Welcome to the 2017 Atlantic Security Conference.

The Support this year from our community has been fantastic and we have really started to gain some international attention. The call for papers was met with overwhelming response and we really had a very difficult time selecting the best content to provide you a stellar conference experience. We are excited to hear from the local members of our community and from those that have travelled from afar.

The Atlantic Security Conference continues to grow in both attendance and sponsorship. Some of our sponsors have been here since the very beginning supporting Atlantic Canada whether it be AtlSecCon sponsorship or presenting at a HASK meeting. We ask that you please take a moment to visit with them because without their support we could not make this happen.

Please enjoy the presentations, visit with some old friends and make some new ones. We have some great prizes including a grand prize draw and we wish you the very best conference experience.

Thank you,

~Travis Barlow, Andrew Kozma, Steve Quinn, Darryl Macleod and Nick Gyorfi. ~
At GoSecure, our reason for being is to protect your information assets and allow you to focus on your business. As a go to information security partner, we offer a wide range of specialized services allowing increased security operations ROI, cutting-edge security testing for IT and facilitate security to be integrated in new or existing software and hardware systems. Strengthened by eleven years of experience dedicated exclusively to information security, our team has had to deal with a wide gamut of security breaches and threats and stands today as a group of leaders in technologically complex security mandates in the industry. We continue to invest in advanced security research with our private and public partners. For us, security only makes sense when it serves the best interest of your organization and helps you reach your goals. You can count on us as your long-term partner in assessing and developing all the elements of your technical security for the threats of today and tomorrow.
<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 - rm 200</th>
<th>Track 2 - rm 301</th>
<th>Track 3 - rm 304</th>
<th>Track 4 - rm 305</th>
<th>Track 5 - rm 306</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 AM</td>
<td>Registration</td>
<td>Opening Remarks - rm 200</td>
<td>Opening Keynote - Jessica Barker - rm 200</td>
<td>Morning Break</td>
<td></td>
</tr>
<tr>
<td>9:00 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:30 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:45 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Getting Off the Back Foot – Employing</td>
<td>Breaking Electronic Door Locks Like You’re On CSI: Cyber – Colin O’Flynn</td>
<td>No Phishing Beyond This Point – Grant Boudreau</td>
<td>Dark Skies: Trying to Navigate Data</td>
<td>The Enemy Within: Detecting and Mitigating Insider Threats – Daniel Cybulskie</td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Lunch - rm 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Measuring Adversarial Behavior in</td>
<td>Software defined murder – Julien Savoie</td>
<td>Lessons Learned Hunting IoT Malware – Olivier Bilodeau</td>
<td>Evolve or you will be compromised ... or you are already! – Xavier Trépanier</td>
<td>Chris Vernon - To Shamoon and Back!</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>Cyberattacks – Aunshul Rege</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:45 PM</td>
<td>Afternoon Break</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00 PM</td>
<td>Is Your Security Team Set up To Fail? –</td>
<td>Feeding the Machine – Alexander Keddy</td>
<td>Malware Research Using OSINT and Open Source Tools – Raul Alvarez</td>
<td>Security by default: Preventing application vulnerabilities at the source – Philippe Arteau</td>
<td>TBD</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>Andrew Hay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 PM</td>
<td>Closing Keynote – Liam Randall – rm 200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:00 PM</td>
<td>AtlSecCon Social Mixer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Registration:
- Opening Remarks - rm 200
- Opening Keynote - Jessica Barker - rm 200
- Morning Break
- Lunch - rm 100
- Afternoon Break
- Closing Keynote - Liam Randall - rm 200
- AtlSecCon Social Mixer
- Speakers Dinner - Murphy’s (Ticket Required)
We’re Canada’s dynamic communications and media company. We make sure you stay inspired, informed and in touch, with our advanced networks, powerhouse media brands and technologically advanced communications services.
# Day 2 Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 - rm 200</th>
<th>Track 2 - rm 301</th>
<th>Track 3 - rm 304</th>
<th>Track 4 - rm 305</th>
<th>Track 5 - rm 306</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:15 AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Morning Break</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>WebSockets Are Gonna Change the Pen Test World - Adrien de Beaupre</td>
<td>Using social engineering to improve dev/secops - Kevin Baun</td>
<td>Advanced Persistent Bots (APBs) and How to Mitigate Risk - Stephen Singam</td>
<td>Building your Personal Threat Model - Geoffrey Vaughan</td>
<td>Social Threats – Social Media as an Attack vector for Cyber Threats - Stewart Cawthray</td>
</tr>
<tr>
<td>11:45 AM</td>
<td></td>
<td></td>
<td></td>
<td>Lunch - rm 100</td>
<td></td>
</tr>
<tr>
<td>2:00 PM</td>
<td>Hacking the Internet of Dongs - RenderMan &amp; Murdoch Monkey</td>
<td>A Cocktail Recipe for Improving Canadian Cybersecurity - Michael Joyce</td>
<td>TBD</td>
<td>Come to the Dark Side, we have cookies - Marc-Andre Belanger</td>
<td>TBD</td>
</tr>
<tr>
<td>3:00 PM</td>
<td>How I Learned To Stop Worrying And Love The Cloud - Kellman Meghu</td>
<td>Security Modelling Fundamentals Panel</td>
<td>Improve Your IT Security - Serge Nault</td>
<td>Identity Assurance, the evolution of MFA - James Mandelbaum</td>
<td>TBD</td>
</tr>
<tr>
<td>3:45 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00 PM</td>
<td></td>
<td></td>
<td>Closing Keynote - TBD - rm 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 PM</td>
<td>Closing Remarks and Prize Draws - rm 200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7:00 PM</td>
<td></td>
<td></td>
<td>After Party - Lower Deck Tap Room (Bring Badge)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GOLD SPONSORS

Pulse Secure
SentinelOne
Cisco
OnX
VMware
Dr Jessica Barker

Dr Jessica Barker specialises in the human side of cybersecurity. Running her own consultancy business, Jessica is engaged by organisations of all sizes, from large multinationals to SMEs across the defence, financial, health, and retail sectors. She works with organisations to help them keep their information safe while getting the most out of it. Her particular specialisms cover governance, strategy and policy, risk and resilience, and learning and development.

Jessica is keen to make cybersecurity a more engaging and accessible subject to all, and as such makes regular media appearances to discuss current cybersecurity issues. Jessica’s consultancy experience, technical knowledge and sociology background equip her with unique insight, and she has a talent for translating technical messages to a non-technical audience.

