Monday, September 16	
9:00-9:15 am	*Welcome & Opening Remarks* • **Jason Dely** **@jasonjdely,** Practice Director – Industrial Control Systems, Cylance; Instructor & 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** **Steve Slawson**, Director – IT Security & Compliance, Occidental Petroleum 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.
10:00-10:30 am	**Networking Break**
10:30-11:05 am	**Securing the Technology Supply Chain** **Keith Turpin**, CISO, Universal Weather and Aviation This presentation covers best practices and considerations when operating a supply chain security program. It is based on more than a decade 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.
11:10-11:45 am	**Five Steps to Secure Your Industrial Control System/SCADA Network** **Pedro Serrano** **@InfoSecPedro**, Security Architect, Cimarex Energy This presentation will provide a quick look at the most important steps that need to be taken to secure industrial control systems. We'll examine measures that are realistically obtainable and that can make a difference in your environment. The emphasis will be on what you CAN do.
11:50 am – 12:25 pm	**ICS, SCADA, and Mitre ATT&CK: How It Helps and Where It Hurts** **Neal Humphrey**, Director, Threat Intelligence Engineers, ThreatQuotient 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.
12:25-1:30 pm	**Lunch & Learn** *Presented by* McAfee
1:30-2:05 pm	*Panel* **SANS ICS Survey Results: Top 3 Initiatives for Increasing ICS/OT Security** **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,** Principle ICS Security Engineer, Shell 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
2:05-2:40 pm	**Breaching the IT/OT Boundary – Wedge Points and How to Secure Them** • **Jackson Evans-Davies,** Penetration Tester, Honeywell • **Connor Leach,** Penetration Tester, Honeywell 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.
2:40-3:10 pm	**Networking Break**
3:10-3:20 pm	**Fueling the Exchange of Cyber Intelligence: Why ONG-ISAC Matters** **Angela Haun** **@EDAngelaHaun**, Executive Director, ONG-ISAC

	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.
3:25-4:00 pm	**Improving Pipeline Operational Visibility to Avoid Costly Downtime** **Paul Smith** **@paul_timothy,** Director of Product Research and Strategy, Nozomi Networks The main priority for midstream oil and gas operators is to keep their product flowing through pipelines in a secure and safe manner. It is also critical that they have visibility to mitigate any cybersecurity issues and to detect any potential outages that could impact services. When visibility into what is really happening is reduced, significant problems and costs can arise. This is unfortunately what happened with a major pipeline organization when a PLC went down and caused the company $1.9 million in lost revenue and downtime. In this session, Paul Smith will take a deep dive into this case and other real-world use cases to share lessons learned and best practices from years of field experience helping oil and gas organizations pave the way for successful OT visibility and cybersecurity on a local or global scale.
4:05-4:40 pm	**A Roadmap to Help Enterprise Security Operations Centers Expand Duties to OT Environments** **Vernon L. McCandlish** **@malanalysis,** Principal Security Analyst, Dragos Inc. 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
4:45-5:20 pm	**SCADA Cyber Security for Pipelines: API 1164 and Updates from the Trenches**

	• **Tom Aubuchon**, Sr. Director Cyber Security Strategy and Programs, Baker Hughes • **Jason D. Christopher** **@jdchristopher**, CTO, Axio; Certified Instructor, SANS Institute 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 up-, mid-, and downstream operations, and will further expand to include measurements for the NIST Cyber Security 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.
5:20-5:30 pm	*Closing Remarks & Action Items* • **Jason Dely** **@jasonjdely,** Practice Director – Industrial Control Systems, Cylance; Instructor & Summit Co-Chair, SANS Institute • **Mike Pilkington** **@mikepilkington**, Researcher, Certified Instructor, Summit Co-Chair, SANS Institute
5:30-7:00 pm	*Networking Reception*

