CYBER SECURITY
FOR OIL AND GAS
CANADA

January 27-28, 2015 • The Westin Calgary, Calgary, Alberta, CA

Building the Foundation for Advanced Information & Cyber Security Practices

Featuring, industry user-led, in-depth discussions on security best practices such as:

Craig Coughlan
Supervisor Incident Response
Threat Assessment
Enbridge

Review case studies of the benefit threat intelligence can drive to your security operations

Hani Mansi
Director, Risk & Information Security
ATCO

Information security program maturation, planning and implementation strategy

Staff Sergeant Ryan Jepson
Electronic Surveillance Unit
Calgary Police Service

Senior Constable Shafik Punja
Technological Crimes Team (TCT)
Calgary Police Service

Sgt Corey Dayley
Cybercrime Support Team (CST)
Calgary Police Service

Development of a digital forensics team and reviewing the means to start, develop process & protocols, team oversight and the technical details of enacting digital forensic analysis in your organization

Zoltan Palmai
Team Lead, Network Security -
Security & Access Operations IRSM
Chevron

Management of joint ventures and vendor partnerships to ensure security protocols are adhered to and network connections are secured across the supply chain

Chris Shipp
CISO
Fluor Federal Petroleum Operations

Management of joint ventures and vendor partnerships to ensure security protocols are adhered to and network connections are secured across the supply chain

"Excellent conference to bring oil and gas industry together and share cyber security issues and solutions" – Patrick McNallen, Vice President, **Elbit Systems**

Top Benefits of Attending:

- Access an intimate industry forum to discuss the most effective strategies to harden your information/cyber security practices

- Develop knowledge of industry trends for the implementation of cyber defense, incident response, risk management, governance & forensics plans

- Identify advances in global cyber threat trends, vulnerabilities, outlets for support and best of breed solution providers/partners to ensure development of your security practices

- Expand your network of industry contacts to create potential opportunities for secure threat intelligence sharing

- Interface with government agencies and regulatory experts for assurance on your GRC plans

Connect With Us:

REGISTER TODAY! www.cybersecurityoilgas.com • 1-800-882-8684 • enquiryiqpc@iqpc.com

CYBER SECURITY
FOR OIL AND GAS
CANADA

January 27-28, 2015 • The Westin Calgary, Calgary, Alberta, CA

Dear Executive,

As part of critical infrastructure, the oil & gas industry has developed a rather large target for international cyber criminals and malicious actors looking to cause disruption. The Canadian industry in particular, as region of significant growth and new high-level opportunity, has begun to attract an increased level of targeted and probing cyber-attacks. As the attack surface of oil & gas organizations continues to widen in the digital oilfield age and with the propagation of personal device programs, can you identify the most vulnerable threat vectors in your network? Do you feel confident that your organization is equipped with the proper intelligence & operational capability to address the next level of rapidly advancing cyber threats in the wild?

With the proliferation of state sponsored hacking groups and established botnets perpetrating thousands of attacks on Canadian companies on a daily basis the time to take action on cyber security is upon us. The Canadian oil & gas industry will need to **keep up with cyber attack advancements in the present** to capitalize on the chance to continue to **provide valuable support for the business and enable growth opportunities.** The challenge is huge to be able to deliver a network environment that is secure and prepared to deal with major unexpected threats like the Shell Shock Bash bug & Heartbleed in addition to all of the other, more targeted attacks coming in to your organization on a daily basis. Join your industry peers this **January 26-28, 2015 in Calgary, AB** for the **IQPC Cyber Security for Oil and Gas Summit Canada,** which will build on the existing support of this established event in the US.

About the Summit:
Utilizing the combined knowledge of domestic and international peers, the **IQPC Cyber Security for Oil and Gas Summit Canada** will provide a forum to get your information / cyber security team prepared to combat the most pressing challenges facing the industry today. By establishing a place in the industry as a group ready to share insight, and learn to more effectively manage the risks of operating in the threat landscape currently facing the oil & gas industry you will undoubtedly advance your corporate goals in respect to information & cyber security. This forum will provide a unique opportunity to continue the **advanced learning opportunities & training of your information/cyber security employees** alongside their industry colleagues who will need to remain current to prepare themselves for the year ahead in 2015. Industry leaders will share thoughts on what has worked for them in the past and what strategies are being considered going forward, but will you be there to join in this essential security conversation?

