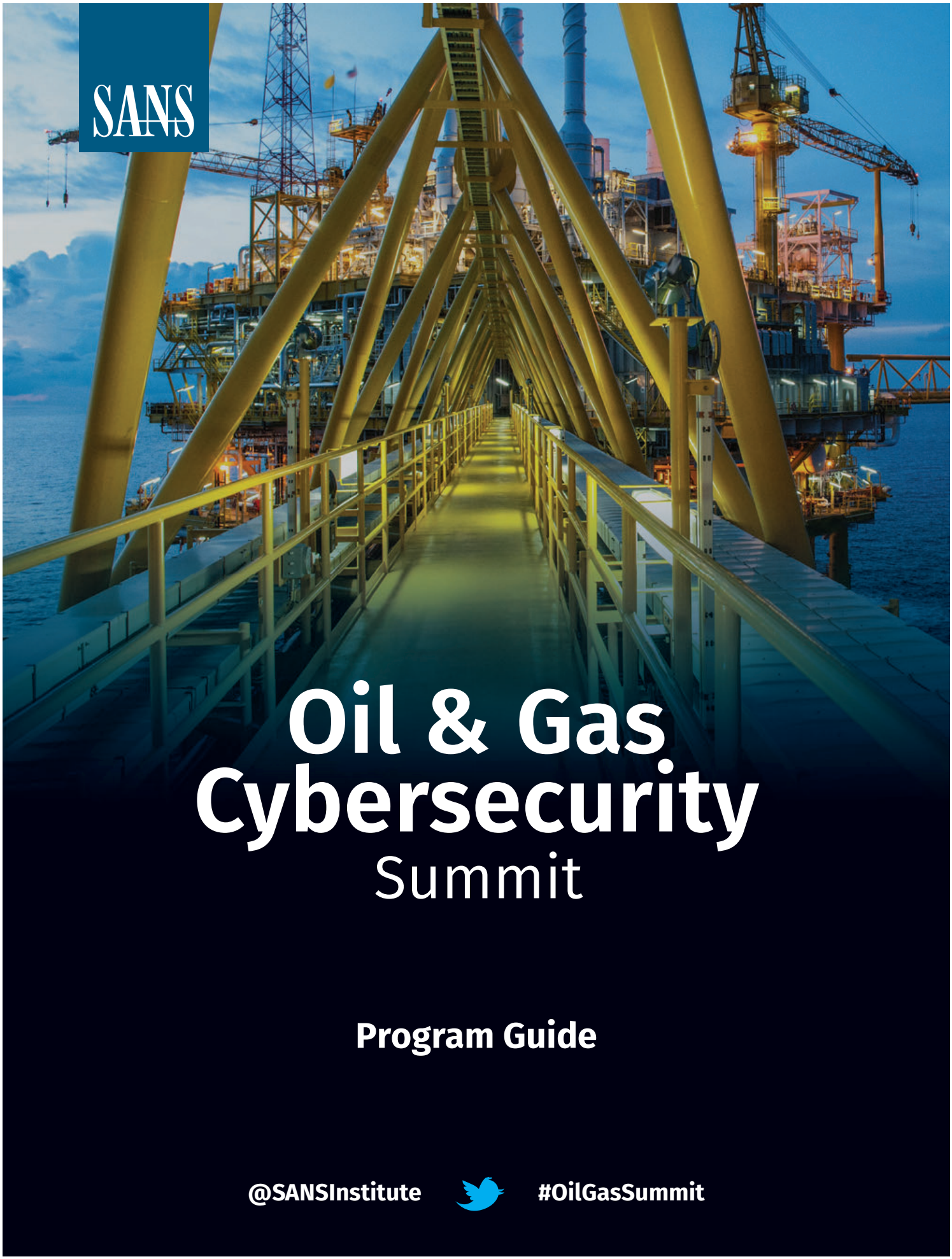

SANS

Oil & Gas Cybersecurity Summit

Program Guide

@SANSInstitute #OilGasSummit

Agenda

All Summit Sessions will be held in the Regency AB Foyer (unless noted).

All approved presentations will be available online following the Summit at ***sans.org/summit-archives/ics***

Sunday, September 30

6:00-7:30 pm	**Welcome Reception & Early Registration** (LOCATION: REGENCY FOYER) Pick up your Summit materials and get a jump on networking at the Sunday evening welcome reception. Join us as we kick off the event and discuss trends and challenges facing the oil and gas industry and keys to operational security success.

