Thank you for attending the 2015 Atlantic Security Conference.

This is our 5th year and we are proud of the quality and the content of this year’s presentations and its speakers. Whether you are in management, a techie or work with security professionals there is something here for everyone. The core philosophy of the Atlantic Security Conference is to educate and deliver relevant information on current trends, emerging threats and exploits within our ever changing and rapidly evolving industry.

We are exceptionally pleased to present what we consider to be well-rounded content; balanced between defensive security measures and current attacks and exploits. The conference drew a lot of international attention and we are excited to hear from the members of our community.

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. 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 old friends and make some new ones. We have some great prizes and a grand prize draw and we wish you the very best conference experience. Feel free to approach any of us with regards to content, we are always cooking up something and would love to hear your feedback.

~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.

Cisco delivers intelligent cybersecurity for the real world. This vision is based on a threat-centric approach to security that reduces complexity while providing superior visibility, continuous control, and advanced threat protection across the entire attack continuum. With this new security model organizations can act smarter and more quickly before, during, and after an attack.
## DAY 1 AGENDA

**Agenda – Day 1 – Thursday April 16, 2015**

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 - Room 200B</th>
<th>Track 2 - Room 200D</th>
<th>Track 3 - Room 200C</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00  AM</td>
<td><strong>Registration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:45  AM</td>
<td><strong>Opening Remarks &amp; Opening Keynote by Keren Elazari</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td><strong>Dave Lewis</strong> - SCADA Security: Stories From The Trenches</td>
<td><strong>Peter Scheffler</strong> - DDos Threat Landscape</td>
<td><strong>Peter Morin</strong> - “Where are the bad guys hiding?” – A Forensic Approach to Incident Response</td>
</tr>
<tr>
<td>10:45 AM</td>
<td><strong>Morning Break</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td><strong>Winston Morton</strong> - Security Best Practices – Cloud Based Network Function Virtualization</td>
<td><strong>Rick Vanover</strong> - Data protection and security: Don’t make this the back door</td>
<td><strong>Guillaume K Ross</strong> - iOS App Analytics VS Privacy: An analysis of the use of analytics</td>
</tr>
<tr>
<td>11:45 AM</td>
<td><strong>Catered Lunch sponsored by Mimir Networks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00 PM</td>
<td><strong>Jeremy Richards</strong> - Firmware Vulnerability Analysis</td>
<td><strong>Sylvain Levesque</strong> - Mobile Devices and BYOD Security: Deployment and Best Practices</td>
<td><strong>Aamir Lakhani</strong> - Gods and Monsters: A tale of the dark side of the web</td>
</tr>
<tr>
<td>2:00 PM</td>
<td><strong>Anna Manley</strong> - Mandatory Key Disclosure and Self Incrimination in Canada</td>
<td><strong>Dennis Moreau</strong> - Datacenter Security Improvements through Aggressive Network Virtualization</td>
<td><strong>Marc-André Bélanger</strong> - Why don’t they care? well.. until it’s too late..</td>
</tr>
<tr>
<td>2:45 PM</td>
<td><strong>Afternoon Break</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00 PM</td>
<td><strong>Julien Savoie</strong> - Attacking The Onion Router</td>
<td><strong>Andrew Caldwell</strong> - Let’s stop an attack!</td>
<td><strong>Gabriel Tremblay</strong> - Homemade vulnerabilities : How your most trusted resources will bring havoc to your digital dream</td>
</tr>
<tr>
<td>4:00 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 PM</td>
<td><strong>Closing Keynote by Kellman Meghu</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:00 PM</td>
<td><strong>Social Mixer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Speakers Dinner (Ticket Required)</strong></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.

Backed by IMP Group International, IMP Solutions is a leading IT company delivering a full suite of Professional Consulting Services, product sales, Cloud and Managed IT Services. IMP Group has gained a solid reputation internationally, and has achieved the prestigious Platinum status for six consecutive years as one of Canada’s 50 Best Managed Companies.

F5 Networks provides solutions for an application world. We help organizations successfully deliver applications to anyone, anywhere, at any time. The world’s largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends.

The Dell SonicWALL family of firewalls tightly integrates intrusion prevention, malware protection, and Application Intelligence and Control with real-time Visualization. The Dell SonicWALL Reassembly-Free Deep Packet Inspection engine scans 100% of traffic and massively scales to meet the needs of the most high-performance networks.

Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.
<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1 - Room 200B</th>
<th>Track 2 - Room 200D</th>
<th>Track 3 - Room 200C</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 AM</td>
<td>Opening Remarks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 AM</td>
<td><strong>Ksenia Dmitrieva</strong> - How to use Content Security Policy the right way</td>
<td><strong>Rick Dill</strong> - Are You Orchestrating Your Network Securely?</td>
<td><strong>Glen Roberts</strong> - Take Charge of Your Infosec Career!</td>
</tr>
<tr>
<td>10:45 AM</td>
<td>Morning Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 AM</td>
<td><strong>Colin O’Flynn</strong> - In Hardware We Trust</td>
<td><strong>Paul Madsen</strong> - The Two Sides of Mobile Identity</td>
<td><strong>Paul Halliday</strong> - Squirt - An open source web interface for Network/Enterprise Security Monitoring</td>
</tr>
<tr>
<td>11:45 AM</td>
<td>Catered Lunch sponsored by Mimir Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00 PM</td>
<td><strong>Ben Goodspeed</strong> - Formal Methods in Computer Security</td>
<td><strong>Predrag “Pez” Zivic</strong> - Ways to Protect From North Korea Hackers</td>
<td><strong>Daniel Merritt</strong> - Planning for Failure: An Introduction to Traffic Logging in Network Forensics</td>
</tr>
<tr>
<td>2:00 PM</td>
<td><strong>Luis Corrons</strong> - Operation Oil Tanker</td>
<td><strong>Henry Anzarouth</strong> - Protect What Matters: Guarding Against The Data Breach</td>
<td><strong>Milos Stojadinovic</strong> - More Data, Less Voodoo</td>
</tr>
<tr>
<td>2:45 PM</td>
<td>Afternoon Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00 PM</td>
<td><strong>David Shipley</strong> - How UNB is using policy, practice and technology to enhance cyber security</td>
<td><strong>Pascal Fortin</strong> - Weak Links in Cyber Security: Root Causes in the Real World</td>
<td><strong>Patrick LaRoche</strong> - Logs, Logs and more Logs</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>Closing Keynote - Matias Katz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 PM</td>
<td>Closing Remarks and Prize Draws</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Day 1 Opening Keynote Speaker

Keren Elazari

Keren Elazari brings years of experience in the international cyber security industry to the stage. Since 2000, Keren has worked with leading Israeli security firms, government organizations, Global Big 4 and Fortune 500 companies.

Keren holds a CISSP security certification, a BA in History and Philosophy of Science and is currently a senior research fellow with the prestigious Security & Technology workshop at Tel Aviv University.

In 2012, Keren held the position of Security Teaching Fellow with Singularity University, a private think tank, founded by Dr. Ray Kurzweil and sponsored by Google & NASA amongst others. Since 2013, Keren covers emerging security technologies and trends as a security industry analyst with GIGAOM research, a leading independent media hub.

In 2014, Keren became the first Israeli woman to be invited to speak at the prestigious international annual TED conference. Keren’s TED talk has been viewed by 1.2 million people, translated to more than 20 languages and selected for TED’s list of ‘Most Powerful Ideas in 2014’ and for Inc.com’s list of ‘Top TED Talks of 2014’.

Day 1 Closing Keynote Speaker

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.

Day 2 Closing Keynote Speaker

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!!
LogRhythm, the leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company’s patented and award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.
Marc-André Bélanger
Marc-André Bélanger has been in security since the end of the Y2K gold rush. He is currently acting as a Senior Risk Officer within the Insurance Industry and worked, throughout his career, in Retail and Banking. He accumulated extensive experience in Incident Management, computer and mobile forensics and IT risk mitigation. A serious fan of hacking games and contests, hardware hacking and lock picking. He currently holds certifications in Fraud (CFE), Physical Security (CPO), Pen-Testing (CEPT), and Information System Security (CISSP).

**Why don’t they care ? Well, until it’s too late...**
Every day, the news is making headlines with Cyber Security incidents and every now and then, a new world record is set. Data theft is going old school as organized crime are now leaving the low hanging fruits to the rookies and they are going back to good old cash. The first half of February has set light on both the biggest data breach of all times and the biggest Cyber bank heist, that is estimated at a billion dollars. As security experts, we are asked to assess those Risks and sometimes, the path between the actual technology exploit and the business impact is so far, that the message does not seem to reach.

Luis Corrons
Luis Corrons has been working in the security industry since 1999, specifically in the antivirus field. He is the Technical Director at PandaLabs, the malware research lab at Panda Security. Luis is a WildList reporter, member of the Board of Directors at AMTSO (Anti-Malware Testing Standards Organization) and member of the Board of Directors at MUTE (Malicious URLs Tracking and Exchange). He is also a top rated industry speaker at events like Virus Bulletin, HackInTheBox, APWG, AVAR, M3AWG, Security BSides, etc.

**Operation Oil Tanker**
In the latest years we have seen how Advanced Persistent Threats (APTs) work, targeting high profile victims from strategic sectors. Some of them are clearly state sponsored attacks, with a lot of funding behind, which explains the “Advanced” in the APT acronym. However this is not always the case, and in this talk I will show you the new APT evolution, known as RPT.

RPT is a new approach to this kind of attacks, apparently capable of circumvent most of the defenses we have in place, while it keeps its ability to be persistent and a real threat. I will illustrate this RPT with a real case discovered in 2014, which is still under investigation by LEA. This attack is targeting different organizations from different countries around the world, mainly from Asia and Europe, and all of them work in the same field. We will analyze the attack, the targets, and the final goal of this RPT. And of course, what is hidden behind the mysterious ‘R’.

Ksenia Dmitrieva
Ksenia Dmitrieva is a Senior Security Consultant at Cigital with over six years of experience developing and securing web applications. As a Senior Consultant, Ksenia helped clients in financial services, entertainment, and telecommunications to implement security programs, assess and secure their applications. She performs penetration testing and code reviews focusing on web applications, web services, new web technologies and frameworks. Ksenia often delivers training sessions and has previously presented at Nullcon, BSides Security London, and LASCON.

**How to use Content Security Policy the right way**
Content Security Policy is a new HTML5 technology that provides a novel approach to fixing XSS. With CSP, if you keep dynamic data and static code separate on your site, and the conforming browsers enforce the policy to ensure that the
data never gets interpreted as code. The intricacies of the technology are in how CSP policies are combined and what limitations they place on web development. Although the first version of CSP wasn’t widely adopted, the new version brings features that should yield faster adoption rates and better protected websites. Several leading companies are successfully using CSP to protect their sites and monitor attack. What can we learn from these implementations?

