BSIDES CALGARY 2023

Security | Privacy | Technology

Hosted By

Bow Valley College

Hybrid Event Details

URL: https://hopin.com/events/bsides-calgary-2023

Where

Bow Valley College

345 6th Ave SE

Calgary AB

When

November 16 8:00 AM—4:00 PM MDT

November 17 8:00 AM—5:20 PM MDT

Twitter @bsides_calgary

Email bsidescalgary@bsidescalgary.org

Online https://www.bsidescalgary.org

MESSAGE FROM THE BSIDES CALGARY 2023 ORGANIZING COMMITTEE

Welcome to BSides Calgary 2023! The organizing committee has been very busy putting together this event and we are honored to have so many exceptional speakers, sponsors, volunteers and attendees show dedication to this year's event. We're grateful to have so many high-calibre speakers respond to our Call for Papers with amazing talks and presentations. We were able to fill two full days of in-depth security related talks (spread over four tracks), a sponsor technical track, as well as workshops, from leading security researchers, consultants and local hackers as well as new speakers from across several different countries.

A capture the flag competition is also available to anybody who wants to test their skills and knowledge. There are challenges for all levels so that everybody can partake. If you are interested in playing, please see https://ctf.bsidescalgary.org.

In addition to our great Sponsors, we're hosting Community and Special Interest groups at the event. Be sure to check out the community group and sponsor booths!

Over the next couple of days, you will have a chance to network with fellow security practitioners as well as share, discuss and learn about information security and technology in Calgary. We hope that you enjoy what we have worked hard to build and welcome your comments and feedback over the next two days.

If you have any questions during the event, the organizing committee and volunteers will be happy to assist. Just look for anybody with the term 'volunteer' or 'organizer' in their title on Hopin, or volunteer lanyards at the event.

proudly sponsored by:

day one

8:00 AM	**Coffee / Registration / Networking**
9:00 AM	**Opening Keynote**—Michael Spaling
10:30 AM	**Session 1**
11:30 AM	**Session 2**
12:20 PM	**Lunch & Network / Door Prizes**
1:00 PM	**Session 3**
2:00 PM	**Session 4**
3:00 PM	**Session 5**

10:30 AM—7:00 PM: Capture the Flag Competition—Onsite

BSIDES CALGARY 2023

10:30AM_11:20AM

TRACK 1

How effective are cybersecurity risk assessments in mitigating the risk of cyberattacks?

Stefan Myroniuk

Many small-to-medium -sized businesses (SMBs) have adopted the practice of regularly conducting cybersecurity risk assessments (CRAs) to safeguard their operations against cyber threats. However, CRAs often demand substantial resources, including time and financial investments.

The presentation will examine the research objectives of prevailing practices and the risk management frameworks implemented in CRAs.

TRACK 2

Legacy Macs, Modern Solutions: A Hacker's Approach to Mac Sustainability

Mykola Grymalyuk

A look into how Apple's desktop operating system has evolved over the years, and examine the systems deployed to help protect users from malicious actors. Primarily focused as an introduction to macOS internals, while including more technical information for those more familiar with the topic.

TRACK 3

Loidy: Unleashing Blockchain in Threat Intelligence

Kai Iyer

The existing public threat intelligence model lacks a reliable way of verifying the quality and authenticity of intelligence feeds. The introduction of Blockchain can help address this issue.

The talk is focused on a Decentralized and Rewarding Cyber Threat Intelligence Sharing Model. The Decentralized Application (DApp) employs a proof of quality protocol for sharing and validating cyber threat intelligence. The rewarding algorithm distributes rewards to participants based on their contributions and the impact made by their inputs.

.

10:30AM_11:20AM

TRACK 4

Skill up on Wireshark

Doug Warden

This will be an introduction into Wireshark for those uninitiated or looking to improve their understanding and skill level. We'll break down how the application works and work through some security specific network traffic captures - things like logons, attacks, port scans etc. and take a look at how using a tool like Wireshark can help with your understanding of how a protocol works and how it might be exploited.

