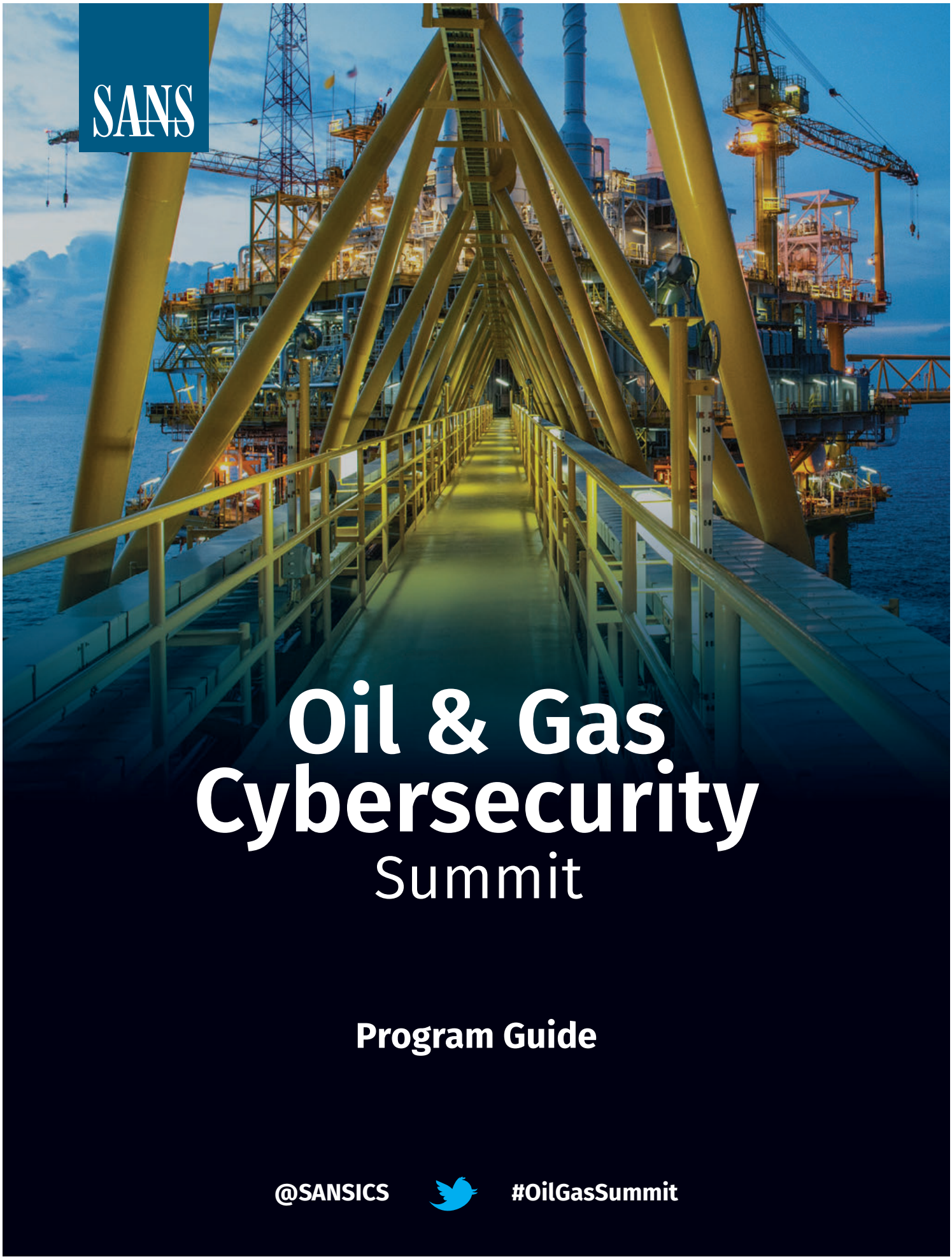

SANS

Oil & Gas Cybersecurity Summit

Program Guide

@SANSICS #OilGasSummit

Agenda

All Summit Sessions will be held in the Discovery A (unless noted otherwise).

