their tools, and system exploits. OT-ISAC also partners with government, private vendors and other information sharing organisations to acquire and disseminate timely and relevant information for the resilience of member companies.

Interested organisations in energy, water, and other OT-using sectors may contact AJ Eserjose to inquire about membership: aeserjose@grf.org.

Learn more on Twitter and LinkedIn or visit www.otisac.org