Level 2

Main Stage: 2m x 7m @ 24" high with TCL Backdrop

Main Lobby

Show Office

WASHROOMS

FIRE EXIT

Atlantic Security Conference
April '16

The Business Exchange: Plenary
57 ovals open-ended ovals of 8

For Book Signing

Buffet Lunch Rolling 6fts

Track 2 and Track 4 on 3rd floor

Techn: 2m x 5m @ 24" high

freight elevator

Solutions Track

Private Office

Event Production Office

Private Speakers Lounge

Show Office
Welcome to the 2016 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, Scott Walsh 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.

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 1 AGENDA

Schedule is subject to change without notice.

### DAY 1 – THURSDAY APRIL 7, 2016

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 - Main Plenary</th>
<th>Track 2 - 301/302</th>
<th>Track 3 - 203/205</th>
<th>Track 4 - 303</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 AM</td>
<td>Registration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:15 AM</td>
<td>Opening Remarks &amp; Opening Keynotes by John Siaio</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:45 AM</td>
<td>Morning Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Jeff Man - The Art of the Jedi Mind Trick</td>
<td>Vic Chung - Towards a multi-stakeholder approach to vulnerability disclosure for better security</td>
<td>Rick Vanover &amp; Clint Wyckoff - Security practices and Data Protection: Tips to avoid a backdoor</td>
<td>Peter Morin - Is Your Supply Chain Secure? Exposing and Understanding the Risks of Third Parties</td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Catered Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Raul Alvarez - Reversing a Polymorphic File-infecting Ransomware</td>
<td>Milos Stojsadinovic - Paper Trails: What are you leaving behind?</td>
<td>Mortiz Reabe &amp; William Ballenthin - FLOSS every day – automatically extracting obfuscated strings from malware</td>
<td>Kurtis Armour - Browser and Environment Hardening</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>Dave Lewis - An Examination Of The Epistemology Of The Modern Botnet</td>
<td>Jordan Rogers &amp; Guillaume Ross - Real solutions from real incidents: save money and your job!</td>
<td>Yuan Nielsen - Protect Company Data from the Most Pervasive Cyber Security Threat!</td>
<td>Lily Chalupowski - Enumerating PE File Structure Security Protections and Custom Base 64 Steganography</td>
</tr>
<tr>
<td>2:45 PM</td>
<td>Afternoon Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00 PM</td>
<td>Ofir Maoz - Software Signoff - Engineering Better, Safer, More Secure Software</td>
<td>Julien Savoie - How to run a dark market (without getting caught)</td>
<td>Aion Sadah - Building a Sophisticated Endpoint Defense Strategy with Full Security Lifecycle Protection</td>
<td>David Nichols - Running a Bug Bounty Program</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>Closing Keynote by Keliman Meghu</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 PM</td>
<td>Social Mixer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:00 PM</td>
<td>Speakers Dinner (Ticket Required)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company’s fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry’s highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations’ most important security challenges, whether in networked, application or mobile environments -- be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at http://www.fortinet.com, the Fortinet Blog or FortiGuard Labs.

At Cisco (NASDAQ: CSCO) customers come first and an integral part of our DNA is creating longlasting customer partnerships and working with them to identify their needs and provide solutions that support their success. Cisco has shaped the future of the Internet by creating unprecedented value and opportunity for our customers, employees, investors and ecosystem partners and has become the worldwide leader in networking transforming how people connect, communicate and collaborate.

Datto is an innovative provider of comprehensive backup, recovery and business continuity solutions used by thousands of managed service providers worldwide. Datto’s 180+ PB purposebuilt cloud and family of software and hardware devices provide Total Data Protection everywhere business data lives. Whether your data is onprem in a physical or virtual server, or in the cloud via SaaS applications, only Datto offers endtoend recoverability and singlevendor accountability.
<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 - Main Plenary</th>
<th>Track 2 - 301/302</th>
<th>Track 3 - 203/205</th>
<th>Track 4 - 303</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 AM</td>
<td>Opening Remarks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Anna Manley - Life is Short… Sue Everyone: Legal Perspectives on the Ashley Madison Hack</td>
<td>Michael Davis - The Thin Line Between the Insider and the Outsider</td>
<td>Garry Coldwells - Cloud Security – SaaS and the imperative to abandon your proxy approach</td>
<td>Eldon Sprickerhoff - New Techniques To Prepare For Next-Generation Corporate Insider Threats</td>
</tr>
<tr>
<td>10:45 AM</td>
<td>Morning Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Catered Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Sunny Wear - No Time for REST: Web Services Security</td>
<td>Paul Halliday - A Beginner’s Guide to OSINT</td>
<td>Michael Bluteau - Who owns this account? Reduce risk with Access Governance</td>
<td>Evan d’Entremont - Defeating next gen firewalls</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>Olivier Bilodeau &amp; Thomas Dupuy - Internet of {Things, Threats}</td>
<td>Colin O’Flynn - Hardware Hacking - Lightbulbs &amp; Hard Drives</td>
<td>Sebastien Bigras - The unsexy practice of keeping your virtual windows and doors locked</td>
<td>Fahmy Kadiri - Advanced Threats: Eliminating the Blind Spot</td>
</tr>
<tr>
<td>2:45 PM</td>
<td>Afternoon Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00 PM</td>
<td>Closing Keynote - Mattias Katz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 PM</td>
<td>Closing Remarks and Prize Draws</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7:00 PM</td>
<td>After Party at the Lower Deck Tap Room (AllSecCon Badge Required for Entrance)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CounterTack puts enterprises back in control of security at the endpoint. Through a combination of tamperresistant, behaviorallybased detection, analysis and response technology, integrated on top of the most advanced Big Data platform, CounterTack equipsteams with authoritative visibility and comprehensive attack context into endpoint behavior and processes.

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall1 and its patented stateful inspection technology.
John Sileo

John Sileo's identity was stolen by a business insider and used to embezzle $300,000 from his clients. The exposure destroyed John's company and consumed two precious years as he fought to stay out of jail. Combining real-world experience with years of study, John became an award-winning author, trusted advisor and leading speaker on managing privacy and reputation in an economy plagued by digital overexposure.

John leverages his story of transforming risk into reward and the emotional connections it creates to evoke the skills of instinct, inquiry, and initiative that empower his clients to take control of their data exposure before it's too late. John is the CEO of The Sileo Group, which advises clients on balancing risk, defending privacy and multiplying profits by building a culture of deep trust.

John's body of work includes engagements with the Pentagon, USA Today, Blue Cross, the FDIC, Pfizer, 60 Minutes, Homeland Security, AARP, Anderson Cooper, Prudential, The Washington Post, the Federal Reserve, Fox Business and organizations of all sizes.

John graduated from Harvard University with honors and spends his free time with his amazing wife and two highly spirited daughters.