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

Monday, September 16

7:00-9:00 am	**Registration & Coffee** (LOCATION: DISCOVERY B)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Jason Dely*** *@jasonjdely, Practice Director – Industrial Control Systems, Cylance; Instructor and Summit Co-Chair, SANS Institute* ***Mike Pilkington*** *@mikepilkington, Researcher, Certified Instructor, Summit Co-Chair, SANS Institute*
9:15-10:00 am	***Keynote: Risk-Based Approach to Protecting Industrial Control Systems*** We are faced with a sprawling, heterogeneous industrial control system landscape into which we have little visibility. So what do we do? In this presentation, we'll lay out the steps we took to get our arms around what we have, and to prioritize both the lines of business and the preventative and mitigation controls needed to lower the risk of a catastrophic breach of our control systems. We'll describe how we framed risk, how we prioritized the deployment of controls, how we communicated with executive management, and how we leveraged internal audit and executive support to change the organization. You'll come away with ideas of how to apply these steps within your own organization.. ***Steve Slawson****, Director – IT Security & Compliance, Occidental Petroleum*
10:00-10:30 am	**Networking Break** (LOCATION: DISCOVERY B)
10:30-11:05 am	***Securing the Technology Supply Chain*** This presentation covers best practices and considerations when operating a supply chain security program. It is based on more than a decade of service working in all aspects of supply chain security, from building such a security program for a Fortune 50 company to helping draft the first ISO standard on supply chain security and being involved in every aspect of the process from risk assessments to contract negotiations. We'll discuss some of the impacts of supply chain failures, including walking through a few pertinent examples. The presentation will also cover the various reasons supply chains may be targeted. The issue of supply chain visibility and the challenges of controlling risks when you only have limited knowledge of your exposure will be covered, as will be the steps to improve awareness, assess supplier risk, identify critical factors, and evaluate impacts. We'll then turn to contractual considerations for supply chain security in both your upstream and downstream business relationships. Contracts have limitations, especially when they cross international boundaries, and this will be covered in detail. Finally, we'll discuss what it takes to build an effective program and look at what you should be doing to avoid supply-chain-related fraud. ***Keith Turpin****, CISO, Universal Weather and Aviation*

Monday, September 16

11:10-11:45 am

A Process-Based Approach to ICS Security

ICS security is often performed by the heroic efforts of a few good ICS Security professionals in organizations. While this may work for a time and season, it hinges on the heels of a few individuals, and is difficult to both scale and mature. Security needs processes injected from an asset to global level to ensure controls are maintained, and badness is kept at bay. This talk will address key areas in your organization where processes can be implemented to improve your security program maturity.

***Michael Hoffman**, Principal ICS Security Engineer, Shell*

11:50 am – 12:25 pm

ICS, SCADA, and Mitre ATT&CK: How It Helps and Where It Hurts

The Mitre ATT&CK framework has many potential uses within SCADA and industrial control system environments. This presentation will dive deep into the process of using the framework to describe specific attack patterns and courses of action around the Triton/Trisis/HatMan attacks. The aim is to support the identification and ultimate resolution of vulnerabilities. In addition, we'll cover the use of the Mitre ATT&CK framework as well as mitigating and compensating controls that can be used in both business and production networks. Expected takeaways include data and analysis on the Triton/Trisis/Hatman attacks and guidance on how to use Mitre ATT&CK as a communication and validation tool across teams within an organization.

***Neal Humphrey**, Director, Threat Intelligence Engineers, ThreatQuotient*

12:25-1:30 pm

Lunch & Learn (LOCATION: DISCOVERY A)

McAfee™

Make Cloud the Most Secure Environment for Business

As much as Cloud has improved productivity and accelerated business, it has presented challenges in mitigating the risks that come along with its adoption. With appropriate security measures in place, however, Cloud can turn into the most secure environment for business. This session will focus on comprehensive security coverage across SaaS, IaaS, and PaaS in a Cloud First world.

1:40-2:05 pm

Panel: SANS ICS Survey Results: Top 3 Initiatives for Increasing ICS/OT Security

Survey says: we're getting better all the time, but we've still got lots of work to do as an industry. Our panel will discuss the top three areas of focus identified by the most recent SANS ICS Survey with recommendations for improvement. We'll look at:

- Increasing visibility into control system cyber assets and configurations.
- auditing control systems networks and security assets
- Invest in general cybersecurity awareness programs for employees including IT, OT and hybrid IT/OT personal

MODERATOR:

***Jason Dely** @jasonjdely, Practice Director – Industrial Control Systems, Cylance; Instructor & Summit Co-Chair, SANS Institute*

PANELISTS:

