CYBER SECURITY
FOR CRITICAL ASSETS | USA

March 26th - 28th 2019

www.cs4ca.com/usa

#CS4CA

Houston, Texas

DoubleTree Hilton Hotel Houston, Greenway Plaza

OVERVIEW OF THE CONFERENCE:

Now in its 7th year, CS4CA Summit USA boasts two dedicated streams for IT and OT, allowing delegates to hone in on their specialist areas of interest, as well as plenary sessions addressing the common issues that bind both groups of professionals. Each stream is curated by a group of industry-leading experts to ensure innovative, detailed and up-to-date content.

Expect to be challenged and learn to see existing issues as well as solutions from a fresh angle, as we gather some of the world's top cybersecurity innovators to enrich your understanding of the landscape. A variety of session formats, ranging from large-scale keynotes from leading industry execs, via interactive panel debates, case studies to platforms to showcase the best of tomorrow's technology.

SPONSORS:

PAS®

FORTINET®

DRAGOS

IBM Security

Indegy
Activate All Your Senses

F-Secure

Check Point
SOFTWARE TECHNOLOGIES LTD.

illumio

FORESCOUT

tdi
technologies

SILVERFORT

nccgroup

CLAROTY
Clarity for OT Networks

DISPEL

CYBERX
BATTLE-TESTED INDUSTRIAL CYBERSECURITY

Honeywell

tripwire

DARKTRACE
INDUSTRIAL

DNV·GL

OWL
Cyber Defense

tenable

GATE SCANNER
Presented by BATTELLE

DUO

NOZOMI
NETWORKS

BlackBerry

VERICLAVE

أرامكو السعودية
saudi aramco

SecurityGate

QATALYST GLOBAL
Accelerating Growth

DRIVING INNOVATION AND PROVIDING VALUE IN CRITICAL INDUSTRIES

www.qatalystglobal.com

CONFERENCE DAY ONE
TUESDAY MARCH 26TH 2019

08:00 REGISTRATION

08:50 OPENING ADDRESS

OPENING PANEL

09:00

The State of Security Vs Level of Preparedness

- Security is not a tick box for other departments – how do ensure other departments agree?
- How are you differentiating between noise and actual threat?
- Who are you using as a benchmark and how often is it being updated?

OFFICIAL KEYNOTE

09:40

So You've Been Hacked. Now What?

- How can bad actors can create unsafe conditions by making simple changes?
- What value does detailed configuration management bring to your ICS Cybersecurity strategy?
- How can you improve both ICS Cybersecurity and process reliability by better managing the configuration of your ICS assets?

KEYNOTE PRESENTATION

10:20

A Review of the Threat Landscape Across the United States

- What impact has growth of networks and communication systems had and exposed as vulnerabilities?
- Do utility companies fully understand the scope of their cyber security posture across the company?
- Is the financial support available to meet the business and regulatory requests?

10:50 NETWORKING BREAK & 1-2-1 MEETINGS

PRESENTATION - IT STREAM

11:30

Is Edge Computing the Answer for Security Around IoT

Described as a mesh network of micro data centers to process or store critical data locally and push all received data to a central data center or cloud storage repository. Edge computing like IoT is considered a way to cut costs and innovate process. But what are the practical elements around it and how does implementation look?

Edge computing, in turn, helps to:

- Cut latency by bringing storage and compute closer to the user
- Optimize bandwidth by controlling traffic flow
- Preserve the energy capabilities of IoT devices by incorporating "a flexible task offloading scheme which considers the power resources of each device"
- Reduce network overhead by aggregating and preprocessing "trivial packets"

PRESENTATION - OT STREAM

Five Ways to Ensure the Integrity of Your Industrial Operations

In the course of the last twenty four months, there have been unprecedented changes to industrial operations such as yours. With a more heterogeneous community accessing your OT network on more devices and conducting more operations through IIoT enabled devices, the integrity of those operations has never been more complex. Failure to adjust to this new reality can result in visibility, security and control gaps, which can put your organization at risk.