Speaker Biographies

Tom Aubuchon, Sr. Director Cyber Security Strategy and Programs, Baker Hughes
Tom Aubuchon is responsible for IT, OT, and Product cybersecurity strategies. In conjunction with his Baker Hughes responsibilities, Tom is the co-chair of the American Petroleum Institute's Standard 1164 – Pipeline Control System Cybersecurity update working group. Previously Tom was co-chair of the Interstate Natural Gas Association of America's Natural Gas Pipeline Security Guidelines. Tom has over 36 years in OT Security, IT Security, Product Security, Information Technology, and Industrial Control Systems industries in executive, managerial, consultant, architect, designer, and PM roles. Previously he was also CISO for a fortune 100 ONG company responsible for convergence and management of both IT and OT security into a single DT security function. Tom graduated magna cum laude from Oakland University, Rochester MI and is a Certified Information Security Manager.

Tim Conway, Technical Director – ICS and SCADA, SANS Institute
Tim serves as the Technical Director - ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Additionally, performing contract and consulting work in the areas of ICS cyber security with a focus on energy environments.
A recognized leader in CIP operations, he formerly served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), and was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric.

Jason D. Christopher **@jdchristopher**, CTO, Axio; Certified Instructor, SANS Institute
Jason D. Christopher is the Chief Technology Officer for Axio. His responsibilities include providing technical leadership on security and resilience issues relevant to Axio, its partners, and clients, and the development of all Axio technology platforms for security metrics and benchmarking.

Prior to Axio, Jason led the research for cybersecurity metrics and information assurance at the Electric Power Research Institute. Previously, he was the technical lead for cybersecurity capability and risk management at the US Department of Energy, where he managed the Cybersecurity for Energy Delivery Systems Operations program, which included the Cybersecurity Capability Maturity Model and other collaborative efforts. Jason also served as the program lead for both Critical Infrastructure Protection Standards and Smart Grid Security at the Federal Energy Regulatory Commission.

Jason Dely **@jasonjdely,** Practice Director – Industrial Control Systems, Cylance; Instructor & Summit Co-Chair, SANS Institute
Jason Dely is responsible for leading the critical infrastructure and industrial control systems (ICS) security practice for Cylance. Prior to joining Cylance, Jason held many roles at Rockwell Automation where he assisted clients with their research, design, integration, testing and response activities across a variety of application, security and infrastructure initiatives. During this time, Jason gained in-depth ICS product, protocol and operational experiences that are invaluable when it comes to evaluating and building defenses within critical infrastructure organizations. His security passion over the past 18 years

of experience with ICS is founded upon balancing business requirements against people, process and technologies unique to each organization to ensure their operations are safe, reliable and secure.

Jackson Evans-Davies, Penetration Tester, Honeywell
Evans-Davies has been with Honeywell for over a decade, doing penetration testing and red-team testing of enterprise and ICS environments. He also performs security research and offensive security training. He holds the GPEN and GXPN certifications from GIAC.

Angela Haun **@EDAngelaHaun**, Executive Director, ONG-ISAC
Appointed as ONG-ISAC Executive Director in September 2018, Angela is a retired FBI Special Agent with extensive experience in cybersecurity and protecting critical assets. Since joining the ONG-ISAC, she has expanded the ONG-ISAC's membership with a Strategic Partnership Pilot Program, bringing new organizations, expertise, resources and funding to support the ISAC's efforts. In addition, Angela has been a subject matter expert speaker, organizer and participant in numerous energy-related conferences, briefings, exercises, meetings, webinars and other events. Ms. Haun is actively pursuing upgraded technologies and additional benefits for ONG-ISAC member analysts and executives.

Michael Hoffman, Principle Industrial Control Systems (ICS) Security Engineer,
Hoffman is Principle Industrial Control Systems (ISC) Security Engineer with over 18 years combined automation, administration and security experience with ICS systems. He is an experienced SCADA administrator and has a strong background in ICS device configuration and system programming.