The **IQPC Cyber Security for Oil and Gas Summit Canada** will bring together leading professionals from domestic and international oil and gas companies, field services organizations and government agencies to discuss the next steps for protecting one of the nation's largest industries and most sensitive exports. Ensure your board of directors can remain confident in the security of your organizations operational & corporate data and support your initiatives to align information/cyber security with corporate goals to enhance overall business outcomes. The **IQPC Cyber Security for Oil and Gas Summit Canada** will develop awareness within your team and allow them to **identify a wider range of strategies for growth in your security practices** and deliver value to the bottom line.

Very respectfully,

John O'Connor
Program Director
Oil & Gas IQ

P.S. If you haven't received our physical invitation for your IT department don't hesitate to reach out at enquiryiqpc@iqpc.com and be sure to sign up early so you don't miss out on the team discounts and early bird pricing.

Facts and figures

✓ Last year malware hosting on Canadian websites increased 25% bringing Canada to #10 in the world

✓ Bot networks on Canadian soil increased 83% last year bringing Canada to #8 in the world

✓ Canada is #3 globally for hosting command & control servers that communicate advanced malware

✓ Canada is #4 globally for phishing attacks with social engineering falling in volume but becoming more targeted and sophisticated in its approach

Cite: Websense Threat Labs Report

✓ Globally, the cost of cybercrime has risen to US$113 billion and cost Canadians alone more than $3 billion in 2013

✓ In Canada, $4.7 billion was lost in productivity and remediation costs, seemingly, to malware remediation and reactive measures

Cite: Norton Cybercrime report

"**Quality of speakers/ presenters was excellent. Good to have multiple perspectives on the challenges & to learn their strategic approaches.**"

–Trevor Odell, BAE Systems

Agenda at a Glance

Pre-Summit Workshop Day: Monday January 26, 2015

12:00pm	Registration	3:00pm	Afternoon Refreshments & Networking Break
1:00pm	Industrial Control System Security Keynote Address: Hacking Critical Infrastructure Explained: Common Attacks and Good Defense ***Including a Live Hacking Demonstration & Explanation***	3:30pm	Delivering Critical Infrastructure Protection in a Rapid Growth Environment and Defining Governance for Effective ICS Security Management
		5:00pm	End of Pre-Summit WorkshopDay

Main Summit Day One: Tuesday, January 27, 2015

7:45am	Registration & Morning Refreshments	2:20pm	Maturing Your Information Security Program **ATCO**
8:45am	Chairperson's Welcome and Opening Remarks - ISC²	3:05pm	Noble Energy's Implementation of Waterfall Unidirectional Security Gateways on Off-Shore Rigs in Equatorial Guinea **Waterfall Security Solutions Noble Energy**
9:00am	Digital Forensics and Cyber Crime Investigations: The Calgary Police Service Perspective **Calgary Police Service**		
10:30am	Morning Refreshments & Networking Break	3:35pm	Afternoon Refreshments & Networking Break
11:15am	The Cyberwar of Attrition **Checkpoint Software Technologies**	4:20pm	Disaster Recovery Preparedness & Reaction Time: Making the Case for Technical IT Infrastructure and Security Knowledge at the C-Level **Independent**
12:00pm	Roundtable Discussions: • Sponsored by **OpenDNS** • Sponsored by **eSentire, Inc.** • Sponsored by **Cisco Security Systems**	5:05pm	Deliver Incident Response and Threat Intelligence Value Using Open Source Security Tools **AECOM**
1:00pm	Lunch	5:50pm	Chairperson's Summary and Closing Remarks - ISC²
2:00pm	Session Sponsored by IBM	6:00PM	Post-summit Dinner Sponsored by IBM

Main Summit Day Two: Wednesday, January 28, 2015

7:30am	Registration & Morning Refreshments	11:15am	The Oil & Gas Security Cybersecurity Hat Trick: Physical, Process Control, and IT Security Convergence **Lockheed Martin Industrial Defender**
8:30am	Chairperson's Welcome and Opening Remarks		
8:45am	Senior Management Panel: Evaluating Strategic Planning for Cyber-Security **ISC² Alberta Chapter Husky Energy**	12:30pm	Lunch
		1:30pm	Manage Risk in Collaborative Network Access for Joint Ventures Partners and Vendors **Chevron**
9:45am	Adding Context to Control Systems Networks **Palo Alto Networks**	2:15pm	Afternoon Refreshments & Networking Break
10:15am	Morning Refreshments & Networking Break	2:30pm	Red Teaming your Own Network to Better Understand and Pre-empt Potential Breaches
11:00am	How to Sort through Inundation of Threat Intelligence Information and Get the Most Relevant Resources for Your Operations **City of Calgary**	3:15pm	Case Study: Stay Tuned **Enbridge**
		4:00pm	Chairperson's Summary and Closing Remarks