TECHNICAL DEEP DIVE

IronSpear

Join our gold sponsor, IronSpear as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

BSIDES CALGARY 2023

11:30AM_12:20PM

TRACK 1	TRACK 2	TRACK 3
Social Engineering in the Era of AI: Emerging Trends and Challenges Sourabh Aggarwal In the era of artificial intelligence (AI), the landscape of social engineering is rapidly evolving, presenting new opportunities and unprecedented challenges. This presentation explores the emerging trends and challenges associated with social engineering in the context of AI. The talk begins by providing an overview of social engineering and its traditional techniques, highlighting malicious actors' fundamental concepts and strategies to exploit human vulnerabilities. It then delves into the integration of AI into social engineering.	Red and Blue Teaming and the Powers Gained! Adversarial Emulation Jason Maynard In this session we will learn about adversarial emulation and how both red and blue teams can benefit from it use. We learn about the tools available to us and then build out an operation leveraging Open Source and Commercial tools without preventive capabilities. We will then review the adversarial outcomes which includes reviewing the outcomes on our passively deployed Security portfolio. The knowledge gained ensures defensive teams understand the opportunity to increase our defenses.	Chained Exploitation: Perspectives in Security Testing Ian Lin This talk will attempt to highlight the concept of vulnerability chaining. Vulnerability chaining is a well-established technique of adversaries to achieve a specific objective. Many penetration tests are written in report formats, however, this does not always help organizations to understand which to address first. Many organizations opt to address high risk vulnerabilities, whilst leaving the low/ medium findings around thinking that their overall risk is reduced. However, it is difficult to "break up the chain."

11:30AM_12:20PM

TRACK 4

Hacking 101

An intro workshop with Doug Leece for those interested in getting into the world of hacking.

TECHNICAL DEEP DIVE

TechDemocracy

Join our silver sponsor, TechDemocracy as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

proudly sponsored by:

1:00PM_1:50PM

TRACK 1

Is AI a boon or bane for cybersecurity?

Parul Khanna

The cyber threat landscape is continuously evolving and this had led to an exponential growth in the cyber attacks.

This presentation will explore AI's potential in improving cybersecurity by harnessing its strengths, capabilities and identifying the challenges associated with it

TRACK 2

Demystifying "Zero Trust" in ICS

Stephen Mathezer

This talk will explore the realities of ICS networks, the various inherent challenges in implementing strong cybersecurity controls in such environments, what "Zero Trust" really means in this context, and how we have already been, and can continue to implement strong cybersecurity controls (however we label them) to protect our most critical assets.

TRACK 3

Untangling the understanding of Incident Response

Syed Zaidi

Each day, each hour, an incident happens in your life, and we take appropriate actions to come out of those Incidents. Then why do businesses not take appropriate action against the Incidents they have witnessed? It looks like there is a gap in how people understand Incident Response. Let's understand the simple way via live examples, use cases, and tabletops.

1:00PM_2:50PM

TRACK 4

Phishing Expedition

20,000 Leagues Under Accounting, your digital crime syndicate has established a foothold in a business. What happens next is up to you.

Phishing Expedition puts you and your group in control of a fictional criminal enterprise determined to earn big before you're evicted from the infrastructure.

BSIDES CALGARY 2023

2:00PM_2:50PM

TRACK 1	TRACK 2	TRACK 3
Shining a light into the security blackhole of IoT and OT	Unveiling the Hidden Gem: Pre-Sales Engineering	Imposter Syndrome: Pitfalls and How To Overcome
Huxley Barbee	Rick Byrne	Andrew Campbell
This presentation will explore the unique challenges that IoT and OT pose for network scanning and provide solutions for effectively addressing these challenges while ensuring the safety and availability of these systems. The presentation will cover topics such as identifying IoT and OT devices on a network, understanding the context of vulnerabilities associated with these devices, and implementing appropriate security controls to mitigate these risks while ensuring the safety and availability of these systems.	In the fast-paced world of technology sales, a critical yet often overlooked role exists: pre-sales engineering. This presentation aims to uncover the hidden potential of pre-sales engineering, providing valuable insights into how to enter this domain, why it stands as an exceptional career choice, and the essential attributes required to excel in this often underappreciated field. The presentation will commence by defining pre-sales engineering and its pivotal purpose within organizations.	I want to share my personal experience being in cybersecurty. Before starting on my journey I was completely unaware of the impact of "imposter syndrome." While I still struggle with it, I have built in strategies to help me combat it. I feel the strategies I have done can help others as well. I like talks that add comedy, so my talk will be a light hearted look at how imposter syndrome has impacted me. A few parts in the story of my career have added to imposter syndrome which would make people wonder why I subject myself to such torture. We'll face imposter syndrome head-on.

