BRISSEC

AISA
Cyber | smart · safe · secure

An intelligent IoT vulnerability detection tool with the case study of smart airports

The prevalence of Internet of Things (IoT) devices in contemporary networks and environments has resulted in added cyber security risks due to weaknesses inherent in the heterogeneous IoT devices. Moreover, the rush for digital transformation often comes without proper security measures in place, especially in identifying and mitigating vulnerabilities in IoT. In the space of IoT vulnerability identification the existing contemporary tools utilised in the industry rely primarily on pre-designed rules or policies for the detection and assessment of vulnerabilities. These tools have two major limitations:

1. They need regular updates by domain experts to discover existing attack surfaces and face limitations when tasked with identifying unknown vulnerabilities; and
2. They cannot analyse attack surfaces from heterogeneous data sources simultaneously, such as network traffic and telemetry data from IoT sensors.

In this presentation, the outcomes of a recent R & D work with Cyber Security Cooperative Research Centre (Cyber Security CRC), which addresses above challenges and delivers a novel vulnerability identification software system tool using AI technology will be presented. This tool has been developed with new features to detect and assess attack surfaces using an intelligent deep learning-enabled mutation-based fuzzing process through which both known and unknown vulnerabilities can be identified. The efficacy of the solution has been validated in a realistic smart airport IoT testbed built for the purpose of this project at the University of New South Wales (UNSW) Canberra. The content presented in this talk is the result of collaborative effort of Cyber Security CRC partners: UNSW Canberra, Australian Federal Police and Tata Consultancy Services.

Presenter:
PRAVEEN GAURAVARAM

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
10:45 AM – 11:25 AM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Applying a risk-based approach to security control selection, that is prescribed in regulatory frameworks

The session describes the challenges and lack of maturity in the industry to applying a risk-based approach to security control selection, that is prescribed in regulatory frameworks such as ASCS ISM, APRA CPS234 and NIST Risk Management Framework (RMF).

GRC consultants and engineering teams working in regulated industries are often required to apply a risk-based approach to control selection. Observations within the industry are that this approach could be more consistent, bespoke and highly opinionated. It's based on individual experience and choices rather than following a standard and consistent process. Regulatory frameworks point to 'conduct a risk assessment'; however, this is too broad of an approach to be helpful, which is why results are often so subjective.

This session demonstrates how security patterns can be applied to simplify compliance and provide a risk-based approach to control selection. Using a standardised security pattern approach, organisations can effectively assess and prioritise their security risks, allowing them to select and implement the most appropriate controls for their specific needs. This approach can help organisations save time and resources while ensuring compliance with industry standards and regulations.

Participants will be provided a practical example of applying this process for migrating sensitive workloads into cloud, that requires assessment of required security controls and adherence to compliance frameworks. The target audience for this session is GRC consultants and security architects.

Presenter:
KEN FITZPATRICK

HUMAN FACTORS
10:45 AM – 11:25 AM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Nation state actors: An analysis of TTPs, frameworks and the need for education

This presentation explores the current curriculum and education approaches of major cyber security frameworks and whether they address the larger scale and more advanced techniques available to the nation-state hacker.

While most organisations concentrate on techniques, tactics and procedures of the cyber criminal, nation-state hackers have more advanced techniques and different objectives than your usual cyber-criminal.

With an analysis of APTs from the Mitre ATT&CK framework, this presentation identifies some of their more edge-case techniques and determines whether they are contained in the curriculum of the major Bodies of Knowledge (BoK), frameworks and industry certifications.

The following topics will be discussed:

- What is different about a nation state operator
- What attack methods are used by nation states
- What does MITRE ATT&CK have for these groups
- What frameworks cover the attack methods investigated
- What can be done to improve our operators knowledge and organisation resiliance

Presenter:

MARCUS HERSTIK

COPS AND ROBBERS: GRC & CYBER CRIME

10:45 AM – 11:25 AM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Federating the fight against cyber crime... without the jargon!

In the fight against cyber crime, it's fair to say that a lot of folk claim to have developed the silver bullet! But the growing number of cyber attacks would suggest that most, if they are indeed bullets at all, probably aren't silver and may not not even be aimed at the right targets!

Indeed, out of a sample of almost 30 ransomware incidents over the last six years with which the presenters have first hand experience, none of the victims were lacking at least several advanced cyber tech controls - silver bullets - like EDR, email gateways, SOC/SIEM and others. Each control, in theory, should have stopped the attack, but didn't due to a lack of intelligent federation between them. Cyber federation isn't a silver bullet, but it does have the potential to be like a bulletproof vest when the adversary tries to fire one at you!

