Sunday, February 22

8:00-9:00 am

CRPA Registration

(LOCATION: GRAND REPUBLIC FOYER)

8:30 am - 4:30 pm

Advanced CRPA/C2M2 Workshop

(LOCATION – GRAND REPUBLIC C)

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

The Electricity Sector Information Sharing and Analysis Center (ES-ISAC) is pleased to announce a free member daytime training opportunity to further enhance your master facilitator-level CRPA (Cyber Risk Preparedness Assessment) skills and knowledge towards developing and conducting robust, technically informed incident response exercises.

Included:

- Introductory overview of the complementary Department of Energy (DOE) Electricity Sub-sector Capability Maturity Model (ES-C2M2) with the latest practices, lessons learned, and model perspective
- Updated CRPA 2015 Kit 3.0 expanded coverage providing deep insights into the exercise development process, aligning with goals and objectives, using templates, applying/creating specific injects (libraries), and building overall Master Scenario Events List (MSEL).
- A realistic, simulated reference entity and active participation following the CRPA methodology
- Exercise materials compliments of the ES-ISAC

The information provided by ES-ISAC personnel and technical partner Lofty Perch along with the updated kit will assist with participants independently developing and executing their own table top exercises.

4:00-7:00 pm

Summit Registration

(LOCATION – BALLROOM OF THE AMERICAS LOBBY)

5:00-6:00 pm

ES-ISAC Briefing

LOCATION – GRAND REPUBLIC C

ES-ISAC
ELECTRICITY SECTOR
INFORMATION SHARING AND ANALYSIS CENTER
OPERATED BY NERC

Meet the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) staff for an informal round table discussion. The round table is a chance to learn about what the ES-ISAC has been working on over the last year, learn what's coming in 2015 and for the ES-ISAC to answer questions and get feedback from its membership.

5:00-7:00 pm

Welcome Reception

(LOCATION – BALLROOM OF THE AMERICAS LOBBY)

Hosted By

paloalto
networks.

Kick off your ICS Summit experience at the Welcome Reception. Enjoy food and drinks and get a chance to network with peers prior to the Summit sessions.

7:00-10:00 pm

Exposure 2 Closure: 2015

(LOCATION – BALLROOM OF THE AMERICAS B)

Sponsored by

ES-ISAC
ELECTRICITY SECTOR
INFORMATION SHARING AND ANALYSIS CENTER
OPERATED BY NERC

For the sixth straight year, **Exposure 2 Closure: 2015** will run for an exclusive one-night-only engagement at SANS ICS Orlando Summit and Training 2015. This is a dramatic stage performance opens in the midst of a multi-year cyber campaign attacking critical infrastructure networks across the world. Exposure 2 Closure: 2015 features an entertaining fictional yet techno-realistic storytelling of a game of cat and mouse. The drama raises questions surrounding industrial control systems security, forensic investigations, vulnerability mitigation, and national security policy considerations. Tim Roxey will emcee the cast of characters including defenders, attackers, researchers, to intelligence analysts. Audience members will be on the edges of their seats as our cast of security geeks takes an entertaining star turn, but will also walk away with practical, applicable knowledge including:

- Real-life lessons of incident monitoring and response from seasoned professionals
- How cyber attacks can penetrate into the most secure ICS networks
- Emerging cyber threat intelligence methodology being applied by leading security firms
- Overview of how governments can (and can't) assist companies security programs

Exposure 2 Closure: 2015 is a perennial fan favorite, and is a fun and interactive way to illustrate how the global security community works together in partnership to evaluate emergent threats to, and vulnerabilities in, ICS networks.

Monday, February 23

All Summit Sessions will be held in the Fantasia G (unless noted).

Summit presentations will be posted via the following URL, ***http://ics.sans.org/resources/summit-archives,*** *within 5 business days. An email will be sent to all attendees once live.*

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

8:00-9:00 am

Registration & Coffee

(LOCATION: EAST REGISTRATION DESK - LOWER LEVEL CONFERENCE CENTER)

9:00-9:45 am

Beyond Stuxnet: The Next Generation of Cyber Warfare

Kim Zetter, *Author, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*

Zetter's painstakingly researched new book, Countdown to Zero Day, dives deep into the game-changing Stuxnet worm, but ranges far beyond Stuxnet itself. In this keynote, Zetter will draw upon her research to discuss how digital warfare developed in the US. She'll take us inside today's flourishing zero-day "grey markets," in which intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks. She reveals just how vulnerable many of our own critical systems are to Stuxnet-like strikes, from nation-state adversaries and anonymous hackers alike—and shows us just what might happen should our infrastructure be targeted by such an attack.

