CCTX 4th Annual Collaboration Event - FEBRUARY 12, 2020

THEME “Give and Take”

7:30 – 8:30	**Registration and Breakfast**
8:30 – 08:40	**WELCOME, OPENING REMARKS, AGENDA REVIEW AND LOGISTICS** **Master of Ceremonies: Paul Martinello, Vice President Information Technology Services, Energy+ Inc.** **“Give and Take” event theme introduction based on the book and analysis by Adam Grant.**
8:40 – 09:25	**OPENING KEYNOTE – How to Keep Good Software from Behaving Badly** **Chris Hallenbeck, CISO for the Americas, TANIUM** As security teams mature, attackers are adapting their tradecraft to avoid detection. The most alarming shift, has been an increasing number of high-profile attacks on the software supply chain. While supplier risk management has matured, and is now part of the NIST Cybersecurity Framework, security best practices around the software supply chain remain more elusive. This gap provides a new and vulnerable target for attackers. In this presentation, Chris, using his past experience as a member of the US Department of Homeland Security's Computer Readiness Team will examine the emergence of software supply chain attacks and examples of associated high profile breaches; common challenges preventing organizations from securing the software supply chain and practical approaches any enterprise, using or developing software, can implement to mitigate such risks.
9:25 – 9:45	**“LION’S DEN” INFOMERCIAL COMPETITION - PART ONE WITH HOST: DANIEL TOBOK, CYTELLIGENCE**
9:45 – 10:15	**“GIVE & TAKE” SHARING PANEL: Examples of Sharing that are Making a Difference** **Moderator: Paul Martinello, Energy+ Inc.** **Panelists: Stephen Weston, VP Store Technology, Canadian Tire Corporation** **Dr. Ali Dehghantanha, Director, Cyber Science Lab, University of Guelph** **Daniel Tobok, Founder and CEO, Cytelligence Inc.**
10:15 -10:35	**“LION’S DEN” INFOMERCIAL COMPETITION - PART TWO WITH HOST: DANIEL TOBOK, CYTELLIGENCE**
10:35 – 11:05	**COFFEE BREAK & SPONSOR NETWORKING**

11:05 – 11:50 Workshop Group A	**Topic 1: Accelerate Response to Security Incidents through Orchestration and Automation** Karl Klaessig, Director of Product Marketing, Security Operations **Sponsored by: Service Now** Room 201B	**Topic 2: Scanning Isn't Enough: Measuring True Risk and Business Impact with Risk-Based Vulnerability Management Programs** Nathan Wenzler, Chief Security Strategist **Sponsored by: Tenable** Room 201C	**Topic 3: Security Considerations in Evolving Enterprise Networks** Dominique Gagnon, GM, Cybersecurity Wadah Ely Aalaoui, GM, Enterprise Networks & Cloud, Bell Canada **Sponsored by: Zscaler** Room 202A	**Topic 4: From Zero Trust to Zero Touch with Intelligent Security** Anthony Toric, Senior Director Technical Solutions **Sponsored by: BlackBerry** Room 202B
11:50 – 12:45	**LUNCH (SPONSORED BY BEYOND TRUST) & SPONSOR NETWORKING**			
12:45 – 12:50	**“LION’S DEN” INFOMERICIAL COMPETITION - WINNERS ANNOUNCED**			
12:50 –1:35	**NETWORKED – Strengthening Canadian Cybersecurity** Nikolas Badminton, Futurist The world has changed. Networks, connected devices and platforms have democratized technology and created a stateless, modern quicksand for life. That state is the new trillion-dollar business model and the new challenge for cybersecurity experts and their community. Nikolas will take us through our technological evolution and dive into our world where we need a bionic approach to cybersecurity - one that develops and harnesses behavioural, cognitive and network capital to create resiliency and anticipate the actions of bad actors.			
1:35 – 2:20 Workshop Group B	**Topic 1: Threat Intelligence - Capturing Cybercrime DNA** Keith Rayle, Senior Security Strategist **Sponsored by: Fortinet** Room 201B	**Topic 2: The Top 10 Immutable Security Facts of 2020** Ron Winward, Security Evangelist **Sponsored by: Cisco** Room 201C	**Topic 3: Achieving Zero-Time Threat Prevention Using Deep Learning** Brian Black, Senior Principle Architect & Technical Evangelist **Sponsored by: Deep Instinct** Room 202A	**Topic 4: A Blueprint: Managing Your Enterprise and Reducing Risk In Your Enterprise** Mark Holub, Security Solutions Architect **Sponsored by: Qualys** Room 202B