**Aamir Lakhani**

Aamir Lakhani is a cyber security researcher and practitioner with Fortinet and FortiGuard Labs, with over 10 years of experience in the security industry. He is responsible to provide IT security solutions to major commercial and federal enterprise organizations. Lakhani has designed cyber solutions for defense and intelligence agencies, and has assisted organizations in defending themselves from active strike back attacks perpetrated by underground cyber groups. Lakhani is considered an industry leader in support of detailed architectural engagements and projects on topics related to cyber defense, mobile application threats, malware and advanced persistent threat (APT) research.

In its recent list of 46 Federal Technology Experts to Follow on Twitter, FedTech magazine described Aamir Lakhani as “a blogger, infosec specialist, super hero...and all around good guy.” Lakhani runs blog, DrChaos.com which was ranked as a leading source for cyber security by FedTech Magazine. Additionally, he is a published author, has been featured on Federal News Radio. His books include best sellers such as Web Penetration Testing with Kali Linux, XenMobile MDM, and Pentesting with Kali Linux on Raspberry Pi.

**Gods and Monsters: A tale of the of the dark side of the web**

Researcher and Security strategist, Aamir Lakhani (known as Doctor Chaos) will dive in the hidden and shadowy world of the Deep Web.

He will demonstrate how easy it is to get Deep Web thru proxies and the Tor network. He will explore that despite recent takedowns by law-enforcement, how easy it is to find service brokers weapons, drugs, and other questionable services.

The talk will showcase interaction with real attackers using techniques around malware, zero-day attacks, and social engineering to attack organizations. Learn how attackers plan sophisticated attacks to infiltrate organizations and steal intellectual property.

Aamir Lakhani will conclude by showcasing cutting research in cyber security that may be able to mitigate some of these risks. This includes advances in threat research, open intelligence, and big data.

**Dave Lewis**

Dave Lewis has almost two decades of 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. Dave writes a column for CSO Online and Forbes.

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’.

**SCADA Security: Stories From The Trenches**

A discussion about SCADA security and critical infrastructure with stories pulled from personal experience.
INFOSEC TRACK

SPEAKERS

**Rafal Los**
Rafal Los, Director of Solutions Research and Development within the Accuvant Office of the CISO, leads a team developing research-backed guidance addressing key program challenges for enterprise security leaders. His team brings together diverse, researched perspectives to develop strategy guidance coupled with maturity and operational models from leading practices to drive meaningful security program action.

**Losing Battles, Winning Wars -- Frustrating Adversaries with Threat Intelligence**
When it comes to intrusions and breaches, most companies take a short-game view. This means that they look at events as discrete and individual, when in reality many are part of an ongoing campaign. While not universally detrimental, this view does harm the overall security of an organization in the “long game”. This talk focuses on how incident responders can utilize atomic indicators together with strategic threat intelligence to frustrate adversaries and win.

**Ben Goodspeed**
Ben Goodspeed is a Software developer, specialized in TDD, Ruby and Idris, Academic and hobby security researcher, BCSc (2005) and Certified Scrum Master since 2012. Currently running an IT consultancy while pursuing an MSc.

**Formal Methods in Computer Security**
How have we used formal mathematical methods in security research? The idea of bringing the certainty of mathematical proof to security is an alluring concept. Research has been undertaken in this area since the 1970s, starting with the landmark work by Bell and LaPadula. Some formalizations have found success, improving security and changing the way we think about secure systems, but, we still haven’t closed all the gaps. Why is that, and can we do better using different mathematical tools? In this presentation we will look at the way we’ve used math to formalize the meaning of security, how it changes depending on the context (like operating systems, cryptography, and programming languages), and the limitations of formalism. From there, we’ll examine where the gaps were in many of these formulations, and what can be done to reduce and even eliminate some of these gaps. Finally, we’ll wrap up with a discussion on the way we can use new tools developed for mathematical research to bring further assurance of security.

**Paul Halliday**
Paul Halliday began work on squert in 2006; the first incarnation a quick hack so that he could access IDS alert data via a web browser. While initially intended as a simple event viewer it has slowly evolved into a usable and feature rich event driven console for the Suricata (or Snort) Intrusion Detection system and the Bro Network security Monitor. It is available for free on Github and can also be found on the popular Security Onion Linux distribution. It has been featured in Richard Bejtlich’s book “The Practice of Network Security Monitoring” and is also covered in most talks on Security Onion.

**Squert - An open source web interface for Network/Enterprise Security Monitoring**
This session will introduce squert and its capabilities and future path. It will also describe how it is used by the Nova Scotia Community College (NSCC) to detect and respond to threats.
Patrick LaRoche
Patrick LaRoche is a Co-founder of topLog, a Halifax based start-up that focuses on getting useful information out of application level logs, helping customers detect anomalies in their platforms before the customer feels it. Patrick has a Master’s degree in Computer Science (and moments away from PhD) where his focus has been on privacy and security. Patrick also spent the required amount of time being a mediocre penetration tester, security analyst and consultant, working with some of the Atlantic region’s top IT firms.

Logs, Logs and more Logs
Today’s tools and platforms for logging and log analysis have come a long way since syslog and rsyslog, but they haven’t solved all issues. In this presentation I will be showing live examples of building up an ELK stack (elastic search, logstash and Elastic Search) as well as talking about the pros and cons of such deployments. I’ll also speak about where we go once we have all our logs in one place, how we can become pro-active using log data instead of being simply re-active.
Attendees will be encouraged to try out the live demo during the talk, but not required. Having Vagrant and VirtualBox previously installed on their laptops would help if they want to follow along.