9:45-10:30 am

Technical Briefing: ICS-Targeted Threats

Liam O Murchu, *Senior Development Manager, Symantec*

This talk with take a technical deep dive into the ICS-modules associated with the Havex RAT and Sandworm. Learn how discovered ICS plug-ins work and explore identified delivery vectors used in campaigns to target ICS-reliant organizations.

10:30-11:00am

Networking Break & Vendor Showcase

(LOCATION: FANTASIA H)

11:00-11:45 am

ICS Active Defense

Robert M. Lee, *Co-Founder, Dragos Security LLC*

"Defense is hard! The attacker always wins!" That is a statement heard too frequently throughout the security industry. In ICS it seems even worse; discussions of vulnerable networks and assets chip away at optimism quickly – people burn out. The community must do better to empower security personnel to take an active approach to network security. Active Defense is not about hacking back, quite the opposite, it is about valuing defense and taking an active approach to understanding the network, utilizing threat intelligence, identifying attackers, and responding to threats in your environment – all to make ICS more reliable. This presentation will start with a historical discussion on Active Defense, dispel the focus on hacking back, and introduce the Active Defense Cycle for ICS. After all, defense is doable.

11:45 am - 12:30 pm

Harmonizing ICS Security and Compliance

MODERATOR:

Mike Assante, *ICS & SCADA Security, SANS Institute*

PANELISTS:

Matt Davis, *Senior Manager, Information Security, Ernst & Young*
Perry Pederson, *Principal, The Langner Group, LLC*
Josh Sandler, *NERC CIP Compliance Lead, Duke Energy*

For many organizations, ICS security is primarily driven by compliance. Standards like NERC CIP are creating a higher level of saturation for security across more locations and facilities. In this case panel we will hear the perspective from an asset owner, a vendor, and global consultancy organizations that are all working on transformational ICS security program from both a technical and a business perspective. Panelist focus witll be on highlighting critical success factors such as controls development and process alignment, as well as supply chain engagement in the process to ensure a operations, cybersecurity, and regulatory balanced approach.

12:30-1:45 pm

LUNCH & LEARN

(LOCATION: GRAND REPUBLIC A)

Presented by

WATERFALL
Stronger Than Firewalls

Emerging Best Practice for ICS Perimeter Cyber Security

Michael Piccalo, *Director of Industrial Security, Waterfall Security*

Malware continues to evolve becoming more powerful and more elusive, putting the safety and reliability of our critical infrastructure increasingly more at risk. Cyber security experts increasingly assert that IT firewall / perimeter defenses are porous, and that other measures must be deployed to protect IT networks. This advice is a poor fit for control system networks. The nature of control system networks is that they will always be softer targets than IT networks. Firewalls and other software-based security solutions, even when deployed in layers, have been compromised time and again.

In this session, we will explore some of the reasons why firewalls and other IT technologies are no longer effective against modern threats and we explore how unidirectional security gateway technology, a global emerging best practice that utilizes hardware to enforce security, can help mitigate modern threats while keeping the real-time data feed available to the business users that rely on this information.

LUNCH & LEARN

(LOCATION: GRAND REPUBLIC B)

Presented by

NEXDEFENSE

High-Value ICS Network Monitoring and Anomaly Detection – Table Talk

Mike Sayre, *Co-Founder & CEO, NexDefense*
Mike Chipley, *PhD, GICSP PMP LEED AP, President PMC Group*
Jason Dely, *Principal Security Consultant, Rockwell Automation*
Billy Rios, *Founder, Laconicly*
Graham Speake, *Chief Product Architect, NexDefense*

Small group networking and conversations (8-10 people at a table) led and facilitated by selected cybersecurity experts across several industries over lunch! No presentations or sales pitches!!

NERC CIP v5 and the NIST Cybersecurity Framework both stress the importance of network monitoring in keeping critical infrastructure and processes secure and reliable. However, the definition of "network monitoring" can be wide-ranging in methods, resources employed and value derived. At each table, the group will explore what monitoring practices our experts and you see employed today and what they/you believe it will take to meet the requirements and guidelines from NERC and NIST in the next few years, as well as monitoring processes and tools that will provide the highest ROI in security and reliability in the future.