2:20 – 3:05 Workshop Group C	**Topic 1: Understanding Threats, Defence, and Applying Your Own Behaviour** Sam Smagala, Manager Cyber Security, MNP Joe Mauko, Regional Manager (Canada), Vectra AI **Sponsored by: MNP & Vectra** Room 201B	**Topic 2: Context is King: Creating Cybersecurity Awareness Campaigns That Matter** David Shipley, CEO **Sponsored by: Beauceron Security** Room 201C	**Topic 3: Quantum Update Panel** **Moderator: John M. Scott,** CEO, 2Keys **Panelists:** Michele Mosca, Co-founder of the Institute for Quantum Computing, University of Waterloo Bridget Walshe, Director of Cryptographic Security and Systems Development, Canadian Centre for Cyber Security Bruno Couillard, President and CEO, Crypto4A Room 202A	**Topic 4: Vulnerability Management and Patch Prioritization with Threat Intelligence** Maulik Limbachiya, Threat Intelligence Consultant, Team Lead **Sponsored by: Recorded Future** Room 202B
3:05 – 3:30	**COFFEE BREAK & SPONSOR NETWORKING**			
3:30 – 4:00	**CLOUD ATTACKS: HOW THEY WORK AND HOW TO STOP THEM** Sandy Bird, Co-founder and CTO, Sonrai Security AWS and Azure, like every advanced cloud platform, have configurations that can lead to catastrophic problems if not paying careful attention. One of the most dangerous allows innocuous identities usually granted to workloads or developers to escalate to admin-level privileges. Such attacks work because a sequence of seemingly unimportant missteps in the configuration in different parts of the public cloud allows the escalation to occur. During this session, we will cover the top 3 patterns to look for to prevent this and sequences SOC teams should be using to detect escalation.			
4:00 – 4:45	**R & D UPDATE FROM THE CANADIAN INSTITUTE FOR CYBERSECURITY** Dr. Ali Ghorbani, Director, Canadian Institute for CyberSecurity, Tier 1 Canada Research Chair, IBM Canada Faculty Fellow Some of the CIC's current areas of Research and Development include network security, systems security, security analysis and risk management, security visualization, security simulation – benchmark datasets, IoT-Big data security and privacy, critical infrastructure protection and people-centric cybersecurity. During this presentation, Dr. Ghorbani will briefly introduce the Institute, it's vision and mission and then walk us through some of the latest projects and plans underway.			

4:45 – 5:00	**CLOSING REMARKS, PASSPORT AWARDS**
5:00 - 6:00	**NETWORKING RECEPTION** **Note: Shuttle will depart Beanfield at approximately 5:15 pm and 6 pm.**

ABSTRACTS FOR WORKSHOPS

WORKSHOP GROUP A – 11:05 AM

Topic 1 – Room 201B – Accelerate Response to Security Incidents through Orchestration and Automation – Karl Klaessig

Given the dramatic annual increase in threats that analysts face, security analysts cannot continue to address incidents with manual processes, emails and spreadsheets. This process has and will always be a slippery slope and essentially hampers team's effectiveness. What's needed is a purpose-built security operations platform that delivers automated workflows with best-practice driven orchestrated response. This approach not only strengthens and accelerates incident response but scales your teams and grows their expertise, helping you to attract and retain the best talent. We will explore how such solutions can benefit your organization right out of the gate and contribute strongly to the organizations short and long term goals.

Topic 2 – Room 201C – Scanning Isn't Enough: Measuring True Risk and Business Impact with Risk-Based Vulnerability Management Programs – Nathan Wenzler

The threat landscape isn't just changing at blinding speeds, it's expanding into areas and devices that many never considered before. Vulnerability Management (VM) tools have been around for many years, but like any other security function, have to adapt to better account for the scope and scale of the devices security teams are protecting. In this discussion, we'll take a look at some of the challenges security teams are facing when trying to mitigate vulnerabilities as well as discuss how a risk-based approach to prioritization of vulnerabilities is a force multiplier versus traditional VM methodologies. We will review a data science-driven model for assigning risk, even as the threat landscape changes, and show how these approaches can be brought together to improve your security posture and encourage a better security culture in your organization.

Topic 3 – Room 202A – Considerations in Evolving Enterprise Networks – Dominique Gagnon, Wadah Ely Aalaoui

Organizations are in the midst of a digital evolution. A cornerstone to this journey is transforming the network to meet new challenges such as enabling the proliferation of devices on our networks, seamless access to cloud workloads, and our ever growing demand for real-time access to data. The network of tomorrow must not only accommodate these trends but also address the security challenges associated with this new paradigm. We will discuss how SD-WAN can help the enterprise achieve these new business objectives and what to consider when embedding security into this new architecture.

Topic 4 – Room 202B – From Zero Trust to Zero Touch with Intelligent Security – Anthony Toric

The future of mobile endpoint security requires AI and data-driven adaptive security beyond traditional policy management as well as a robust mobile threat defense. In this session, we'll explore how Intelligent Security leverages the power of adaptive security, continuous authentication and AI to enhance mobile endpoint security in zero trust environments with live demonstrations and use case discussions.