This highly engaging discussion reviews the top five things you need to know to help reduce the security risk that has found its way into industrial operations and how, by implementing them, you can increase the efficiency of your operations while simultaneously reducing costs.

PRESENTATION - IT STREAM

12:00

DevSecOps: Shifting from DevOps to SecOps

- Integrating security into the process
- TBC

PRESENTATION - OT STREAM

Mitigating and Owning Residual Risk

- 4 ways to deal with residual risk. How do you know which one to use when?
- Reduce it, avoid it, accept it or transfer it

PLATFORM PRESENTATION - IT STREAM

12:20

Protecting the Unprotectable with Next-Generation Authentication

- Multi-factor authentication is a critical security measure yet many critical IT and OT systems remain unprotected, why is that?
- How can Next-Generation Authentication strengthen the security of these systems?
- Why is it important to apply adaptive access controls that are based on holistic AI-Driven risk analysis?

PLATFORM PRESENTATION - OT STREAM

Results of Real-World ICS Malware Discovered

- What can we learn from examination past nation-state attacks on critical infrastructure?

12:30 SEATED LUNCH HOSTED BY PAS

01:30 PRESENTATION - IT STREAM

To Secure Peace We Must Prepare for (Cyber) War

- Explore the realities of cyber conflict in an increasingly volatile world
- Delve into the details of our recent investigations into advanced persistent threats and details into planning for new threats, technology vulnerabilities and security risks
- Discuss the mutually-influential relationship between the cyber domain, trade and international relations

02:00 PRESENTATION - IT STREAM

AI and Cybersecurity: Friend or Foe?

- The oportunities are vast but are AI threats understood?
- TBC

02:30 PRESENTATION - IT STREAM

Key Steps for Security Road Mapping

- Protect, Control, Detect, Respond

PRESENTATION - OT STREAM

Improving Visibility of your Digital Forensic Data

- How to pragmatically get to implementation of protective controls through visibility and continuous monitoring

CASE STUDY

Introducing IoT and Making sure Security is a Part of the Process

- The complexity of the Industrial Internet of Things can be overwhelming, where do you start and how do you maintain control?

PRESENTATION - OT STREAM

Separating Human Threat with Vs Bot

03:00 NETWORKING BREAK & 1-2-1 MEETINGS

03:30 ROUNDTABLES

Table 1: The Role Humans Play in a World of Automation

Table 2: An attacker delivers software updates which enables a back door critical information system, what next?

Table 3: TBC

Table 4: Insider Threats

Table 5: ISO 27001... Why? Why now?

Table 6: Creating a Culture of Support for OT

Table 7: Role of IAM for Your Industrial Plant

Table 8: Your OT Cybersecurity Has Become Overwhelming. How Can You Prioritize & Reduce Complexity?

04:10 PRESENTATION

Securing the Future of Energy and Utilities

- Insider Threats to Critical Infrastructure, Trends Impacting IT/OT Convergence
- The Impact of Visibility, Control and Analytics in an Era of Digital Transformation
- Ingredients for an Energy 4.0 Cybersecurity Strategy

04:40 PRESENTATION

GridEx – North America's Bi-annual Cyber/Physical Security Exercise and Lessons Learned

05:10 PANEL DISCUSSION

Governance, People and Processes

- Are all 3 playing their part to fill the security gap? What more can be done?
- A successful strategy relies on the strength of partnerships, where are the current weaknesses?

05:50 CLOSING REMARKS:
Don't forget to fill in your evaluation form!

06:00 NETWORKING DRINKS HOSTED BY BlackBerry

07:00 DINNER HOSTED BY: (By invitation only) NOZOMI NETWORKS

CONFERENCE DAY TWO
WEDNESDAY MARCH 27TH 2019

08:15 REGISTRATION & BREAKFAST HOSTED BY: DUO

08:50 OPENING ADDRESS FROM THE CHAIR

OPENING PANEL

09:00

Strategies to Support Outdated and Vulnerable Systems and Assets

- Industrial cyber security is ever evolving, with organizations now aligning budget and resources against threats but how can we get older assets to do their part?
- How supportive is firewall segmentation in supporting outdated assets?
- How do you know what you know? What is it being verified against?