Jessica regularly delivers thought-provoking and engaging presentations at corporate events as well as practitioner and academic conferences. Known for her ability to engage everyone from senior executives to ethical hackers and creative workers, she brings energy, enthusiasm and fun to cybersecurity.

Jessica runs the website www.cyber.uk, dedicated to cyber security news, information and guidance for anyone interested in cyber security, and is a co-founder of the Risk Avengers.

Liam Randall

With a career spanning 20 years, Liam is a passionate supporter and contributor to many open source communities. An early supporter of the Bro project, he has trained 1000’s of students in the principles of Network Security Monitoring and large scale network monitoring. As a serial entrepreneur he has founded multiple network security related startups, including Critical Stack, which was recently acquired by Capital One Bank.

While still leading Critical Stack he is serving as a board member at the security startup accelerator Hack Secure advising seed stage startups where he continues to support open source security with investments in companies such as Kolide, the OS Query company. Find him online at www.LiamRandall.com.
Jen Andre
Jen is the founder & CEO of Komand, the fastest way to automate your time-intensive security processes. Before Komand, she co-founded Threat Stack, a pioneering cloud security monitoring companies and serves on its board of directors.

Jen has spent her career in security operations and product – starting off in the SOC as an analyst and later working as a researcher and developer at security companies Mandiant and Symantec.

A recognized speaker in the security and engineering world, she also supports security innovation as a board member of the hacksecure.org cybersecurity investment syndicate.
Raul Alvarez
Raul Alvarez joined Fortinet in 2004, and is currently working as a Senior Security Researcher/AV Team Lead. I am also one of the Lead Trainer responsible for training the junior AV/IPS analysts in malware analysis and reverse engineering.

I have presented in different conferences like BSidesVancouver, BSidesCapeBreton, OAS-First, BSidesOttawa, SecTor, DefCamp, BCAware, AtlSecCon, BSidesCalgary, and TakeDownCon. I am also a regular contributor to the Fortinet blog and also in the Virus Bulletin publication, where I have published 22 articles.

Malware Research Using OSINT and Open Source Tools: Empowering Everyone
The mystic world of malware research is clouded by fear of infecting oneself. It is never far from the truth. The good news is, there are lots of information lying around in the web to help us out in our quest for information about a specific malware. We just have to know where to look.
In this presentation, we are going to cover some available source where we can get intel on a given malware. We are also going to look into some free downloadable system and tools to do your own research.

Philippe Arteau
Philippe is a security researcher working for GoSecure. He is the author of the widely-used Java static analysis tool Find Security Bugs. He is also working on a static analysis tool for .NET called Security Guard. He has also built many plugins for Burp and ZAP proxy tools: Retire.js, Reissue Request Scripter and others.

He has discovered many vulnerabilities in popular software including Google Chrome, Dropbox, Paypal, RunKeeper and Jira.

Security by default: Preventing application vulnerabilities at the source
It is common to hear that application security has not evolved recently. We can hear “the vulnerabilities of the 2000s are still actual” or “Security is a lost battle”. These pessimistic thoughts are not representative of the reality. In this presentation, we will demonstrate that the use of modern framework can eradicate complete classes of vulnerabilities. Choice of technology is key when creating or maintaining a Web application. Examples from popular frameworks of different languages will be given to showcase the significant advances.
While the complexity of applications tend to increase over time, the tools available to developers and analysts have improved and became much more efficient. As examples, two demonstrations of code analysis tools will be presented to the audience.
This presentation is intended for both optimists and nihilists in the field.
SPEAKERS

Tom Bain
Tom Bain leads the strategic go-to-market, Marketing research and AR efforts at CounterTack with over 14+ years of experience with leading IT Security organizations. He also serves as a key security evangelist for CounterTack.

Bain’s strategic experience spans endpoint, database, network and application security, security services, security training and cyber-security. Prior to CounterTack, he spent time with Security Innovation, Q1 Labs (an IBM Company) and Application Security, Inc. (a Trustwave company), and has worked with leading security brands including Wave Systems, Sophos, CA, Red Hat and AffirmTrust.

Bain has been an industry speaker at conferences including Hacker Halted, Global CISO Summit, SecureWorld Expos, OWASP, Strata + Hadoop World, GoSec, Rocky Mountain Information Security Conference, Terrapin Cyber Security Conference, America’s Growth Capital, The Montgomery Summit, ASCS, Camp IT and Boston Security Conference. He earned an MS degree in International Relations and Public Affairs from UMASS and holds a BA in Communications from Rhode Island College.

Security Modelling Fundamentals: Should Security Teams Model a SOC Around Threats or Just Build Layers?
What governs how a security analyst prioritizes the layers within an organization’s infrastructure? In other words, starting from ground zero, how does an analyst know where to protect the business from the outset? Does this start fundamentally with securely developed applications, deploying a firewall, or focusing on device security? And what do you do outside the firewall? Do you prioritize where you know don’t have visibility like within Office 365, or on distributed devices, or do you prioritize based on threats faced historically? What’s impacting organizations are multi-layered, multi-phase, targeted threats that require multiple detection engines typically.

Enterprise security teams aren’t starting from ground-zero though – they are consistently fighting fires, and regularly looking for better, faster and more robust technologies to integrate to better counter the threats they face, knowing that attackers are going to flock to where users are to exploit them.

Fundamentally, the two big questions this panel hopes to address and gain some much-needed expert perspective on:
1. Today – should security teams take an inside-out approach, or an outside-in approach to building their security operations center in addition to their overall security program?
2. However, based on today’s threat landscape, how would you recommend a security team model a SOC and an approach to security?

Panel participants:
Tom Bain – moderator
Travis Barlow – GoSecure

Kevin Baun
By day Kevin masquerades as a mild-mannered Network Defence SME (Sr. Systems Engineer). By night, however, he whiles away the hours breaking other people’s code. Because schadenfreude is fun when nobody is getting hurt! Kevin has nearly 20 years of experience in software development and information security. He also has a M.Sc. in IS Security as well as more than a dozen industry certifications, including: CISSP, CEH, and CCISO. The fastest way to his heart is through the rib cage and the fastest way to earn his scorn is to log passwords in plaintext on a production system.

Hacking the handlers: Using social engineering to improve dev/secops
Building an effective team can be a challenge in any environment. This challenge has been enhanced by the emergence of multifaceted operations teams such as development operations (devops) and security operations (secops). In this talk we will examine technical and interpersonal hurdles to getting what you need from management and what you want from your engineers. Each of these problem domains will be decomposed and techniques will be presented to address them. Special attention is given to the role of the CISO. The rapidly evolving role of the CISO is frequently found in the nebulous grey space between operations, engineering, and management. This presents some unique challenges, which we will discuss and offer potential solutions for.

