SANS Oil & Gas Solutions Forum

July 10, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Jason Dely

Sponsored by: Cyberinc, SWIMLANE, ThreatConnect, DISPEL, tripwire, Cisco Umbrella, Siemplify

AGENDA

9:00 - 9:30am	**Join Slack Workspace (https://join.slack.com/t/sansoilgasforum/shared_invite/zt-fstwwl10-npJG7ehz9KCvhEPvnZFGMQ) & Webcast (https://www.sans.org/webcasts/112760)**
9:30am - 10:10am	**Welcome & Keynote** Over the last 15 or so years, Oil & Gas organizations, vendors and service providers have been steadily improving their awareness of the emerging cyber threats to their operations and the need to improve their security. With this prioritization in mind, while also still meeting or exceeding regulatory obligations, a security initiative must be right-sized and coordinated across the 5 domains of Identify, Protect, Detect, Response and Recover. How will organizations establish these objectives? What is needed to meet these objectives? This briefing will explore these questions while showcasing current capabilities available today. *Jason Dely, Forum Chairperson & SANS Instructor*
10:10 - 10:45am	**The Past, Present and Future of Security Orchestration, Automation and Response** There are numerous cybersecurity tools available to help oil and gas organizations detect threats across their IT and OT environments. While these tools aim to improve your organization's security posture, many of them require experienced, technical staff with extensive training to leverage effectively. These systems often generate so many alerts that even highly-skilled staff are unable to analyze and respond to real threats in a timely manner. This is not sustainable for even the largest security operations centers (SOC). There is a way to maximize the productivity of your existing security tools and staff while gaining greater visibility, reducing response time, and improving team efficiency: automation. In this session, you will learn practical strategies and techniques for navigating out of a reactive focus on detection and instead move towards a proactive, automated SOC model to reduce risk. Key takeaways include: • Active automation strategies for users who have a security orchestration, automation, and response (SOAR) solution. • Automation-friendly workflow and process designs for those who are not yet using SOAR. • Strategies for prioritization of alerts and events using correlation and automated research. *Jay Spann, @cyberspann, @swimlane, SOAR Evangelist & Technical Product Marketing Manager, Swimlane*
10:45 - 11:20am	**Adjusting Processes to Meet Today's Evolving Environment** Understanding how the cyber threat landscape has changed in today's world and why it's important to put the right resources in place in order to help your organization and personnel do their jobs more effectively. There is no one size fits all solution and more than ever there is a need for organizations to continuously do more with less. This presentation will cover topics that will help your organization understand more about how they are conducting security and threat operations and how to streamline those efforts across the 5 domains of Identify, Protect, Detect, Response and Recover. *Jody Caldwell, @threatconnect, Senior Director of Customer Success, ThreatConnect*
11:20am - 11:35am	**Break**

SANS Oil & Gas Solutions Forum

July 10, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Jason Dely

11:35am - 12:10pm	**Shrink your (attack) surface, sharpen your (cyber) security** Digitization and cloud adoption are rapidly accelerating in the oil & gas industry. According to industry research, 70% of companies in the sector are either planning to or actively investing technology to accelerate decisions, predict issues, and optimize costs across exploration, production, transportation, refining, and marketing. With growing digitization comes the obvious growth in cyber risks. The connectivity improvement brings operational efficiency, yet exposes production data and industrial machinery, not just end users and IT systems, to new threats. And users now find tools like the browser have become core components of their life in the cloud. Oil & gas facilities continually face threats from both opportunistic attackers as well as state-sponsored actors. These threats include social engineering, such as phishing, disruptive events such as ransomware, or even concealed attacks via malvertising that target end-user machines as well as ICS and supervisory control and data acquisition (SCADA) systems via vulnerable end users. The browser often acts as a common denominator for attackers to infiltrate systems across upstream, midstream, and downstream operations. Attackers use the web and email to get in, and once they're in, they move around looking for appropriate targets to cause maximum damage. Attendees at this webcast will learn: • How do these threats proliferate? • How does remote working environment impact our security? • The role of the browser isolation in ensuring security • What can we do to maximize our security dollar in today's environment? *Rajiv Raghunarayan, @raraghun, @cyberinc, Senior Vice President of Products and Marketing, Cyberinc*
12:10 - 12:45pm	**Evolving Security Operations in Oil and Gas for the Covid-19 Era and Beyond** The COVID-19 pandemic has had far-reaching consequences on organizations across the world. Like every business function, security operations was forced to adjust and go remote, introducing both "generic" challenges as well as ones specific to oil and gas security teams. On the operational front, security analysts are no longer able to tap the shoulder of the analyst next to them to jointly address a potential threat - the "group of people in a dark room" SOC paradigm is going through a major shift, which calls for rethinking the collaboration that is critical for any successful security practice. From the security landscape perspective, Covid-19 has introduced both targeted threats as well as new attack vectors such as employees working from non-company issued machines which need to be addressed. In this session, we will share unique insights and best practices on how world-leading security operations teams are and should be adjusting to the "new normal" of the Covid-19 era. The session will include both high-level strategy and specific examples to oil and gas as to what organizations are doing to maintain effective security operations from detection to response. With the importance of remote operations likely persisting beyond Covid-19, these best practices will hold true for cutting-edge security teams for years to come. *Nimmy Reichenberg, @siemplify, Chief Strategy Officer, Siemplify*
12:45 - 12:55pm	**Break**

SANS Oil & Gas Solutions Forum

July 10, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Jason Dely

12:55 - 1:30pm	**Design & Implementation of OEM ICS Cybersecurity Frameworks: The Good, The Bad, and The Ugly** A plethora of ICS cybersecurity frameworks abound, but the strength of their implementation can be challenged if special consideration is not made for unique equipment, configuration and architecture that are required by the Original Equipment Manufacturer (OEM). In this talk, we will discuss an approach to the design and implementation a customized cybersecurity framework and touch on some key considerations that came along with it. *Robert Landavazo, @rdlando, @TripwireInc, Systems Engineer, Tripwire* *Michael Zavislak, Cyber Security Engineer, Nexus Controls, a Baker Hughes Business*
1:30 - 2:05pm	**Security, Speed, Scalability, Sustainability, and Survivability - An OT Remote Access Story** Slow tools sink teams and reputations. This talk is about the design, development, and deployment of a remote access system geared towards meeting the five "S"s of optimal OT remote access - Security, Speed, Scalability, Sustainability, and Survivability. We will cover the stories that guided the system's evolution; the lessons learned along the way; how to build or buy it; and, briefly, a mathematical approach to designing or selecting the optimal remote access system for the task at hand. *Ian Schmertzler, @dispelhq, President & CFO*
2:05 - 2:10pm	**Closing Remarks**