CYBER SECURITY

FOR CRITICAL ASSETS | USA

www.cs4ca.com/usa
@QatalystGlobal
#CS4CA

March 6th - 8th 2018

Venue: JW Marriot, Houston, USA

Overview of the Conference:

Now in its 6th year, CS4CA USA has never been more relevant as the platform for IT and OT leaders across North America to come together to fight tomorrow's cyber security battle across the Oil and Gas, Pharma, Energy, Utility, Chemical and Petrochemical, Water and Aerospace industries. Allowing thought leaders to discuss industry challenges, share experiences and investigate the best practice guidelines, CS4CA will move discussions from recovery-focused to proactive approaches to bridge the gap between IT and OT.

The event's strengths lie in its ability to combine case studies of what has occurred alongside keynotes of what to expect and group discussion sessions where we benchmark, align, innovate and collaborate with thought leaders to inform Cyber Security policies for years to come and protect the future of the USA's critical assets.

Why Attend the CS4CA USA Summit?

- *Learn about the integration of ICS & Corporate Systems*
- *Discuss the role of security professionals in the critical assets sector*
- *Explore future threats of cyber security as a form of warfare*
- *Find out how cyberinsurance fits into risk management*
- *Network with industry leaders and peers*
- *Listen to case studies on how key players are combatting & recovering from cyber attacks*

EVENT SPONSORS:

ARBOR NETWORKS
The Security Division of NETSCOUT

PAS

CYLANCE

Indegy
Industrial Cyber Security

DARKTRACE

CLAROTY
Clarity for OT Networks

sath

FORTINET

CyberX
Trusted. Industrial. Cybersecurity.

SKYBOX SECURITY

tripwire

ABSOLUTE

BAYSHORE

Check Point
SOFTWARE TECHNOLOGIES LTD.

axio

tenable

QATALYST GLOBAL

CREATING BESPOKE STRATEGIC BUSINESS EVENTS, CONFERENCES, SUMMITS AND WEBINARS
www.qatalystglobal.com

CONFERENCE DAY ONE
TUESDAY 6TH MARCH 2018

08:00 REGISTRATION

08:50 OPENING ADDRESS FROM THE CHAIRMAN:

OPENING PANEL

09:00

How is Legislation and Framework Here and Globally Shaping your Approach to Insider Threats?

- How does being CISO for a life and death industry differ from other sectors?
- When does incident response move to disaster recovery and continuity?
- How must priorities change now operations have moved up attackers' target list?
- On the front line: how should critical asset owners and governments respond to increasing state-sponsored attacks?
- Are current risk management approaches and reference architectures appropriate?
- How do you balance compliance requirements with effective cybersecurity strategy?
- Is there a role for cyber-offence in the critical asset CISO's arsenal?

KEYNOTE PRESENTATION

09:40

How should Wannacry, Petya and notPetya influence your strategy towards Ransomware?

- Ransomware is not going away and is becoming more virulent, are you doing the basics to protect yourself?

PRESENTATION

10:20

Post-Breach - Recovering for the New Normal - Getting it Right

- Why are nation state attacks increasing? How common and dangerous might they become?
- In Ukraine, 2015 saw the first successful attack on an electricity grid, is the US prepared for a similar attack?
- How DHS is supporting the private sector's fight on the front line of state-sponsored cyber-attacks?

10:50 NETWORKING BREAK & BUSINESS CARD EXCHANGE

PRESENTATION - IT STREAM

11:30

Critical Assets In The Cloud: Are Cybersecurity Teams Ready?