Marc-Andre Belanger
Marc-Andre Belanger is acting as a Senior Risk Officer within the banking industry. Previously a speaker at AtlSecCon and Quebec’s Hackfest, Marc-Andre concentrate his personal research toward understanding, and evangelizing, how information security is no different than the other fields of security that protect the day to day of our loved ones. He has been, fulltime, part of the Information Security Workforce since the Y2K gold rush. Marc-Andre has recently started working toward preparing trainings for the next generations of Jedis that will defend our organisations: today’s teens…

Come to the Dark Side, we have cookies – An Introduction to Cyber Security
How did we managed to go from Information System Security to Cyber Security… What is Cyberspace anyway.. Is my server farm part of the Cyberspace ? How such a large landscape of devices not even under our control that includes refrigerators, watches, cars and even medical equipment became a Threat to my Bank or Insurance cie. How come our customers, buying goods from some lazy manufacturers, are putting themselves at risk and us at the same time… Considering the fact that the landscape changes every minutes… we will not go through a typical introduction to Cyber Security (for that Google has over 800,000 entries for that). We will take the path of the Dark Side and walk our way on an attacker perspective. A bit of Threat Modeling can go a long way into understanding the patterns that put your organisation at risk… even if the risk changes on a daily basis.

Charles Bernard
Charles has managed to combine his passions for aircraft and computers into an unlikely career. After a brief stint as a web developer, he moved to Ottawa and earned a B.Eng. in Aerospace Engineering (Electronics & Systems) from Carleton University. He is currently working part-time towards a M.A.Sc. in Computer Engineering at the Royal Military College of Canada, where he is a member of the Computer Security Laboratory.

To fund his motorcycle purchases and beer brewing gambits, Charles spends his days as a System Security Engineering Officer in the materiel acquisition arm of the Department of National Defence, providing security advice to the aircraft acquisition projects and the fleet maintenance offices of the Royal Canadian Air Force.

Make Cyber Space Again: Applying Network Security Concepts to Aerospace Systems
While the information security industry has a relatively good handle on securing enterprise-style networks of servers, laptops, smartphones and tablets, the concept of security as it applies to embedded systems can be more…nebulous. Things get even more interesting when a hodge-podge of embedded systems are connected together, live in an austere environment, and must be no-fail. Now do it with technology from the 70s. Using aircraft systems as an example, this talk is designed to introduce the audience to the security problem within the aerospace systems context, and to show how to begin breaking it down into manageable chunks. A few of the
frameworks and guidelines currently in use will also be introduced, as well the types of skillsets that are often most valuable in this domain.
While some technical concepts will be discussed, this talk is geared to be accessible to new practitioners in the community, and by managers and executives with a modest technical background. We won’t save the world or open a bunch of CVEs as a result of this talk, but we’ll hopefully walk away with a basic understanding of this new and exciting problem. and maybe share a war story or two along the way.

Olivier Bilodeau

Olivier Bilodeau is leading the Cybersecurity Research team at GoSecure. With more than 10 years of infosec experience, Olivier managed large networks and server farms, wrote open source network access control software and recently worked as a Malware Researcher.

Passionate communicator, Olivier has spoken at several conferences like BlackHat Europe, Defcon, SecTor, Derbycon and many more. Invested in his community, he co-organizes MontréHack—a monthly workshop focused on applied information security through capture-the-flag challenges—, he is in charge of NorthSec’s training sessions and is hosting NorthSec’s Hacker Jeopardy.

His primary research interests include reverse-engineering tools, Linux and/or embedded malware and honeypots. To relax, he likes to participate in information security capture-the-flag competitions, work on various open-source projects and brew his own beer.

Lessons Learned Hunting IoT Malware

Permeating the entire spectrum of computing devices, malware can be found anywhere code is executed. Embedded devices, of which many are a part of the Internet of Things (IoT), are no exception. With their proliferation, a new strain of malware and tactics have emerged.

This presentation will discuss our lessons learned from reverse-engineering and hunting these threats. During our session, we will explain the difficulty in collecting malware samples and why operating honeypots is an absolute requirement. We will study some honeypot designs and will propose an IoT honeypot architecture comprising several components like full packet capture, a man-in-the-middle framework and an emulator. Additionally, reverse-engineering problems and practical solutions specific to embedded systems will be demonstrated. Finally, we will explore three real-world cases of embedded malware.

First, Linux/Moose, a stealthy botnet who monetizes its activities by selling fraudulent followers on Instagram, Twitter, YouTube and other social networks. Second, a singular ELF binary of the MIPS architecture which serves as a dropper. Third, LizardSquad's LizardStresser DDoS malware known as Linux/Gafgyt. Attendees will leave this session better equipped to hunt this next generation of malware using primarily open source tools.

Grant Boudreau

Grant Boudreau is an IT professional in Nova Scotia's public education sector. He holds a bachelor degree in Information Technology – Network Management from Cape Breton University, is an OSCP and OSWP graduate from Offensive Security, and has several other industry certifications.

No Phishing Beyond This Point

This talk will dive into the world of phishing. Malware and ransomware campaigns have been rampant this year with many organizations suffering due to this. I’ll be going through the five stages of grief and loss that many users are faced with once they realized they’ve been duped. I’ll then talk about what we, as security people, need to do in order to protect our organizations. There is no simple answer and no simple blinky box that can stop phishing. However, there are many ways that we can make users be more aware and be more vigilant with their daily computer use, which will in turn protect our organizations.
Stewart Cawthray
Stewart leads product management for enterprise security solutions at Rogers. With a background in security architecture, incident response and ethical hacking Stewart brings his real world experience to the solutions he makes available to Rogers enterprise customers. He is responsible for setting the strategy and driving solution development and partnerships to bring industry leading and data sovereign secure solutions to the Canadian enterprise market. Prior to Rogers Stewart held senior positions with IBM and HP security service organizations in addition to experience protecting one of Canada’s largest banks. Stewart is a 4-time recipient of Microsoft’s Most Valuable Partner for Enterprise Security.

Stewart holds several industry certifications including CISSP, CISM, CRISC, CEH and ITIL V3 Expert, in addition to vendor certifications from Microsoft and IBM.

Social Threats – Social Media as an Attack vector for Cyber Threats
Social media has become a core business & communications platform and every industry now faces a unique set of risks on social, many of which have put organizations in the press or at the center of controversy. Whether it’s blocking targeted phishing attacks, protecting corporate accounts from compromise, fighting fraud or defending against scams and impersonating accounts, social media security is critical for modern business success. Social media is an evolving attack vector which many organizations are blind to. This session will review the types of threats and why organizations should be concerned about them.