Who you will meet:

The **IQPC Cyber Security for Oil & Gas Summit Canada** will be focusing on the latest developments in cyber security threat detection best practices, . You will have the opportunity to interact with the individuals responsible for IT/cyber security at international and domestic oil & gas companies, field service companies, and leading security vendors. Experts who have previously attended this summit in Houston include:

- Chief Information Officer
- Chief Technology Officer
- CISO
- Vice President and Director of IT
- Director of Global Information
- Global Information Security Manager
- Director of Cyber Security
- Director of IS Operations
- Senior Executives, IT Infrastructure Executives
- IT Security Professionals
- Information Security and Risk Management Personnel
- Senior Network Administrator
- Senior Information Security Engineer

About the Organizers:

Oil & Gas
a division of IQPC

iQ

Oil and Gas IQ is the information based portal dedicated to providing the latest oil and gas intelligence. At IQPC we are a mission-driven group dedicated to exploring oil & gas industry developments and facilitating continued professional learning opportunities for oil and gas professionals. We offer more than 100 technical and strategic oil and gas conferences across the US, Europe, Asia, and the Middle East. Every year we facilitate the empowerment of 5,000+ strategic and practical executives annually.

Pre-Summit Workshop Day

Monday January 26, 2015

12:00PM | **Registration & Afternoon Refreshments**

1:00pm | **INDUSTRIAL CONTROL SYSTEM SECURITY KEYNOTE ADDRESS: Hacking Critical Infrastructure Explained: Common Attacks and Good Defense**

Including a Live Hacking Demonstration & Explanation

Cyber security attacks on industrial control systems have increased in number and complexity in the last few years. Attacks like Stuxnet and Night Dragon have proven that cyber attacks can have significant negative business impacts and potentially even loss of life. This workshop will provide an overview of current successful cyber attacks and threats, followed by a live hacking demonstration of a control system, and conclude with a case study demonstrating important security components in control systems. The case study will focus on the implementation of Emerson DeltaV—a commonly used control system. However, the concepts and security mechanisms discussed are applicable to all control systems.

- Address the risk facing oil & gas industry infrastructure through cyber threats
- Explaining the hack and potential attack points through a live hacking demonstration
- Review risk mitigation practices and defense strategies

Chris Shipp
CISO
Fluor Federal Petroleum Operations

3:00pm | **Networking Break**

3:30pm | **Delivering Critical Infrastructure Protection in a Rapid Growth Environment and Defining Governance for Effective ICS Security Management**

As the line between corporate & production computing environments continues to blend in the age of the digital oilfield, security needs to be addressed in a meaningful way with defined constructs. Ensuring the integrity of the high-volume of data coming from digital oilfield technology and assets is of paramount importance to enable business continuity and optimize production output. This session will address the imperative nature of defining a governance framework for managing ICS security and ensuring you can provide the business continuity case for implementing a most robust structure for security needs.

- Addressing the advancements in real-time data collection and the need to ensure production data integrity
- Developing robust ICS security governance and management frameworks
- Delivering tangible ROI and value to the business through continuity of operations

Eric DiTillio
Director of IT
Eclipse Resources

5:00pm | **End of Pre-Summit Workshop Day**

7:45am	**Registration & Morning Refreshments**

8:45am | **Chairperson's Welcome and Opening Remarks - ISC²**

9:00am | **Digital Forensics and Cyber Crime Investigations: The Calgary Police Service Perspective**

A brief overview of the history of Technological Crimes Team (TCT) and CST from inception to overall management

- Internal and external factors that influence TCT and CST operations
- Practical example of TCT scenario and CST scenario and challenges for DFIR
- Proposed future Cyber Forensics model specifically for Calgary Police Service.
- Challenges for DFIR.