- IT can feel like they are losing control of security when moving to the cloud, but the opposite is often the case

PRESENTATION - OT STREAM

Protecting ICS systems

- Keeping your industrial control systems safe

PRESENTATION

12:00

Setting A New Standard For The Whole Industry: The NIST Cybersecurity Framework

- OT requires a very different approach to security than enterprise IT, NIST 800-82 lays out practical implementations that help OT managers ensure their control systems are secure
- With presidential authority now backing the adoption of the NIST Cybersecurity Framework has become the keystone for securing the nation's infrastructure
- Practical Implementations For Industrial Control Systems: NIST Specification 800-82

PLATFORM PRESENTATION - IT STREAM

12:30

End the Dark Endpoint Epidemic

- Why yet another endpoint agent is not the answer
- How to benchmark against cybersecurity frameworks to strengthen your security posture
- How you can achieve full visibility across all your devices and data - regardless of user or location
- How this technology already exists in your devices today and how you can utilize it to rapidly remediate threats

PLATFORM PRESENTATION - OT STREAM

Network Mapping

- Understanding your ICS network is the first step to securing it, but that is often easier said than done

12:40 SEATED LUNCH

PRESENTATION - IT STREAM

01:40

Managing Security in Hybrid IT/OT Environments

- How IT threats are being applied to OT environments, with a quick look at recent attacks and proof-of-concepts
- How hybrid network modeling unifies IT/OT security management to reduce risk, improve uptime and maintain safety
- What tools and processes are needed to prioritize patching or identify compensating controls when patching isn't an option

PRESENTATION - OT STREAM

Darktrace defending against OT attacks

- How do you keep your ICS safe?

CASE STUDY - IT STREAM

02:10

Safely And Securely Enhancing Enterprise IT Efficiency Through The Cloud

- Working with your cloud provider to ensure it can securely interface with your systems
- How do you secure your cloud system against penetration and detect any malicious actors?
- Working with compliance managers and regulators to ensure cloud-based systems remain compliant

CASE STUDY - OT STREAM

Why Two-Way Communication And Education Is Essential To IT/OT Working Together In Harmony

- There is no magic bullet which will allow OT and IT teams to work together, but communication is vital
- Setting up channels so that IT and OT can learn from each other is essential and makes life much easier
- Operational priorities are business priorities and with communication and education IT can enable that

PRESENTATION - IT STREAM

02:40

Know Your Enemy: Responding To Threat Intelligence

- Replacing old systems with mobile devices can you're your company leaner and more responsive, but keeping your mobile services secure requires careful planning

PRESENTATION - OT STREAM

Securing An Industrial Control System: Monitoring And Detecting Unusual Activity On Your Network

- Threat intelligence is essential for protecting your systems and operations, responding quickly and effectively to that intelligence is more important than ever

03:10 NETWORKING BREAK & BUSINESS CARD EXCHANGE

ROUNDTABLES

03:40

How is Legislation and Framework Here and Globally Shaping your Approach to Insider Threats?

T1: Bringing Together IT And OT Teams: What Works, What Backfires?

T2: Identifying 3rd Party Risks: How Can You Ensure Your Suppliers Don't Compromise You?

T3: Replacing Hardware: How Do You Push Cybersecurity Up The Procurement Priority List?

T4: Patching ICS Systems: How Do You Find The Right Balance To Maintain High Capacity Utilisation?

T5: Combatting Spearphishing: How Best Can People Be Educated About The Risks Of Enhanced Targeting?

T6: Threat Hunting in IT and OT Environments

T7: Keeping Your Strategy Up-To-Date: Watching For Threats And Updating Your Approach

T8: Department For Homeland Security In Southern Texas: What Can DHS Do For You?

T9: What Are The Secrets To Keeping The Board Constantly And Intelligently Engaged In Cybersecurity?

KEYNOTE PRESENTATION

04:20

Defending against DDoS

- DDoS is an old problem but a potentially devastating one

PRESENTATION

04:50

How Should You Respond To The Ukraine Electricity Grid Attack?

- The Ukraine grid attack was complicated, coordinated and terrifying even if its scale was limited. In this session you will hear more about how the attack unfolded and how you should respond to this type of threat.