Daniel Cybulskie
Daniel Cybulskie has been in the information security industry for over a decade. During his career, he has been sought after as a dynamic, and highly educated, speaker on various Infosec subjects. His deep knowledge of information security principles and trends has led to speaking engagements in Silicon Valley, Interop Las Vegas, and all across Canada. For the past three years he has been focused on helping organizations protect themselves from insider threats against their most rapidly growing data repositories.

The Enemy Within: Detecting And Mitigating Insider Threats
Ransomware is both scourge and savior. While it’s not typically considered an insider threat, it acts from the inside, using insider identities, encrypting files these insiders have access to on endpoints and file shares. Learn how organizations are using ransomware to identify and confront vulnerabilities that expose them to rogue employees, abusive administrators, and hackers.

Adrien De Beaupre
Adrien de Beaupre is a certified SANS instructor and works as an independent penetration tester in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response, and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). Adrien is actively involved with the information security community, and organizes the #BSidesOttawa conference. When not geeking out and breaking stuff he can be found with his family, or at the dojo.

Websockets Are Gonna Change The Pen Test World
Modern web applications more and more make use of WebSockets or HTTP/2 to deliver real time and richer content
to their clients. As penetration testers, we not only have to be aware of these newer protocols, we have to adapt to testing them, and the unique and fascinating attack surface they provide. Unfortunately the tools we typically use have not adapted to the new reality quite yet. Tune in to hear advanced web application penetration techniques for HTTP/2 and WebSockets from one of the authors who literally wrote and deliver the Advanced WebApp Penetration Testing SANS course on the topic, SEC642.

**Evan D’entremont**
Evan d’Entremont is a Senior Software Engineer and HASKer who spends his time solving complex problems. He is currently developing secure industrial control solutions, and his background includes web application development and securing legacy applications.

**Vaccinating The Internet Of Targets**
The “internet of things” is an important consideration for any organization’s infosec plan. As professionals we need to ensure the proliferation of smart devices can be managed in a safe and controlled way, and answer the looming questions of liability when things go wrong. Just within the last year, there have been several record-breaking 1Tbps DDOS attacks because only a few default credentials were leaked; we will explore how real world incidents like this could have been mitigated by herd immunity, and virtually prevented with simple programming. We’ll also address the standards required of industrial telematics, and why “Bank Grade” isn’t good enough.

**Olivia Lucca Fraser**
Lucca is a cybersecurity researcher and developer, living in the Halifax area. She is a graduate student in the Dalhousie Computer Science Department, in the NIMS network security lab, and works as a researcher and software engineer at Tenable Network Security.

**Return-Oriented Programme Evolution With Roper**
ROPER is a genetic ROP-chain compiler that I have designed and developed. It compiles ROP-chains, by creating a miniature ecosystem in which ROP-chains evolve. In my talk, I will introduce the tool, explain how Return-Oriented Programing (ROP) works, and how genetic programming can be used in return-oriented exploit development. I will give a live demo, showing how ROPER can be used to develop payloads — including payloads that exhibit learned or evolved behaviour — unlikely to be developed by humans.

Definitions:
1. Return-Oriented Programming is an exploit technique that, instead of writing malicious code (“shellcode”) into a process’ executable memory, collages together a series of “gadgets” that already subside in executable memory. This is useful when the process has no memory segments that are flagged as both executable and writeable (W^X/DEP).

2. Genetic programming is the implementation of natural selection in code. A population of random programmes (in this case, ROP-chains) is generated. A fitness function is then defined, and used to rank the results of their execution. Fitter programmes are made more likely to breed. Mutation operators are applied to the offspring, and the next generation of the process begins. This carries on until the desired outcome is obtained.
Michael Joyce
Michael Joyce is the Knowledge Mobilisation Coordinator at the Smart Cybersecurity Network (SERENE-RISC). He is responsible for SERENE-RISCs online knowledge sharing platform, the quarterly cybersecurity digest and other knowledge mobilisation efforts.

A Cocktail Recipe For Improving Canadian Cybersecurity

The Smart Cybersecurity Network (SERENE-RISC) is a federally funded, not-for-profit knowledge mobilization network created to improve the general public’s awareness of cybersecurity risks and to empower all to reduce those risks through knowledge. This presentation will show how SERENE-RISC mobilizes knowledge, is improving Canadian Cybersecurity, how these efforts can increase profitability for Canadian Cybersecurity companies and how to mix a great drink to greet spring.

Alexander Keddy
Alexander is an IT professional holding a Master’s degree in Computer Science from Dalhousie University. Over his academic career, he has worked on projects ranging from machine learning on cattle genomes to applying GIS to visualize distributions of pathogens. He currently uses the skills he developed in academia to lead development at GoSecure Atlantic, with a special interest in R&D applying machine learning to cyber security. When not attempting to make his laptop as smart as his robot-like coworkers, Alex can be found driving motorcycles throughout the province (when the seasons are not emulating the planet Hoth).

Feeding the Machine
In the modern world, we are becoming inundated with the sheer range of abilities computers possess. More and more we fear the rise of machines hell bent on the termination of us humans in a James Cameron-eske apocalypse. In this growing landscape of metal, carnage and bot attacks, we are forced to ask ourselves the same questions as a failing band of resistance; can the machines also be our salvation? Certainly, many of the worlds top researchers at locations such as Google, Facebook and IBM think so. These are the frontrunners in commercial machine learning projects, hoping to secure our futures by applying machine intelligence to everything from search queries to diagnosing medical issues.

In this talk, aimed at cyber security researchers and practitioners alike, we will demonstrate simple techniques to transform human readable network alert data into food for our prodigious machine savours (and nothing is more delicious to them than data). As many alert systems today were designed to be interpreted by humans and not a machine, processing is required to convert raw sentences to bits, or to draw out context from key information to a categorical format. From this machine edible format, the power of this information can be assessed through statistical analysis to find unexpected behaviour and predict malicious players.

Here, techniques such as text parsing, vectorization, and numeric feature considerations will be addressed. Taking this one step further, we will practically apply this machine-readable data to intelligent models to make predictions on the safety of future events. While these models are far cries from those used at placed like Google, they do provide the ground work for future learning on the subject.
Paul Kitor
Paul Kitor, CISSP is a Senior Solution Architect focused on Fortify technologies within the Enterprise Security Products business unit at HP. In this role, Mr. Kitor acts as the primary technical advisor to develop and position a broad range of Application Security solutions with customers. In his responsibilities, Paul provides technical leadership and technical depth concerning HP Fortify solutions. He works closely with customers and partners in assisting them meet their strategic Application Security initiatives and also provides thought leadership and insight regarding the ever changing global threat landscape. He possesses 20+ years of Information Security experience in the areas of Application Architecture, Java/C/C++ Development, Agile SDLC, and Application Security. Prior to joining HP Canada, Paul worked as a Solution Architect at Oracle, BEA Systems, and Borland Software. He also lead Java development teams at Airmiles.ca and Points.com.