WORKSHOP GROUP B – 1:35 PM

Topic 1 – Room 201B – Threat Intelligence – Capturing Cybercrime DNA – Keith Rayle

In this presentation we will discuss methods of 'fingerprinting' attacks according to methodology frameworks, creating patterns that can be used for further analysis. We will then unpack how orchestrated attacks can be linked upwards to individuals and cybercrime rings, providing the potential to use current technologies to develop predictive attack insight. During this session you will learn about the current use of advanced technologies to analyze malware; attack frameworks and patterns they can reveal and cybercriminal countering methods.

Topic 2 – Room 201C – The Top 10 Immutable Security Facts of 2020 - Ron Winward

Do you know what will disrupt established application and infrastructure security practices this year? Are you sure what questions you should be asking about your threat posture and potential vulnerabilities? In this session from Cisco, Radware's Security Evangelist for North America will guide you through the 10 security facts that will impact your business and IT environment in 2020. From the public cloud to 5G to WAF and botnets, if you've ever asked how to protect APIs and cloud native applications running in dynamic, encrypted service meshes…this session is for you.

Topic 3 – Room 202A – Achieving Zero-Time Threat Prevention Using Deep Learning – Brian Black

Machine learning is a big step forward in combatting cyberattacks but is still no silver bullet. Many traditional cybersecurity solutions available today are causing huge operational challenges as they are inadequately defending against today's complex and sophisticated threats. It has become increasingly evident that the solutions used to protect your company and its data need to work pre-emptively to prevent attacks, rather than just detect and respond to them. Fortunately, AI technologies are advancing, and deep learning is proving to be the most effective cybersecurity solution, resulting in unmatched prevention rates with proven lowest false positive rates. As you evaluate new technologies for your organization, understand the differences and benefits of Artificial Intelligence, Machine Learning and Deep Learning.

Topic 4 – A Blueprint: Managing Your Enterprise and Reducing Risk in your Enterprise – Mark Holub

A blueprint for your environment. This session will walk you through key concepts of how to effectively detect, prioritize and remediate vulnerability and compliance issues to infrastructure in your environment. This talk covers traditional and new data methodologies organizations can use to extract key information from systems that are otherwise difficult or impossible to assess. Learn how to achieve this crucial protection by eliminating blind spots and prevent exposure to cyber-attacks across all infrastructure.

WORKSHOP GROUP C – 2:20 PM

Topic 1 – Room 201B – Understanding Threats, Defence and Applying Your Own Behaviour – Sam Smagala, Joe Mauko

Behaviour. Often questioned and often misunderstood, we break the cybersecurity industry down into the different concepts that make each wheel turn.

- Offering processes to effectively interpret and implement threat intelligence
- Discussion on both strategic ideology and tactical actions in context to real world threats and incidents are presented
- Latest trends of attacks researched by Vectra, and what you can do about them.

We ultimately prove that understanding the behaviour of the threat is your best chance to defend against it.

Topic 2 – Room 201C – Context is King: Creating Cybersecurity Awareness Campaigns that Matter – David Shipley

Far too often if an organization has a cybersecurity awareness campaign, it's a check-the-box, compliance driven effort using generic out-of-the-box context talking about the same security highlights that employees have heard countless times. But a truly effective awareness campaign is one that ultimately results in behaviour change at the individual and organizational levels. During this presentation, we will talk about how to create truly compelling and engaging educational experiences for users and provide practical examples from a number of firms and industries. We'll guide participants through the creation of a high-level awareness strategy leveraging a new framework for cybersecurity awareness.

Topic 3 – Room 202A – Quantum Update Panel – Michele Mosca, Bridget Walshe, Bruno Couillard, John M. Scott

This panel will provide us an update on some of the latest academic, commercial and applied Quantum activities underway in Canada. Panelists will discuss bridging strategies between our current pre-quantum to post quantum world and the steps we need to be planning now. Learn from industry experts and experienced quantum practitioners whether we should be worried or not with the coming quantum wave.

Topic 4 – Room 202B – Vulnerability Management and Patch Prioritization with Threat Intelligence – Maulik Limbachiya

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. Threat Intelligence applies across all security use cases (third party risk, brand protection, vulnerability management, security operations, geopolitical & physical security). This workshop will focus on vulnerability management; with thousands of new vulnerabilities disclosed each year, companies can't patch everything and unpatched vulnerabilities leave openings for attackers to strike. It is an inherently cumbersome and costly process. In this session, we will introduce Recorded Future's mission and how the Recorded Future platform gathers vulnerability data, processing it into a Risk Score in real-time to streamline the patch prioritization process. We'll share case studies on how adopting a risk-based approach to vulnerability management allows security teams to patch what matters – prioritize effectively and securely mitigate risk.