However, for all its potential, the concept of cyber federation is confusing and, like many terms in our industry, means different things to people. Some see it as being about APIs, others about ZTNA; and others still describe it as a MESH, or in some cases, just being an identity or data thing. And then there is the discussion about the need for a common data schema... but which one? There's STIX/TAXII for threat intelligence, OCSF for investigations and for tactics analysis, there's ATT&CK. Frankly, cyber-federation doesnt need to be this complex; and all of the acronyms really don't help anyone!

In this presentation, we use real case studies to both demystify, as well as operationalise the key concepts around intelligent cyber security federation. By the end of the discussion, the goal is that the audience will all agree on what the term encompasses, and how to apply it in a way that makes it akin to cyber-kevlar!

Presenters:
DIRK HODGSON & ADAM GREEN

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
11:30 AM – 12:10 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Diminished trust and the trouble with ‘Privacy by Design (PbD) Lite’

Community awareness of the personal data economy, large scale data breach events and a fascination with social surveillance have all served to diminish community trust in our organisations. This has many organisations refocusing on security and privacy, with attention to Privacy by Design (PbD) reflected in policy, product offerings and communications. However, a selective approach to PbD – ‘PbD lite’ – is becoming increasingly mainstream, with technology providers, online platforms and services, telcos and even our public bodies. PbD lite can create an impression that an organisation is effectively meeting security and privacy expectations and can be trusted over others; however it has a sinister side that cannot be overlooked.

A 10-minute session primer delivered by Nicole Stephensen will be followed by a facilitated panel session on building a PbD ethos within government and organisations, where participants will hear perspectives of a privacy regulator (Susan Shanley), privacy lawyer (Sophie Bradshaw), privacy officer (Nicola Bevitt) and privacy consultant (Nicole Stephensen) on moving from ‘PbD lite’ to right.

Key takeaways:

- Learn about the factors diminishing community trust in our organisations
- Refresh understanding of Privacy by Design (PbD)
- Learn about PbD lite and the pitfalls of taking this approach
- Hear perspectives of a privacy regulator, privacy lawyer, privacy officer and privacy consultant on building a PbD ethos within government and organisations

Presenters:
NICOLE STEPHENSEN, SUSAN SHANLEY, SOPHIE BRADSHAW & NICOLA BEVITT

HUMAN FACTORS
11:30 AM – 12:10 PM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Lazy writing: The information security nightmare that is AI generated text

ChatGPT is taking the world by storm! ChatGPT is an AI chatbot that uses natural language processing to create humanlike conversational dialogue. The language model can respond to questions and compose various written content, including articles, social media posts, essays, code and emails.

Marketers love it. Schools and universities are altering the way they assess students because of it. However, the knock-on effects of AI-generated text are yet to be seen. The labour of writing documents from scratch can be greatly reduced, and with it, the cost of those deliverables. And all the while, your information flows through an uncontrolled portal.

In this presentation, we will discuss the dangers inherent to allowing third-party software to create content for your organisation, and the logical result of this new technology.

Presenter:
KRISTINE SIHTO

COPS AND ROBBERS: GRC & CYBER CRIME
11:30 AM – 12:10 PM
QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Managing burnout and fatigue in security operations

Fatigue and burnout is a significant risk for security operations teams, and the organisations that rely on them to keep them safe through their detection and response capabilities. With the increasing threat environment, there is more demand than ever for experienced security operations staff. But there are also more stressors than ever on them. This can lead to burnout, which can decrease engagement, performance or retention.

In this presentation, Phil talks about his experiences in security operations, and looks at what are some of the key drivers behind fatigue and burnout, and what we can do to address these risks.

Presenter:
PHIL COLE

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
1:15 PM – 1:55 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Develop and implement cyber security assurance programs for major infrastructure projects

A goal of owners, operators and constructors building major infrastructure projects is to ensure that the infrastructure is safe and secure when it goes into operation. Ensuring cyber security risks have been appropriately addressed within the infrastructure project starts with clearly defining the risk framework governing the major infrastructure and scoping the required systems and services. It ends with the regulators allowing the infrastructure to enter the operation and maintenance phase of the assets.

Throughout this time, there are many challenges, including the extended duration of an infrastructure project, the way construction contracts are structured, the requirements of direct and indirect stakeholders, and the need to satisfy regulatory authorities who provide the approval to operate.