TECHNICAL DEEP DIVE

iON United

Join our Gold sponsor, iON as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

proudly sponsored by:

proudly sponsored by:

3:00PM_3:50PM

TECHNICAL DEEP DIVE

Fortinet

Join our silver sponsor, Fortinet as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

BSIDES CALGARY 2023

3:00PM_3:50PM

TRACK 1

The Packet has left the Network

George Nazarey

When do you have to worry about an actual breach? Is it when the adversary:

1. lands on your network?

2. browses your network?

-or-

3. Takes information from your network?

While the first two cases can keep you up at night, it really becomes real when your information leaves your networks and gets into the hands of an adversary.

TRACK 2

Beyond Prevention: The Vital Importance of Data Protection in Cybersecurity

Derran Guinan

While preventative cybersecurity tools play a crucial role in safeguarding our systems, we must recognize the indispensability of data protection as the ultimate fallback when these measures fail. Effective data protection practices not only mitigate the potential impact of a breach but also ensure compliance with regulations, build customer trust, and safeguard the confidentiality, integrity, and availability of data.

TRACK 3

Offensive Security through a GRC lens

Dennis Chaupis & Rodolfo Vilchez

Ever wondered why many vulnerabilities are not fixed? We are not talking about the ones as a result of VM scanning, but those that either broke or found weaknesses in processes, those where maybe IT is an enabler but not a process owner. This non-technical talk aims to explain to Offensive Security Professionals the other side of the table after a report is provided; all through the lens of a GRC Program, including remediation strategies such as the layered approach.

TRACK 4

Security Efficacy Testing: Is our stack is protecting us?

Sean Hittel

With each appearance of a major incident in the news, some of us have lost sleep wondering if we would be next or asking ourselves “Would we be protected against that type of attack?” It’s a complicated question to answer, and the solution starts with efficacy testing.

proudly sponsored by:

day two

8:00 AM	**Coffee / Networking**
8:40 AM	**Opening Keynote**—Michelle Balderson
9:30 AM	**Session 6**
10:30 AM	**Session 7**
11:30 AM	**Session 8**
12:20 PM	**Lunch & Network**
1:00 PM	**Session 9**
2:00 PM	**Session 10**
3:00 PM	**Session 11**
4:00 PM	**CTF Results and Closing Remarks**

8:00 AM—3:45 PM: **Capture the Flag Competition—Onsite**

BSIDES CALGARY 2023

9:30AM_10:20AM

TRACK 1	TRACK 2	TRACK 3
Introduction to AI Security Vincent Chiew The spread of both AI (Artificial Intelligence) opportunities and threats are so prevalent these days. Will it take over the world and possibly humanity? This talk will try to answer this question by providing a brief general understanding of AI. How AI works historically up to today. With this knowledge we can better handle and control AI. We will do this by leveraging some basic security fundamentals. In conclusion, hopefully all the questions you are afraid to ask will be answered. Finally, we can be one with AI.	Designing Games to Solve Security Problems A.J. Leece In this talk, I discuss the development journey of Incidents & Accidents, an incident response tabletop experience, designed for everyone to learn, grow, and have fun. This talk covers how I discovered how non-security people learn information security, cultivating new skills during difficult times, growing a new business in a market with a low tolerance for risky ideas, all while managing to preserve mental and physical health as it went from a cool thing to do, to a full-time job tackling important parts of the security program organizations tend to ignore.	Unveiling the Hidden: A Glimpse into TSCM from an Infosec Perspective JJ Giner Join me on an exciting journey as we delve into the captivating world of Technical Surveillance Countermeasures (TSCM). Together, we'll unlock the secrets and strategies to safeguard your most valuable information. I will personally guide you through the tactics employed by eavesdroppers and unveil the cutting-edge countermeasures that can shield your sensitive data and fortify your organizations.