Staff Sergeant Ryan Jepson
Electronic Surveillance Unit
Calgary Police Service

Senior Constable Shafik Punja
Technological Crimes Team (TCT)
Calgary Police Service

Sgt Corey Dayley
Cybercrime Support Team (CST)
Calgary Police Service

10:30am | **Morning Refreshments & Networking Break**

11:15am | **The Cyberwar of Attrition**

- Managing the constant attack that your business, infrastructure and employees are under
- As the risk to your business rises, your IT budget is shrinking, how can you do more with less?
- How do we fight back against the Cyberwar of Attrition? History has the answer and it may surprise you

Nick McKerrall
Security Engineer
Checkpoint Software Technologies

12:00pm | **Roundtable Discussions:**

Join your colleagues for a collaborative, open discussion to share ideas about security best practices and insight on past experience to build on your strategies for the future

- Sponsored by **OpenDNS**
- Sponsored by **eSentire, Inc.**
- Sponsored by **Cisco Security Systems**

Led by Kathy Macdonald, MOM
Security Professional, Law Enforcement (Retired)
Cyber Security Awareness Specialist, Independent

1:00pm | **Lunch**

2:00pm | **Session Sponsored by IBM**

2:20pm | **Maturing Your Information Security Program**

- High-level overview of the foundational GRC components of an Information Security Program
- Steps that need to be taken to mature the effectiveness of your Information Security Program
- Lessons learned through implementation of a robust Information Security Program

Hani Mansi
Director, Risk & Information Security
ATCO

3:05pm | **Noble Energy's Implementation of Waterfall Unidirectional Security Gateways on Off-Shore Rigs in Equatorial Guinea**

- A review of the network/threat environment
- What was deployed to secure the platforms and why
- Lessons learned from implementation

Andrew Ginter
VP of Industrial Security
Waterfall Security Solutions

Stuart Bailey
Senior Information Security Analyst
Noble Energy

3:35pm | **Afternoon Refreshments & Networking Break**

4:20pm | **Disaster Recovery Preparedness & Reaction Time: Making the Case for Technical IT Infrastructure and Security Knowledge at the C-Level**

- Uncover examples of the major savings that could be made to IT budgets through advanced network infrastructure awareness
- Align the IT team with senior leaders through the ability to speak technical language and creatively address complex issues
- Bring security to the forefront of IT operations across the lifecycle of projects from procurement to implementation so as to prevent operational downtime and save money on costly breaches and data loss

James Williamson
IT Risk & Compliance
Independent

5:05pm | **Deliver Incident Response and Threat Intelligence Value Using Open Source Security Tools**

- Lay the foundation for security team growth through tactful application of sound tools and processes for breach identification & response
- Address cyber security in a cost effective manner by employing open source tools where applicable
- Demonstrate value in the application of security tools for preventing crucial data loss

Richard Rowlandson
Network Security Analyst
AECOM

5:50pm | **Chairperson's Summary and Closing Remarks - ISC²**

6:00PM | **Post-summit Dinner Sponsored by IBM**

7:30am | **Registration & Morning Refreshments**

8:30am | **Chairperson's Welcome and Opening Remarks**

8:45am | **Senior Management Panel: Evaluating Strategic Planning for Cyber-Security**
- Match the need to manage the CAPEX cost of IT security and developing a comprehensive corporate cyber-security strategy
- Create corporate culture that adapts to the imperative nature of digital security inside and outside of work environments
- Integrate cyber security with physical IT security to address the rising cyber-physical threat landscape

Moderator:

Vincent Chiew
President & Co-Founder
ISC² Alberta Chapter

Panelists:
Jason Hinchliff
CISO
Husky Energy

9:45am | **Adding Context to Control Systems Networks**
- Imbue deep application understanding, control & user identification into security policy
- Increase user awareness and alertness to control system anomalies
- Allow for incremental visibility and control for operators of control system networks through added context

Geoff Shukin
Senior SE Western Canada
Palo Alto Networks

10:15am | **Morning Refreshments & Networking Break**

11:00am | **How to Sort through Inundation of Threat Intelligence Information and Get the Most Relevant Resources for Your Operations**
- Identify the right vulnerability CVEs relative to your operations and act on those reports
- Act on the most pertinent information from you SIEM solution and ensure up-to-date processes for cyber-response
- Further develop public/private partnership to manage the growing cyber threat and leverage the advancements within the government to address them