Kellman Meghu

Kellman Meghu heads up a team of Security Architects for CheckPoint Software Technologies Inc., the worldwide leader in securing the Internet. His background includes almost 20 years of experience deploying application protection and network-based security. Since 1996 Mr. Meghu has been involved with consultation on various network security strategies to protect ISP's in Southern Ontario as well as security audits and security infrastructure deployments for various Commercial and Governmental entities across Canada and the Central United States.

Kellman has delivered security talks in private corporate focused events, at school internet safety classes for students and teachers, as well as public events such as, SecureWorld Seattle, The Check Point Experience, Bsides St. Johns, Bsides San Francisco, Bsides Iowa, Bsides Detroit, Secure360, Trilateral Conference, and Sector lunch keynote for 2014. Kellman has contributed to live TV interviews in the Toronto area with CP24, CityNews, and CHCH TV, as well as radio station interviews and news articles across Canada and the US.

Matias Katz

Matias Katz is a Penetration Tester who specializes in Web security analysis. He loves to build simple tools to perform discovery and exploitation on any software or network. He has spoken at BlackHat, H2HC, Ekoparty, TEDx, Campus party, OWASP and many important conferences. He is the founder and CEO of Mkit Argentina (www.mkit.com.ar), a company that specializes in computer, physical and human security solutions. He is also the founder of Andsec conference (www.andsec.org). And he is Super Mario World master!!
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, and DefCamp. And I also have presented in HASK security group and at the University of BC. I am a regular contributor to the Fortinet blog and also in the Virus Bulletin publication, where I have published 22 articles.

REVERSING A POLYMORPHIC FILE-INFECTING RANSOMWARE
Virlock is a polymorphic file-infecting ransomware. It is capable of infecting executable files and at the same time, hold your computer hostage. Running a single infected file is a sure way of infecting your computer all over again. That is one of the main goals of Virlock. As a ransomware, the malware makes sure that you won’t be able to use your computer until you pay the ransom demand. And to make our lives, even harder, Virlock employs an on-demand polymorphic algorithm, where each and every copy of the infected executable file is different from each other. And there is more, Virlock is not only a polymorphic file-infecting ransomware. The initial set of the malware code is metamorphic in nature. In this presentation, we will dive deep in Virlock’s code to expose how it generates its metamorphic code, how it uses an on-demand polymorphic algorithm, how it infects an executable file, and every complicated algorithm that it has in its sleeves. We will also look into its code structure on how everything comes together. A few demonstrations will be provided to show how some of its algorithms execute in the context of a debugger. Given Virlock’s code complexity, is there a way we can have protection from this malware? We will answer that question and more.

Kurtis Armour
Kurtis Armour is a security professional who has been working in the industry for 5 years. He enjoys working on research projects and increasing his security knowledge. Pastime activities include mountain biking, golfing, squash, skydiving and more.

Browser and Environment Hardening
In today’s threat landscape, many corporate users are being compromised by exploit kits and phishing campaigns. These offensive techniques are successful because they target outdated software and unsuspecting users. There are tools and configuration options to help prevent the execution of malicious binaries, the exploitation of web browsers, and the third party applications that are utilized by the browser. This presentation will cover methods for organizations to strengthen their environment from exploitation and compromise.

Philippe Arteau
Philippe Arteau is a security researcher working for GoSecure. He is the author of the widely used Java static analysis tool Find Security Bugs. He has also build many plugins for Burp and ZAP proxy tools. He has discovered many vulnerabilities in popular software including Google Chrome, Dropbox, Paypal, RunKeeper and Jira.

The new wave of deserialization bugs
Recently, there have been several deserialization bugs released. In 2015, many Java softwares - including WebLogic, Jenkins and JBoss - were found vulnerable because of a common bug pattern. This talk will present the risk associated with deserialization mechanism and how it can be exploited. While a fix is available for some of the known vulnerable
applications, your enterprise might be maintaining a proprietary application that is at risk. A tool will be presented to identify the vulnerable pattern. This vulnerability can be applied to any languages. Examples will be given for PHP and Python.

Olivier Bilodeau & Thomas Dupuy
Olivier Bilodeau is the head of Cybersecurity Research at GoSecure a consultancy firm specializing in cybersecurity services for the public and private sector. With more than 10 years of infosec experience, Olivier worked on Unix servers at Bell Canada, managed a portion of Air Canada's network, wrote open source network access control software at Inverse and worked as a Malware Researcher at ESET. He likes to reverse engineer everything that crosses his path, participate in information security capture-the-flag competitions, hack open source code and brew beer. He has spoken at various conferences (Defcon, Botconf, VirusBulletin, Derbycon, …), used to lecture on information security at ETS University in Montreal, drives the NorthSec Hacker Jeopardy and co-organizes the MontreHack capture-the-flag training initiative. His primary research interests include reverse-engineering tools, Linux and/or embedded malware and honeypots.

Thomas Dupuy is a Malware Researcher at ESET Canada. Thomas has breakfast reversing binaries, contribute to open source projects during lunch and plays CTF by night. Curious by nature Thomas likes to analyze malware of exotic architectures.

Internet of {Things, Threats}
More and more devices are connected to the Internet. Under the moniker “Internet of Things” (IoT) these “things” generally run an embedded Linux system of the MIPS or ARM architecture. The unresolved problem of software updates and short vendor support cycle combined with the lack of effort into systems security and application security makes these devices an easy target. This last year we have analyzed several malware samples targeting these architectures. Internet accessible embedded systems are being compromised via vulnerabilities (like Shellshock) or because of their weak default configuration.

Our presentation will cover some of the analysis we performed:
* Linux/Moose, a malware that propagates by itself and perform social network fraud on Twitter, Facebook, Instagram and more
* LizardSquad and foreign actors that are leveraging embedded systems to perform distributed denial of service attacks (DDoS)
* Win32/RBrute, desktop malware that changes router settings in order to infect more victims. This is distributed by the Sality botnet.
* An Exploit Kit that leverages router vulnerabilities through a Web browser to perform “DNS poisoning”

Finally, some advice will be given to the audience in order to help protect themselves, their organizations and their families.

Jon Blanchard
Jon Blanchard is a Speaker, Technology Columnist with Canada.com and the Globe and Mail as well as the Ethics Lead for the Nova Scotia Technology Guild based in Halifax, Canada. Mr Blanchard (@dexterdyne) is a regular and popular presenter on the challenge and promise of hackism at the Atlantic Security Conference(AtlSecCon), High Technology Crime Investigation Association (HTCIA) and Atlantic Internet Marketing (AIM) Conferences - as well as Halifax Area Security Klatch (HASK), Third Wednesdays (3W) and Podcamp Halifax.
Anonymous 3.0 - the Telecomix Derivation
Following a year long hiatus to rejoin things Telecomix, Jon Blanchard returns to discuss Security Theatre, #C51 and how Open Data might none the less save your life one day.
Exclusively included free of charge with your #AtlSecCon 2016 pass, there will be a long overdue Maritime Top Ten Hacked Sites report as well as several live National easter eggs. nope, we don’t know yet either - so don’t ask...