The True State of Security in DevOps and Expert Advice on How to Bridge the Gap
Rapid application delivery is dramatically transforming how software is created and delivered, pushing the limits on the speed and innovation required of development teams. If you are wondering how this change in culture, process and operations affects Application Security, you are not alone.
HPE research reveals that while fully mature DevOps programs are rare, well over half of organizations surveyed are implementing key DevOps methodologies such as Automated Testing and Frequent Delivery. And while most agree that this presents an opportunity to integrate Application Security methodologies – that is not the reality. In fact, only 20% of organizations cite Static Testing during the coding process. HPE’s Paul Kitor will discuss practical advice that DevOps and Application Security Teams, of any maturity level, can take away from these findings and begin to build a roadmap for building security into every step of the SDLC, from coding through production.

Aamir Lakhani
Aamir Lakhani is a leading senior security strategist. He is responsible for providing IT security solutions to major enterprises and government organizations.
Mr. Lakhani was a technical lead for CryptoWall 3 research paper that was nominated for paper of the year 2016 by Virus Bulletin. He is a forensics and cyber-criminal investigator. He is a leading cyber security researcher. He works with law enforcement, and leading organizations to investigate cybercrime, malware, and breaches.

Inside The Threat Actor Studio
After being hired to investigate a simple e-commerce crime by a city attorney and a local police department, my investigation led me to uncover a ring of cyber criminals selling online accounts, credit cards, and gift cards. The criminals breached health care systems and other organizations located around the globe. My investigations led me thru unknowing accomplices, mules and patsies, to an organization with members in 3 different continents conducting a criminal activities targeting a major city. This talk will examine how our team investigated the crime, the political and legal hurdles we had to deal with, the methods used by criminals to profit, and the technical attacks they used. This talk will help you gain a understanding of a cyber-crime forensics investigation, and help you identify methods to protect your organizations against cyber criminals.
Dave Lewis

Dave Lewis has over 20 years industry experience. He has extensive experience in IT operations and management. Currently, Dave is a global security advocate for Akamai Technologies. He is the founder of the security site Liquidmatrix Security Digest and co-host of the Liquidmatrix podcast. Dave also serves on the (ISC)2 Board of Directors.

Prior to his current role, Dave worked in the finance, healthcare, entertainment, manufacturing and critical infrastructure verticals. He has worked for a defense contractor as a security consultant to clients such as the FBI, US Navy, Social Security Administration, US Postal Service and the US Department of Defense to name a few.

When not at work Dave can be found spending time with his family, playing bass guitar and polishing his “brick of enlightenment”.

Barbarians At The Gate(Way)

This talk will examine the tools, methods and data behind the DDoS and web attacks that are prevalent in the news headlines. Using information collected, I will demonstrate what the attackers are using to cause their mischief and mayhem and examine the timeline and progression of attackers as they move from the historical page defacers to the motivated attacker. I will look at the motivations and rationale that they have and try to share some sort of understanding as to what patterns to be aware of for their own protection.

Rafal Los

Rafal Los brings a blend of pragmatism and thought leadership in his approach to enterprise information security. As managing director, solutions research and development at Optiv, Los helps organizations build mature, defensible and operationally efficient security programs. Leveraging over 15 years of technical, consulting and management skills his team researches, develops and delivers program strategy frameworks, maturity models, and provides operational guidance from across industry verticals and varying maturity levels.

Getting Off the Back Foot – Employing Active Defence

Security, at the program level, has largely been stagnant and predictable for a very long time. This talk will provide a realistic definition of Active Defence then discuss a framework and provide real-world examples of how its principles are literally changing how security mobilizes in progressive organizations. It’s unrealistic, and illegal, for security teams to go on the offensive, but that doesn’t mean sitting around waiting for the red lights to blink. We will explore strategies for more intelligence defensive capabilities through actionable threat intelligence, focused incident response and management, and engineering/architecture. Being on a blue team doesn’t mean being a punching bag and with the appropriate blend of intelligence, process and action enterprise security can be more. The content for this talk is derived from 1,000+ hours of research and based off of the Threat Intelligence Blueprint framework, which is an outcome-oriented and capabilities driven model for more effective enterprise security.

James Mandelbaum

James is the Identity Architect for the Americas with RSA Security and has worked with some of the largest companies pre and post breach. He has provided guidance to organizations on methods to build out a secure access and Identity plan during these times of consistently evolving security landscapes. James is a standing member of the High Tech Criminal Investigations Association and volunteers with police investigations in high tech crimes.
**Identity Assurance, the evolution of MFA**

The natural evolution of Cloud Based Applications as well as Mobility has changed the game in Authentication. Come learn how Identity Assurance is the solution that aligns with how we are removing the traditional perimeters.

**Nick Manikas**

Nick Manikas has been in the IT Industry for close to two decades. Prior to his current position at Pulse Secure, Nick has held positions at Cisco Systems as Sr. Network Engineer and more recently as Sr. Security SE at TELUS. As a senior member of the SE team at Pulse Secure, Nick consults with clients to develop Secure Access solutions that address the Enterprise as well as the SMB. Throughout his career, Nick has gained exposure to a vast array of technologies and organizations through multiple perspectives. This diversity of experience has allowed him to develop a unique mix of technical and business acumen that is leveraged in the design and delivery of projects from the simple to the complex.

**Anna Manley**

Anna Manley is an internet and privacy lawyer based in Sydney, NS. She is the principal of Manley Law Inc. and founder of Advocate Cognitive Technologies Inc. Anna advises companies and individuals on all things law and tech related.

**Criminalizing Security: Outlawing Cryptography in a “Post-Privacy” World**

Encryption has gone from legitimate and ubiquitous security measure to villain du jour. Governments around the world have taken steps to curb encryption measures to give themselves a key to the backdoor and there is every indication more stringent regulation of encryption is coming down the pipe. How far have governments gone to criminalize encryption? What encryption methods are legal? What is the state of the law in Canada? How does C-51 impact encryption in Canada?

Let’s explore these questions as well as where we’re headed in criminalizing encryption.