Owen Key
CSO
City of Calgary

11:45am | **The Oil & Gas Security Cybersecurity Hat Trick: Physical, Process Control, and IT Security Convergence**
- Compare your organization against results from Lockheed Martin's/Ponemon proprietary Oil and Gas Cybersecurity survey
- Learn how to enhance defenses by capitalizing on the convergence of three security domains (IT,OT, Physical)
- Hear real-examples of how the a unified approach has improved the security posture of energy companies

Bill Lawrence, Ph.D.
Commercial Cyber Security Services
Lockheed Martin

Kim Legelis
Vice President
Lockheed Martin Industrial Defender

12:30pm | **Lunch**

1:30pm | **Manage Risk in Collaborative Network Access for Joint Ventures Partners and Vendors**
- Methods to ensure your business partners share and adhere to your rigorous standards of cyber-security
- How to incorporate new users into collaborative network environments and mitigating the risk of their credentials being compromised
- Utilize strategic partnerships to augment your security and avoid unnecessary risk

Zoltan Palmai
Team Lead, Network Security –
Security & Access Operations – IRSM
Chevron

2:15pm | **Afternoon Refreshments & Networking Break**

2:30pm | **Red Teaming your Own Network to Better Understand and Pre-empt Potential Breaches**
- Invest in your personnel, improve your ROI through smarter security
- Use the enemy's tactics against them by deploying an active defense strategy to augment your security
- Develop an effective employee vetting process to limit the potential for internal threat and retain integral personnel

3:15pm | **Case Study: Stay Tuned**
Craig Coughlan
Supervisor Incident Response Threat Assessment
Enbridge

4:00pm | **Chairperson's Summary and Closing Remarks**

" **"Amazing opportunity to gather the information and meet such high quality presenters"**

–**George Bara, Telecommunications Specialist, Shared Services Canada**

About our Sponsors

IBM

IBM Canada Ltd. is one of the largest technology, services and consulting companies in Canada, backed by over a century of business and systems innovation. Our people are dedicated to building a smarter planet – a world where intelligence is infused into the systems and processes that make business and society work better. IBM Canada is headquartered in Markham, Ontario, and has nationwide responsibilities for sales, marketing and service. Canada is also home to IBM's largest semiconductor packaging and test facility in Bromont, Quebec and the largest software development organization in the country, with sites in Markham, London and Ottawa, Ontario; Edmonton, Alberta; and Vancouver and Victoria, British Columbia.

FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 2,500 customers across 65 countries, including over 150 of the Fortune 500.

Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Because of our deep expertise, steadfast commitment to innovation and game-changing next-generation security platform, more than 13,500 customers have chosen Palo Alto Networks and this number grows every day. Our platform natively brings together all key network security functions, including firewall, URL filtering, IDS/IPS, and advanced threat protection. Because these functions are purposely built into the platform from the ground up and they natively share important information across the respective disciplines, we ensure better security than legacy products. As a result, organizations can safely enable the use of all applications critical to running their business, maintain complete visibility and control, confidently pursue new technology initiatives like cloud, SDN and mobility, and protect the organization from the most basic to multi-faceted and complicated cyber attacks – known and unknown.

The Information Systems Security Certifications Consortium Inc.

Celebrating its 25th anniversary, (ISC)² is the largest not-for-profit membership body of certified information and software security professionals worldwide, with over 100,000 members in more than 135 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSPÒ) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLPÒ), the Certified Cyber Forensics Professional (CCFPSM), Certified Authorization Professional (CAPÒ), HealthCare Information Security and Privacy Practitioner (HCISPPSM), and Systems Security Certified Practitioner (SSCPÒ) credentials to qualifying candidates. (ISC)² offers education programs and services based on its CBK®. Visit www.isc2.org.

Waterfall Security Solutions Ltd.