***Tim Conway**, Technical Director – ICS and SCADA, SANS Institute*

***Michael Hoffman**, Principal ICS Security Engineer, Shell*

Monday, September 16

2:05-2:40 pm	***Breaching the IT/OT Boundary: Wedge Points and How to Secure Them*** The IT/OT boundary is one of the most important security controls to protect OT networks. OT security personnel are becoming more proficient at patching and protecting OT services accessible from IT networks. This increase in maturity is forcing attackers to move from traditional technical exploits to soft vulnerabilities (it's a feature, not a bug) to breach the IT/OT boundary. This talk will explore common techniques and tactics attackers (and Pentesters) employ to footprint and breach OT networks. We'll provide examples that show why network segmentation alone is no longer adequate and should be extended to domains, applications, and platforms, including a demonstration of improper application segmentation by leveraging Windows Server Update Services to target OT systems. We will also discuss common sources of OT information on the IT network and various ways OT users are identified and leveraged to gain access to OT networks. We'll demonstrate various credential theft techniques and look at how attackers can hijack established IT/OT sessions. We'll also cover why a properly configured multi-factor authentication solution can be extremely potent at the IT/OT boundary. In summary, this talk will explore the IT/OT boundary from an offensive standpoint and examine how that boundary, when properly secured, can be one of the most important security controls to protect OT networks. ***Jackson Evans-Davies**, Penetration Tester, Honeywell* ***Connor Leach**, Penetration Tester, Honeywell*
2:40-3:10 pm	**Networking Break** (LOCATION: DISCOVERY B)
3:10-3:20 pm	***Fueling the Exchange of Cyber Intelligence: Why ONG-ISAC Matters*** ONG-ISAC serves as a central point of coordination and communication to aid in the protection of exploration and production, transportation, refining, and delivery systems of the ONG industry, through the analysis and sharing of trusted and timely cyber threat information, including vulnerability and threat activity specific to ICS and SCADA systems. Executive Director Angela Haun shares how your organization can both help and benefit from ONG-ISAC's efforts. ***Angela Haun** @EDAngelaHaun, Executive Director, ONG-ISAC*
3:25-4:00 pm	***If it isn't Secure, it isn't Safe: Incorporating Cybersecurity into Process Safety*** Process hazard assessments (PHA) are a well-established practice in process safety management. These assessments focus on failures (aka deviations) that are typically caused by equipment failures or human error. By design, PHAs do not consider cyber threats to industrial control systems (ICS). However, cyber threats represent additional failure modes that may lead to the same health, safety and environmental consequences identified in the PHA. Functional safety (i.e. ISA 84 / IEC 61511) and industrial cybersecurity standards (i.e. ISA/IEC 62443) recognize this issue and provide guidance on how to integrate these two disciplines to ensure that cyber incidents cannot impact process safety. This presentation will discuss the guidance provided in industry standards regarding ICS cyber risk assessments (aka Cyber PHA) and the benefits and business justification for performing them. ***John Cusimano**, VP of Industrrial Cybersecurity, aeSolutions*

Monday, September 16

4:05-4:40 pm	***A Roadmap to Help Enterprise Security Operations Centers Expand Duties to OT Environments*** This presentation will use a case study of the Xenotime activity group to demonstrate why having the ability to monitor, detect, and respond in an Operational Technology (OT) environment is vital to human safety and continuous operations. Attendees will learn what adversaries are targeting in the OT space, with an emphasis on safety-instrumented systems. We'll also look at what needs to be taken into consideration when adding or expanding monitoring, detection, and response capabilities for OT environments to an existing enterprise Security Operations Center. Finally, we'll present a high-level workflow to get started with OT monitoring, detection, and response in your organization. ***Vernon L. McCandlish*** *@malanalysis, Principal Security Analyst, Dragos Inc.*
4:45-5:20 pm	***SCADA Cybersecurity for Pipelines: API 1164 and Updates from the Trenches*** API 1164 is a security standard written specifically for oil and natural gas pipelines—and it's now going through a massive update to be more relevant to today's threat landscape and technology advancements. The new scope may be applied to upstream, midstream, and downstream operations, and will further expand to include measurements for the NIST cybersecurity framework. This presentation will cover all the major things you need to know about the update directly from members of the drafting team and provide insight into what these advancements will mean for individual energy companies. ***Tom Aubuchon****, Sr. Director Cyber Security Strategy and Programs, Baker Hughes* ***Jason D. Christopher*** *@jdchristopher, CTO, Axio; Certified Instructor, SANS Institute*
5:20-5:30 pm	***Closing Remarks and Action Items*** ***Jason Dely*** *@jasonjdely, Practice Director – Industrial Control Systems, Cylance; Instructor and Summit Co-Chair, SANS Institute* ***Mike Pilkington*** *@mikepilkington, Researcher, Certified Instructor, Summit Co-Chair, SANS Institute*
5:30-7:30 pm	**Networking Reception** (LOCATION: DISCOVERY B) Join us in the vendor room where we'll have a complimentary open bar and an indulgent array of appetizers.

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.