LUNCH & LEARN

(LOCATION: GRAND REPUBLIC C)

Presented by

Ultra ELECTRONICS 3eTI
Connect & Protect Critical Operations

Just How Easy is it to Hack a DCS?

Dr. Alex Tarter, *Technical Director, Cyber Security Group, Ultra Electronics, 3eTI*

This session will be based on specialist experience with reverse engineering a major brand's distributed control systems (DCS) protocol. It will review what was discovered and how easily the system was penetrated. The session is designed to provide unique insights not easily attained elsewhere into the less well-known and investigated side of industrial control systems (ICS) – distributed control systems. Topics covered in the presentation will include an overview of information that is freely available, and information that can be inferred. It also will review information types that require further investigation to capture. Attendees will also discover ways in which the vulnerabilities identified can easily be exploited, as well as the resulting impact to the DCS environment and steps that can be taken to prevent and mitigate intrusions.

1:45-2:45 pm

Live ICS Attack Demonstration

***Tim Collins**, Software Architect - Critical Infrastructure Protection, ViaSat*
***David Lawrence**, Technology Development Manager – Emerging Technology, Duke Energy*
***Steve Lusk**, Program Manager - Critical Infrastructure Protection, ViaSat*
***Nick Saunders**, Software Lead - Critical Infrastructure Protection, ViaSat*

This lively and entertaining demonstration will offer an in-depth look at an ICS attack; it's sure to be an eye-opener. The demonstration will utilize example configurations with representative equipment that can be found in numerous ICS facilities. A moderator will walk through an attack that is targeting ICS protocols and trusted communication paths to impact operating conditions.

2:45-3:45 pm

SOLUTIONS SESSION

(LOCATION: GRAND REPUBLIC B)

Presented by

paloalto networks

Network, Endpoint & Cloud: A Platform Approach to Stopping Cyberthreats to Industrial Control Systems

***Del Rodillas,** Sr. Manager of SCADA/ICS Initiative, Palo Alto Networks*

Cyberthreats to today's ICS/SCADA systems are diverse, ranging from internet-borne, targeted attacks, malicious insiders and even unintentional incidents such as erroneous system programming. A new approach based on a prevention-focused, end-to-end cybersecurity platform is required to effectively address these cyberthreats, even the zero day threats, while improving the productivity of often oversubscribed control systems security teams.

SOLUTIONS SESSION

(LOCATION: GRAND REPUBLIC C)

Presented by

KPMG

Creating Quick Wins by Optimizing Operational Technology and Information Technology Process Controls

***Michael Gomez**, Principal, KPMG LLP (U.S.)*
***Brad Raiford**, Sr. Associate, Information Protection, KPMG LLP (U.S.)*

Traditionally, information technology (IT) and operational technology (OT) are managed as siloed domains necessitating segregated technology stacks and conventions, standards and paradigms, and governance structures. The underlying technology of OT systems, spanning communications, platforms, software, and security is swiftly beginning to resemble IT systems. Coupled with the emergence of disruptive technologies and evolving business processes, the need to establish integrated enterprise policies accommodating OT and IT solutions with processes for harmonizing data modeling and semantics is greater than ever. Within a truly integrated IT/OT environment, it is possible to institutionalize a data driven value chain to better convert real time data into actionable intelligence, identify high-impact use cases, derive quick wins and initiate further optimization based on hard facts.

3:45-4:15 pm

Networking Break & Vendor Showcase

(LOCATION: FANTASIA H)

4:15-4:55 pm

Cybersecuring DoD Industrial Control Systems, One Year Later…

***Michael Chipley, PhD**, GICSP PMP LEED AP, President*

In March 2014, the DoD adopted the NIST Risk Management Framework and began the arduous task of developing the implementation guidance to migrate from the DIACAP to the RMF. The application of the RMF to Industrial Control Systems is particularly challenging and this session will provide an update on the progress made to include the publication of the NIST SP 800-82 R2, incorporation of the new DoD and NIST publications into the DHS CSET tool, integration of the ICS Overlay and security controls into the electronic Mission Assurance Support System (eMASS), and efforts underway to develop the Continuous Monitoring capability with support from CYBERCOM and DHS.

4:55-5:40 pm

System-Wide Cybersecurity Failures: Are We Entering A New Phase?