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.

Mandatory Key Disclosure and Self Incrimination in Canada
You’ve been lawfully arrested. The police have lawfully seized your computers. You’ve encrypted some or all of your data. Can the police legally compel you to provide the encryption key? Sections 11(c) and 13 of the Charter of Rights and Freedoms cover non-compellability and privilege against self-incrimination; however Canadian courts have yet to grapple with the issue of mandatory key disclosure on a constitutional level. When can a person be required to provide authorities with an encryption key? By what mechanism?

Daniel Merritt
Daniel Merritt is Chief Technology Officer at Mirmir Inc., a company based out of Cape Breton working on developing innovative network security solutions. With over fifteen years in the computer industry, he has worked on diverse products across the financial, security, manufacturing and networking sectors. He has degrees in neuroscience, botany, mathematics and philosophy.

Planning for Failure: An Introduction to Traffic Logging in Network Forensics
Sound network security practices can significantly reduce the risk of compromised hardware, but 0-Day Attacks, social engineering, inside attacks and simple human weakness all ensure that even the most secure network will eventually experience compromise. Determining the extent, origin and vector of the compromise are key to preventing future attacks, but doing this accurately can be a significant challenge for network security professionals, both because logs on compromised machines cannot be relied on and because some of the most crucial information generally isn’t logged.
In this talk, we will outline the value that accurate and detailed forensics offer to security professionals, review the
challenges that have historically hindered efforts to perform forensics, describe how full traffic logging addresses these challenges, and explain where it fits into an organization’s overall security plan. The differences between full traffic logging and traditional, low-resolution approaches like NetFlow and IPFIX will be reviewed, as well as important considerations when determining capacity and scope of capture on a network. Case studies of famous attacks will be used to illustrate the role of traffic logging in network forensics.

Peter Morin
Peter Morin is a Senior Information Security Specialist with Bell Aliant. His position focuses on information security risk management, penetration testing, cyber threat response, application code analysis, malware analysis, and computer forensics. Peter has over 18 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. Prior to Bell Aliant, Peter has held positions with KPMG LLP and Ernst & Young LLP as Senior Manager in their IT Security, Risk Advisory & Forensic practices, as well as worked with numerous tech start-up companies and various government and military agencies. 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, DEFCON, 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 publications including SC Magazine. Peter sits on numerous executive boards including the High Technology Crime Investigation Association International Board of Directors, HTCIA International Conference, ISC2, and ISACA - Atlantic Provinces Chapter. Peter holds numerous security-related designations including the CISSP, CISA, CGEIT, CRISC, and GCFA.

“Where are the bad guys hiding?” – A Forensic Approach to Incident Response
Our networks and systems are under siege by attackers more now than ever. What a scary time to be a systems administrator, application owner or CEO. Organizations are looking everywhere for solutions to assist them in identifying threats on their networks and the real-time knowledge on when and how to respond to incidents. This presentation will introduce the audience to some of the popular incident response processes, the concept of indicators of compromise and specific forensics tips and tricks that organizations can use to identify possible attacks and breaches of their networks and applications.
This presentation will also walk through some real-world examples such as the Target breach and show the audience some valuable indicators of compromise, techniques and tools that could be used to identify and suppress these attacks.

Winston Morton
Winston Morton has more than fifteen years of experience in senior technology roles for telecommunications, data center, Internet security and cloud services companies varying in size from start-up to Fortune 500. Winston is the founder of Nuviser which specializes in cloud acceleration programs. Previous to Nuviser, Winston was the Vice President of Technology with LinkBermuda, an International telecommunications firm, where he lead the deployment of a cloud services platform focused on the re-insurance and financial industries. He is passionate about driving corporate growth and efficiency through the use of cloud technologies. As an enthusiastic mentor and coach, Winston regularly speaks at industry events and sits on various advisory boards.

Security Best Practices – Cloud Based Network Function Virtualization
With the advent of self-service cloud stacks, a tremendous amount of flexibility has been derived from virtualizing
and automating networking capabilities. Network Function Virtualization (NFV) provides cloud administrators the ability to deploy network based services in real-time such as virtual switches, firewalls, and virtual private networks making these services a key component the deployment of cloud services. In many cases the NFV creates a number of challenges using the traditional network security tools we use to aid in Intrusion Prevention, Incident Response, and ongoing Network Audit requirements but when used effectively, NFV can also be a powerful tool in the hands of a knowledgeable security administrator. This presentation explores best practices that help Security Administrators address security and privacy using NFV in the Cloud.

**Mark Nunnikhoven**

Mark Nunnikhoven focuses on helping organizations as they move from the data centre to hybrid environments to working fully in the cloud. Bringing over 15 years of practical experience to the table, he is regularly sought after to speak on cloud computing, usable security systems, and modernizing security practices.

**Whodunit? : The mechanics of attack attribution**

With all the press around attacks and the hype about North Korea in the Sony case, the time is right for a candid discussion on attack attribution. This talk would not only have broad appeal (_everyone’s_ heard about NK + Sony) but also be an eye opener for most. I honestly don’t think the majority of security practitioners (let alone the rest of IT folks) truly understand how difficult it is to attribute an attack to meet any sort of legal case standards. More importantly is it even worth doing?