This session explores vital activities to help cyber security and risk practitioners understand essential elements of managing cyber security in infrastructure projects and what roles are required to help smooth the transition into operations.

Presenter:
PETER CLISSOLD

HUMAN FACTORS
1:15 PM – 1:55 PM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Cyber Presilience - Engaged people are the strongest layer in a cyber defence strategy

Cyber security is Presilience in action. Presilience is proactive prevention, enhanced decision making and high performance leadership. Each one make up the elements required for a layered cyber defense strategy. One element is missing. People. Individuals in an organisation represents the biggest vulnerability, but can also create the best opportunity for an organisation to achieve it's cyber objectives, fit for purpose. No threat vector is impenetrable. The human factor is one of the most powerful defense strategies in the continual pursuit of a more mature cyber posture.

Cyber is so much more than a technical risk and we need to understand the business and human risk considerations and opportunities. It's also not just about compliance but also resilience and Presilience in action.

Policies are driven from the top down, and often not adopted by the masses for a variety of reasons. Implementation must be adopted from the bottom up. Understanding how the individual manages their own risk, and makes decisions based on their personal, work and virtual life is the first step to embedding good cyber risk behaviour. How teams interact with one another, perform and make decisions, creates a high performing culture, which results in a Presilient organisation that uses cyber risk as an opportunity to perform better and proactively reduce the impact or the likelihood of a successful breach. Focusing on business growth is important, but it's as important to identify what factors can prevent such advancement and use that as a spring board for proactive prevention.

Presenters:

DR GAVRIEL SCHNEIDER & DAVE COHEN

COPS AND ROBBERS: GRC & CYBER CRIME

1:15 PM – 1:55 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

I am whoever I say I am: Stealing client data from around the world

Users entrust their data to the companies and agencies they share it with. Security teams however are finding just how painful having gaps in the systems really are. How well do these controls work? And how much assurance do you have that an attacker can be stopped? From ransomware to full breaches, how do attackers see the network and breach client data?

In this presentation, you will hear from a seasoned red teamer about the insights learned after breaking into dozens of systems and the common mistakes security teams make that allow an attacker to get behind the defences.

You will get a glimpse behind the scenes of the techniques real attackers use to frightening effect, how they operate and what they avoid in an entertaining look on the state of security today.

Presenter:
JAMES ANDERSON

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
2:00 PM – 2:40 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

The communications playbook: The key to successful and impactful cyber conversations with executives

Security leaders are constantly dealing with a mix of changing threat environments, rapidly evolving technology and ever-increasing operational challenges - but they regularly point to one challenge that they find the most difficult – communicating to leadership outside security.

Getting buy-in from the board or senior leadership can be critical to funding initiative or changing business practices – but to succeed, objectives, progress and outcomes need to be framed in language that provide business and risk perspectives outside of the security sphere.

In this presentation, Yvette will draw upon her experience in communicating with senior leadership and boards and will help you develop effective and impactful communications to articulate cyber risk to a non-cyber audience.

The following topics will be discussed:

- Why is it important to align with leadership
- Important things NOT to do
- What is top of mind for boards
- The three most common questions asked by leadership and the board
- How to effectively communicate your program

Presenter:
YVETTE LEJINS

HUMAN FACTORS
2:00 PM – 2:40 PM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Nailing the first 100 days as a CISO

With the recent spate of cyber attacks and the accompanying media scrutiny, cyber security is front and centre of many boardroom discussions in Australia. Needless to say, there has never been more pressure on cyber executives to get their strategy right. But, what exactly should a new cyber leader do within their first 100 days to set up for success? How can they filter out the noise, to prioritize key activities that will yield the most benefits?

In this session, Ashwin will share a framework on the key initiatives new and seasoned cyber executives can implement within the first 100 days. This approach has been refined over time through hard lessons learnt in the trenches by industry veterans who have mastered the art of stakeholder management.

The session will resonate with new and inexperienced cyber leaders looking for guidance on how to succeed in a CISO or a cyber-executive role. They will learn the key initiatives to prioritize to maximize their impact early on and gain the support of the C-suite.

This session will divide the first 100 days into various phases. Ashwin will share key considerations prior to taking on a CISO type role, importance of understanding the business, alignment of cyber strategy to business objectives, stakeholder management, how to gaining executive sponsorship for cyber security programs, importance of incident response and tabletop exercise, assessment of current cyber maturity, risk management and gap analysis, and much more!