Neal Humphrey, Director, Threat Intelligence Engineers, ThreatQuotient
Neal Humphrey is currently Director of North American TIEâ€™s for ThreatQuotient. He has been active and advising in the security industry for over 15 years and in technology for 20 plus. Previously, Neal served as a Technical Solutions Architect at Cisco and Security Engineer at Sourcefire.

Connor Leach, Penetration Tester, Honeywell
Connor is a Senior Penetration Tester with the Honeywell Industrial Cybersecurity (HICS) team. A graduate of Computer Engineering Technology from Conestoga College, Connor is also an Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), GIAC Penetration Tester (GPEN), Cisco Certified Network Professional (CCNP), and VMware Certified Professional (VCP). Connor has over 9 years of experience providing offensive and defensive consulting to industrial clients, including penetration testing, blue team preparation, security research of industrial software and hardware, and securing industrial environments.

Vernon L. McCandlish **@malanalysis,** Principal Security Analyst, Dragos Inc.
Vern is retired from the New York State Police. He now uses digital forensics to do incident response and help build new capabilities for detecting attacks. He serves as an Adjunct Professor of Cybersecurity at Utica College. Vern is passionate about helping victims and teaching.

Mike Pilkington **@mikepilkington**, Researcher, Certified Instructor, Summit Co-Chair, SANS Institute
Before joining SANS full-time, Mike led the US incident response team and the global internal investigations forensics team at Shell. Prior to Shell, Mike had several roles in IT at Halliburton, including senior incident responder for the last several years of his tenure there. Mike's core responsibilities were responding to malware and intrusion cases, leading various enterprise DFIR tooling projects, and consulting with internal groups on security reviews and initiatives. Over the years, Mike has accumulated a broad range of technical expertise, having spent significant time performing software quality assurance, Windows systems administration, LAN and WAN network administration, firewall and IDS/IPS security administration, computer forensic analysis, and incident response. As a forensic analyst, he worked HR investigations, including cases involving intellectual property theft, inappropriate use of the Internet, employee hacking, IT administrator privilege abuse, and illegal downloading of copyrighted materials.

Pedro Serrano **@InfoSecPedro**, Security Architect, Cimarex Energy
Pedro Serrano has over 35 years of experience managing and installing cyber security controls in networks around the world, 20 of those in military systems while serving in the United States Air Force. He is the Security Architect for Cimarex Energy. Pedro serves as the President of the Information System Security Association (ISSA) chapter in Tulsa, Oklahoma and holds the CISSP certification from ISC2.

Steve Slawson, Director – IT Security & Compliance, Occidental Petroleum
Steve Slawson joined Occidental Petroleum Corporation in 2002, formerly working for Shell, Continuum Resources, and Energy Innovations in geophysical and management roles. At Oxy, Steve was previously Oxy's Petrotechnical Solutions manager before moving to IT in 2005. In IT, Steve has served as the Director of International IT Services, Director of Automation Technology, Director of Infrastructure, and most recently as the Director of IT Security, Governance, Risk & Compliance. His cyber security experience started in 2011 as part of Oxy's early efforts to protect their industrial control systems. Steve holds both a Bachelors (1987) and Masters (1989) Degree in Electrical Engineering from the University of Houston, where he was a member of the Honors College.

Paul Smith **@paul_timothy**, Director of Product Research and Strategy, Nozomi Networks
Paul Smith is an ICS and cybersecurity expert. During his 15+ year career, he pioneered the use of new technology in the energy, utility, and critical infrastructure sectors, and helped develop cyber security strategies for some of the world's largest government contractors, industrial organizations, and municipalities.

Keith Turpin, CISO, Universal Weather and Aviation
Keith Turpin serves as Chief Information Security Officer at Universal Weather and Aviation, a billion-dollar international aviation services and fueling company operating 50 locations in 20 countries. He is a former Technical Fellow at The Boeing Company, leading Supply Chain Security and International IT

Security Operations. He’s also a former U.S. delegate to the International Standards Organization's (ISO).

#end#