(CS)²AI Online™ Symposium: Control System Cyber Security for Energy

Part 1: Oil & Gas Sector

Today's Program

1:00 - 1:10 PM	Kickoff: Derek Harp, Founder & Chairman of (CS)²AI
1:10 - 2:00 PM	Keynote: Oil & Gas Threat Intelligence Briefing (+Q&A) with Daniel Kapellman Zafra
2:10 - 2:35 PM	OT Threat Hunting: What "Good" Looks Like (+Q&A) with Neal Gay
2:35- 3:00 PM	OT Cyber Process Hazard Analysis (+Q&A) with Hossain Alshedoki
3:00 - 3:25 PM	Leverage the Right Tools to Uplift Your Detection (+Q&A) with Richard Diver
3:25 - 3:50 PM	Cyber Response: Lessons Learned from OT Incident Response with Rob Caldwell & Rob Labbe
4:15 - 4:40 PM	Command & Control: 4 Things You Can't Live Without (+Q&A) with Megan Samford
4:40 - 5:00 PM	Cyber Resiliency: Disruptive Thinking is Needed for OT Resilience (+Q&A) with Ronald Heil
5:00 – 6:00 PM	CISO Panel with Ryan Boulais, Gustavo Diaz, and Talal Baeshen
6:00 – 6:05 PM	Symposium Wrap-Up Bolt-On Technical Bonus Session
6:05 - 6:50 PM	Cyber Oil & Gas Lab Demonstration (+Q&A) with Pablo Almada, Deovanny Manzanero, & Matias Manassero

For LIVE SPANISH translation, please visit our Zoom room at: https://us06web.zoom.us/j/**85809024652**

Derek Harp, Symposium Host

Derek Harp
Founder and Chairman, the Control System Cyber Security Association International – (CS)^{2}AI
https://www.linkedin.com/in/derekharp/

Keynote: Oil and Gas Threat Intelligence Briefing

Intelligence often makes the difference for organizations between being prepared to defend and being a victim. To defend, we must know who is targeting us, what they are after and how they maneuver. Knowing whether you are vulnerable to compromise for Oil and Gas can not only mean loss of revenue, but impact to whole countries. Empower your team with Mandiant's uniquely dynamic view of the threat landscape – specific to the Oil and Gas industry. Join Daniel Kapellmann Zafra for an in depth look at the threats facing Oil and Gas; what behaviors to understand and what vulnerabilities to address in defending against the todays advanced threats.

Daniel Kapellman Zafra,
Manager, Threat Intelligence, Mandiant
https://www.linkedin.com/in/danielkapellmannzafra/

OT Threat Hunting: What "Good" Looks Like

Exposing attackers that your technical controls may have missed often with cyber threat hunting requires advanced security skills that are hard to keep on staff. Hunting across our OT environment is not as simple as conducting sweeps and matching the latest attacker techniques to the results. How do you know if your team, or your provider, has got what it takes to find todays advanced attacks in your environment? Join Neal Gay for a look inside Mandiant's OT Threat Hunting team and learn what is required to hunt across endpoint, network, and logs for stealthy attacks to OT infrastructure.

Neal Gay
Senior Manager, Managed Defense, Mandiant
https://www.linkedin.com/in/neal-gay-401338a/

Cyber Process Hazards Analysis

What if communication stacks have been hacked, Remote Access Trojans have compromised control, or Safety Instrumented Systems have been hacked. Then here we are introducing a safety risk which was a consequence of a cyber-attack. In this session, Hossain Alshedoki is going to introduce the Cyber PHA approach to identify the safety risks which can be triggered by Cyber-attack, so this approach can help organization for a better preparation, detection, response planning within the Cyber program.

Hossain Alshedoki
Associate Director, IT/OT Cybersecurity & Privacy ENR Sector Lead, KPMG-Saudi Arabia
https://www.linkedin.com/in/hossain-alshedoki-29a76aa9/

Leverage the Right Tools to Uplift Your Detection

Do you have tools that align your IT and OT security tech stack for swift threat detection? Do you have the security expertise you need to defend against today's sophisticated attackers? Join Microsoft's Richard Diver to learn how to leverage Microsoft Azure Defender to identify cyber-attacks and prevent them from disrupting your operations. Richard will demonstrate how Defender fits into your existing tech stack to add needed visibility and detection ability to your defense.

