BSIDES BRISBANE 2019

The Birth of BSides Brisbane…

BSides is known around the world as a technical con with great content. Even more than that, cons open up the social side of hacking--getting the community together to teach and learn from each other.

With BSides Brisbane, we want to help build an exciting atmosphere to learn and inspire the next generation of hackers.

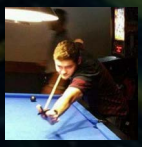
Running a local BSides has given us the chance to focus on some things where we're really interested in. For us, this takes the shape of:

Technical Presentations
Hands-on Workshops
Hardware, IoT, and ICS hacking
Hacking Competitions

We want to provide an opportunity for everyone to get involved--keeping the event affordable for students and everyone! The help of our generous sponsors and volunteers has made this possible. With this in mind we've also been working hard to bring in tech that a lot of people may not have had a chance to work with (PLCs, IoT, ICS protocols) and provide a really valuable and unique experience!

Thank you all for making the first BSides Brisbane possible.
Be excellent to each other!
- the BSides Brisbane Crew <3

Speaker Bios 1.



Mike Monnik
@securitymeta_

A Beginner's Introduction to Drone Security- I lead the Privasec RED and DroneSec team in Melbourne, Australia. DroneSec specialises in drone security, hardening and hacking. My passion projects are within Open-Source Intelligence, Drones and Counter-Terrorism. I once accidentally landed a job as a chef during a red team engagement; hence being known as 'chef' within Privasec.

Christopher Biggs
@unixbigot

Solving The Pigeon Obesity Crisis - Christopher Biggs was there at the birth of Linux and 386BSD. His interest in electronics and connected devices goes back even further. Christopher is now the principal of Accelerando Consulting, a boutique consultancy specialising in IoT, DevOps and Cloud Data. He also organises the Brisbane Internet of Things interest group, and is an international conference speaker.

David
@shh_dontell

Spent the last 9 years in financial services working across a range of security disciplines, but a good chunk of that time in security governance. Over the last 2 years I have been focused on cloud (all 3) and application security.
Currently I am working as a security architect and heavily focused in GCP on a production Kubernetes workload. Speaker at BSides Melbourne 2019.

Dr Monique Mann
@DrMoniqueMann

Dr. Monique Mann is the Vice Chancellor's Research Fellow in Technology and Regulation at the Faculty of Law, Queensland University of Technology. Dr Mann is advancing a program of socio-legal research on the intersecting topics of algorithmic justice, police technology, surveillance, and transnational online policing. She is on the Board of Directors of the Australian Privacy Foundation.

Traditional boundaries have shifted

The technology revolution has shifted traditional boundaries. Businesses now operate in an increasingly interconnected digital ecosystem. While offering opportunities for innovation and productivity, the Cyber era also presents new risks and challenges.

PwC is all about you. Your personal and professional development, your achievement, your lifelong learning, your individuality and your choices. Whether you're just starting out or an experienced professional, your future starts here.

www.pwc.com.au/cyber

pwc

Cyber Security for Operational Technology (OT) and Critical Infrastructure (CI)

Securing critical environments from digital disruption

As critical infrastructure and services continue to increase their dependence on technology, the risk of digital disruption through cyber attacks is also increasing. PwC Cyber offers a range of services to help organisations and governments build cyber resilience against these threats drawing on global experience working with multiple industry sectors, including Energy, Utilities, Resources, Manufacturing and Transportation. We pride ourselves on bringing together cyber technical expertise with deep industry knowledge – a team capable of engaging across the spectrum of stakeholders from OT engineers in the field to executives in the boardroom.

Tailored Security Testing

Understanding your operational risks and providing a tailored approach towards executing security tests on critical assets within your environment highlights areas of opportunity to strengthen cyber resilience. We have developed a proven methodology for conducting this type of testing in a safe and controlled manner that simulates real-world impacts and consequences.