MODERATOR:
***Mike Assante**, ICS & SCADA Security, SANS Institute*

PANELISTS:
***Mike Ahmadi**, CISSP, Global Director – Critical Systems Security, Codenomicon, Ltd.*
***Paul Forney**, Cyber Security Deployment Manager, Schneider Electric*
***Billy Rios**, Founder, Laconicly*

In March of 2014 the discovery of Heartbleed sent shockwaves through the world of technology, affecting vast numbers of technological systems globally, including ICS. Within the remaining year we saw the emergence of Shellshock and SSL 3 (POODLE) vulnerabilities. What is most alarming about these particular bugs is that they are both easily exploitable and system wide in nature. Additionally, the mean time between such massive bugs seems to be shrinking. This raises the question: Have we entered a new phase in cybersecurity challenges? If so, are we currently doing enough to effectively manage the situation? What are some potential reasons why researchers seem to be getting better at what they are doing? Where are we potentially falling short in the ICS world, and what can we do to change it? Join this session for a discussion that will shed some light on these topics.

5:40-6:00 pm

Play to Win: How to Build Awesome Professional Skills Through Cyber Security Challenges

***Tim Medin**, Senior Technical Analyst, CounterHack and Certified Instructor, SANS Institute*

Challenges like CyberCity give defenders a rare chance to get inside the minds of attackers. Additionally, there are countless other great challenges available on the Internet for people to develop their skills. The bragging rights alone are worth the long hours and late nights that competitors put in, but these challenges offer a unique and safe setting to try out new skills and take risks that would be unacceptable in any other environment. Learn how these challenges and games translate to real professional skills that can raise your security profile.

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.

6:00-7:00 pm

Networking Reception

(LOCATION: FANTASIA H)

7:00-10:00 pm*

WOPR: Shall We Play a Game?

Choose from three exciting hands-on challenges to help you build skills,
learn from fellow attendees, and enjoy some fast-paced competition.

**Some games may end earlier than 10 pm, allowing participants the chance to observe other games. All are welcome as observers.*

NETWARS CYBERCITY

(LOCATION: GRAND REPUBLIC B)

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, military, government, and commercial organizations are realizing an increasing need for skilled defenders of critical infrastructures. We engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructures. CyberCity engages participants to defend the city's components from terrorist cyber attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

KIPS SECURITY MONOPOLY**

(LOCATION: GRAND REPUBLIC C)

KIPS, Kaspersky Industrial Protection Simulation, is essentially a "Security Monopoly" game for maximizing enterprise revenue while building an ICS security capability. It features a simulated water utility trying to accomplish its mission to produce and sell water to the community, while dealing with and resolving unexpected cyber events. Registered participants will form teams that will run the same water utility trying to outperform others. Every response a team makes will have a knock-on effect on the running of their plant, so participants need to analyze data and make decisions despite uncertain information and limited resources. Sounds like real life? That's the point.

**All Cybati and CyberCity participants will need a laptop.

CYBATI GAME NIGHT***

(LOCATION: GRAND REPUBLIC A)

Are you interested in testing or expanding your ICS Cybersecurity skills for free? Have you spent your career defending ICS environments and always wanted to spend some time attacking an ICS environment in a safe way? The SANS Game Night will provide a unique opportunity for you to test your abilities in a number of different live environments with a variety of skill level options. The exercise will feature hands-on local kits from the CYBATI ICS mastery stations.

The CYBATI stations will challenge attendees through a series of cyber-physical red team exercises ranging in skill set from beginner/observer, to intermediate and advanced. The objectives and exercises during this free event will allow participants to transition through the typical ethical penetration testing lifecycle of: information gathering and analysis, vulnerability identification, penetration attempts and mitigating control recommendations.

***Participants are encouraged to arrive 30 minutes early. Each team participating in the KIPS exercise will need a laptop or iPad.

Tuesday, February 24

All Summit Sessions will be held in the Fantasia G (unless noted).

Summit presentations will be posted via the following URL, ***http://ics.sans.org/resources/summit-archives****,*
within 5 business days. An email will be sent to all attendees once live.