**Colin O’Flynn**

Colin O’Flynn is pursuing a PhD in embedded hardware security, and as part of this work has designed the open-source ChipWhisperer project. This project won second place in the Hack-a-day Prize 2014 and has been presented widely at everything from Blackhat USA/EU/Abu Dhabi to a number of academic conferences.

**In Hardware We Trust**

Attacking hardware devices might be easier than you expect – this presentation details some attacks against hardware platforms, including attacks capable of breaking ‘military-grade encryption’ using nothing but a laptop and a few hundred dollars of equipment. Whether you design embedded hardware, architect systems with secure hardware, or are simply an end user of Internet of Things (IoT) technology, this presentation promises to make you question how secure hardware devices really are.

This presentation details not only the technical workings of side-channel power analysis and glitching attacks, but also how they apply to real systems, and what this means to those designing those systems. All the tools used in this presentation are open-source, giving attendees the ability to dive into more details and try their hand at power analysis and glitching attacks.

**Jeremy Richards**

Jeremy Richards is a vulnerability researcher for SAINT Corporation - performing research and uncovering weaknesses in a variety of technologies, and developing security software professionally for nearly a decade. These days he spends his time writing remote unauthenticated vulnerability checks by reverse engineering changes introduced by security patches and identifying the root cause. Jeremy has recently started developing a framework to extract data from firmware images and perform automated analysis. His research in this area has uncovered a compelling number of undocumented risks that impact a large number of devices and user environments.
Firmware Vulnerability Analysis

Bad code is everywhere and the tools to dig it up are maturing at an astonishing rate. The day of reckoning has come for device manufacturers who have neglected the adoption of secure development practices. Join us as we dive into firmware updates for many different devices and uncover undocumented ‘recovery features’ (backdoors), hardcoded accounts, direct url access/permissions issues and buffer overflows.

This presentation will discuss bindiff for automated extraction and dd to carve useful data out of firmware files manually. We use IDA to dive deep and analyze MIPS ELF binaries. We use QEMU to emulate processes remote debug in IDA with GDB.

Glen Roberts
Glen Roberts, CISSP is the CEO of Charlotte Cybersecurity, Inc. and the Host of the Hackers On Fire Podcast. He is on a mission to encourage more people to enter the information security field and help those who are already there to advance in their careers. He has interviewed dozens of information security professionals for the weekly podcast in which guests share their stories and lessons learned with the audience.

Take Charge of Your Infosec Career!
You spent $5,000, a plane trip, a hotel and a full workweek on your last infosec course but when was the last time you invested even just a few hours of your time exclusively to developing your infosec career in a truly meaningful way? This talk will challenge the way you view your career and give you actionable steps for taking charge of your information security career to optimize the rewards and fulfillment you receive from your work. Glen will leverage the stories and best practices from dozens of information security professionals to help inspire your infosec career journey. This presentation will be engaging and speak to the soul in a way that instills ownership of your own career and generates a passion for finding and carving out your own authentic career path.

Guillaume K Ross
Guillaume K Ross is a Senior Security Consultant in Rapid7 Strategic Services. With over 10 years of experience in security and IT, in verticals such as finance, mining, education, engineering, and services, he provides expert advice, helping customers define a program that fits their needs and meets their unique objectives. In the last year, he presented research on iOS URL Schemes, premiered at AtlSecCon, which resulted in multiple security fixes by vendors such as Apple and Twitter.

iOS App Analytics VS Privacy: An analysis of the use of analytics
As developers attempt to tailor their applications to customers, obtain more information about how they are used and how reliable they are, the use of app analytics services on mobile devices is now very common. During this talk, we will look at the usage patterns of analytics services by the most popular apps in various categories, such as games and productivity applications, as well as different application business models (free, freemium, paid, etc.).

What does it all mean for your privacy? Can you prevent it? What types of apps are the greatest offenders? How can you detect it?
These are questions we will answer, as we look at the patterns, the analytics providers used, and explore the type of data that is sent as well as the privacy policies of these analytics service providers.
Julien Savoie
Julien Savoie was born in Oxford England and brings a combined 15 years of work experience in IT, in various sectors including government, academic and private. A graduate of UNB’s computer science program, he has worked in Boston, Ottawa, and Curacao. His core competencies include coding, networking, and cryptography. He currently works in Halifax, Nova Scotia.

Attacking The Onion Router
With much talk about “the darkweb” in the media of late, we attempt to cut through the hype and answer some basic questions. What is Tor? How does it work? What are some of the attacks that have been effective against it? What areas need work? And fundamentally, how well does it stand up in a post-Snowden revelations world?

David Shipley
David Shipley is a member of the IT Security team at the University of New Brunswick. He is responsible for monitoring UNB’s networks and systems, responding to incidents and assisting in long-term security strategy and planning. David also assists with user education and behaviour change.

How UNB is using policy, practice and technology to enhance cyber security
Universities are among the highest risk targets for cyber threats due to their nature as places that promote the exchange of information. Encouraging and helping 10 000+ minds to collaborate and research on a range of topics is a challenging mission for any IT organization. Having to secure that environment is even tougher.
The University of New Brunswick’s IT Security Action Team faces a range of threats on a daily basis. From hactivists to denial of service (DDoS) attacks, from target intrusions to trying to handle the daily deluge of malicious software, this team has seen it all.
In this talk, UNB’s David Shipley will discuss the team’s approach to securing this vibrant environment while helping the University achieve it’s educational and research objectives.
With that foundation in place, David will discuss how UNB put in place a monitoring practice that helps the team efficiently manage their incident response process. This provides the team with the visibility they need to see what’s happening on their networks and the threat intelligence they need to properly react.
By using the right combination of technology and processes, the team at UNB has managed to strike the right balance between reactive and proactive security. This talk will highlight the techniques they used so you can do the same.