Crisis Simulation and Game of Threats™

Responding to cyber events in an OT/CI environment demands coordinated cross-functional planning and simulated testing. PwC's unique offering in this space combines realistic table-top simulation exercises with our Game of Threats™ – a gamification of cyber attacks that immerses participants in an attack scenario for a highly effective learning experience.

Asset Discovery and Identification

In order to protect critical assets a key first step is gaining full visibility of the technology environment. We have partnered with market-leading technology providers that specialise in discovery of assets within critical infrastructure and industrial control system environments and provide ongoing visibility of changes to minimise risk of disruption.

Secure Design and Collaboration

Critical Infrastructure and OT environments require 'secure by design' principles to be embedded across multiple layers – not only technology (hardware, software and networks) but also across broad stakeholder groups including IT, operations, health and safety, legal and government/regulatory bodies. We can help you navigate these complex interactions and guide you throughout the development and implementation of tailored security strategies, frameworks, standards and architectures.

Cyber Threat Modelling

Understanding the cyber threat landscape is key to ensuring CI and OT systems are designed and built to be resilient against relevant threats, which can manifest themselves digitally and/or physically. Our threat modelling exercises establish a risk-based foundation to guide investment decisions and areas of focus from initial design and build through to remediation of known issues.

For more information visit pwc.com.au

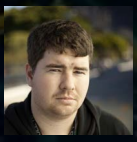
Main Presentations Hall Schedule

Main presentation hall is room GP-Z-411

Start	Finish	Talk Info
9:00am	**9:30am**	**OPENING**
		Presented by: Founders and MC BSides founders and MC welcome participants to the conference, introduce the days MC and kick things off!
9:30am	**10:30am**	**A BEGINNER'S INTRODUCTION TO DRONE SECURITY**
		Presented by: Mike Monnik @securitymeta_ Mike has joined the #BSidesBrisbane2019 lineup to talk about drone security, and how they can be used for offensive engagements in Red Teams, Pen Testing and even Terrorism, as they tie SDR, InfoSec and Physical-Kinetics into one crazy, hovering laptop.
10:30am	**11:00am**	**SOLVING THE PIGEON OBESITY CRISIS**
		Presented by: Christopher Biggs @unixbigot We welcome Chris to #BSidesBrisbane2019! He will be presenting on key management within the IOT space, with a focus on how the hardware element of IOT attempts provide a secure channel for certificate distribution.
11:00am	**12:00pm**	**PURPLE CONTAINERS: ATTACK & DEFENSE ACROSS THE FULL CONTAINER STACK**
		Presented by: David @shh_dontell David will be presenting a dense but fascinating talk on the securing of containers from the top to bottom of the stack; Highlighting threats & problems at each layer and importantly the solutions to address them.
12:00pm	**1:00pm**	**LUNCH BREAK**
1:00pm	**1:30pm**	**'ASS ACCESS' BUT NOT 'A BACKDOOR'?**
		Presented by: Dr Monique Mann @DrMoniqueMann Monique will be examining the #waronmaths, including issues such as impacts on privacy and information security, the local tech industry, transnational data flows, and oversight (or lack thereof) of the new powers.

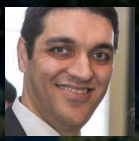
Start	Finish	Talk Info
1:30pm	2:30pm	**BLUE TEAMING YO ICS**
		Presented by: Bruce Large @belarge Bruce will cover some of the common cyber security frameworks that are relevant for Operational Technology (OT)/ Industrial Control Systems (ICS). This presentation includes a bunch of stuff he wishes he had known when operating OT networks.
2:30pm	3:00pm	**Simon Harvey**
		Presented by: Simon Harvey Simon will be presenting his thoughts on the current state of mental health within the cyber security industry, and will touch on how we can identify, support and help each other through the mental ups and downs; while also detailing what we can practically do to support each other at the community level.
3:00pm	4:00pm	**RED TEAMING COWBOYS: WHY SHOULD WE CARE ABOUT INFRASTRUCTURE?**
		Presented by: Riley Kidd Riley will demonstrate, by example, different approaches and what can go wrong when deploying and configuring your Red Teaming infrastructure. We will present a mature and resilient solution while also explaining how a simple 8-bit checksum could blow your whole covert operation wide open.
4:00pm	5:00pm	**BEYOND THE HYPE: MACHINE LEARNING FOR SECURITY**
		Presented by: Anthony G. Tellez @anthonygtellez Anthony is a data scientist at Splunk and will give an overview of ML & AI Concepts, including what data science is and the promise of AI for security analysts. He will also give us a walkthrough of use cases in detection of ransomware and botnet using machine learning.
5:00pm	5:30pm	**CLOSE OUT**
		Presented by: Founders and MC BSides founders and MC will close out the first BSides Brisbane security conference, announce details around the after party, and provide an update on the year to come.