9:30AM_10:20AM

TRACK 4

Securing Cloud Workload Identities: Understanding the (AWS) Instance Metadata Service as part of the Identity and Access Management Layer for Cloud Virtual Machines

Sam Ezebunandu

In today's rapidly evolving cloud landscape, managing identities for cloud-hosted workloads has become a paramount concern. The AWS Instance Metadata Service (IMDS) plays a critical role in enabling cloud virtual machine instances to communicate with other cloud services. However, as with any powerful tool, IMDS introduces its own set of challenges, particularly in its earlier iteration, IMDS v1.

In this workshop we will delve into the intricacies of securing cloud workload identities for virtual machines running in the AWS cloud. This talk will shed light on the vulnerabilities associated with IMDS v1.

TRACK 5

Artificial Insecurity: Secure code in LLMs? It AI-n't happening.

Henrique Pereira

In the rapidly evolving digital age, artificial intelligence is opening new avenues in diverse sectors, including cybersecurity. This talk offers a compelling delve into an underexplored dimension of cybersecurity: the potential threats posed by Large Language Models (LLMs) and their generated code.

Our presentation will begin with a concise introduction to LLMs, setting a clear context for understanding their role in code generation. However, the central pivot of our discourse will be focused on the potential insecure code churned out by these AI models. By laying bare the security holes and potential loopholes often overlooked in this realm, we aim to shed light on this new kind of cybersecurity concern.

TECHNICAL DEEP DIVE

SecuredNet Solutions

Join our gold sponsor, SecuredNet Solutions as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

BSIDES CALGARY 2023

10:30AM_11:20AM

TRACK 1

Self-Pwning Through Cybersecurity Hiring and Candidacy

Adam McMath

News Article: “3.5 million unfilled cybersecurity jobs!”

Candidates: “I’ve applied online to about 100 cybersecurity, jobs but can’t seem to get any responses?”

There’s a troublesome disconnect between cybersecurity’s hiring managers and job seekers.

Let’s use this session to have an honest conversation, and social-engineer ourselves into better hiring-manager and candidacy collaboration.

TRACK 2

Car Hacking

Harsh Modi

Various concepts methodologies, tools and a deep dive into radio hacking.

TRACK 4

Hacking Workshop (Wifi)

An intro course for those interested in a learning how to hack Wifi with Doug Leece.

TRACK 3

Pentesting Active Directory Infrastructure to own root privileges

Swar Shah

In the world of cybersecurity, securing Active Directory (AD) infrastructure is of paramount importance due to its critical role in managing authentication and authorization for an organization's resources. However, as the complexity and sophistication of attacks continue to evolve, it is crucial for organizations to assess the security of their AD environment through penetration testing.

This talk aims to explore the art of pentesting an Active Directory infrastructure with the objective of achieving root privileges.

proudly sponsored by:

11:30AM_12:20PM

TRACK 1

Lets Make Fun of Cyber Security

Prashant Prashant

This talk is based on cartoons in cyber security and sharing core and important cyber security concepts from people, process, technology perspective to the audience. It leverages famous themes/cartoons to share the life of a cyber professional, how risk management is done, what are the threats facing the world today, the world of geeky nerds, privacy, cyber warfare, cyber political satire in an all in one presentation. This talk attempts to go little off beat from serious cyber talks and pave the way for learning by laughing.