PANNEL DISCUSSION

05:20

You Can't Patch The Human Factor

- Are high profile attacks making staff more receptive to cybersecurity messages?
- How do you create a culture of continual response, rather than relying on responses to particular threats or incidents?
- How do you vary messages and techniques to keep everyone engaged in cybersecurity year after year?
- If your staff are not always taking your cybersecurity seriously how can you be sure 3rd parties are?
- Insider threat: how do you minimise the risks posed by your own people?

06:00 CHAIRMAN'S CLOSING REMARKS

06:10 NETWORKING DRINKS

CONFERENCE DAY TWO
WEDNESDAY 7TH MARCH 2018

08:15 REGISTRATION

08:50 OPENING ADDRESS FROM THE CHAIRMAN:

OPENING PANEL

09:00

Partial IT/OT Convergence Is Still Holding Back Your Cybersecurity

- What are the keys to keeping IT from contaminating OT? How can OT best implement IT best practice?
- How centralised should your cybersecurity function be? How decentralized should implementation of your strategy be?
- Is there still a role for separate IT and OT teams or is it time to merge them?
- Does Industrial IoT, Big Data and cloud analytics mean a complete IT/OT convergence is ultimately inevitable anyway?
- How does incomplete IT/OT convergence make remote access and 3rd party risk management harder?

KEYNOTE PRESENTATION

09:40

Creating A Constant State Of Preparedness For Cyber-Attacks

- 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?

PRESENTATION

10:10

Threat Intelligence and ICS Systems

- TBC
- TBC

10:40 NETWORKING BREAK & BUSINESS CARD EXCHANGE

PRESENTATION - IT STREAM

11:30

Keeping Mobile Solutions Safe

- Advanced persistent threats are constant worries for critical assets, they are difficult to detect but are not impossible to defend against

PRESENTATION - OT STREAM

There Will Be No End Point In The Quest To Secure Endpoints

- Replacing old systems with mobile devices can you're your company leaner and more responsive, but keeping your mobile services secure requires careful planning

CASE STUDY - IT STREAM

11:50

Securing The Internet Of Things

- Due to rapidly falling costs Industrial IoT can be deployed faster than it can be secured, but the extra endpoints, networks and IT/OT interfaces don't need to make your operations less secure
- How can you ensure your IoT-enabled assets are secure by design and deliver the promised benefits of IoT without the risks?

PRESENTATION - IT STREAM

Do You Really Understand Your Network Architecture To Properly Protect It?

- If you're going to ensure your ICS is safe you need to understand it, and that means ensuring a sensible network architecture that is well-understood by your team
- Why do network architectures become so unclear and how can you map out and secure your network?
- How do you prevent network architectures getting messy?

PLATFORM PRESENTATION - IT STREAM

12:20

Keeping Mobile Solutions Safe

- Mobile solutions are popular with you and with cyber attackers, find out how to keep them safe

PLATFORM PRESENTATION - OT STREAM

Securing An IoT Network

- Keeping an IoT network secure involves a more comprehensive approach than simple IT or OT systems, but the principles are the same

12:30 SEATED LUNCH

PRESENTATION - IT STREAM

01:30

Your New Most Valuable Asset: Keeping Your Data Under Secure Lock And Key

- Getting data protection policy right can give you a critical advantage against hackers

PRESENTATION - OT STREAM

Meeting Security Requirements For A SCADA System

- SCADA systems require their own approach for cybersecurity, in this session we will talk about how you can ensure they stay secure at maximum utilisation

PRESENTATION

02:00 **Do We Need To Completely Change Our Approach to IoT To Keep The World Safe?**

- The world is installing computing power at a phenomenal rate and much of it is unsecured or inadequately secured
- What implications does the explosion of computingpowers, sensors and connectivity have for cybersecurity?
- Do we need to change how we approach IoT completely?