Waterfall is the leading provider of strong network security products which protect the safety and the reliability of control system networks. Waterfall Security Solutions' mission is to eliminate the use of firewalls in critical infrastructure control systems. The company develops products which provide stronger-than-firewall protections for industrial control networks. Waterfall's products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and the Middle-East. Waterfall's innovative products dramatically reduce the cost and complexity of compliance with NERC-CIP, NRC, NIST, CFATS and other regulations, and include support for leading industrial applications, including the OSIsoft PI™ Historian, the GE Proficy™ iHistorian, Siemens SIMATIC™/Spectrum™ solutions and GE OSM™ remote monitoring platforms, as well as OPC, Modbus, DNP3, ICCP and other industrial protocols. Frost & Sullivan describe Waterfall's solutions as ensuring "optimum security for networks across user verticals" and awarded Waterfall the 2012 Network Security Award for Industrial Control Systems Entrepreneurial Company of the Year and the 2013 North America Award for Customer Value Enhancement. For more information visit: www.waterfall-security.com.

iON Secured Networks

iON Secured Networks is a privately owned and full service IT security assessor, integrator, IT infrastructure support and management facilitators. Established on March 26th, 2003, iON has quietly emerged into one of the most trusted names in network security in Western Canada, providing clients with superior service, best of breed products and support. We continue to commit to excellence in retaining Canada's top clients while attracting Canada's top talent.

Check Point

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 FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization.

eSentire
eSentire® is the leading managed security service provider to more than 450 financial services firms, legal, extractive and healthcare organizations. eSentire pioneered Continuous Advanced Threat Protection, which leading analyst firm Gartner Research began covering in June 2014 as a best practices framework for defending against the most egregious cybersecurity attacks. eSentire delivers continuous monitoring, real-time threat detection and containment technology as a service with human threat analysts on a 24x7x365 basis.

Lockheed Martin
Lockheed Martin has successfully developed and delivered a single unified platform to secure and manage heterogeneous control environments including gas SCADA systems, drilling platforms, pipelines, and other aspects of operational infrastructure. Our solutions deliver cybersecurity, compliance, and change management for industrial control systems. Our flagship product, Industrial Defender Automation Systems Manager™, and a wide range of cybersecurity services ensure the availability and reliability of key industrial processes amid escalating cyber threats, increasing regulatory burdens, and accelerating operational challenges. More than a third the Fortune 500 oil and gas firms rely on Lockheed Martin to reduce costs, manage risks, and enhance operational excellence.

The Herjavec Group
Dynamic IT entrepreneur Robert Herjavec, founded Herjavec Group in 2003 and it quickly became one of North America's fastest-growing technology companies, accelerating from $400K to $140 million in sales over 11 years. Herjavec Group delivers managed security services globally supported by a state-of-the-art, PCI compliant Security Operations Centre (SOC), operated 24/7/365 by certified security professionals. This expertise is coupled with a leadership position across a wide range of functions including compliance, risk management, incident response, networking and storage. Herjavec Group has offices across North America and two headquarters in Toronto (Canada) and Dallas (US). For more information, visit www.herjavecgroup.com

Thycotic:
Thycotic creates intuitive, reliable, IT security solutions that empower companies to remove the complexities associated with proper control and monitoring of privileged accounts. An Inc. 5000 company, Thycotic is recognized as the fastest growing, privately held privileged account management (PAM) provider in the USA. Rated #1 in customer satisfaction and trusted by over 180,000 IT professionals worldwide – including members of the Fortune 500, enterprises, government agencies, technology firms, universities, utilities, non-profits, and managed service providers.

OpenDNS:
OpenDNS provides a cloud-delivered network security service that blocks advanced attacks, as well as malware, botnets and phishing threats regardless of port, protocol or application. Our predictive intelligence uses machine learning to automate protection against emergent threats before your organization is attacked. OpenDNS covers devices worldwide in minutes and stays up-to-date without admin intervention because there is no hardware to install or software to maintain.OpenDNS handles more than two percent of the world's daily Internet requests. Our global network has proven 100 percent uptime, adds no latency, and powers our big-data analytics for unique visibility of where attacks are staged on the Internet.

Cisco:
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.

Fortinet
Fortinet (NASDAQ: FTNT) is a worldwide provider of high performance network security appliances and a market leader in unified threat management (UTM). The company's products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Customers include enterprises, service providers and government entities worldwide. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's product line goes beyond UTM to help secure the extended enterprise - from endpoints, to the perimeter and the core, including databases and applications.

SecureAuth
SecureAuth's identity and information security solutions deliver innovative access control for cloud, mobile, web and legacy systems. Our customer-first approach is combined with outside the box thinking and standards based development. This ensures we solve even your toughest access control problems with solutions that are quick to deploy, easy to integrate with your existing infrastructure and deliver exceptional value for your investment.