**Isaiah Mcgowan**

Isaiah is a Senior Risk Consultant with RiskLens. He is a former network security engineer, penetration tester, and IT auditor who now works with the largest organizations in the world to apply quantitative risk models to problems in the security realm. Isaiah is one of the foremost domain specialists in FAIR (Factor Analysis of Information Risk) and has trained hundreds of security practitioners on the FAIR methodology. He currently holds the OSCP and OpenFAIR certifications.

**Why risk is our bridge between security and business worlds**

There is a need to make well-informed security decisions that align with business expectations. It’s always been there; we’re just more explicit about it today. This session focuses on a core tenant that bridges the gap in communication between security and business focuses: risk. Our most familiar approaches to risk measurement are failing us. What else is out there? And what are the implications for various security disciplines? We will dive into these topics and flesh out a way forward that aligns our security concerns with their business needs.
SPEAKERS

Victoria McIntosh
Victoria McIntosh is an Information and Privacy professional here in Halifax. She received an honours BA in History from Mount Allison University, an MLIS degree from the University of Western Ontario, and is certified by the International Association of Privacy Professionals as an Information Privacy Technologist. Presently, Victoria is operating as a freelance consultant under her business name: Information in Bloom Management Services.

Dark Skies: Trying to Navigate Data Sovereignty in the Cloud
Does your organization issue passports for its information? Unless you’ve developed a cloud space made entirely of data storage on international waters, the information your business collects has to make landfall somewhere. Yet as countries continue to embrace high cyber surveillance and protection policies, information residency and law in the global marketplace continues to get more complex. There’s interest in your product from Russia? Intent on working with both the U.K. and E.U.? Prep yourself for some heavy problem solving. From an international intelligence perspective, data sovereignty is that security practice looking good on paper, but gets frustrating when applied to real-world problems.
In Canada data sovereignty isn’t a new issue. Provincial and industry legislations prohibit specific sectors from exporting information outside the country. However, they do raise challenges when trying to comply. How do you possibly keep data protected in its country of origin, while meeting the cost, technology and tool requirements of your users? Even if the data residency and access are both from the same country of origin, does that make it safe from outside surveillance? Privacy Technologist Victoria McIntosh explores the benefits, setbacks, and that challenges that make data sovereignty such a mockery in the digital world.

Kellman Meghu
Raised my children with a firewall; shamed a large airline into using SSL for check-in; front line for the security as some of the biggest corporations went online for the first time; 20 years of helping every sector define, deploy, and defend their infrastructure; Thinks learning a new programming language is a great way to relax on holiday; Dreams in key/value pairs; Obsessed with putting everything in containers; Loving every minute of it.

How I Learned To Stop Worrying And Love The Cloud
A fun, and sometimes antagonistic look at the security industry. Using personal stories (with the names changed to protect the guilty) we explore what the security industry as evolved into. Stripping away marketing and promises, this session challenges us to rethink how we protect ourselves in an always on, always available, always sharing world. This is about philosophy and architecture, not products, and some harsh changes we will face trying to keep up. Topics will include cloud as an architecture, realistic value of machine learning, as well as the promise and pitfalls of blockchain applications.

Fernando Montenegro
Fernando Montenegro is a security professional with a strong background in network and cloud security. He is currently an independent consultant working on multi-cloud security. His experience includes pre and post-sales technical roles with vendors in areas such as micro-segmentation, fraud detection, high performance network architecture, and enterprise computing. His work across enterprise customers in Canada, Latin America, and the US has provided insights into the underlying economic dynamics of common security scenarios. His areas of interest include security economics – particularly behaviour economics – data science, and cybercrime. He holds a bachelor’s degree in Computer Science and industry certifications.
Economics of Cyber Security

When we take a deeper look at common security issues – user and software security, cybercrime, we realize they’re affected by their underlying economics. Effectively addressing them requires understanding how they can be seen as economics problems: Information Asymmetry, Market Failures, Cognitive Biases, and so on. This session offers an overview of economics concepts and their application.

Peter Morin

Peter is a frequent speaker on the subject of critical infrastructure protection, risk management, penetration testing, malware analysis and forensics and has presented at numerous events held by the HTCIA, Black Hat, PMI, Computer Security Institute, Interop, SANS, and ISACA. Peter is a frequent guest lecturer at numerous colleges and university throughout North America and has also been featured in numerous newspapers and publications including SC Magazine.

Peter is a Principal Cyber Engineer and Security Evangelist with Forcepoint, a Division of Raytheon where he is responsible for the overall security of their commercial and federal products. Peter is responsible for assisting in the architectural direction of Forcepoint’s products and also manages their Product Security Incident Response Team.

Peter has over 20 years of in-depth information technology experience in the fields of enterprise computing and networking with an emphasis on IT security, application development, business continuity, incident response and forensics and has held senior management positions with Bell Canada (BCE), KPMG LLP and Ernst & Young LLP as well as worked with numerous tech start-up companies and various government and military agencies.

Peter holds numerous security-related designations including the CISSP, CISA, CGEIT, CRISC, and GCFA

Building a Product Security Team – The Good, the Bad and the Ugly – Lessons from the Field

Ensuring that the products and services we build and deliver are as threat resistant as possible is extremely important today. Meeting this challenge is not just about building secure applications since we all know that rapid development of software as well as the evolution of threats and vulnerabilities can see our applications as secure today but vulnerable tomorrow. That is why having an established product security team and response capability is extremely important.

During this discussion, I will discuss, using real-world examples, including that of my own, how organizations can meet the demands of product security including:

– Building a culture of security within your organization beyond firewalls and anti-virus
– How to “sell” security to executive management and explaining what product security does and doesn’t do (i.e. staffing, budgets, etc.)
– Building and deploying software using the “’DevOps’” approach
– The difficulties of wearing multiple hats, with security being one of them
– Embedding “security” in the software development life cycle (SDLC)
– Establishing a proper security “response” program
– Product vulnerability transparency and developing a disclosure policy
– How to measure the success of your program
– Establishing a bug bounty program
Serge Nault
Serge Nault is an IT veteran with over 25 years of experience under his belt. He has spent his career with industry-leading IT vendors such as HP, Symantec, VMware and now ESET. His current role as a trusted security advisor in the Quebec and Atlantic Canada region is based on the positive ESET philosophy to Enjoy Safer Technology. Serge is a pro-technology believer and his aim is to enhance the activities of people and companies alike, to help them enjoy the benefits provided by the careful and informed use of technology. Serge holds a Bachelor of Business degree from Ryerson University, and is currently based out of Montreal.