Monday, October 1

8:00-9:00 am	**Registration & Continental Breakfast** (LOCATION: REGENCY AB FOYER)
9:00-9:15 am	***Welcome & Introductions*** ***Doug Wylie****, Summit Chair*
9:15-10:00 am	***Keynote: Blurring the Lines between IT and OT: Building a Better Defense through Partnership*** Traditionally, information technology (IT) and operational technology (OT) have had fairly separate roles, dividing the security conversation into confidentiality, integrity, and availability, versus safety and reliability. The continuing digitization of all aspects of the oil and gas industry has created an interdependence that many IT and OT professionals still fail to recognize, and the divisive "IT versus OT" conversation has grown stale. Chevron's CISO discusses the critical need for building partnerships between IT and OT and finding the common ground to more secure and productive operations. ***Steve Neiers****, Chief Information Security Officer, Chevron*
10:00-10:20 am	**Networking Break** (LOCATION: REGENCY AB FOYER)
10:20-11:05 am	***Using Augmented Reality to Streamline Design, Construction, and Operations of a Major O&G Facility*** BP has long-established policies and procedures for digital security management and assurance. Like many similar companies, it has been a challenge to align existing facilities and their associated practices to meet these requirements and keep up with the ever-changing security landscape. This presentation highlights some of the challenges and opportunities for BP in the development of a major new facility, in particular: • The challenges of securing the IT/OT environment: working with multiple vendors, with existing and new technology. • Balancing ease of use and accessibility: Remote access demands in a multi-vendor environment. • New technology adoption: Applying LTE, Augmented Reality and other technology to streamline project and operations activities. ***Steve Mustard*** *(@steve_mustard), Digital Security & Risk Consultant* ***Ken Nguyen****, Mad Dog 2 IT&S Program Manager, BP*

Monday, October 1

11:05-11:50 am	***A Look Inside a Real-World O&G Industrial SOC*** Building a fully-functional industrial security operations center (SOC) for oil & gas process control systems from the ground up requires a combination of vision, talent and perseverance. For those who succeed, the payback can be high and deliver positive effects on key business imperatives to include safety, availability, productivity and profitability. In this session, hear directly from an O&G asset owner about overcoming technical and organizational hurdles while building an industrial SOC to gain greater insight into the security posture of ICS/SCADA systems. What technologies are at work in the security stack? What dashboard views and intelligence do OT SOC analysts have of process control networks? What KPIs are tracked? How does the team facilitate asset life-cycle management, incident response, forensics, while also reducing risks to the company's OT systems? Beyond just theory and discussion, real practical knowledge, lessons-learned and actual experience gained through their investments will be shared—and also learn why Idaho National Labs (INL) took particular note of this industrial SOC as a model that others might follow. ***Daniel R. Crandell*** *GICSP, CISM, CISSP, PMP, Manager of Cyber Security for Critical Infrastructure, Enterprise Products LP*
11:50am – 1:15 pm	**Lunch Panel** (LOCATION: REGENCY AB ***The Motives are Clear(er): Safety + Security Implications from Attacks on O&G/Process Automation Systems*** The cybersecurity risks to some industrial OT systems have permanently changed. They are no longer limited to just a likelihood or probability for data loss, reconnaissance, or adversary actions that might disrupt operations. Risks are now much more pronounced. In some cases, they even present possibilities for serious impacts that extend well beyond physical damage to equipment. Recent publicized attacks on industrial control systems, including those used throughout the oil & gas industry and a bevy of other process automation applications reveal some attackers are more prepared than ever to push risk-boundaries. They are clearly moving closer toward causing outright destruction. Nothing appears to be sacred in ICS, including the very safety systems and protective controls put in place to prevent events that would ultimately put human lives at risk. This panel of esteemed cybersecurity experts will discuss the changes that have been seen in the attack-strategies and tactics directed towards a growing number of mission-critical industrial automation systems. They will explore the 'how' factors, and the consequences that can result, such as a broad-scale loss of operations, loss of property, and even wide-spread loss of life should these attacks succeed. Fodder for discussion may include industry-focused campaigns and malware with the likes of TriSIS, VPNfilter, BlackEnergy; safety-critical process automation systems; chemical plants that work with chlorine, Russia & Energy Sector, means, motives, plus other timely topics. MODERATOR: ***Marty Edwards*** *(@ics_marty), Managing Director, Automation Federation* PANELISTS: ***Marc Ayala****, Senior Lifecycle Services Manager, aeSolutions* ***Jonathan Homer****, Hunt and Incident Response Team – ICSG Chief, U.S. Dept. of Homeland Security* ***Robert M. Lee****, Dragos Inc. & SANS Institute*