Milos Stojadinovic
Milos Stojadinovic is currently employed as Red Team lead at NCI. His primary focuses are on red teeming, penetration testing, and other offense geared services. He holds a bachelors degree in information sciences (specializing in information security) and teaches part time at Sheridan college. Milos also spends time consulting in the payment card industry and risk assessment space. In his free time, Milos enjoys working on offense related research projects, continuous expansion of his infosec knowledge, generally being pretty awesome, and cramming more horsepower in his car.

More Data, Less Voodoo
The infosec industry is maturing, and with it, the old school reliance on ‘common knowledge’ and ‘best practices’ no longer makes the cut. There is a serious need to employ data analytics within information security programs to drive
real world measurement of the programs efficacy. This talk delves in to forgoing the old school voodoo approach ('trust me - I have a beard') and discusses real world metrics that help an organization understand their ability to see what is going on in their network, withstand attack, and react to inevitable breach. The metrics discussed are largely derived from the Critical Security Controls, originally created by SANS. The goal of this talk is to get people thinking about how they can measure the performance of their information security program (using repeatable metrics) in order to determine what changes will have meaningful and valuable impact.

Gabriel Tremblay
Gabriel Tremblay is the CEO of Delve Labs, inc. and head of Northsec in Montreal. After spending many year as a highly specialized freelance pentester he now works with Delve Labs to the creation of intelligent next-generation security solutions. As the head of Northsec, Gabriel also invests a lot of his time to make sure Montreal keeps it’s vibrant security community alive and well trained. He is also quite funny.

Homemade vulnerabilities : How your most trusted resources will bring havoc to your digital dream
While most high profile security bugs such as Heartbleed and Apple’s famous dual goto can cause tremendous harm to your organization, most of them will come with an official fix in the next hours following their release. However, when the security vulnerabilities are inserted in your systems by your own developers or sysadmins they can be exploited for months without raising an alarm. This talk will focus on some pervasive bugs that tends to pop everywhere in the industry these days. We will see how bad PRNG usage, leftover files, incorrect use of strong cryptography and more will usually be found and exploited by criminals and how organizations can detect those hard to spot vulnerabilities over time.
Henry Anzarouth

Henry Anzarouth is an information security technical sales engineer. He has more than 25 years of professional experience in the software industry representing companies that include Lotus, IBM, iPlanet/Netscape, Sun Microsystems, Oracle and currently Vormetric. In his role he has worked with organizations and partners of all sizes and industries to deliver Web, identity, and security solutions that match their business needs. He holds a degree in Economics and Computer Science from McGill University and is a Certified Information Systems Security Professional.

Protect What Matters: Guarding Against The Data Breach

Perimeter security and physical security are ineffective during advanced persistent threats, especially when your data is everywhere. We will explore how (to use Vormetric) to protect your data from unauthorized administrative accesses including insider threat and external cybercrime. We will see how you can do this in a way that is transparent yet centralized to all your applications, databases, platforms and business processes.

Frank Breil has a Bachelor of Commerce with Distinction from Concordia University. He has been involved in technology sales and sales management for over 25 years in areas such as hardware, application software, 4GL programming languages and CASE tools and business intelligence. Frank has been in network security for the past 8 years and was formerly employed with Fortinet and is now working for INSA.

Frank Breil

Frank Breil has a Bachelor of Commerce with Distinction from Concordia University. He has been involved in technology sales and sales management for over 25 years in areas such as hardware, application software, 4GL programming languages and CASE tools and business intelligence. Frank has been in network security for the past 8 years and was formerly employed with Fortinet and is now working for INSA.

Andrew Caldwell

Andrew Caldwell, CISSP, P. Eng. Trend Micro consultant and sales engineer for Canadian Government and Atlantic Canada. Born and raised in New Brunswick and a graduate of UNB, Andrew has 15 years of diverse IT and software experience covering many complex implementations of security solutions for small, medium and large enterprise customers and governments globally. Andrew held roles previously at IBM, Blackberry and TITUS with extensive pre-sales and post-sales technical support and consulting. With Trend Micro, Andrew helps solve customer’s evolving security and compliance issues.

Let’s stop an attack!

A one of a kind highly interactive session where the audience will participate in stopping a targeted attack. Everyone will have to balance pressures of budget, time and career. Choose badly, and, well,
let's just say things don’t go so well. Technology experience not required.
You’ll learn:
1) How to cut through the noise and hubbub of the “targeted attacked” lingo,
2) How easy it is to be a victim,
3) New considerations on protecting your organization without breaking the bank.

Rick Dill
As a Security Sales Engineer for Tufin, Rick Dill supports New England and Canada pre-sales efforts where he continues to forge cooperative working relationships as well as identify and formulate strategic revenue-generating partnerships. Rick is a well accomplished sales engineer with over 15 years of demonstrated success in leading start-ups and driving fast-track growth of high-technology companies.

Are You Orchestrating Your Network Securely?
Enterprises are being held more accountable for cyber-threats aimed at today’s complex, heterogeneous environments. In this session we will show how IT decision-makers can meet challenges for business continuity and agility like implementing network changes securely in minutes and proactively analyze risks associated with network changes prior to the actual change.

