BRISSEC

AISA
Cyber | smart · safe · secure

Zero Trust: The secret sauce to secure business enablement

Businesses have spoken. They want more flexibility, remote work, always-accessible data and they want it fast. If we look at cyber security strategies popular in the past, they almost run counter to those 4 things.

This is where Zero Trust and its principles can come in - to help enable businesses securely with the flexible technology they need. A future where cyber security is seen as an approachable protector rather than a bouncer standing at the front door of a venue checking the list and saying “No” over and over again. Patrons will try to sneak around the bouncer, so let’s discuss how to use Zero Trust to be the approachable protector.

Lee will also share three quick wins that any organisation can implement tomorrow to begin their Zero Trust journey.

Session covers the following topics:

- Challenges with balancing security, flexibility and business enablement
- How a positive cyber security team reputation within a business leads to reduced risk
- Where and why alignment with Zero Trust can help
- Three quick wins you can implement tomorrow

Sponsored by: sekuro

Presenter:
LEE ROEBIG

ROUNDTABLE DISCUSSION

10:45 AM - 11:25 AM; 11:30 AM - 12:10 PM; 1:15 PM - 1:55 PM & 2:00 PM - 2:40 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Is the Identity Layer the key to detecting and responding to lateral movement?

Identity Threat, Detection and Response has been highlighted by Analyst firms as a critical gap for many organisations.

Red Teams and attackers are usually successful when they go after Active Directory, because it is hard to detect and stop and the payoff is unfettered network and application access as well as persistence. The post-attack analysis for recent high profile attacks demonstrates the need to focus on the middle of MITRE - Credential Access, Discovery, Lateral Movement .

This roundtable will be facilitated by Attivo Networks, who are leaders in Identity Detection and Response. Come prepared with stories and questions from your own experience about how gaps in detection capability inside the network can lead to blind spots to share with your peers.

Session covers the following topics:

- If you protect end point and network and cloud infrastructure should you also protect identity?
- How can you detect attacks on identity infrastructure?
- If you detect an attack on identity infrastructure what can you do about it?
- How stolen credentials lead to breaches, and ideas on how to stop it

Presenters:

JIM COOK & MICHAEL GIOIA

Sponsored by: Attivo NETWORKS

ROUNDTABLE DISCUSSION

10:45 AM - 11:25 AM; 11:30 AM - 12:10 PM; 1:15 PM - 1:55 PM & 2:00 PM - 2:40 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

From Space Invaders to Attack Surface Management? What has changed since the 80s and how can you protect your attack surface?

Attack surface management is a term used in the industry to define an organisation's exposure to external (and internal) threats. The attack surface has evolved over the past few decades and this session will be a collaboration of ideas on how to define and protect your organisation's attack surface. And yes, there will be retro gaming included, as there is no better protection than the original air gap (i.e. no internet).

This discussion is lead by Trevor Laughton who is part of the Rapid7 Australia team in the role of Senior Account Executive. Trevor is a cyber security and cloud solution business professional with over 20 years' experience delivering customer expectations through sound Account Management and Technology Evangelism. Trevor's experience is built on a foundation of commercial success, technical skills and business management that ensure clients requirements are always exceeded. Trevor is also an enthusiastic Retro gamer whose favourites include Atari 2600, Super Nintendo and Sega Masters systems.

Session covers the following topics:

- Attack Surface Definition and naming conventions
- How can you protect what you don't know about?
- Strategies and mitigations for protecting your attack surface
- Retro Gaming – Yes there will be retro gaming in this session!

Sponsored by: RAPID7

Presenter:
TREVOR LAUGHTON

ROUNDTABLE DISCUSSION

10:45 AM - 11:25 AM; 11:30 AM - 12:10 PM; 1:15 PM - 1:55 PM & 2:00 PM - 2:40 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

The truth behind why 83% of Australian organisations are victim to a Privileged Account breach

There are two common denominators we continue to see amongst the alarming 83% of Australian organisations who have suffered a Privileged Account breach. Phising and Ransomware.

During this session, we will take you through how to identify a breach, how they happen, what strategies you can implement to avoid them and the contributing factors for why the attacker succeeds.

Get the answers to these questions:
- Why is it happening?
- Why are people being compromised when allocating budget into security?
- What is the common denominator behind these attacks?

