ICS EUROPE SUMMIT 2024

SANS

AGENDA

Sunday 12th May

Time (CEST)	Description
8:30 - 9:15am	**Registration & Networking**
9:15 - 9:25am	**Opening Remarks** Tim Conway, Senior Instructor, SANS
9:25 - 9:55am	**Threat-Intelligence Based Defense-In-Depth Implementation in OT Environments** Matan Dobrushin, Field CTO, OTORIO This talk explores the concept of Defense in Depth (DID), its relevance in OT environments, and a new approach proposing using open-source threat intelligence sources to prioritize the implementation plan of DID in OT. The talk explores the detection and protection mechanisms that suit the unique characteristics of OT environments, ensuring robust cybersecurity in the face of the latest threats discovered (with case studies included). We will address the practical aspect of prioritizing Defense in Depth strategies within OT networks. With limited resources, the audience is encouraged to critically analyze their cybersecurity investments to the most effective utilization of their budget. If you had only one dollar to allocate, what would be the most impactful step to take? We will showcase a new, promising Threat-intelligence knowledgebase by MITRE called MITRE D3FEND, and showcase how it can be leveraged it in order to help with that mission. Key Takeaways: • Understanding Defense in Depth (DID) and its relevance in OT environments. • Leveraging DCS and other ICS security features to enhance DID effectiveness. • Tailoring detection and protection mechanisms to suit the uniqueness of OT environments. • Prioritizing defense strategies with limited resources for optimal cybersecurity outcomes, based on threat-intelligence knowledgebase like MITRE D3FEND.
10:00 - 10:30	**Breaking The Loop of Uncertainty: How To Get Back to Normal After an OT Incident** Kai Thomsen, Certified Instructor, SANS The talk will present some case studies of recent incidents we have responded to and highlight what works and what doesn't in providing enough certainty, situational awareness, and a recommended course of action to go back online and back to normal after an incident has either touched an ICS/OT environment directly or forced operators to severe connections to the business network.

ICS EUROPE SUMMIT 2024

SANS

Time (CEST)	Description
10:30 - 10:50am	**Networking Break**
10:50 - 11:20am	**Threat Hunting Does Not Have to Be Hard** Don C. Weber, Certified Instructor, SANS Threat hunting to find EVIL can be a difficult endeavor, if you let it. Many people think that they are using threat hunting to find the bad guys in the network. Threat hunting can identify malicious insiders and hackers but it most often identifies misconfigured applications, servers, and network devices. It can also provide context around normal and abnormal user and administrative behaviors. Weather you are a medium sized shop, small shop, or a one-person IT / network / cybersecurity staff your team can use threat hunting to improve operations while also reducing risk. In this talk, Don will simplify threat hunting activities. The goal will be to provide a repeatable process that can be used by yoru administrators to understand what is really happening on the network. The process will also provide the basis for justifying equipment and work hours to make this important process successful. All of this will, in turn, dramatically reduce the time it takes your team to respond to a compromise.
11:25 - 11:50pm	**The BackupAlchemy Tool: Utilising Backups to Improve Security Posture of Complex Environments** Falk Lindner, Expert on Industrial Systems Cybersecurity, Airbus Operations GmbH Daniel Meister, Cybersecurity Project Leader, Airbus Defence and Space GmbH In today's fast-paced digital landscape, protecting critical data is essential. Organizations rely on robust backup strategies to safeguard sensitive information, including conducting thorough security analyses on backup files. As part of our innovation initiative, we're unveiling a groundbreaking project demonstrating the use of open-source GitHub projects to directly scrutinize backup files of Operational Technology (OT) systems or extensive collections of Virtual Machines (VMs). The outcomes seamlessly integrate into cybersecurity operations, incident response, and compliance audits, drastically reducing conventional timeframes from hours or days to just minutes or seconds, particularly beneficial for isolated or legacy systems where traditional methods aren't feasible. This versatile tool can be executed locally for ad-hoc operations or centrally in locations with access to backup archives. We'll delve into leveraging open-source tools for efficient data collection and analysis, generating customized security reports, and enhancing daily security operations, including configuration and vulnerability management, as well as incident response activities like response preparation and root cause analysis.

ICS EUROPE SUMMIT 2024

SANS

Time (CEST)	Description
11:50 - 12:15pm	**SCADAsploit: A Command & Control for OT. How to Break an ICS System.** Omar Morando, Head of OT Cybersecurity, HWG Sababa Industries heavily rely on Operational Technology (OT) and Supervisory Control and Data Acquisition (SCADA) systems, making robust cybersecurity measures crucial. This presentation delves into comprehensive studies evaluating and enhancing security practices in OT/SCADA environments. Real-world case studies and experiences will be explored, highlighting challenges faced and lessons learned in implementing and managing security measures. Key topics include threat landscapes specific to OT/SCADA, vulnerabilities in legacy systems, and the evolving cyber threat landscape targeting critical infrastructure. Practical insights from successful security implementations, incident response strategies, and the importance of risk management will be shared. Emphasis will be placed on the collaborative efforts between IT and OT teams to establish a holistic security framework. Participants can expect to gain a deeper understanding of unique security considerations in OT/SCADA environments and actionable takeaways to strengthen their systems against emerging cyber threats. This presentation aims to provide valuable insights to professionals in industrial control systems, fostering a proactive approach to cybersecurity in critical infrastructure.
12:15 - 1:15pm	**Networking Lunch**
1:15 - 1:50pm	**What You Need To Know About the NIS II Directive From an ICS Perspective** Brian Correia, Director of Business Development, GIAC, SANS Institute Tim Conway, Senior Instructor Kai Thomsen, Certified Instructor Don Weber, SANS Instructor Join us for a panel discussion with top ICS practitioners on what you need to know to get your organisation up to speed on the upcoming disclosure requirements for all critical sector organisations doing business in the European Union. Some of the items we will cover include: • The goals of the NIS II Risk Management, Strategy, Governance and Incident Disclosure. • What do you need to do to stay compliant from an ICS perspective? • What should be included in your yearly report to ENISA? • What are considered best practices in ICS to avoid cyber incidents? Moderated by Brian Correia, Director of Business Development at GIAC, join Tim Conway, SANS curriculum lead in ICS, Kai Thomsen, certified SANS instructor and Don C Weber, certified SANS instructor, on what you need to know and solutions from faculty members in meeting the new requirements by October 2024.