PRESENTATION

02:30 **AI And Situational Awareness**

- Artificial intelligence and machine learning promise a big leap forward for identifying suspicious traffic on networks
- AI combined with analysts who understand a network can rapidly improve how quickly penetrations can be detected

03:00 NETWORKING BREAK & BUSINESS CARD EXCHANGE

PRESENTATION

03:30 **What Role Should Cyberinsurance Play In Your Risk Management Strategy**

- Collaboration Between Risk, IT And Everyone Else: How Do I Understand My Risk Profile?
- Getting Board Buy-In: How Do You Sell Cyberinsurance Internally?
- Making Cyberinsurance A Reality: Where Cyberinsurance Does And Doesn't Help

GROUP DISCUSSION

04:10 **How Can CISOs Build A Skilled Workforce And Internal Capacity Needed To Keep Their Systems Secure?**

- That's not enough! How do you make your budget stretch to hire the staff you need?
- Changing corporate culture: how do you ensure a constant insurgency against cyber threats?
- Tackling the cybersecurity skills shortage: what can firms do internally to promote local talent?
- Retaining staff: how do you keep staff engaged in a fight they will never conclusively win?
- Is critical asset cybersecurity sexy enough to lure people away from the tech sector?

06:00 CLOSING ADDRESS FROM THE CHAIRMAN:
Perry Pederson, Senior Control Systems Security Manager, Pacific Northwest National Laboratory

CYBER-SECURITY WORKSHOP: DAY THREE

THURSDAY 8TH MARCH 2018

(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.

Overview: This training course will help you think like a cyber attacker and respond accordingly. You will leave this day of intensive training thinking differently about your risk and vulnerability, with a better understanding of the tools, techniques and weapons which will be targeted against you. With an extensive interactive element and an industry-leading trainer this course will give you concrete takeaways and a fresh outlook on your strategy.

08:30 REGISTRATION & COFFEE

08:50 OPENING ADDRESS
Dr. Sujeet Shenoi, Professor of Computer Science & Chemical Engineering, University of Tulsa

09:00 **Assessing Cyber Risks, Threats & Responses - Learning to think like an attacker**

11:00 **Cyberoffence Workshop - Learn about the tools used to attack your critical assets**

12:30 SEATED LUNCH

02:30 **Group Exercise - Simulate a cyber-attack and try to bring down a critical asset**

04:00 **Group Exercise - Compare and contrast your work with your peers - What will you do differently in future?**

05:00 CLOSING REMARKS & END OF WORKSHOP

CYBER SECURITY
FOR CRITICAL ASSETS | USA

www.cs4ca.com/usa
@QatalystGlobal
#CS4CA

Upcoming Events:

Industrial Internet of Things

CYBER SECURITY FOR CRITICAL ASSETS

CYBER SECURITY FOR CRITICAL MANUFACTURING MANUSEC

DACH iso
SECURING THE DACH REGION FROM CYBER THREATS

ItaliaSec
SECURING ITALY FROM CYBER THREATS

Diary Dates:

USA - CHICAGO
18th - 19th April 2018

CHINA - SHANGHAI
30th - 31st October 2018

EUROPE - MUNICH
6th - 7th November 2018

USA - HOUSTON
6th - 8th March 2018

MENA - DUBAI
9th -10th April 2018

EUROPE - LONDON
2nd - 3rd October 2018

EUROPE - MUNICH
7th - 8th February 2018

USA - CHICAGO
9th - 10th October 2018

GERMANY - FRANKFURT
20th - 21st March 2018

ITALY - ROME
15th - 16th May 2018

Media Partners:

Embedded COMPUTING DESIGN

ENTERPRISE MANAGEMENT 360°

StaySafeOnline.org
National Cyber Security Alliance

CrowdReviews
Buyers Guide Based On Client Reviews

infosecurity
STRATEGY /// INSIGHT /// TECHNIQUE

CDM CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

DIGITAL FORENSICS / MAGAZINE

InfoSec Conferences

peerlyst

iChainnel

CIOReview

ISA

ISF Information Security Forum