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

7:45-9:00 am

Breakfast Panel: Emerging Solutions for Evolving Threats

LOCATION: GRAND REPUBLIC B

MODERATOR:

Derek Harp*, ICS & SCADA Security, SANS Institute*

PANELISTS:

Eric Cornelius*, Director of Critical Infrastructure & ICS, Cylance*
Adam Meyer*, Chief Security Strategist, SurfWatch Labs*
Graham Speake*, VP & Chief Product Architect, NexDefense*
Doug Wylie*, Director – Industrial Security Program, Rockwell Automation*

As cyber threats have evolved over the last few years to become more targeted at ICS environments, the awareness of this activity has spawned an entirely new breed of cyber security solutions. This discussion will put the spotlight on the emerging solutions that have been brought to market by entrepreneurs and thought leaders who want to help us defend the infrastructure that services our communities and drives our economies.

9:00-10:00 am

Condition-Based Kill Chains and the Maturity of Next-Gen Attackers

Matthew Carpenter*, Principal Security Researcher, Grimm*
Mark Fabro*, CISSP, CISM, President and Chief Security Scientist, Lofty Perch, Inc.*

Threat assessment processes that have supported design basis threat (DBT) have traditionally not included cyber components. However, recent research results suggest that adversarial techniques are evolving to create new paradigms in cyber/physical attack methods. Historical separation of security responsibilities have resulted in new opportunities for attackers, opportunities that can be exploited based on customized capability and intent. This session will revisit the traditional attack kill chain and look at both theoretical and technical methods used by attackers and will empower the audience with a deeper understanding of how to better understand the realistic risk associated with their critical control systems.

10:00-10:45 am

Project SHINE: What We Discovered, and Why You Should Care

Bob Radvanovsky*, CIFI, CISM, REM, CIPS, Infracritical, Inc.*

Over the course of two and a half years, Project SHINE (named for SHodan INtelligence Extraction) undertook a comprehensive global data collection and analysis effort researching the size and magnitude of SCADA and control systems devices directly connected to the Internet. The intent was to identify a baseline of, and answer any possible risks associated with, having these discovered devices directly connected to an unsecured network. The scope of this presentation is not limited to the United States alone, but encompasses the seriousness of this issue from a Worldwide perspective. Many organizations and governments have expressed serious concern over this issue. Here, one of the lead researchers will present the surprising findings and explain why and how your systems may be more vulnerable than you think.

10:45-11:15 am

Networking Break & Vendor Showcase

(LOCATION: FANTASIA H)

11:15 am - Noon

Managing Risk in the Supply Chain

One of the most common topics raised over the past ten years of ICS Summits and from students in the SANS ICS-focused courseware has been: What are we supposed to do to reduce supply chain threats and how do we encourage our vendors to take action? In this session, you will hear perspectives of asset owners in regards to the programmatic steps they are implementing and internal controls being utilized to manage supply chain risk. You will also hear about the programs suppliers have in place to ensure delivery of trusted products that meet the cybersecurity demands of their customers. Finally, you will learn about collaboration among industry associations, government organizations, suppliers and asset owners in the development of frameworks, tools and approaches that can be used by all stakeholders in the management of the supply chain risk.

MODERATOR:

***Derek Harp**, ICS & SCADA Security, SANS Institute*

PANELISTS:

***Nadya Bartol**, VP Industry Affaires and Cybersecurity Strategist – UTC*
***Samara Moore**, Senior Manager CIP Security and Compliance – Exelon*
***Melanie Seader**, Senior Cyber and Infrastructure Security Analyst – EEI*
***Doug Wylie**, Director – Industrial Security Program, Rockwell Automation*

Noon - 12:45 pm

Dream Teams: Building the Multidisciplinary Workforce of Tomorrow

To have an appreciable impact in our sector, it's no longer enough to be an expert in just one discipline. IT cyber security pros, control systems operators, electric engineers, even senior and mid-level business executives ... if all they know is the world inside the tightly circumscribed boundaries of their chosen area of expertise, they're not going to be able to affect significant change. For the energy sector security challenges of today and tomorrow, it's time we build a hybrid workforce. Doing it right will require multiple approaches. The panelists will explore what's needed to develop the teams of the future.

MODERATOR:

***Andy Bochman**, Senior Cyber & Energy Security Strategist, Idaho National Lab National & Homeland Security Directorate*

PANELISTS:

***Nadya Bartol**, Vice President of Industry Affairs and Cybersecurity Strategist, Utilities Telecom Council*
***David Brown**, Director of Cyber Talent, SANS Institute*
***Christopher Peters**, VP, NERC Compliance and Critical Infrastructure Protection, Entergy*
***Justin Opatrny**, IT Security Consultant, General Mills*

12:45-2:00 pm

LUNCH & LEARN

(LOCATION: GRAND REPUBLIC A)

Presented by

Check Point SOFTWARE TECHNOLOGIES LTD.