Mark Nunnikhoven
Mark Nunnikhoven helps organizations build securely in the cloud. Opinionated, passionate, driven, Mark is more than a cliched byline. In his 20+ years tackling development and operational challenges around the world, Mark has seen all manner of “interesting” solutions. Teaching the community through his writing, speaking, and code, Mark works hard to help everyone modernize their security practices.

Mark holds a Masters degree in Information Security Systems with specialization Digital Forensics, is an engaging public speaker, an O’Reilly video author, and accomplished computer scientist and security executive.

Mark is available online at http://markn.ca and @marknca.

Is Your Security Team Set up To Fail?
You and your team are fighting the good fight. You’ve got the right people, processes, and products in place. You’re following best practices. But it still takes weeks to deploy new patches, attackers persist on the network for months before being discovered, and users continue to invite attacks by clicking on phishing links. Why are you failing? This session will examine the current state of IT security programs and teams…delving into the structure, goals, and skills prioritized by the industry. Are standard practices still the best options for accomplishing your goals? As cyber threats and technologies evolve, shouldn’t our approaches to combatting these threats also change? Together we will consider these question as well as new approaches to success in today’s rapidly changing IT landscape. Walk away with a new perspective and a set of changes you can implement today in order to win the fight tomorrow.

Colin O’flynn
Colin O’Flynn researches embedded device security, and runs a small startup (NewAE Technology Inc.) that helps people design secure systems. This includes selling the open-source ChipWhisperer which provides the first low-cost platform for performing power analysis and glitching attacks. He lives in Halifax, Nova Scotia.

Breaking Electronic Door Locks Like You’re On CSI: Cyber
Breaking electronic locks looks so fun in the movies – get your “tech wizard” member of the team to plug some gadget in to the control panel on the locked door, the gadget scrolls through all the combinations, and then the door opens. The hardest part is figuring out what cool catch-phrase you’ll use when the door opens. Why can’t real life be like this? This talk will look at a few consumer grade electronic locks, and aims to break them like you’d see in the movies (roughly). Along the way it features a detailed tear-down of the electronics on these locks & discuss vulnerabilities a hardware hacker can exploit to bypass them.
Masarah Paquet-Clouston
Masarah Paquet Clouston is a security researcher at GoSecure, a consultancy firm specializing in cybersecurity services for the public and private sector. She is also an active member of the Serene-Risc Smart Cybersecurity Network as well as a member NorthSec conference’s council. Using her economic and criminological backgrounds, she specializes on the study of market dynamics behind illegal online activities.

Her goal is to conduct scientific research that help the community to better understand these online phenomenon, without falling into the corporate alarmist side. She presented at various international conferences such as Black Hat Europe, Botconf, the International Society for the Study of Drug Policy and the American Society of Criminology.

Besides doing research, she’s passionate about programming, defending online privacy and discussing politics.

Anonymous Online Markets: The Future of Drug Dealing?
Since 2011, drug market participants have had the opportunity to trade illegal drugs through anonymous online marketplaces, dubbed “DarkNet market” or “cryptomarket”. These marketplaces capitalize on the anonymity mechanisms afforded by Tor and the cryptocurrency Bitcoin to offer a user-friendly infrastructure, like eBay, for drug market participants to meet and conduct business. Although these platforms offer a professional and anonymous setting for drug sales, to what extent they are the future of drug dealing is unclear. For six months, we collected data of one of the largest anonymous online marketplaces to analyze market competition and the size and scope of drug vendor activities. This talk will present the results of our analyses which characterize the structure of the drug market hosted on anonymous online marketplaces, offering a deep understanding of the economic setting drug vendors faces when dealing online. It will also discuss the challenges drug vendors face and explain how they arise due to the online, anonymity and illegality features of online drug transactions.

Aunshul Rege
She has extensively examined cybercrimes against critical infrastructures focusing on digital information warfare, the organizational dynamics of cybercriminals and their modus operandi, adversarial decision-making and decision trees, the anatomy of cyber-attacks, the ‘hybridity’ (cyber-physical relationships) of crime, and trend analyses.

She is currently working on two National Science Foundation grants that examine critical infrastructure cyberattacks and adaptive adversarial behavior. She is examining issues of metrics and measurement in the context of adversarial behavior and attack trajectories.

Measuring Adversarial Behavior in Cyberattacks
Conventional cyberattack management is response-driven, which is now considered inadequate, especially in managing adaptive adversaries. Furthermore, the human aspect of adversaries is often downplayed in the technical cybersecurity domain. How do they behave, adapt, and manage defender threats? How do they engage in group dynamics and decision-making? How can these aspects be measured?

Using a Criminological framework and empirical evidence of observations and interviews done at Industrial Control Systems Computer Emergency Response Team’s (ICS-CERT) Red/Blue cybersecurity training exercise held at Idaho National Laboratory, this talk focuses on human behavior in cyberattacks. Specifically, this talk covers how adversaries might engage in research and planning, offer team support, manage conflict between group members, structure attack paths (intrusion chains), manage disruptions to their attack paths, and how limited knowledge bases and self-induced mistakes can possibly impact adversaries. Also discussed are issues in measurement and metrics in capturing human behavior effectively. Finally, the talk discusses how this human aspect can possibly be used to inform the shift towards anticipatory cybersecurity.
Renderman
RenderMan: Pope of the Church of Wifi. Breaker of things, Don of Dongs
Canadian born and raised. He hacks banks during the day and other random things at night (currently sex toys). His interests are very diverse and people seem to like to hear about his work as much as he enjoys sharing it. This has allowed him to speak at conferences and events all over the world and even change it a few times.
Often near infosec news or causing it himself, he can be found on twitter at @ihackedwhat and @internetofdongs

Hacking the Internet of Dongs
Among ‘Internet of Things’ security research, there is one branch that no one has wanted to touch, until now: The Internet of Dongs. Internet connected sex toys in all shapes, sizes and capabilities are available on the market with many more being developed. Like many IoT devices, IoD devices suffer a great many security and privacy vulnerabilities. These issues are all the more important when you consider the private and intimate nature of these devices. To research this, the Internet of Dongs project was founded (https://internetofdon.gs).
This talk will explore this under researched branch of IoT and the security and privacy threats that exist. It will also cover the IoD projects efforts to bring information security best practices to the adult toy industry.

Julien Savoie
Julien Savoie is a returning two time atlsecccon speaker, having given talks on subjects such as anonymity and cryptography. With nearly 20 years of IT experience, Julien is both a programmer and a systems administrator. He has contributed to a number of open source projects, and currently runs a number of relays for Tor project. Julien is also an avid car enthusiast whose interests include performance ECU tuning, and contracts his work part-time through a local performance shop.