Earl Carter
Earl Carter has always had a passion for solving puzzles and understanding how things operate. Mr Carter quickly learned that identifying security weaknesses is just like solving puzzles. Almost 20 years ago, he was introduced to network security when he accepted a position at the Airforce Information Warfare center. In 1998, Mr Carter starting working Cisco and became one of the founding members on the Security Technology Assessment Team (STAT). After spending 15 years identifying new security threats and assisting product teams in hardening their devices and software to mitigate those identified security threats, Mr Carter became a Threat Researcher for Cisco Talos. Now he spends his time hunting for new threats against live customer networks by examining various intelligence feeds and data sources. Among Mr Carter’s significant contributions to Cisco are multiple security patents and authoring multiple Cisco Press Security Books.

Emerging Threats - The State of Cyber Security
Analyzing massive data feeds and working with teams of security experts, Cisco Talos has a unique view into the ever evolving and changing Threat Landscape. We constantly research and identify how threat actors are evolving their skills and tactics. During this talk I will provide detailed analysis of the current threat landscape by examining the major threats that we have researched over the past 6-9 months. Some of the threats I plan to cover include

- SSHPsychos campaign - threat actors attempting to build a massive DDos Botnet by compromising SSH servers
- Evolution of the Cryptowall ransomware
- Angler Exploit Kit – Feature evolution, exposing back- end network configuration
- Rombertik Malware – Sophisticated credential stealing malware specifically designed to avoid detection
- Phishing Campaigns – Techniques used by different campaigns to target users and avoid detection.

The Angler exploit kit research was especially noteworthy in that by working with Limestone networks, we were able to eliminate an Angler network that was generating over 30 Million dollars a year by targeting users with ransomware.

Lilly Chalupowski
Lilly Chalupowski is a first time speaker at AtlSecCon, Penetration Testing Consultant and founder of Arc Network Security. She is an Acadia University alumni who spent a year in computer science and an additional four years in audio engineering, has a minor in sociology and also has taken many information security and programming courses in correspondence over the years. She has written several tools including a SSDP Vulnerability Scanner, pwn-scan (Email Data Breach Scanner), Chameleon (Custom Base 64 Steganography Tool), and Badger (Exploit Development Tool). Lilly has been involved in tearing apart the WAV file format allowing it to have meta-data that isn’t classically possible with the current standards allowing for album art, and karaoke text all by working around the current RIFF file format standards made by Microsoft. She has also done manual meta-data header repair for custom data recovery. Lilly’s passion for hacking started when she was in high school when she got her first TI-83 calculator after that she hasn’t looked back.
Enumerating PE File Structure Security Protections and Custom Base 64 Steganography

This talk will be focused on the exploit development tool called badger and the steganography tool called chameleon. Chameleon is a custom base 64 encoder that can allow you to hide your data but also may have potential use in AV Evasion (Anti-Virus Evasion). There will be discussion of how this works and where you can get the code to incorporate this in your own projects. Badger is a tool designed to enumerate dynamic link libraries and their protections. The layout of the PE file structure will be discussed and how some of the features of badger actually work. There will be an introduction the basic concept of how ASLR (Address Space Layout Randomization), DEP (Data Execution prevention) and Canaries can be bypassed using ROP (Return Oriented Programming) and potentially how badger can be used in combination with these techniques to leverage a successful exploit for exploit developers. There will be a demo of the tools after the talk is completed and time for questions.

Vic Chung

is a Product Security Response Expert with SAP Global Security. Vic is responsible for case-management of vulnerabilities reported by hackers and is the lead for Americas operations. Prior to working at SAP Global Security, Vic managed technical intellectual property compliance for SAP global development teams and has deep expertise in technical program management. Vic has a Master degree in Information Systems from University of Toronto, Canada and a MBA in Technology Management from Open University Business School, UK. When not working with hackers or customers, you will find Vic snowboarding on the mountains along the Canadian west-coast.

Towards a multi-stakeholder approach to vulnerability disclosure for better security

Did Venom, Ashley-Madison data leak, or OPM hack, teach us anything as security professionals? As year(s) go by, we continue to hear high-profile hacks on security headlines. While we can blame technology is evolving and security can never be perfect, we should also ask whether we have approached security properly. In this presentation, I will argue the coordination of vulnerability disclosure remains as a critical area in security for research and development beyond offensive and defensive security techniques. The rise of cloud technologies and Internet of Things provides a complex threat landscape where defensive techniques could be insufficient to mitigate all risks. I will review why current vulnerability disclosure and disclosure capability practices and models are insufficient to lead to better security. I will suggest a forward-looking strategy to extend beyond responsible disclosure is required to handle the complicated technology 'eco-system' we are in today. I will show you cross-disciplinary tools, techniques, and a practical model of collaboration and coordination around vulnerability disclosures with hackers, vendors, security researchers, and customers alike as a novel approach to build better security.

Michael Davis

As CounterTack’s CTO, Michael Davis is responsible for driving the advancement of CounterTack’s revolutionary endpoint security platform, as well as leveraging his visionary approach to push defenders ahead of attackers. Davis is one of the nation’s leading authorities on information technology, authoring top selling book, Hacking Exposed, and contributing to publications such as InformationWeek and Dark Reading. He was voted one of the “Top 25 under 25” by BusinessWeek, and named semi-finalist of the Ernst and Young “Entrepreneur of the Year” award. In 2005, he founded Savid Technologies, an IT security consulting firm. By 2010, Savid was ranked 611 on the Inc. 5000 list of fastest growing companies in America. Prior to Savid, he served as senior manager of global threats at McAfee, where he led a team of researchers investigating confidential and cutting-edge security analysis.
The Thin Line Between the Insider and the Outsider
If you assume that attackers know our networks' topology already, they may have the credentials they need to access your “crown jewels.” The attacker is now behaving like a malicious insider. In this session, we will walk through the methodologies behind new-age threats, and examine specific use cases where attackers were able to infiltrate secure systems under the guise of an internal user.

Evan d’Entremont
Evan d’Entremont is a software developer and HASKer who spends his time solving complex problems. His background includes web application development and securing legacy applications.

Defeating next gen firewalls
This talk will look at next generation firewalls; what they try to solve, and why network level monitoring and interception are doomed to fail. We’ll explore the issues cryptography create for passive monitoring, infiltration/exfiltration methods including DNS tunneling and steganography, and the difficulties of reputation analysis in an increasingly cloud and CDN based world. When combined, these issues create significant challenges for the indefinite efficacy of network security appliances.