Designing a Safe, Intelligent, Security Architecture

***Richard Devera**, Security Architect, Check Point Software Technologies, Inc*

Check Point will highlight major security events and current malware trend found during security assessments. The data included in this presentation is based on recent case studies and collaborative research and in-depth analysis of 200,000+ hours of monitored network traffic from 996 organizations of various industries.

In order to protect against today's evolving threat landscape, while supporting high-demanding network infrastructures, security professionals are asking for best practices in designing security architecture. Check Point will introduce trends in security technologies and best practices, which provides operational resilience and real-time, proactive protection for today's critical network infrastructure.

LUNCH & LEARN

(LOCATION: GRAND REPUBLIC B)

Presented by

RAPID7

Attacker Behavior and Incident Response

Pat Haley

Incident response is a hot area for companies looking to invest in business-critical security processes. This session will offer best practices for investigating attacks, and answer key questions, such as: Do I have the right tools in place for an investigation? Am I on the lookout for the right indicators of compromise? How can I shorten investigation time for each alert? With all the noise from alerts and false positives, do I have an understanding of what constitutes normal activity?

LUNCH & LEARN

(LOCATION: GRAND REPUBLIC C)

Presented by

SECURICON Information Security Solutions

Developing an Industrial Controls Security Framework for Balanced and Targeted Investment

***Ernie Hayden**, CISSP CEH GICSP, Executive Consultant, Securicon LLC*

This presentation will discuss setting the scene for the problem and providing information on how the challenge was solved with an effective framework. It will also include a sense of how the different standards were analyzed and how they were integrated into the single ICS Cyber Security Framework. We will also review how the Framework is being used as a cost savings vehicle. The audience will gain a sense of the challenge faced by these global companies and ICS security; they will understand the desired outcome for this ICS cybersecurity framework, and they will understand the approach taken to build the framework for ultimate use as part of a balanced Cyber Security Program.

2:00-2:45 pm

Missing the Obvious: Network Security Monitoring for ICS

***Rob Caldwell**, Principal Consultant, Mandiant, a FireEye Company*
***Chris Sistrunk**, Senior Consultant, Mandiant, a FireEye Company*

Why haven't we seen more ICS-focused attacks? Perhaps it's because we're not looking for them. The current state of security in Industrial Control Systems is a widely publicized issue, but fixes to ICS security issues are long cycle, with some systems and devices that will unfortunately never have patches available. In this environment, visibility into security threats to ICS is critical, and almost all of ICS monitoring has been focused on compliance, rather than looking for indicators/evidence of compromise. The non-intrusive nature of Network Security Monitoring (NSM) is a perfect fit for ICS. This presentation looks at using NSM as part of an incident response strategy in ICS, various options for implementing NSM, and some of the capabilities that NSM can bring to an ICS cyber security program.

2:45-3:45 pm

SOLUTIONS SESSION

(LOCATION: GRAND REPUBLIC A)

Presented by

SecurityMatters

SilentDefense ICS: Where Cybersecurity Meets Operational Value

***Damiano Bolzoni**, CEO & Co-Founder, SecurityMatters B.V.*

What if cyberattacks were not the biggest threat to industrial networks and systems? Although malware is still a major point of interest, the sword of Damocles for critical industrial networks is represented by system misuse performed by disgruntled employees, contractors and vendors, as well as unintentional operator's mistakes, network and system misconfiguration, and uncontrolled configuration changes; all this could lead to the divergence or failure of critical processes.

In this talk we reshape the concept of ICS security and demonstrate how the network monitoring platform SilentDefense ICS ensures that all these critical threats that slip past other security defenses will be promptly detected and reported to the security operator.

SOLUTIONS SESSION

(LOCATION: GRAND REPUBLIC B)

Presented by

NEXDEFENSE

BYOPcap! - Sophia Industrial Network Anomaly Detection (INAD)

***Loney Crist**, VP of Engineering, NexDefense*
***Graham Speake**, Chief Product Architect, NexDefense*

Bring Your Own Packet Capture and see Sophia in action. NexDefense has released the latest version of Sophia, the world's first Industrial Network Anomaly Detection (INAD) solution. This session will provide a live demonstration of the Sophia technology and the opportunity for attendees to run their own packet captures in order to visualize the behaviors taking place in their ICS networks. Bring a packet capture (pcap) from your live network(s), lab or development set-up and join us for an informative session to learn how to effectively monitor inside your control system networks and quickly identify potentially malicious behavior.