TRACK 2

Unlocking Collaboration: Harnessing the Power of Attack/Defense Capture the Flag Challenges for Cybersecurity Training

Alex Tenney

Your tabletop exercises are boring. This raises important questions: How can we encourage collaboration between teams to strengthen security posture? How can we cultivate employee interest and motivation to tackle critical organizational challenges? Enter Attack/Defense (AD) Capture the Flag (CTF) challenges—a dynamic and enjoyable training approach that encourages collaboration among multiple cybersecurity teams within an organization. During the session, we will delve into the fundamental principles behind AD CTFs and how a typical competition plays out.

BSIDES CALGARY 2023

11:30AM_12:30PM

TRACK 3

ChatGPT for Security Analysts

Greg Leah

ChatGPT is a revolutionary tool that can generate natural language text in a variety of contexts, including cybersecurity. However, its applications go far beyond just generating text. In this talk, we will explore some ways that ChatGPT can be used to streamline the workflows of cybersecurity professionals.

By using ChatGPT to process and analyze data, security analysts, reverse engineers, and cybersecurity enthusiasts can quickly and easily gain valuable insights into emerging threats. This talk will provide attendees with an increased understanding of how ChatGPT can be leveraged to analyze hostile code, extract threat intelligence indicators, generate hunting rules and more.

TRACK 4

Identity & Security: It's time for a hug

Eric Woodruff

Identity and security practitioners groups have not always operated with cohesion, even in the world today where the saying goes - identity is the new security perimeter.

We are at a turning point, and we have a choice of how to forge the path ahead.

TECHNICAL DEEP DIVE

Veeam

Join our silver sponsor, Veeam as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

proudly sponsored by:

Bow Valley College

BSIDES CALGARY 2023

1:00PM_1:50PM

TRACK 1	TRACK 2	TRACK 3
Hackers On The Move: Tools Of The Trade Hank Fordham What tools are hackers and cybersecurity professionals using in their work? What are some less common tools that cybercriminals are starting to use and how can we beat it? Hackers are always on the move: digging inside our technologies, and social engineering their way through our daily lives. In this session, Hank will showcase his knowledge about inventive methods and tools hackers use to identify potential targets within public areas, and exploit them through emotional deception, malicious jewelry, and other masquerades, as well as how to keep yourself safe!	Achieving Zero Trust with IAM Hyma Pandyaram With traditional IAM, attackers who gain initial access can exploit vulnerabilities, move laterally within the network, and potentially gain privileged access. As a result, the need for a Zero Trust Identity and Access Management (IAM) approach has become paramount. This presentation explores the principles of Zero Trust, highlighting the importance of continuously verifying privileges and access. We will discuss how IAM can be leveraged to enforce a Zero Trust model, focusing on the implementation of adaptive and context-aware access controls.	Are we ready to play hide and seek with Service events and Task scheduler ! Satheesh Pandurangan Sophisticated attackers may use process injection techniques to hide their malicious service within the legitimate process or system service to avoid detection. By injecting their code into a trusted process, they can bypass security measures and evade detection by traditional monitoring tools. Let's deep dive with a detailed understanding about the malware attackers mindset and hunting down their malicious persistence methods.

1:00PM_1:50PM

TECHNICAL DEEP DIVE

CANARIE

Join our silver sponsor, CANARIE as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.

1:00PM_2:50PM

TRACK 4

Phishing Expedition

20,000 Leagues Under Accounting, your digital crime syndicate has established a foothold in a business. What happens next is up to you.

Phishing Expedition puts you and your group in control of a fictional criminal enterprise determined to earn big before you're evicted from the infrastructure.

2:00PM_2:50PM

TRACK 1

AI powered Cybersecurity - the good and bad.

Sheik Sahib

As cyberattacks grow in volume and complexity, cyber criminals are employing AI to develop and accelerate their methods. AI can also help under-resourced SecOps analysts stay ahead of the threat landscape. IBM Security is employing AI technologies to detect and defeat cybersecurity threats that threaten businesses, organizations, and governments across Canada. In this session, we review latest cyber-attack trends and discuss how IBM Security is leveraging advanced AI technologies to identify and prioritize threats, investigate the true nature of high priority alerts, and automate remediation. We discuss the role of Watson Cybersecurity – a massive knowledge graph – that help cut through the noise of daily alerts and drastically reduce response times.