Tim Dickinson
Tim Dickinson is a Customer Success Manager and Identity Access Management expert at SailPoint Technologies, Inc. He started his career in R&D at Atomic Energy of Canada and the Canadian Space Agency, but soon found that what he enjoyed most was solving technology problems and making customers’ experiences better. Since that change Tim has been a fiberoptic transmission support engineer, run Nortel’s VPN router and firewall support team for Europe, been the GM of a small satellite broadband company, and a Customer Success leader at CA Technologies. He’s lived and worked for 23 years in Ontario, the UK, and Australia before recently returning to Halifax.

Since joining SailPoint Tim’s sole focus has been to help some of their largest customers get the best possible business outcomes from their investment in Identity Access Management.

The 7 Tenets of Successful Identity Access Management
We have all seen data breaches increase steadily over the past several years, more devices in cloud and mobile, regulatory pressures, and huge increases in IT operational complexity. What you may not see is the temptation companies have with holding onto existing access management systems while wanting to innovate to the next level of access control.

I’ll discuss Identity Access Management via a quick journey of trends my colleagues and I have seen in enterprises attempting to control access to their networks. I will cover:
1. The Identity Account Posture – the new posture in identity access fueled by increases in threats and changes in the workplace dynamics. More access requests to data - not always from your corporate network - through many more devices.
2. The Disappearing Perimeter – There are so many more software-as-a-service offerings today each with their own login credentials that need management, as well as huge increases on mobile device access to corporate resources and cloud data storage.
3. From this we will show you how to assess your identity landscape and understand potential weaknesses.
4. Finally I will walk you through what we have identified as the 7 Tenets of Identity Access Management.
Paul Halliday
Paul Halliday Makes stuff. Very likely to give it away. Engineer @criticalstack

A Beginners Guide to OSINT
This presentation will cover the basics of threat intelligence with the hope of getting newcomers ready to test the waters quickly. I will begin by introducing the different types of threat Intel and potential sources (zeroing in on the more open ones). I will then introduce tools that can be leveraged in both large and small environments to make practical use of this new source of data.

Fahmy Kadiri
Fahmy Kadiri has been providing complex security solutions to large, medium and small businesses across Canada for over 10 years. He has held various Analyst, Consulting, and Architect roles all with a detailed focus on the Cyber Security Industry. Fahmy is currently a Sr. Security Architect for Dell SecureWorks, supporting Large Enterprise clients in Canada and North Eastern United States.

Advanced Threats: Eliminating the Blind Spot
Unfortunately, it’s a foregone conclusion that no organization is 100% safe from a breach. With 49% of security leaders believing zero day attacks against their network will be the most prevalent over the next three years and 65% saying attacks have evaded current preventative security controls, it’s all about mitigating risk and the potential impact to your organization. Join Fahmy Kadiri, (Security Architect) as he talks about Advanced Threats: Eliminating the Blind Spot. Fahmy will present how advanced threat actors can evade traditional information security controls and how you can rapidly detect and respond before they achieve their objective. Join us to learn about defending against something that’s never been seen before and how an organization can quickly and efficiently remediate an ongoing attack. The power of integrating Endpoint and Network Tools will also be addressed. Finally, Fahmy will talk about actionable steps to enhance detection and speed incident response.

Aamir Lakhani
Aamir Lakhani is a leading senior security strategist. He is responsible for providing IT security solutions to major enterprises and government organizations. He has extensive experience around reverse malware engineering, DarkNet research, and offensive security. Known as Dr. Chaos, operates the popular security social media blog by the same name. In its recent list of 46 Federal Technology Experts to Follow on Twitter, Forbes magazine described Aamir Lakhani as “a blogger, InfoSec specialist, super hero…and all around good guy.”

Now you See Me, Now You Don’t
Your first impression is your only impression. However, your first impression may already have been made. Many people leave behind bread crumbs of their personal life on social media, within professional organizations, and on other websites. Your computer, your smartphone, your pictures and credit reports all create a information rich profile about you. This talk will discuss all the different threats that exist that leak your information, and how attackers can use open source intelligence to find you. We will discuss techniques used bye law enforcement and private investigators used to track individuals. Learn how you can hide from the Internet, or use it to uncover someone’s deepest darkest secrets.
Dave Lewis

David Lewis has almost two decades of industry experience. He has extensive experience in IT operations and management. Currently, Lewis is a Global Security Advocate for Akamai Technologies. He is the founder of the security site Liquidmatrix Security Digest and cohost of the Liquidmatrix podcast. Lewis also serves on the (ISC)2 Toronto Chapter Board of Directors. Lewis writes a column for CSO Online and Forbes.

An Examination Of The Epistemology Of The Modern Botnet

This talk delves into the history of botnets up to present day. This talk looks at the data collected on various botnets while tackling the motivations and monetary aspects of the attackers. What types of botnets are there and are they all bad? These are some of the items that will be discussed in this talk.

Jeff Man

Jeff Man is a Strategist and Security Evangelist at Tenable Network Security. He has over 30 years of experience working in all aspects of computer, network, and information security, including risk management, vulnerability analysis, compliance assessment, forensic analysis and penetration testing. Earlier in his career, Jeff held security research, management and product development roles with NSA, the DoD and private-sector enterprises. Prior to joining Tenable, Jeff served as a QSA, first with TrustWave, then with VeriSign and finally AT&T Consulting Services. In this role he has provided PCI consulting and advisory services to many of the nation’s best known brands.

The Art of the Jedi Mind Trick

The hacker/security community continues to struggle with how to get our message across to others. We know what’s wrong, what’s insecure, and what needs to be done to fix the problems. BUT...we seem to hear more stories about failure rather than success stories. Maybe WE are part of the problem. It’s easy to give a talk at a conference where you’re “preaching to the choir” and everyone speaks your language, but how do you fare when you are trying to give the message to your boss, or your bosses’ boss, or C-Level management?

This talk will explore a variety of techniques that I’ve learned over my 20+ years of consulting/advising customers about how to get the right message to the right people so real change happens. I’ll explore obstacles, attitudes, and challenges that I’ve faced in hundreds of companies; practical methods for getting your point across; helping others to understand what you are saying; learning to speak their language; and helping them to draw the desired conclusion.

This is part art, part science, and maybe a little luck - but I believe there are skills you can learn that will make you a successful communicator and get your message heard.

Anna Manley

Anna Manley completed her B.A. and M.A. at McMaster University and obtained a law degree from the University of New Brunswick Faculty of Law. She has a strong interest in privacy and intellectual property law.