Russ Doucet
Russ Doucet is a highly proficient and experienced installer and trainer for Fortigate UTM firewalls and other perimeter security and network forensic products. He has been awarded the Fortinet Xtreme Team Canada 2012 Xtreme Engineer for the National Capital Region “In Recognition of Technical Excellence and Outstanding Individual Contribution”. Additionally Russ is a court recognized computer expert providing forensics and consulting to lawyers on criminal and civil cases.

Targeted Attacks: From Visibility to Action
Gartner has predicted that we will soon live ‘in a state of constant compromise’ and that, due to the success rate of targeted attacks and stealthy malware, security spending will shift dramatically from prevention to investigation and remediation. Increasingly, when malicious code reaches an endpoint, that endpoint will be compromised with potentially severe consequences. With internet-connected devices growing from 11 billion to 50 billion between now and 2020, and most of those devices being BYOD or internet-connected devices such as cameras and smart TV’s, security specialists will be faced with the additional challenges of either not being allowed to force an agent onto a device or dealing with devices that simply cannot support the overhead of an agent.
At INSA’s Targeted Attacks: From Visibility to Action presentation, we will discuss how targeted attacks bypass your firewall, IPS, secure gateway and endpoint antivirus, and manage to evade detection throughout the life-cycle of an attack. We will also discuss approaches to increasing visibility into network traffic across all vectors, with specialized tools that will give visibility into targeted attacks whether they be directed via internet traffic, email or file transfers and how you can leverage this visibility into an enhanced security posture.
Pascal Fortin
Pascal Fortin joined GoSecure in 2004 with the mandate to build a world-class engineering and consulting team and when faced with a management crisis, he stepped up to being president of the company in 2008. Still very active in the field, he provides services as an Information Security and Risk Management Senior Advisor to clients of all business sectors. He has made recent contributions in various national speaking engagements for organizations such as the IIA, Government and private events like GoSec.

Weak Links in Cyber Security: Root Causes in the Real World
The InfoSec field has never had this much executive attention, increased budgets, more security technologies than ever, increased compliance requirements, and nearly 10 times more security focused professionals than at the beginning of the millennium. So why are cyber-attacks still so successful today?
This session presents the ugly face of the way Cyber Security is handled in most organizations, private and public, and why even the big spenders are exposed to much more risk than they believe. A look into the root causes, and some insights into a better future.
Will it take a catastrophic event before real change happens?

Sylvain Levesque
Sylvain Levesque works as a Security Consulting Systems Engineer for Cisco Systems in Canada. A veteran in the Security and IT industry with more than 19 years of experience, he helps customers define security architectures to address their governance, risk management and compliance goals. He holds a computer engineering degree as well as the CISSP and CISM certifications.

Mobile Devices and BYOD Security: Deployment and Best Practices
This session will cover security aspects surrounding the deployment of corporate devices and mobile devices such as smartphones and tablets in a corporate network and their inter-working with network security solutions. Subjects covered will include 802.1x and certificate deployment, VPN and remote access, corporate vs BYOD device differentiation and access control, profiling, posture, web security, MDMs and others.

Paul Madsen
Paul Madsen is a Principal Technical Architect within the Office of the CTO at Ping Identity. He has participated in various design, chairing, editing, and education roles for a number of identity standards, including OASIS SAML, the Simple Cloud Identity Management (SCIM), OAuth 2.0, and TV Everywhere. He holds an M.Sc. in Applied Mathematics and a Ph.D. in Theoretical Physics from Carleton University and the University of Western Ontario respectively.
The Two Sides of Mobile Identity

Mobile identity refers both to using devices to access applications as well as using devices to facilitate user authentication. Identity standards like OAuth 2.0 and Opened Connect 1.0 enable mobile devices as an important application access channels. Emerging standards like FIDO, as well as mobile 2-factor solutions, can enable devices as a powerful authentication factor. We’ll examine how enterprises can build a scalable & secure mobile identity architecture around these standards.

Dennis Moreau

Dennis Moreau is a Senior Engineering Architect at VMware, working on leveraging micro-segmentation and virtualization, to realize highly resilient, scalable, adaptive security, in software defined data centers. 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 over than 35 years of 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 Computer and Computational Sciences. His research has been sponsored by the National Aeronautics and Space Administration, 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.

Datacenter Security Improvements through Aggressive Network Virtualization

A number of recent security innovations have shown great promise for improving security posture, system defense and the fundamental resilience of datacenters (e.g. behavioral analytics, model-based analytics, application centered policy, moving target defenses …). However deploying and maintaining adequate security instrumentation, to provide the requisite east-west isolation and visibility, remains a daunting challenge. The growing deployment of software defined networks/network virtualization (SDN/NV) and network feature virtualization (NFV) capabilities, in software defined datacenters, is laying the foundation for capitalizing on these promises. This session will demonstrate, with concrete examples, how aggressively micro-segmenting a datacenter network topology, using NV and NFV, enables a) the realization of granular/distributed “default deny” security postures, b) tightly aligned security policy across control technologies, c) more actionable mitigation context, d) better signal to noise ratios for security analytics approaches, e) recon and lateral movement inhibition, and f) new mechanisms for achieving service resilience.
Peter Scheffler
Peter Scheffler has over 25 years of experience in the software industry with nearly another 10 years as an amateur programmer. Peter has spent the last 15 years in the world of web application development and application security. As an independent consultant, Peter spent time developing solutions for securing network and application access for Fortune 1000 and security conscious government organizations. Peter currently works with F5 Networks as a Field Sales Engineer where he acts as Lead for the Web Application Firewall SME Team, interfacing with Product Development and Product Management for new features and enhancements.