SOLUTIONS SESSION

(LOCATION: GRAND REPUBLIC C)

Presented by

Elbit Systems of America

ICS Level 1 and 2 Network Anomaly Detection – Fides Has Your Six

***Dennis Murphy**, Director, Cybersecurity Business Development, Elbit Systems of America, LLC*

Communications between a SCADA network's level 1 and level 2 core assets (HMI, PLC, RTU, IED) are rarely viewed by perimeter IDS sensors by design. Localized firewalls and IPS systems can protect these core assets, but they tend to lack the ability to provide high-fidelity forensics capabilities. Continuous monitoring of these two network layers is a growing trend. This session will describe the benefits, risks and challenges of instrumenting your ICS network for continuous monitoring in the core sections of your network.

3:45-4:15 pm

Networking Break & Vendor Showcase

(LOCATION: FANTASIA H)

4:15-5:00 pm

ICS & Automation Security Organizational Model

MODERATOR:
***Mike Assante**, ICS & SCADA Security, SANS Institute*

PANELISTS:
***Andy Bochman**, Senior Cyber & Energy Security Strategist, Idaho National Lab National & Homeland Security Directorate*
***Kevin Staggs**, CISSP, CSSLP, Sr. Engineering Fellow, Honeywell ACS Advanced Technology Lab*
***Doug Wylie**, Director – Industrial Security Program, Rockwell Automation*

Many organizations struggle to identify the right governance structure and organizational model that suites their business and more specifically enables their Operations focused business units to be successful. The panelists will examine some of the lessons learned that they have experienced throughout their careers, discuss some case study examples of organization approaches that could impact operations environments, and provide attendees some example organization approaches that have worked.

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.**

EXHIBITORS

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies, Inc.
Check Point Software Technologies (**www.checkpoint.com**), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices with comprehensive and intuitive security management.

CODENOMICON

Codenomicon
Codenomicon provides a suite of next-generation testing solutions that improve the security and robustness of technology that powers our connected world. Codenomicon's tools empower developers and asset owners to proactively discover, identify, and remediate vulnerabilities in business-critical software and devices ahead of attacks. Build a more resilient world with Codenomicon.

CYLANCE

Cylance
Cylance is a next generation, endpoint protection, product company, specializing in advanced threat security that detects and stops zero-day malware and APT attacks. Using advanced math and machine learning, coupled with the understanding of a hacker's mindset, Cylance provides a proactive, preventive approach to security.

Dexa Systems

Dexa Systems
Dexa Systems is a global, privately held company that provides cyber and physical security solutions for Critical Infrastructure industries, including oil and gas, utilities, petro chemicals, pipeline, upstream, refineries, etc. We have a strategic security model for today's cyber environment and assist our clients in developing a next generation security strategy.

Elbit Systems of America

Elbit Systems
Elbit Systems of America, LLC, develops cyber security products to keep our troops safe and our critical infrastructure operating. Building on global security technology with over 20 years of legacy evidence, our employees are dedicated to supporting those who contribute daily to the safety and security of the United States.

IOActive COMPREHENSIVE INFORMATION SECURITY SERVICES

IOActive
Advances in technology create new opportunities and unforeseen risks. That's why cutting-edge research is central to IOActive services. We are the only global security consultancy conducting chip-to-code assessments with a state-of-the-art hardware lab and deep expertise spanning hardware, software, and wetware. We help industrial clients stay ahead of tomorrow's threats.

KPMG

KPMG
Launched in 2007, the KPMG Global Energy Institute (GEI) interacts with its over 30,000 members through multiple media channels, including audio and video webcasts, publications and white papers, podcasts, events, and quarterly newsletters. In February 2011, the GEI opened the doors of its physical space in the downtown offices of KPMG in U.S.'s Houston office. The leading knowledge center features over 5,000 square feet of executive training facilities, which provide the perfect backdrop to GEI's in-person share forums and conferences

iguana

IGUANA Security
IGUANA Security is a brand developed specifically for the CNI market, and is brought to you by L-3 TRL Technology; with 30 years experience in developing innovative, high technology defence and security solutions. IGUANA Security provides organisations with the necessary security functions to protect the integrity, confidentiality and availability of networks whilst enabling greater business efficiency.