Life is Short… Sue Everyone: Legal Perspectives on the Ashley Madison Hack

The Ashley Madison Hack and the data dump that followed didn’t just fuel the gossip mill – they raised complicated moral and legal questions in both the criminal and civil law arenas. What are the legal implications for a company who gets hacked? What are the legal implications for those who did the hacking? What legal recourse do Ashley Madison users have?
Ofer Maor
Ofer Maor is a security expert and entrepreneur with over 20 years of experience in information and application security. Ofer has been involved in application security from its early days, through research, penetration testing, consulting, and product development. As the founder and CTO of Seeker, Ofer pioneered IAST, the next generation of application security testing technology, currently used by some of the largest organizations in the world to continuously improve their software security. Ofer joined Synopsys when it acquired Seeker in July 2015. Prior to Seeker, Ofer was the Founder and CTO of Hacktics. He led Imperva’s Application Defense Center research group and has also served as the Chairman of OWASP Israel and in the OWASP Global Membership Committee.

Software Signoff – Engineering Better, Safer, More Secure Software
The concept of “Signoff” is common in almost any major engineering disciplinary. From computer hardware, through car and plane manufacturing to large construction. The concept has not yet propagated to software engineering, despite the increasing complexity of the supply chain. In this session we will explain how software signoff can be applied to produce better software.

Mike Milner
Mike Milner spent 10 years fighting organized crime, both online and IRL, while working for government security agencies in Canada and the UK. Now he’s building tech to protect the web as CTO at IMMUNIO.

The State of Web Security
Join me for a wild ride through the dizzying highs and terrifying lows of web security in 2015. Take a look at some major breaches of the year, from Top Secret clearances, to medical records, all the way to free beer.
We’ll look at how attack trends have changed over the past year and new ways websites are being compromised.
We’ve pulled together data from all the sites we protect to show you insights on types and patterns of attacks, and sophistication and origin of the attackers.
Learn about new methods that are used to steal money using compromised websites, like Warranty Fraud and Website Ransomware.
After the bad, we’ll look at the good - new technologies like U2F and RASP that are helping secure the web. Get a headstart on how they can help you keep your customers safe.

Dennis Moreau
Dennis Moreau is a Senior Engineering Architect at VMware, applying virtualization technologies to realize highly resilient, scale-able, adaptive security. He works actively with the National Institute of Standards and Technology (NIST), the U.S. Department of Defense (DoD) and the Mitre Corporation on the development of security/compliance information and automation standards. Dennis has extensive experience in designing security/compliance management solutions. Prior to joining VMware he was a Senior Technology Strategist at EMC/RSA specializing in utility computing security, advanced threat technologies and trust modeling. He was also a co-founder and the CTO of Configuresoft (now a VMware technology) and the CTO for Baylor College of Medicine. He holds a doctorate in Computer Science and has held research and faculty positions in that discipline. His research has been sponsored by NASA, Jet Propulsion Laboratories, the US Department of Commerce, the National Institutes of Health, the National Library of Medicine, AT&T Bell Laboratories and IBM.
INFOSEC TRACK

Attacks, Detection and Defense in the Resilient Datacenter: The Emerging Battlefield

As business exigencies drive datacenters toward ever increasing scales, agility and levels of automation, the underlying technologies expose the need to manage and control deeper stacks, more dynamic configurations and more rapidly evolving system behaviors. The days of relying on telemetry from a few choke points, over a static network topology, with stale behavioral baselines are rapidly receding toward the horizon.

Traditional asset and workload identifiers and physical network topology are becoming increasingly inadequate as a foundation for supporting security correlation, analytics and the development of actionable mitigation context. At the same time, new attacks are stimulating the need for new kinds of visibility and control. As a result, the complexity of leveraging a security portfolio is increasingly a barrier to effective protection.

This session will dive into the implications for both defenders and attackers, of increasing containerization, virtualization and softwarization of security controls. We’ll look at the emerging trends in attack technology including firmware exploits, open source poisoning, side channels and the increasing emphasis on layer 7 intrusion. Finally, we’ll consider opportunities to transform the security portfolio, making security telemetry more effective while concurrently reducing the complexity of detection, analysis and response.

Peter Morin

has over 20 years of experience in enterprise computing focusing on network security, penetration testing, malware reverse engineering, incident response and computer forensics and is currently a Principal Cyber Engineer with Raytheon. Prior to Raytheon, he worked as a senior manager for companies such as BCE, KPMG and Ernst & Young specializing in the areas of critical infrastructure and telecommunications as well as working with numerous tech start-up companies, government and military agencies. Peter is a frequent speaker on the subject of critical infrastructure protection, penetration testing, malware analysis and forensics and has presented at events such as HTCIA, Black Hat, SANS, and ISACA. Peter is a frequent guest lecturer at numerous colleges throughout North America and has been featured in numerous publications including SC Magazine. Peter holds numerous designations including CISSP, CISA, CGEIT, CRISC, GCFA.

Is Your Supply Chain Secure? Exposing and Understanding the Risks of Third Parties.

With over 76% of all data breaches resulting from a third-party which introduced the security deficiencies that were ultimately exploited, it is critical that organizations understand this very important risk. From third party remote access that caused the breach at Target, to the many reports of government computing hardware being tampered with at the source, and the need for cyber supply chain security is much more important in order to minimize the exploitation of vulnerabilities. During this presentation we will look at the various areas of risk as they relate to the supply chain through real-world examples as well as methods that can be used to mitigate these risks.
David Nichols
David Nichols is the Director of the Bug Bounty Services practice at NCC Group, a leading global information assurance firm which helps enable bug bounty and vulnerability reporting programs across industries. He and his team have many years of experience running global bug bounty programs. David was previously a security consultant at iSEC Partners, acquired by NCC Group, performing penetration tests against web applications and web services.

Running a Bug Bounty Program
NCC Group's presentation entitled “Running a Bug Bounty Program” briefly explores the history of responsible disclosure and bug bounties before diving into how bug bounty programs are run and how they can be managed successfully. From improving signal:noise ratios and communication, to payouts and public disclosure, this presentation explores how to run a better bug bounty program from start to finish.

Jordan Rogers
Jordan Rogers is a Senior Consultant for Rapid7’s Analytic Response team, responsible for building out and leading Incident Response Program Development, Tabletop Exercise, Breach Readiness Assessment, and Forensic programs. His background includes incident response, forensics and malware reverse engineering, as well as security architecture design. He has lead training at CircleCityCon, worked security at DerbyCon and CircleCityCon. He has also lead training for private and government entities on malware reverse engineering, incident response and forensics.

Real solutions from real incidents: save money and your job!
This talk will cover scenarios from real incidents and how simple solutions that are very cost effective can be used to prevent them from occurring.

* A scenario based on real incidents will be presented.
* The typical state of security in enterprise will be presented.
* Specific gaps that allowed the incident to occur and for data to be exfiltrated will be scrutinized.

For each observation, a review of how enterprises are protecting themselves, successfully or not, as well as what can be done to potentially prevent the incident from occurring in the first place will be performed.

The presentation will conclude with a discussion on the importance of incident response lessons learned being leveraged to further guide decisions related to security program development.