PRESENTATION

09:40

Current ICS Threat Landscape

The ICS threat landscape is complex and uneven. Threats targeting OT networks are growing with a deliberate pace. Dragos uncovers new OT threats weekly via its OT technology platform, array of services, and threat intelligence monitoring. Surveying the OT threat landscape and detail the major activity groups and the root causes of many recent OT compromises. The presentation will provide the audience with a pragmatic view of the ICS threat landscape sourced entirely from real events. Importantly, six actions asset owners and operators can take today to make themselves more secure.

KEYNOTE PRESENTATION

10:10

Benchmarking Your Corporate Governance Structure for OT to the Framework

10:40 NETWORKING BREAK & 1-2-1 MEETINGS

PRESENTATION - IT STREAM

11:20

TBC

PRESENTATION - OT STREAM

Leveraging Cybersecurity to Improve Operations and Situational Awareness

PRESENTATION

11:50

Innovating OT to make it Undeniably Attractive For IT

12:20 SEATED LUNCH HOSTED BY: FORTINET

PRESENTATION - IT STREAM

01:20

Building an Ecosystem to Establish a Resilient and Adaptable Security Posture

- What does it mean to be prepared for a cyber-attack? Are you prepared?
- How do you ensure that you are not being reactive but are constantly proactive in your approach?

CASE STUDY - OT STREAM

Culture of Interaction Between Human and Robot

- TBC
- TBC

CYBER-SECURITY WORKSHOP: DAY THREE

THURSDAY 28TH MARCH 2019

*Speak to a Member of the Team to Register!

Limited Places Available!*

Led by: Dr. Sujeet Shenoi, Professor of Computer Science & Chemical Engineering, University of Tulsa

Dr. Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, and a member of the technical staff at Johns Hopkins University Applied Physics Laboratory. An active researcher with specialties in cyber security, cyber operations, critical infrastructure protection and digital forensics, Dr. Shenoi works on exciting "problems" ranging from helping solve homicides to penetrating telecommunications systems, oil and gas pipelines, wind farms and voting machines.

This all-day workshop uses several case studies to understand how advanced attackers penetrate critical infrastructures. Understanding the attackers' mindsets and the Infrastructure attack surfaces and vulnerabilities/attacks helps inform the development of countermeasures and effective risk mitigation efforts. The infrastructure assets covered in this workshop include financial entities, gas pipelines, coal mines, telecommunications networks, wind farms and electric power distribution networks.

08:30 REGISTRATION & COFFEE

08:50 OPENING ADDRESS
How Open-Source Intelligence is Used to Attack Critical Infrastructure Assets -
A three-part presentation involving real infrastructure assets

09:00 How they attack and how you can defend your critical infrastructure assets

11:00 Case Studies - Learn from a range of case studies where vulnerabilities were highlighted across critical assets globally

12:30 SEATED LUNCH

01:30 The importance of designing security solutions that integrate science, technology and policy

03:00 Review - Compare and contrast your work with your peers - What will you do differently in future?

04:00 CLOSING REMARKS & END OF WORKSHOP

PRESENTATION

01:50 **Understanding Cyber Insurance Liability**

02:50 NETWORKING BREAK & 1-2-1 MEETINGS

PRESENTATION

03:20 **How Open-Source Intelligence is Used to Attack Critical Infrastructure Assets**

- A 3 Part presentation involving real assets

GROUP DISCUSSION

03:50 **Creating a Culture of Support for IT**

- What impact has the change of technology had on OT?
- Is it time to build a middle layer between IT & OT?
- Best practice for closing the gap to create an offensive rather than defensive environment

04:30 CLOSING ADDRESS FROM THE CHAIR