Monday, October 1

1:15-2:00 pm	***Getting Over a Bad ICS Audit*** Many things can and do go wrong during an ICS audit. Best practices will be shared for identifying and rectifying problems early on to ensure a smooth audit. Real case examples will be exemplified with an emphasis on how to structure your next ICS audit to be a successful engagement for your enterprise. ***Paul Piotrowski**, GICSP, CISSP, CRISC, CBCP, CIPT, Automation Engineer – PCD Integrity, TA2, Asset Support UPO & DW, Shell*
2:00-2:45 pm	***Tactics and Techniques for Threat Hunting in Oil Refineries*** Threat hunting provides an excellent opportunity to boost the current level of defense from both the threat prevention and detection perspective. This talk will highlight lessons learned from threat hunting in oil refineries. We will first share the approach we have found to be the most successful based on the architecture of refinery networks. We will then cover open-source tools and techniques we have found to be particularly successful. Along the way, we will share stories from our threat hunts in refinery environments. Attendees will take away tactics and techniques immediately useful for hunting in refinery environments both in production and during a turnaround. This talk covers threat hunting approaches that can be applied to both passive network traffic and collected host logs. We hope attendees also learn about sources of information within process control networks that they had not considered before. ***Dan Gunter** (@dan_gunter), Principal Threat Analyst, Dragos*
2:45-3:05 pm	**Networking Break** (LOCATION: REGENCY AB FOYER)
3:05-3:50 pm	***Critical Lessons from TRITON: Protecting Safety Instrumented Systems from Advanced Malware*** In December, news of the TRITON attack on the safety system of a critical infrastructure facility sent shockwaves felt by industrial operators and security practitioners worldwide. TRITON is one of a limited, but quickly growing number of publicly identified malicious software families targeted at industrial control systems (ICS) and the first known ICS attack to infiltrate a Safety Instrumented Systems (SIS). In this session, Nozomi Networks will share findings and critical lessons learned from the industry's most extensive analysis of TRITON to date, including: why we believe the shutdown was an unintended outcome that occurred while the attacker was developing the ability to cause physical damage; what oil and gas operators and security experts should know about a much larger attack plan the hackers likely intended; and steps you can take now to protect against these types of attacks. We'll also release code for a tool for detecting an infected controller. TRITON's sophistication, and its targeting of a SIS, cannot be ignored. It highlights the need for appropriate cybersecurity solutions and greater visibility into the entire industrial process. ***Andrea Carcano** (@andreacarcano), Co-Founder and Chief Product Officer, Nozomi Networks*

Monday, October 1

3:50-4:35 pm	***Detecting Counterfeit Software in Oil and Gas Control Systems*** Oil and gas companies depend on their vendors to supply valid software and firmware for control system implementation and upgrades. If this chain of trust is compromised, then malicious software can be introduced that alters core system functionality, potentially impacting critical operations and human safety. Unfortunately, there are currently few safeguards in place to protect IIoT and ICS devices against introduction of counterfeit firmware and software. This is not a hypothetical risk. In 2014, the Dragonfly attack targeted critical infrastructures in North America and Europe by inserting malware into legitimate software bundles available for download on three ICS vendor's websites. As a result, any asset owner that installed these modified software bundles had their critical systems infected. These attacks highlighted the fact that industry currently needs a robust and universal solution for safeguarding against the counterfeit of firmware/software upgrades. This talk reports on the results of a US Department of Homeland Security (DHS) funded research project to investigate the viability of using trust anchor technologies for onsite validation of ICS upgrade packages used in the oil and gas sector. The project investigated methods of generating digital fingerprints of both legitimate and suspect firmware via automated agents and then assigning reputational scores to the artefacts. An API and web tool allows end users to incorporate a validation process into their daily operations, ensuring the legitimacy of updated firmware/software, without impeding critical operations. ***Eric Byres*** *(@ICS_Secure), CEO, aDolus Inc.*
4:35-5:20 pm	***How's Our Industrial Cybersecurity? Go Ask the OT Guys*** A prominent offshore drilling operation was required to make ICS security changes within their operations and production technology group by a key customer's demanding ICS security requirements. The journey resulted in a funded project to create a security operations center (SOC) run by the OT team to monitor and manage industrial security across their rigs and fleet of ships that remain continuously at sea. Four years later, the OT team manages their remote access, application and equipment vendors, OT network and assets through their SOC and are in the enviable position of having funding and equipment to keep their operations secure 7x24x365. This case study has applicability to other industries as well. Attendees will gain insight on corporate drivers for improving industrial cybersecurity, how to set and manage OT priorities and still work with stakeholders, what training, funding and assistance may be needed, and how to manage their vendors for operational success. Appropriate for field technicians to management and any range of cybersecurity knowledge. ***Katherine Brocklehurst*** *(@kat_brock), Senior Director, Claroty* ***Greg Villano****, IACS Cybersecurity Supervisor*
5:20-7:00 pm	**Networking Reception** (LOCATION: REGENCY AB FOYER)
7:00-8:00 pm	***Demo: Dancing in the Dark: Trust, or an Adventure in PLC Data-Table Misinformation?*** This talk and demo will highlight various approaches to manipulating data within a PLC/PAC that can affect a process and impact operational safety, quality, performance and productivity. With PLC/PACs at the heart of many critical systems that also rely on Level 0/1 cyber-physical devices and higher-level products, the integrity and protection of the data used for process logic is paramount. Learn more about these risks and some practical methods to help protect control systems. ***Tim Conway****, Technical Director – ICS and SCADA, SANS Institute* ***Jeff Shearer****, Industrial Cybersecurity Consultant, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.