*Shared talk with Guillaume Ross

Guillaume Ross
Guillaume Ross is a Senior Consultant working for Rapid7’s Global Services team, responsible for Information Security Program development. With a background in IT and Security Architecture, he advises clients on their Information Security Programs as well as on technical topics such as threat modeling, mobile and cloud security, and dreams of well hardened, well designed, secure Active Directory deployments. He has previously presented at AtlSecCon, NorthSec, Converge and BSidesLV as well as private events.
Real solutions from real incidents: save money and your job!
This talk will cover scenarios from real incidents and how simple solutions that are very cost effective can be used to prevent them from occurring.

* A scenario based on real incidents will be presented.
* The typical state of security in enterprise will be presented.
* Specific gaps that allowed the incident to occur and for data to be exfiltrated will be scrutinized.

For each observation, a review of how enterprises are protecting themselves, successfully or not, as well as what can be done to potentially prevent the incident from occurring in the first place will be performed.

The presentation will conclude with a discussion on the importance of incident response lessons learned being leveraged to further guide decisions related to security program development.

*Shared talk with Jordan Rogers

Julien Savoie
Julien Savoie is a returning AtlSecCon speaker and a multiple time HASK contributor. Julien brings more than 15 years of IT experience and has worked in a variety of sectors including government, academia and private. With a background in software development, cryptography and networking, Julien has made code contributions to several OSS projects and maintains a number of Tor relays. His hobbies include photography, modifying cars and finds endless amusement in talking about himself in the 3rd person.

How to run a dark market (without getting caught)
Marketplaces on the “darkweb” have captured the imagination of journalists; with promises of illicit goods of every variety and total anonymity. However, with news of recent busts of (in)famous dark market websites, it’s become obvious that running a dark market website, without getting caught, requires thorough planning.

Explored will be a number of the technical and logistical challenges one would need to address in setting up their own marketplace. We will provide solutions to many. We will also discuss the economics at play and what’s actually available in such marketplaces as a result.

Eldon Sprickerhoff
Eldon Sprickerhoff is a Co-Founder and the Chief Security Strategist of eSentire. He has a B.Math. in Computer Science/Economics from the University of Waterloo but that was so long ago that his degree could have its own Ph.D. by now. His tech celebrity doppelganger is Eric Schmidt. He is currently unarmed.

New Techniques To Prepare For Next-Generation Corporate Insider Threats
Preventing insider threats continues to be a difficult task. While malicious insider threats typically receive more publicity, damage done through unintentional insider negligence may ultimately claim a larger share. From atypical insider motivations (Conscientious Objector) to the more mundane scenarios (Insider Trading), this talk will examine newer detection frameworks, psychometrics and technical defense strategies, with real-world examples of each.

As well, effective response and resolution methodologies (including post-event handling – communication with employees, clients, and regulators) will be detailed.
Mark Stanislav

Mark Stanislav is a Senior Security Consultant on the Global Services team at Rapid7. Mark has spoken internationally at over 100 events including RSA, DEF CON, SOURCE Boston, Codegate, SecTor, and THOTCON. Mark’s security research and initiatives have been featured by news outlets such as the Wall Street Journal, The Associated Press, CNET, Good Morning America, and Forbes. Mark is the co-founder of the Internet of Things security research initiative, BuildItSecure.ly. He is also the author of a book titled, “Two-Factor Authentication”.

Mark earned his Bachelor of Science Degree in Networking & IT Administration and his Master of Science Degree in Technology Studies, focused on Information Assurance, both from Eastern Michigan University. During his time at EMU, Mark built the curriculum for two courses focused on Linux administration and taught as an Adjunct Lecturer for two years. Mark holds CISSP, Security+, Linux+, and CCSK certifications.

Curious about how well your privacy and safety are being taken care of by IoT vendors? Interested in IoT security research and want to understand what flaws are being found in devices today? Skip the hype-only stunt hacking and come hear Mark discuss real-world examples of issues that actively threatened the privacy and safety of the families using connected devices. After all, if it ‘takes a village to raise a child’ it’s going to take a lot of hackers to secure them in the Internet of Things.

**Hide Yo’ Kids: Hacking Your Family’s Connected Things**

This presentation will cover security research on Internet-connected devices targeting usage by, or for, children. Mark will discuss the vulnerabilities he found during this research, including account takeovers, device hijacking, backdoor credentials, unauthorized file downloading, and dangerously out-of-date protocols & software. Devices discussed will include Internet-connected baby monitors, a GPS-enabled platform to track children, and even a Wi-Fi & Bluetooth-connected stuffed animal. Details about mobile reverse engineering, hardware hacking, network traffic analysis, and other research techniques will be presented to help others learn about methods to perform their own research.

Milos Stojadinovic

Milos Stojadinovic is the Red Team lead at NCI Secured Intelligence. His primary focuses are on red teaming, penetration testing, and other offense geared services. He holds a bachelor’s degree in information security as well as a number of industry certifications. Milos enjoys working on offense related projects and tools, sharing knowledge with the community, and is always up for a good laugh.

**Paper Trails: What are you leaving behind?**

Another one landed today, it’s all over your monitor. Damn penetration test reports, they’re all alike... and that’s the problem. Some have written many, others have read many. This talk will delve into a topic seldom discussed; penetration testing deliverables. They seldom include more than technical run downs of identified vulnerabilities and an executive summary with a few pretty graphs. While this is useful information, are these vulnerabilities really the problem or are they just symptoms of larger issues? Is this really all we can provide? This talk is aimed at those who write penetration test reports as much as those who read them. Join me as we walk through structuring penetration testing deliverables to be more valuable, identifying root causes, communicating findings in more meaningful ways, and developing actionable supplementary documentation.

It’s time to raise the bar.
Colin O’Flynn
Colin O’Flynn has been developing hardware professionally for over ten years. He has been breaking hardware for considerably longer than that, but only recently has been breaking hardware on purpose (to find security flaws) instead of just screwing up. He is currently completing a PhD and has a start-up in Halifax called NewAE Technology Inc.

Hardware Hacking - Lightbulbs & Hard Drives
Can we trust hardware? This talk brings some examples of brand new hardware attacks against embedded systems – in particular a discussion of new attacks against internet connected lightbulbs, and how to attack pin-code protected hard drives made by several large manufactures.

Every year hardware hacking becomes more accessible, and this talk demonstrates a few techniques you might need to master to push the envelope of hardware hacking. Whether an academic, professional, or just interested hobbyist there is no reason to stay just an observer!

While this talk has a discussion of several new attacks on real products, the focus is on demonstration of techniques used during development of the attacks and how you can get started.

Moritz Raabe
Moritz Raabe is a reverse engineer on the FireEye Labs Advanced Reverse Engineering (FLARE) team. He currently focuses on automating and simplifying malware analysis. William Ballenthin is also a reverse engineer on the FLARE team. He enjoys tackling malware and developing forensic analysis techniques. His favorite beer is La Chouffe.