ICS EUROPE SUMMIT 2024

SANS

Time (CEST)	Description
1:55 - 2.25pm	**OT Business Continuity Plan and Demonstration - 30 Seconds Recovery From a Ransomware Attack** Oleg Vusiker, CTO, Salvador Technologies In the context of Operational Technology (OT), this lecture emphasizes the indispensable role of a robust Business Continuity Plan (BCP). It explores methods for automating backup procedures, highlighting their critical contribution to sustaining operational resilience. Furthermore, the lecture underscores the significance of offsite backups and the implementation of air-gapped solutions for securing vital operational data. A pivotal aspect of the presentation involves a live demonstration, simulating a ransomware attack on a Human-Machine Interface (HMI), showcasing the rapid recovery capabilities, including a 30-second restoration from an air-gapped storage. Through this practical illustration, the lecture aims to convey the proactive measures taken to bolster security within the dynamic landscape of Operational Technology.
2:25 - 2:35pm	**Comfort Break**
2:35 - 3:00pm	**Tactical Packet Analysis** Julian Gutmanis, Principal Detection Engineer, Dragos Packets and payloads and data and stuff. When you're in the middle of an incident, or dealing with an unexpected event, being able to answer questions about your network quickly is a valuable skill. This talk will provide tactical approaches, examples and code for making sense of your ICS environment, with a dash of stats.
3:05 - 3:30pm	**FuxNet: the New ICS Malware that Targets Critical Infrastructure Sensors** Noam Moshe, Vulnerability Researcher, Claroty Team82 Around April 2024 a Ukrainian affiliated hacking group named BlackJack claimed they attacked Russia's Industrial Sensor and Monitoring Infrastructure company called Moscollector. Not only did the hackers allegedly destroy Moscollector's servers and databases, they also deployed a notorious malware called FuxNet (rhymes with Stuxnet) which bricked many sensor gateways, essentially blinding physical operations monitoring capabilities over tens of thousands of sensors deployed across Moscow. In this talk we will unfold all the events preceding the final attack and discuss the true meaning of a new ICS malware targeting critical infrastructure sensors in a modern city like Moscow.
3:30 - 3:50pm	**Networking Break**

ICS EUROPE SUMMIT 2024

SANS

Time (CEST)	Description
3:50 - 4:15pm	**The Art of Deception - How to Use Modern Honeypots to Secure ICS Environments** Daniel Buhmann, Principal Systems Engineer OT/IoT, Fortinet Most industrial companies already implemented many security measures in their environment. But how do you know if these measures a sufficient? If an attack will bypass these measures, will you be able to detect and respond in the shortest possible time? Honeypots have been around for a while, but deception technology goes well beyond a high interaction honeypot. This presentation will show up why deception technology is a powerful tool for protecting OT infrastructures and that deception technology does not require AI or machine learning and can generate threat intelligence for threat analytics and hunting purposes. The speaker will demonstrate that deception is a technology that includes benefits like non-intrusiveness, ease of installation, lack of false alarms, and cost-effectiveness.
4:20 - 4:45pm	**Cyber War in Ukraine: 2 Years After** Russian war in Ukraine is the first example of a full-scale cyber war. The dramatic increase in the number of cyberattacks and critical cyber incidents was observed in Ukraine since the beginning of the full-scale invasion. This talk will discuss the unprecedented massive attacks aimed at wiping out infrastructure through various types of attacks performed, including DDOS, website defacing, data theft and the use of wipers. The cyberattacks were combined with psychological information operations and were often accompanied by kinetic attacks. Lessons learned will be shared for consideration by defenders working in the critical infrastructure community.
4:50 - 5:15pm	**Easy to Say Hard to Do: Lessons Learned in a Hard Way While Deploying OT Security Monitoring Solutions on a Global Scale** Can Kurnaz, PCD Technology Specialist, Heineken The convergence of Operational Technology (OT) and Information Technology (IT) landscapes has introduced new challenges for organizations striving to secure critical infrastructure. This presentation aims to share valuable insights and lessons learned from the deployment of OT security monitoring solutions on a global scale, with a focus on challenges on the road for roll-out and integration with Security Operations Center (SOC). By sharing these lessons learned, this presentation aims to empower organizations to navigate the complexities of deploying OT security monitoring solutions on a global scale and fostering a cyber-resilient ecosystem that safeguards critical infrastructure.
5:15 - 5:20pm	**Closing Remarks** Tim Conway, Senior Instructor, SANS
5:20 - 7:00pm	**Networking and Drinks**