Richard Diver
Senior Technical Business Strategy Manager, Microsoft
linkedin.com/in/rdiver

Cyber Response: Lessons Learned from OT Incident Response (Recorded Session)

Participate in this Rob Caldwell's discussion with Rob Labbe of Teck Resources as we touch on some of the lessons learned from responding to OT incidents. Rob shares what has worked, as well as some of the challenges he has faced. Rob talks about how the theoretical translates to the practical in real-life scenarios, and what actually happens in the heat of the moment.

Rob Labbe
Director of Information Security at Teck Resources
linkedin.com/in/rob-labbe

Rob Caldwell
Director of ICS/OT, Mandiant
https://www.linkedin.com/in/robert-caldwell-ab67787

Validate: Not Just a Pen Test

Red Team, Blue Team, Purple Team—oh my! Knowing the effectiveness of your people, processes and tools is critical to your overall defense. Hear from Evan Pena as he shares which testing to do when and why. You'll hear about hidden outcomes from validation testing such as: getting a complete picture of the attack surface and finding ineffective controls due to misconfiguration or operational drift.

Evan Pena
Director and Global Red Team Lead, Mandiant
https://www.linkedin.com/in/evan-pena-06a9221b/

Command and Control: Four Things You Can't Manage Without

While the other functions of your cyber defense program establish capabilities to identify, mitigate, and respond to threats, the Command and Control, or management function keeps all of these capabilities aligned to the mission. Organizations often find each group within their cyber defense is acting independently which leads to an ineffective defense. Join Megan Samford as she shares the four things you can do to keep each of your cyber functions focused on the mission.

Megan Samford
VP, Chief Product Security Officer - Energy Management, Schneider Electric
https://www.linkedin.com/in/megan-samford-13282814/

Cyber Resiliency: Disruptive thinking is needed for OT Resilience

Cyber-attacks on industrial environments are on the rise and become more and more impactful. Although these environments are quite vulnerable, the world is (with increasing speed) introducing hyper connectivity over modernization and optimization initiatives like digitalization, Industrial Internet of Things, Cloud usage, etc. It is easy to conclude that this can be a dangerous mix. How can you enable OT Resilience? In this presentation Ronald Heil will highlight 5 core activities and why a mix with Disruptive Thinking is required.

Ronald Heil
Partner & Global Risk Advisory Lead for Energy sector, KPMG-Netherlands
https://www.linkedin.com/in/ronald-heil/

CISO Roundtable

Talal Baeshen
Head of OT Cybersecurity, Ma'aden
https://www.linkedin.com/in/talal-a-baeshen-ab6713183/

Gustavo Díaz
Information Security Senior Director, Tenaris
https://www.linkedin.com/in/gustavo-a-d%C3%ADaz-5a0b66/

Ryan Boulais
VP and CISO, AES
https://www.linkedin.com/in/ryan-boulais-b862129/

Bolt-On Technical Session: Cyber Security Oil & Gas Lab Demo

Pablo Almada
Partner, OT/IIoT Practice, KPMG-Argentina
https://www.linkedin.com/in/palmada/

Deovanny Rafael Gomez Manzanero
OT/ICS Cybersecurity Supervising Senior Consultant, KPMG-Argentina
https://www.linkedin.com/in/deovanny-rafael/

Matias Manassero
OT/ICS Cybersecurity Senior Consultant, KPMG-Argentina
https://www.linkedin.com/in/mmanassero/

1. **Topic of demo:**
   - **a.** Current Cyber Threats.
   - **b.** Cyber-Attack demos in an industrial and controlled set-up.
   - **c.** Real Impact of an Industrial Cyber Attack.
   - **d.** Understand how the capabilities of modern OT/ICS Cybersecurity solutions can help you to prevent and protect undesired operation interruption.
2. **Synopsis of demo:**
   a. Amid the on-going cyber threats impairing operations worldwide, the OT/ICS Cybersecurity Team from KPMG will provide insight about the real impact of an Cyber-attack in an industrial set-up, based on a set of cyber-attacks performed in their brand new OT/ICS Cyber Range.
   b. The cyber-attacks to cover are: Ransomware-based infection, and major failure of a PLC (Fault-Condition).
   c. The cyber-attacks will be performed using production grade equipment (PLCs, media converters) along with scale-model version of the industrial process to mimic the real-life consequence, like: pump cavitation, halting automatic valves remote operation, and loss of visibility (HMI) of the industrial process.
   d. Additionally, the goal is to set up the tone for establishing a Mindshift within the audience, based on the hands-on examples and the OT/ICS cybersecurity practices provided, so they can take them back to work and implement them within their team, for raising OT cyber-awareness.