FLOSS every day – automatically extracting obfuscated strings from malware
The FireEye Labs Obfuscated String Solver (FLOSS) is an open source tool that automatically detects, extracts, and decodes obfuscated strings in Windows Portable Executable (PE) files. Malware analysts, forensic investigators, and incident responders can use FLOSS to quickly extract sensitive strings to identify indicators of compromise (IOCs). Malware authors encode strings in their programs to hide malicious activity and impede reverse engineering. Even simple encoding schemes defeat the strings tool and complicate static and dynamic analysis. Reverse engineers are challenged to decode the obfuscated data in order to fully understand a program. This usually involves recognizing encoded strings, re-implementing the decoding function, and manually applying the algorithm to the data. This process may take several hours for each malware variant. FLOSS automates this down to seconds without requiring the analyst to examine the deobfuscation method.

Although FLOSS uses advanced static analysis techniques such as emulation, the tool can be used by anyone. Incident responders and forensic analysts that understand how to interpret the strings found in a binary will understand FLOSS’s output. FLOSS extracts higher value strings, as strings that are obfuscated typically contain the most sensitive configuration resources – including malicious domains, IP addresses, suspicious file paths, and other IOCs.
Jeremy Richards

Medical Device (In-)Security
Hospitals are connecting medical devices to their wireless networks. Many of these devices are insecure, connected to the internet and very, very exploitable. This talk outlines the research of two medical devices (drug infusion pumps) and the vulnerabilities recently disclosed by the ICS-CERT and the FDA.

Sunny Wear
Sunny Wear, CISSP, CRISC, CEH, SANS GSSP-JAVA, CSSLP is an Application Security Architect and developer. Her breadth of experience includes network, data, application and security architecture as well as programming across multiple languages and platforms. In her 20 years of professional experience, she has participated in the design and creation of many enterprise applications as well as the security testing aspects of platforms and services. She is the author of several security-related books including her most recent entitled Secure Coding Field Manual: A Programmer’s Guide to OWASP Top 10 and CWE/SANS Top 25 (http://www.amazon.com/SCFM-Secure-Coding-Manual-Programmers/dp/1508929572) which assists programmers in more easily finding mitigations to commonly-identified vulnerabilities within applications. She conducts security talks and classes including “Web App Pentesting using BurpSuite” by ISC2 and is recently been an invited speaker for BSides Tampa.

No Time for REST: Web Services Security
This talk discusses the numerous security holes commonly found in web service calls, particularly in RESTful calls. Potential exploits will be discussed and demo'd but, most importantly, defenses and countermeasures will be offered along with sample code. The purpose of this talk is to heighten awareness in this area with architects and programmers commonly tasked with building SOAP and REST service calls whether they are A2A, B2B or B2C.
Michel Bluteau
Michel Bluteau, CISM+CISSP, has been involved with Identity and Access Governance since 2009, and has been involved with Enterprise Security Architecture with many small and large organizations around the world. His ability to contribute to and lead integration workshops involving many participants with different specialties is very appreciated by his customers.

Who owns this account? Reduce risk with Access Governance
Many attacks and breaches start within the perimeter, and since valid credentials and permissions are used, traditional security controls are blind or struggle to detect such illicit activities in a timely fashion. Effective ongoing certification of accounts and permissions across all applications and systems can dramatically reduce the risk allowing to shut down orphan accounts and unneeded permissions.

Sebastien Bigras
Sebastien Bigras is a Director of Technical Account Management at Tanium, with over 10 years of experience in the IT & security industry. He worked with some of the largest organizations in Americas. Sebastien has assisted organizations in defending themselves from ATP attacks. Sebastien is engaged on topics related to cyber defence, malware and advanced persistent threat (APT) research.

The unsexy practice of keeping your virtual windows and doors locked
The thing about enterprise security, from the outside at least, is it reads like a Hollywood thriller. Nation states are after your company’s most valuable assets and they must be stopped at all costs. And yes, some nation state-sponsored hacks have caused tremendous damage. But the best course for most companies isn’t to focus on combatting Mission Impossible-like come through the vent break-ins. It’s the far less sexy practice of simply keeping the virtual windows and doors to your company locked.

Rory Bray
Rory Bray is a Security Architect for IBM’s QRadar products. His current role is leading the development and enhancement of security content within the QRadar products as well as guiding secure engineering practice. Previously, he led the development of network topology modelling in QRadar Risk Manager and has 10 years of experience with QRadar. He has a background both in Software Development and IT Security.

Beyond SIEM: Collaborative Threat Defense with IBM’s QRadar and App Exchange
Criminals and other bad actors organize and collaborate by sharing information, tools and resources. Our security analysts and responders must also leverage common tools, frameworks and openly collaborate on defensive strategies and evolve security infrastructure. Point solutions must integrated into a defensive whole, threat intelligence and other information must be shared rapidly and workflows or use cases for detection and response must be shared easily. IBM Security has invested heavily in the creation of a collaborative security analytics ecosystem to bring all these facets together in a powerful, extensible, platform that fosters this sharing and open cooperation. Learn how anyone can contribute to or extend the QRadar Security Intelligence platform and then package the contribution to share with all QRadar users.
Garry Coldwells
Garry Coldwells has over 20 years in information security experience and has held key product and industry certifications including the CISSP (1998), CCSI, JNCE and PCNSE. In the course of his career he has spoken at IT security conferences across North America. Garry has been involved in security projects of significance and global scope that included federal, provincial, higher education and Financial Services.

Cloud Security – SaaS and the imperative to abandon your proxy approach
I will base the talk on Aperture and will drive home the point that proxy based approaches have lost relevance. I will further dig into the control of sanctioned Apps and why this space is critical to address.

Jason Keirstead
Jason Keirstead is a product architect for IBM QRadar. He has over 13 years experience in security intelligence, and has been highly involved in the design and development of many of IBM’s Security Intelligence portfolio of products over the past decade. Jason loves to work on challenging problems, and his primary mission is to enable simple, intuitive solutions that help to solve the complex security problems of clients. Jason holds a Bachelor of Computer Science from the University of New Brunswick.

Beyond SIEM: Collaborative Threat Defense with IBM’s QRadar and App Exchange
Criminals and other bad actors organize and collaborate by sharing information, tools and resources. Our security analysts and responders must also leverage common tools, frameworks and openly collaborate on defensive strategies and evolve security infrastructure. Point solutions must integrated into a defensive whole, threat intelligence and other information must be shared rapidly and workflows or use cases for detection and response must be shared easily. IBM Security has invested heavily in the creation of a collaborative security analytics ecosystem to bring all these facets together in a powerful, extensible, platform that fosters this sharing and open cooperation. Learn how anyone can contribute to or extend the QRadar Security Intelligence platform and then package the contribution to share with all QRadar users.