2:00PM_2:50PM

TRACK 2

TunnelCrack Unveiled: Exploring Remote Access Security Vulnerabilities

Kyle McKay

Remote access VPNs are an essential part of todays hybrid & remote workforces, providing connectivity to critical applications wherever and whenever the user requires it. In August, 2023, a set of vulnerabilities aptly named 'TunnelCrack' was made public and directly impact many Remote access VPN implementations.

In this session, we will explore TunnelCrack in depth, to shine a light on how this vulnerability can be abused, and how to defend against it.

TRACK 3

Leverage your Network to build your Net Worth in CyberSecurity

Aarti Gadhia

“Your Network is your Net Worth” however for many cybersecurity professionals networking is uncomfortable. Whether you are an introvert, hate small talk or work from home, you can still reap the benefits of networking.

3:00PM_3:50PM

TRACK 1

What is Self Sovereign Identity and why it doesn't need Blockchain

Brechin Piper

Self Sovereign Identity is an evolving concept that individuals can take control of their own data and identity, often spoken of in the same breath as blockchain. Brechin will talk through the existing identity models, compare and contrast to what a self sovereign model could look like, and whether or not it actually requires a blockchain to pull off.

TRACK 2

The Million Dollar CEO Fraud: Anatomy of a BEC

Damien Miller-McAndrews

This talk will detail a real incident I handled where a CEO's compromised email culminated in a small business losing almost one million dollars. I will tie the details of this incident to the MITRE ATT&CK Cloud Matrix and discuss the cybercrime ecosystem behind these attacks.

BSIDES CALGARY 2023

3:00PM_3:50PM

TRACK 3

Silent But Deadly: An Exploration In Using Ultrasonic Sound To Covertly Exfiltrate Data

Isaac Privett

This project focuses on the exploration and demonstration of data exfiltration from air-gapped systems using ultrasonic sound as a side-channeling technique. However, various side-channel techniques have been developed to compromise these systems and exfiltrate sensitive information. Our research investigates the effectiveness of ultrasonic sound as a means of transmitting data from an air-gapped system to a nearby microphone-equipped device without alerting the user or raising suspicion.

TRACK 4

Field Testing Investigation Feasibility Using Deidentified Cyber Event Data

Doug Leece

Despite the well publicized shortage of information security professionals, industry and academia have struggled to create a repeatable training that delivers qualified workforce entrants the way trades and other professions have managed to do. Like flying an airplane or performing surgery, simulation training requires realistic data -- costly to recreate as cyber ranges yet readily generated by every organization searching for qualified cyber talent – which is normally unavailable due to privacy concerns.

Centralized log collection is a regulatory and managed security service provider mainstay, providing analysis capability while simultaneously exposing the security posture of each organization to those with access to the security event data. While this data exposure risk can be contractually mitigated with service providers and regulatory bodies it is not the most robust control.The talk includes explanations for several challenges identified with security event log deidentification and potential solutions as well as an analysis of an intrusion test case from a cyber security investigation perspective.

3:00PM_3:50PM

TRACK 5

Dead Vehicle Bug Hunter tell no tales

Kevin Chen

A couple years ago, we found an interesting bug that can be used to bypass the PIN2Drvie function from Tesla. We have been rewarded by Tesla, who has also added us to the Tesla Hall of Fame list. Last year, we disclosed a creative bug called Rolling-Pwn that affects Honda vehicles globally. And this very same trick helped us win 3rd place with a reward in a hack competition. Bug bounty hunting is the new sexy, and vehicle bug bounty hunting is even sexier. During this talk, the success and failure of our vehicle bug hunting story for the past few years will be presented. And vehicle bug bounty hunting advice will be shared with the community.

TECHNICAL DEEP DIVE

Cohesity

Join our silver sponsor, Cohesity as their experts provide a Technical Deep-Dive of their products and services and apply their expertise to real world scenarios.