DDoS Threat Landscape
Urban Dictionary defines a DDoS Attack as: Distributed Denial-Of-Service: Form of electronic attack involving multiple computers, which send repeated HTTP requests or pings to a server to load it down and render it inaccessible for a period of time. Often used by freedom fighters on the Internet, usually attacking the systems of greedy corporations who want to sacrifice YOUR freedom for their profits.
But what does it mean to you, this surely is only an issue for those Big Guys on the web, right? Why should you worry about them, no one is interested in taking you down, right? Wrong… DDoS attacks are a real threat to your web presence and your business. Whether you have an ecommerce site or your users access corporate apps remotely, your internet presence has now become your business lifeline and there are people out there right now trolling for places to hit – and to even sell the info they find to those that are interested.
Come and learn about the DDoS threat landscape for the rest of us – not just for those web monsters and huge banks. Together, we’ll investigate the threats out there, look at some interesting tools and sites that can show you what’s happening and finally F5 Networks offers a broad spectrum of software, hardware and services to mitigate these growing threats.”

Rick Vanover
Rick Vanover is a Product Strategy Specialist for Veeam. Rick’s passion for challenges led to his commitment to educate and communicate at all levels—engaging those new to virtualization as well as those who are experts. As a popular blogger, podcaster and active member of the virtualization community, Rick builds relationships and spreads excitement about Veeam solutions. Before becoming the “go-to” guy for virtualization questions, Rick was in system administration and IT management. His certifications and designations include MCITP, Cisco Champion, vExpert and VCP.

Data protection and security: Don’t make this the back door
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

Predrag “Pez” Zivic
Predrag “Pez” Zivic has over the past 26 plus years of his security career, Pez has been working for Global Fortune 1000 clients as a senior adviser on security, risk and governance. Predrag’s expertise in business technology, security and risk methodologies, security investigation, has a proven track record with Global 1000 clients executing on many large multi-million dollars projects. He successfully launched and managed security groups at Scienton, Secure-IT, GE Capital and Platinum Technology. Pez is currently working at F5 on development of worldwide enterprise, data center and cloud security solutions.

Ways to Protect From North Korea Hackers
Recently, there was a huge number malware based attacks and hacks. It is obvious that information technology do not invest in appropriate controls to prevent, detect and stop hack and malware attacks. This presentation will analyze today’s protection of existing infrastructure and it will show how today’s protection fares against recent malware attacks. Presentation will analyze malware attacks including ones that happened recently to JPMC, Sony, Tricare and Target. Analysis of these malware tools has been conducted using personal and industry research. Research work will focus on malware infection mechanisms and malware self-protection mechanisms. Going through attack chain, presentation will show malware family of protection mechanisms. Using summary of common malware infection mechanisms, this presentation will present two new additional protection mechanisms that can add value in fight against malware. The goal of the presentation is to show complete environment of hacking and malware attack protection and detection mechanisms. Attendees will learn about common malware spreading mechanisms and learn about new protection mechanisms. This information will enable attendees to use more control in fighting against hacking and malware.
45 Drives offers the most customizable, affordable large-storage solutions on the planet with the Storinator™ line of professional-grade storage pods. From our whisper-quiet Q30 model to the original fully-featured S45 and the ultra-large XL60, there’s a Storinator™ to fit your unique storage needs.
SPEAKERS

EDUCATIONAL SPONSORS

Pentester Academy
a SecurityTube.net initiative

The Hacker Academy
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 manages more than just servers in his current position as Manager of Network Services at Health Association Nova Scotia. As a professional of more than 15+ years in IT, Steve has experience ranging from direct front-line care to back-end and departmental management. As a self-professed generalist, he has had to develop a broad skill-set dealing with clients that range from highly technical to non-computer users. This perspective gives him the ability to look at problems from many angles in the search of solutions both from a technical and ‘big picture’ perspective.
Darryl MacLeod
Darryl MacLeod is a 15 year veteran of the Atlantic Canadian IT community and works for NCI Secured Intelligence as a Senior Security Consultant. He is the founder of the Cape Breton Technology Users Group and the 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 New Security Model

The New Security Model means accounting for the entire attack continuum, Before, During, and After™ an attack.

A CONTINUOUS SECURITY PROCESS TO RESPOND TO CONTINUOUS CHANGE
It’s When, Not If.

LogRhythm’s Security Intelligence Platform unifies SIEM, log management, file integrity monitoring, network forensics & host forensics to help detect and respond to breaches and the most sophisticated cyber threats – faster and with greater accuracy than ever.

To learn more or schedule a demo, visit www.LogRhythm.com

Nothing compares to the security demands of the Department of National Defense. As a principal contractor for DND and the Royal Canadian Air Force, securing data is ingrained in the DNA of IMP Group. IMP Solutions, a division of IMP Group, delivers secure cloud and managed IT services to some of the most influential organizations in Atlantic Canada. Our clients trust our technical experience and security level clearance to ensure that their networks are proactively managed and secure. As cloud services continue to become the new standard in IT, clients of IMP Solutions depend on our knowledge to align cloud services that provide maximum efficiencies for their business, while minimizing risk.

If you would like to explore how cloud and managed IT services could benefit your business, contact us today to arrange a no obligation consultation. Managed.services@impsolutions.com
Thank you and see you next year!