Software defined murder
Can a hacker cause a car crash? Software plays an ever expanding role in controlling various aspects of our daily lives, including the transparent management of our safety. In this talk we will attempt to answer a simple question. Is it possible to kill someone with malicious software alone? In doing so, we will focus on automotive firmware. Fundamentals such as how an engine control unit works, and what responsibilities it plays in a vehicles normal operation will be explained. We will not be speaking about purely theoretical attacks. Instead we will discuss and demonstrate (through pre-recorded video) practical examples, some requiring little in the way of programming knowledge.

Stephen Singam
Stephen is an Information Security & Technology Management professional with extensive experience in the Financial Services, Startups, Media & Entertainment and Cybersecurity Consulting industries, who has held senior cybersecurity positions at Hewlett Packard (Asia Pacific & Japan), Commonwealth Bank of Australia (Sydney), 20th Century Fox/News Corporation (Los Angeles), Salesforce.com (San Francisco), IBM Corp (New York) and Nokia (Helsinki, Finland).

Advanced Persistent Bots (APBs) and How to Mitigate Risk
Simple malicious bots were originally created as command line scripts to download websites and pilfer content. Being “dumb,” they’re a dying breed. Today advanced persistent bots (APBs) fly under the radar of many existing security solutions and, as such, are much harder to identify and block than their predecessors. APBs have several advanced
abilities. They include mimicking human behavior, loading JavaScript and external resources, cookie support, and browser automation. They're persistent in that they can randomize their IP address, headers, and user agents. We will review current malicious bot mitigation methodologies and their limitations, discuss the rise of APBs, in addition to their new threat vectors such as cookie harvesting, poisoning, and the enabling of malicious content injections that target websites. Among innovative risk detection and mitigation approaches to be covered are: -The use of high-entropy fingerprinting, such as using WebGL.

We'll conclude with a look at future trends regarding APB mitigation using deception technologies. Automating the creation of traps, or decoys—mixed within existing web application resources—these provide an extra layer of protection to stop APB attackers who have successfully penetrated systems.

Xavier Trépanier
Expert in Cyber Defence at RSA and having worked as a security specialist for more than 9 years, Mr. Trépanier has extensive knowledge of advanced attacks. He has executed various security mandates for many international companies working in the banking, pharmaceutical, governmental and technological fields. He also participated in complex technology projects and was a key player in investigations in several countries such as Canada, the United States, France and Italy.

Evolve or you will be compromised … or you are already!

The evolution of advanced attacks forces us to review our ways of doing things and our tools. The various Zero-Day attacks using: Malware, APT, Rootkit, Ransomware and other techniques to bypass traditional methods of detection and prevention are now widespread and easy to use. The maturity, process and risk analysis of our security operations center, SOC, must evolve. How to improve this? Better visibility of our entire infrastructure will enable us to rapidly improve and detect threats and execute a fair risk analysis and develop!

Rick Vanover
Rick Vanover (Cisco Champion, MVP, vExpert) is the Director of Technical Product Marketing & Evangelism for Veeam Software based in Columbus, Ohio. Rick’s IT experience includes system administration and IT management; with virtualization being the central theme of his career recently. Follow Rick on Twitter @RickVanover or @Veeam.

Tips and tricks to prevent data protection from being the backdoor to IT Security

When it comes to data protection, the risks are high. Too many times companies take adequate protections for live workloads; but are the same standards are applied to the durability of the data protection scheme? Different backup technologies offer different opportunities and risks for security the backup data. Additionally, how can backup technology be resilient for ransomware?

In this breakout session, join backup expert Rick Vanover for practical security tips for data protection administrators to avoid being the next headline. Topics covered in this session include:

- Storage security strategies for backups
- Backup resiliency for ransomware strategies
- Managing multiple security techniques
- Identifying backdoors from data protection solutions
- Implementing controls for each step of the data protection process
Geoffrey Vaughan
Geoffrey is a security engineer with Security Innovation. He spends his time hacking and securing web applications, mobile apps, robots, 3D printers, infrastructure, embedded devices, and anything with a Biometric. He is passionate about security and helping others build secure products.

Building your Personal Threat Model
What's in your personal threat model? What assets are you trying to protect? Learn how to improve your personal security and privacy online through best practices and security tips. This talk is for everyone, whether you're a seasoned security professional or complete novice. Hopefully, you will take away a few areas where you can better protect your personal information.

Chris Vernon
Chris Vernon, CISSP, is a Senior Sales Engineer within Symantec's Technical Sales Organization, based out of Montreal. As a security professional, he has advised government and commercial organizations on information security practices across North America, Europe, and Asia. He regularly works with Canadian businesses to help solve the challenges of securing data on-premises and in the cloud. Chris holds a B.Sc. in Computer Engineering.
Travis Barlow
has over 16 years of experience in the IT field, the majority of it in the IT Security realm. Currently he is the VP of Advanced Security Services and General Manager Atlantic with GoSecure. He is the founder of the Atlantic Security Conference (AtlSecCon) and the Halifax Area Security Klatch (HASK), a local security community. He has been recognized by Digital Nova Scotia as an Industry Leader. He is also an avid speaker, having spoken at multiple security events and is frequently booked for future events.

Andrew Kozma
is currently the Team Lead of the Active Response Centre at GoSecure. He is responsible for the development of information security policies, standards, procedures, and their management and implementation. In addition to network and security architecture audit responsibility, Andrew is also trained to look for weaknesses and vulnerabilities in target systems and to use his knowledge as a hacker to identify, report and mitigate risk. Andrew is also actively involved with the Halifax Area Security Klatch (HASK).

Steve Quinn
has been in the IT industry for 19+ years with a wide range of responsibilities. From being responsible for network infrastructure to manning a helpdesk, his latest challenge has been moving to Go Secure as IT Security Analyst – Endpoint Security Lifecycle. As he has always had a love of InfoSec he has been working with the Atlantic Security Conference and the Halifax Area Security Klatch since their inception.

Darryl MacLeod
is a 16 year veteran of the Atlantic Canadian IT community and works for MNP as a Senior Consultant, CyberSecurity. He is the founder of the Cape Breton Technology Users Group and the former lead organizer of the Security B-Sides Cape Breton conference.

Nick Gyorfi
is an IT Professional with over 10 years experience in various information technology roles from global organizations to Government and educational institutions. Nick holds a Bachelor of Commerce Degree from Saint Mary’s University, a diploma in Information Technology from Nova Scotia Community College and various IT certifications. Nick has a passion for information security and helps to run the Halifax Area Security Klatch (HASK).
Thank you and see you next year!