Join us for a discussion to uncover the real reasons why such a significant percentage of Australian organisations are being breached, but more importantly the actions you can take now to get ahead of the curve and avoid ever being a part of that statistic.

Session covers the following topics:
- Why are organisations being compromised when they have allocated funding into security
- Why is this happening?
- How could it have been avoided?

Sponsored by: Delinea

Presenters:
JANE STEVENS & JEREMY POULTON

ROUNDTABLE DISCUSSION

10:45 AM - 11:25 AM AND 11:30 AM - 12:10 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Best practices to balance employee productivity, security and responsibility

Where we work, how we work and who we work with are more critical than ever, especially as the blended work environment will continue to be a popular model going forward. As a result, security, governance and compliance have increased – alongside risky habits and behaviours that employees have adopted to get their productivity up to get the job done.

Delinea research found that 79% of employees engage in risky behaviours, despite being aware of cybersecurity dangers. And 51% say their IT department should have sole responsibility to protect them and their organisations from cyber threats.

Session covers the following topics:

- Risky employee habits and behaviours to be aware of
- Ways that employees are sacrificing security for productivity
- Approaches to raise awareness of security issues in a blended workforce
- Building security compliance into your solutions to manage risk

Sponsored by: Delinea

Presenters:
JANE STEVENS & JEREMY POULTON

ROUNDTABLE DISCUSSION
1:15 PM - 1:55 PM AND 2:00 PM - 2:40 PM
QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Goodbye passwords, be gone forever!

There are so many good reasons for us to permanently remove the need for passwords forever, what's holding us back? The necessity to have a unique, strong password for every service is creating a significant security risk. You can't remember them all, it's just not possible. Using the same password more than once or an overly simple one are obvious no-nos and what's causing a lot of stolen credential issues.

Session covers the following topics:

- Credential stuffing is on the rise and stolen credentials are still the number one attack vector for data breaches
- If passwords are now passé, what should we use? What could be as secure as a password?
- We all want a smooth, fast, seamless user experience but rarely get it. Why is UX not a priority alongside security?

Sponsored by: okta

Presenter:
JAMES DARWIN

ROUNDTABLE DISCUSSION

10:45 AM - 11:25 AM; 11:30 AM - 12:10 PM; 1:15 PM - 1:55 PM & 2:00 PM - 2:40 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

The explosion of ransomware and proliferation of access brokers

Over the course of the last three years, in particular since the pandemic has begun, ransomware operations have exploded across the globe. Multiple highly sophisticated e-crime adversaries are operating ransomware for their own use, or selling access to ransomware-as-a-service variants, such as Conti and Lockbit 2.0. In the vast majority of these attacks, harvested credentials played a major role in the initial access phase. In this session we will discuss the tradecraft, proliferation of access brokers, and solutions to these problems.

Session covers the following topics:

- Ransomware deployments have increased over 400% since 2019/Q1 and continues to rise
- e-crime ecosystem is an interconnected web of adversaries selling specialty capabilities to criminals
- Identity has played a major role in initial access in most ransomware attacks

Sponsored by: CROWDSTRIKE

Presenter:
SCOTT JARKOFF

ROUNDTABLE DISCUSSION

10:45 AM - 11:25 AM AND 1:15 PM - 1:55 PM

QUEENS BALLROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Cyber implications of the Russian-Ukraine conflict

Offensive cyber operations have played a major role in the Russian-Ukraine conflict, in the lead-up to the conventional attack on Feb 25, and throughout the conflict thus far. Russian information operations and destructive cyber capabilities have been showcased over the course of the last 6-7 weeks, with a recent attack to the Ukrainian power grid having been perpetrated by VOODOO BEAR, the same actor responsible for attacking the Ukraine power grid in 2015 and 2016. In this session we will discuss the background of Russian cyber capabilities, and how that has played a supporting role in the kinetic attack.

Session covers the following topics:

- VOODOO BEAR and EMBER BEAR have engaged in destructive attacks and disinformation campaigns throughout the conflict
- Russia has a history of targeting Ukraine via offensive cyber operations
- Collateral damage and unintended consequences from these attacks has the potential to affect the entire globe

Sponsored by: CROWDSTRIKE

Presenter:
SCOTT JARKOFF

ROUNDTABLE DISCUSSION

11:30 AM - 12:10 PM AND 2:00 PM - 2:40 PM

QUEENS BALLROOM