Presenter:
ASHWIN RAM

COPS AND ROBBERS: GRC & CYBER CRIME
2:00 PM – 2:40 PM
QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

SOARing automation for Blue Teams

Automation is a subject fraught with a mixture of fear and admiration. From our earliest history with evolving technology, manufacturing and fear of job loss, the rise in AI and machine-based learning has only expanded the problem space considerably.

Early efforts to apply automation technology in a security context have been met with mixed success, with many leading practices shying away from automation. This has led to innovations in the offensive realm where tactics, techniques, and procedures as well as tooling have evolved to make use of automation. Therefore, it stands to reason that a modern SOC must also embrace the benefits of automation if Blue Teams are to successfully defend their organisations.

In this presentation, we will provide an “in the trenches” perspective from both speakers experiences, inside a SOC working as a Managed Services Security Provider (MSSP) that has leapt headfirst down the automation rabbit hole. This presentation will provide context on security automation from an offensive and a defensive angle, address many of the fears and concerns to do with automation and provide high level use cases for security automation and SOC enhancements that anyone can apply to their environment.

Presenters:
JARROD LOIDL & KYLE LAMONT

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
2:45 PM – 3:25 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Weak signals, weak signals everywhere! A framework for early-detection of organisational vulnerability to cyber attacks

Adopting a holistic approach to protect modern organisations from cyber breaches is more easily said than done. What should we be focusing on? How should we prioritise cyber risks? What vulnerability factors are under our control? Where are our organisational boundaries? Whilst acknowledging the importance of human and organisational factors, current approaches to vulnerability management focus overwhelmingly on the technical side of things - protect your networks, gain intel on current threats, select the most appropriate architecture, rely on reputable MSPs, educate your workforce, etc. No one, however, has the perfect recipe for the "do-it-all".

In this presentation, Dr Ivano will propose a comprehensive framework for early detection of organisational vulnerability to cyber breaches based on Macro Ergonomics, a well established approach coming from safety and reliability engineering. Macro Ergonomics 'slices' organisations in 4 + 6 layers (these being Individual, Tools & Technology, Task, Environment and Organisational Policy, Culture, Communication, Structure, Implementation and Strategy). Organisational performance is affected by factors that originate at each of those 4 + 6 layers. For example, negligence in detecting a threat alarm can originate at the Individual layer (e.g., adverse psychological state in a SOC operator; human factors).

The proposed Macro Ergonomic framework is the result of an intense research activity conducted in the last year, investigating industry best practices and academic literature on the topic and applying the framework to a real-world organisation. By joining this session, participants will be more familiar with Macro Ergonomics and will be able to apply it in their organisations, through a practical step-by-step guide on how to do so.

Presenter:
DR IVANO BONGIOVANNI

HUMAN FACTORS
2:45 PM – 3:25 PM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Building a bridge for young (cyber) engineers

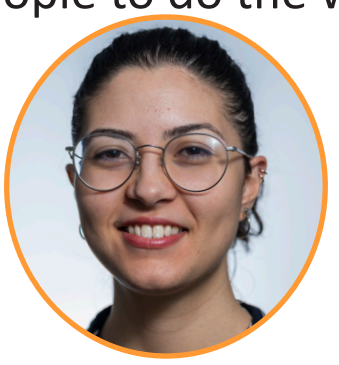
The cyber security industry is in desperate need of more people, but we also demand mid-to-senior level engineers for every role. Rather than there being an easy bridge for people like the 2020 version of myself to waltz across from university into the workforce, we ask young people everywhere to step into an abyss with little more than a loosely fixed and slightly frayed tightrope to keep them safe on their journey into cyber security!

As a young engineer, who knows many other young engineers, I know first-hand how difficult it can be to find a role when every single one requires a certain level of experience. I also know there's a solution, a bridge that can be built, and it's not as complex as people might think.

It is commonly known that when you network yourself well, it can be easier to enter a workforce. Still, that requires being able to attend the appropriate events to meet the appropriate people. As a young engineer, I only managed to start doing this once I'd broken into the industry, and thus got invited to these networking events. Before that, people like me didn't even know they existed!

As an entire industry, we need to do better and move these opportunities beyond the metaphorical perimeter. We can't complain about not having enough people to do the work when we're not making it easy for people to get into the industry, to do the work. We need to be reaching out to the new generation, hosting events for them to attend, running workshops to help them (and us) expand our security skills.

This presentation is all about sharing ideas to build a 6-lane superhighway bridge to encourage young engineers into cyber security.



Presenter:
JORDAN WATSON

COPS AND ROBBERS: GRC & CYBER CRIME
2:45 PM – 3:25 PM
QUEENS BALLROOM