Yuan Nielsen
Yuan Nielsen is a Marketing & Community Manager / Co-Founder / Innovation Mentor with fluency in Danish and Chinese, family ties across four continents, and history in 40+ countries. Genuine curiosity for culture and diversity along with experiential skills honed in previous Psychology and Performing Arts careers strengthen a dynamic understanding of consumer behavior and relationship management.

Protect Company Data from the Most Pervasive Cyber Security Threat!
To prevent cyber criminals from gaining access to corporate data and business critical systems, it has become increasingly crucial to adopt an additional authentication layer to remote access systems. Usernames and passwords will not provide enough protection, and old token-based ‘two-factor’ authentication technology has become outdated inadequate. Please join Yuan Nielsen, Marketing Manager of SMS PASSCODE to find out how to stay ahead of today’s cyber criminals.
Alon Sadeh
Alon Sadeh has been working in the software industry for over 20 years including taking various roles at some of the world's largest software companies. Alon's background includes security, systems management and data management.

Building a Sophisticated Endpoint Defense Strategy with Full Security Lifecycle Protection
Attackers are more sophisticated than they've ever been. They're targeting our intellectual property, sensitive customer information, user information and much more. The network is not the target—it’s the endpoint where that data resides. To combat today's threats, organizations need to deploy a defense-in-depth strategy at the endpoint that delivers:

- Continuous monitoring and recording for gapless endpoint visibility
- Multiple forms of prevention that minimizes the attack surface for advanced threats
- Aggregated threat intelligence and customized detection techniques that go beyond signatures
- Recorded history for instant root-cause investigations and complete kill chain visualization
- Open and extensible capabilities that enables robust integrations for best-of-breed prevention, detection and response

Ben Smith
Ben Smith is Field Chief Technology Officer (Field CTO - US East) with RSA, The Security Division of EMC. He is a trusted advisor and consultant to RSA's global financial services customers, as well as customers in other vertical markets. With over 25 years' experience in the networking, information security and telecommunications industries, he is responsible for consulting on RSA's strategic vision around architecture and technical roadmaps for the company's security and risk management solutions. Prior to joining RSA, he held senior technical positions at UUNET, Intuit, CSC, and the US Government, along with a string of technology-oriented startups. He holds a number of professional technical certifications, including the Certified Information Systems Security Professional (CISSP) certificate, and has presented on RSA's behalf, both domestically and internationally, at cybersecurity events sponsored by Gartner, FS-ISAC, ISSA, ICI, (ISC)2, ISACA, InfraGard, HTCIA and other organizations.

Measuring Security: How Do I Know What a Valid Metric Looks Like?
There is no universally accepted method to measure security. So how do we translate operational measurements into meaningful security metrics for the business? Doing so effectively is essential, because you can't manage what you don't measure. This session will touch on the following general questions: Why are security metrics important, from both a compliance and an operational perspective? What are some best practices to keep in mind when selecting security metrics? Does your audience(s) dictate which metrics to select? What behaviors are you trying to influence with these metrics? What are some unexpected sources of security metrics? How should you communicate those metrics internally within your organization for maximum impact? Are there any examples of poor metrics which should be avoided in most cases?
Detect malware like a pro!

The new generation of malware and APT evade any traditional system like DIDS, IPS, HIPS, Antivirus and even sandbox. RSA ECAT will look at any behavior to be able to identify any types of attack on any kind of endpoint. Be able to find bad behavior easily without searching for it! Be able to know what you need to look for! RSA ECAT is the unique solutions to be able to identify any type of attacks! Let’s detect malware like a pro!

Security practices and Data Protection: Tips to avoid a backdoor

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.

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
- Managing multiple security techniques
- Identifying backdoors from data protection solutions
- Implementing controls for each step of the data protection process
Experience the industry’s most realistic penetration testing, training and certifications. Taught by the core developers of Kali Linux, our information security training will immerse you into the deepend of real world penetration testing. We know penetration testing. Between Offensive Security Training, Kali Linux and the ExploitDatabase, you can trust that we have the expertise, knowledge and experience to provide you with high end penetration testing services. Offensive Security funds and develops several prominent information security niches, such as Kali Linux, the ExploitDatabase, Google Hacking Database and Metasploit Framework Unleashed (MSFU) free training.

World-class Cyber Security education for anyone, anywhere. Concise Courses is a leading speciality Cyber Security training company. As a business, we always aim to deliver what we promise. We work together, applying our expertise in advanced information security training solutions that are valued by our customers. We have operations in the United States and United Kingdom and have successfully offered training to over 15,000 Cyber Security professionals from over 50 countries.
Pentester Academy plans to revolutionize online infosec training by providing comprehensive, highly technical, hands-on courses at the most affordable price! Our dream of making infosec training affordable for everyone can only come true with your support!

Dalhousie University introduced the Master of Engineering (MEng) in Internetworking in 1997. Offered through the Faculties of Engineering and Graduate Studies, it's the world's longest running graduate program dedicated to Internetworking.
Travis Barlow
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. When he is not performing penetration testing, incident response or other security related work he enjoys multiple outdoor pursuits such as hunting, fishing, extreme winter survival camping and spending time with his son.

Andrew Kozma
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
Steve Quinn has been in the IT industry for 19+ years with a wide range of responsibilities. Being the Manager of Network Services, he is responsible for all aspects of the environment, including information security, infrastructure integrity and policy and procedure development. 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
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.

Scott Walsh
Scott Walsh currently works for an industry leading vulnerability assessment company. In addition to seeing new security exploits on a daily basis, he builds hardware and software projects to test, and sometimes break, digital and physical security.

Nick Gyorfi
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).
The Halifax Area Security Klatch (HASK), provides a forum for experts to encourage discussion and share expertise in understanding the latest trends and security threats facing computer networks, systems and data. Our membership includes Information Security practitioners, managers, network administrators, students, and anyone who is interesting in learning more about securing information. We meet at the Halifax Club in Halifax, Nova Scotia. Typically, we meet the last Monday of the month except for March, June, July, August, and December; unless otherwise notified.

ISACA Atlantic Provinces Chapter, with over 100 members, incorporates members from all Atlantic Canadian provinces including New Brunswick, Nova Scotia, Prince Edward Island and Newfoundland and Labrador. As a chapter of ISACA International, “our mission is to support enterprise objectives through the development, provision and promotion of research, standards, competencies and practices for the effective governance, control and assurance of information systems and auditing.”

The High Technology Crime Investigation Association (HTCIA) was formed to provide education and collaboration to our global members for the prevention and investigation of high tech crimes. As such, we are an organization that aspires to help all those in the high technology field by providing extensive information, education, collective partnerships, mutual member benefits, astute board leadership and professional management. The High Technology Crime Investigation Association is composed of 8 regions within the United States and 6 international regions, including Canada. The Atlantic Chapter is one of five chapters in the Canadian region. Internationally there are 38 chapters overall.
Thank you and see you next year!