EXHIBITORS

NexDefense, Inc.
NexDefense empowers automation and control system operators in critical infrastructure and defense facilities with the real-time knowledge needed to maintain system integrity and combat security threats. Its software solution, Sophia, maintains constant insight into and visualization of ICS network communications, giving security professionals visibility into potential threats without disrupting productivity or performance.

Palo Alto Networks
Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters in today's dynamic computing environments: applications, users, and content.

PFP Cybersecurity
PFP Cybersecurity provides a new category of cyber protection, physics-based integrity assessment, which reduces the detection gap's time-to-discovery to mere milliseconds. The PFP physics-based solution uses patent pending, advanced signal processing on side channel data (e.g., instantaneous power consumption) to derive information about the internal execution status of the user's hardware and firmware. PFP has demonstrated its solution with many applications including Stuxnet-like attacks on industrial control systems, SCADAs and PLCs.

Pwnie Express
Pwnie Express provides an end-to-end security assessment solution that delivers real-time wired and wireless asset discovery, continuous vulnerability scanning, pentesting, risk trending and alerting. It provides sensors for individual locations and an enterprise-class Pwn Pulse solution using its sensors combined with central management for scalable continuous intelligence across remote locations.

Rapid7 Inc.
Rapid7 security analytics software and services reduce cyber threat exposure and detect compromise for 3,000 organizations across 78 countries, including over 250 of the Fortune 1000. We understand the attacker better than anyone and build that insight into our solutions to help you improve risk management and stop threats faster.

Recorded Future
RecordedFuture arms you with real-time threat intelligence to proactively defend your organization from cyber attacks. Our patented Web Intelligence Engine indexes and analyzes the open web to provide you full context into emerging threats. Four of the top five companies in the world rely on Recorded Future to understand and mitigate threats.

Rockwell Automation
Rockwell Automation, the world's largest company dedicated to industrial automation, makes its customers more productive and the world more sustainable. Our flagship Allen-Bradley® and Rockwell Software® brands are globally recognized for innovation and excellence. Every day we help to solve automation challenges and support safe, secure and reliable operation of industrial control systems around the world.

EXHIBITORS

Securicon
Securicon provides expert application, system and network security consulting services. These services include: cyber program development, vulnerability assessments, compliance audits and consulting, security architecture consulting, application security evaluations, penetration testing, EMS and DCS assessments, device testing, and more. These services are delivered across corporate America, with special focus in the Utilities, Water, Oil & Gas, Transportation, Manufacturing, Pharmaceutical and Financial Services industries, as well as Government and all Corporate Enterprise networks and Real-time system infrastructures.

SecurityMatters
SecurityMatters is an international company that brings to the market the next generation network monitoring, intelligence and protection technology to make Critical Infrastructure organizations more secure and in control. SecurityMatters has business in a number of control industries including Oil & Gas, power generation, electric-power transmission and distribution, water supply and manufacturing.

SurfWatch Labs
SurfWatch Labs delivers powerful cyber risk intelligence analytics and applications through a business intelligence approach that helps organizations improve their long-term cyber resiliency. Created in 2013 by former U.S. Government intelligence analysts, SurfWatch Labs solutions go beyond the low-level threat data and security tactics that organizations can drown in, by providing insights into cyber risks and their impact on key business operations. SurfWatch Labs: Cyber In Sight. For more information, visit **www.surfwatchlabs.com**.

Tempered Networks
Tempered Networks protects critical infrastructure and information from cyber attacks, misuse by trusted or untrusted users, and from other systems and devices. We provide a purpose-built, hardened security appliance that cloaks your critical infrastructure. The solution securely extends and segments your network. Our deep experience is delivering business value to Fortune 500 companies today.

Ultra Electronics, 3eTI
Ultra Electronics, 3eTI is a leading cyber-technology company with products and systems that secure critical infrastructure and improve operational efficiency. 3eTI helps connect and protect operations through advanced machine-to-machine (M2M) security, secure wireless networks and sensor network applications, leveraging new and legacy systems while complying with highest government and industry standards. **www.ultra-3eti.com**

Waterfall Security
Waterfall Security is the leading provider of network security products enabling safe and secure IT/OT integration for critical infrastructures, industrial sites and manufacturing facilities. The company develops products which provide stronger-than-firewall protections for industrial control networks. Waterfall's products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and the Middle-East in a number of power and nuclear plants, on/off-shore platforms, refineries, utility companies plus many more.