Pricing, Registration & Location

End User

Package	Register & Pay By Oct 31	Register & Pay By Nov 21	Register & Pay By Dec 19	Standard Price
Main Conference Only	$1,995 CAD **Save $500 CAD**	$2,095 CAD **Save $400 CAD**	$2,295 CAD **Save $200 CAD**	$2,495 CAD
All Access: Main Conference + Workshops	$3,095 CAD **Save $500 CAD**	$3,195 CAD **Save $400 CAD**	$3,395 CAD **Save $200 CAD**	$3,595 CAD
Workshops	$549 CAD each			

* **Note the All Access gives 1 free workshop/ 3 for the price of two*

Vendor

Package	Register & Pay By Oct 31	Register & Pay By Nov 21	Register & Pay By Dec 19	Standard Price
Main Conference Only	$2,495 CAD **Save $500 CAD**	$2,695 CAD **Save $300 CAD**	$2,795 CAD **Save $200 CAD**	$2,995 CAD
All Access: Main Conference + Workshops	$3,595 CAD **Save $500 CAD**	$3,795 CAD **Save $300 CAD**	$3,895 CAD **Save $200 CAD**	$4,095 CAD
Workshops	$549 CAD each			

Team Discounts*

Number of Attendees	Savings
3 to 4	10%
5 or more	15%

Discounts apply to registrations submitted together, at the same time. Cannot be combined with any other discount

Please note:
- IQPC reserves the right to determine who qualifies as an end user
- All 'Early Bird' discounts require payment at time of registration and before the cut-off date in order to receive any discount.
- Any discounts offered (including team discounts) must also require payment at the time of registration.
- All discount offers cannot be combined with any other offer.
- Please view our registration policy for full information about payment, cancellation, postponement, substitution and discounts.
- Please note multiple discounts cannot be combined.
A $99 processing charge will be assessed to all registrations not accompanied by credit card payment at the time of registration.

MAKE CHECKS PAYABLE IN U.S. DOLLARS TO: IQPC
Prices in Canadian dollars are subject to a 13% HST.
* CT residents or people employed in the state of CT must add 6.35% sales tax.

Team Discounts: For information on team discounts, please contact IQPC Customer Service at
1-800-882-8684. Only one discount may be applied per registrant.
Special Discounts Available: A limited number of discounts are available for the non-profit sector, government organizations and academia. For more information, please contact customer service at 1-800-882-8684.

Details for making payment via EFT or wire transfer:
Bank Name: HSBC
Account #:   002-385-007-001
Swift Code: HKBCCATT
Reference: IQPC: Event Code

Payment Policy: Payment is due in full at the time of registration and includes lunches and refreshment. Your registration will not be confirmed until payment is received and may be subject to cancellation.
For IQPC's Cancellation, Postponement and Substitution Policy, please visit www.iqpc.com/cancellation

Special Dietary Needs: If you have a dietary restriction, please contact Customer Service at
1-800-882-8684 to discuss your specific needs.

Media Partners:

Register Online, by Email, Phone, Fax or Mail

Web: www.cybersecurityoilgas.com
Email: enquiryiqpc@iqpc.com
Phone: 1.800.882.8684
Fax: 646.378.6025
Mail: IQPC
535 5th Avenue, 8th Floor
New York, NY 10017

Location & Lodging Information

This event will be held at **The Westin Calgary in Calgary, AB.** As soon as a specific venue is confirmed we will post the information online. If you would like to be notified via email as soon as the information becomes available please email **enquiryiqpc@iqpc.com** with the following in the subject line: **"Cyber Security Summit Canada"**

Sponsorship and Exhibition Opportunities Still Available!

For more information please contact **Eric Pompei** at 212-885-2693 or **Eric.Pompei@iqpc.com**

For more information on our call for papers & opportunities to participate as a presenter please contact **John O'Connor** at 646-502-3255 or **John.OConnor@iqpc.com**

Stay Connected!

Visit www.cybersecurityoilgas.com today to:
- Register for the event
- View the complete speaker roster and biographies
- Gain free access to relevant podcasts, videos, articles, interviews, whitepapers, and past presentations at our resource center
- Learn more about the location, venue, and hotel discounts
- Learn more about our sponsors, exhibitors, and media partners

And much more!