Speaker Bios 2



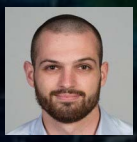
Bruce Large
@belarge

Bruce is a telecoms engineer who enjoys low latency & low jitter pings. He is down for Cyber Security Frameworks and time synchronised logs.



Simon Harvey

Simon is an Information Security Professional with nearly 20 years of Information Security-related Academic Research, Business Consulting and Management experience. He is currently employed as an Enterprise Security Architect at a large financial services organisation; and is overcoming his natural shyness by becoming more actively involved within the local InfoSec community, such as being part of the organising team for AISA's BrisSec Conference between 2017 and 2019.
He is unfairly tarnished by his peers for his terrible Dad Jokes.



Riley Kidd

Riley is a Technical Manager in Assurance Services for eSecure and has worked across a broad range of technically focused security services including large-scale international Red Teaming and penetration testing. When he isn't breaking things on purpose across layers 1-7, he is doing it by accident in layer 8.

Anthony G. Tellez
@anthonygtellez

Staff data Scientist @ Splunk

Workshops Schedule

ROOM GP-Z-606	
8:00am to 12:00pm	**Windows Privilege Escalation**
12:00pm to 12:30pm	**Lunch Break**
12:30pm to 4:00pm	**Garden Variety Automation**

ROOM GP-Z-607	
8:00am to 12:00pm	**Hacking SkyNet**
12:00pm to 12:30pm	**Lunch Break**
12:30pm to 4:00pm	**APNIC Training**

CTF

9:00am-4:00pm

ROOM GP-Z-504

Sponsored by Red Hat

Red Hat Product Security is hiring for Offensive Security Engineers, and Vulnerability Analysts in Australia to work on Hosted Products and Services offerings.

Offensive Security Engineer - Brisbane preferred, Remote Australia possible
You'll be finding vulnerabilities, and developing exploits against our Host Products and Services offerings. You will then collaborate with relevant product teams to address these vulnerabilities. You should have a deep understanding of vulnerability development and exploitation, solid understanding of container technologies, such as OpenShift, and Kubernetes. Strong understanding of linux internals, and user toolchains, particularly Red Hat Enterprise Linux.

Vulnerability Analyst - Brisbane preferred, Remote Australia possible
You will be analysing and triaging vulnerabilities relevant to hosted products and services. You will be working with product teams to develop and verify thread models, challenge security assumptions, and address vulnerabilities in existing, and upcoming products. You should have excellent written and spoken communication ability in English. Solid experience with security vulnerability response, as well as with code, and application auditing.

Please contact Gabriel Rocha <grocha@redhat.com> from Red Hat Product Security for inquiries.

Security Assurance

Managed Security

Security Testing

TSS Cyber

Australia's Leading
Cyber Security Company

@TSSCyber

tsscyber.com.au

medium.com/tsscyber

Arm your analysts. Power your SOC.

Security analytics at the speed of thought

elastic

proud sponsors

Notes

Where to eat

Burger Urge (11:00am – 6:00pm)
Located Y Block Level 4 – Ground Floor

Origin Kebab (9:00am – 3:00pm)
Located P Block Level 3 Food Court

Raw Press (8:00am – 3:00pm)
Located B Block; Corner of B Block off Main Drive

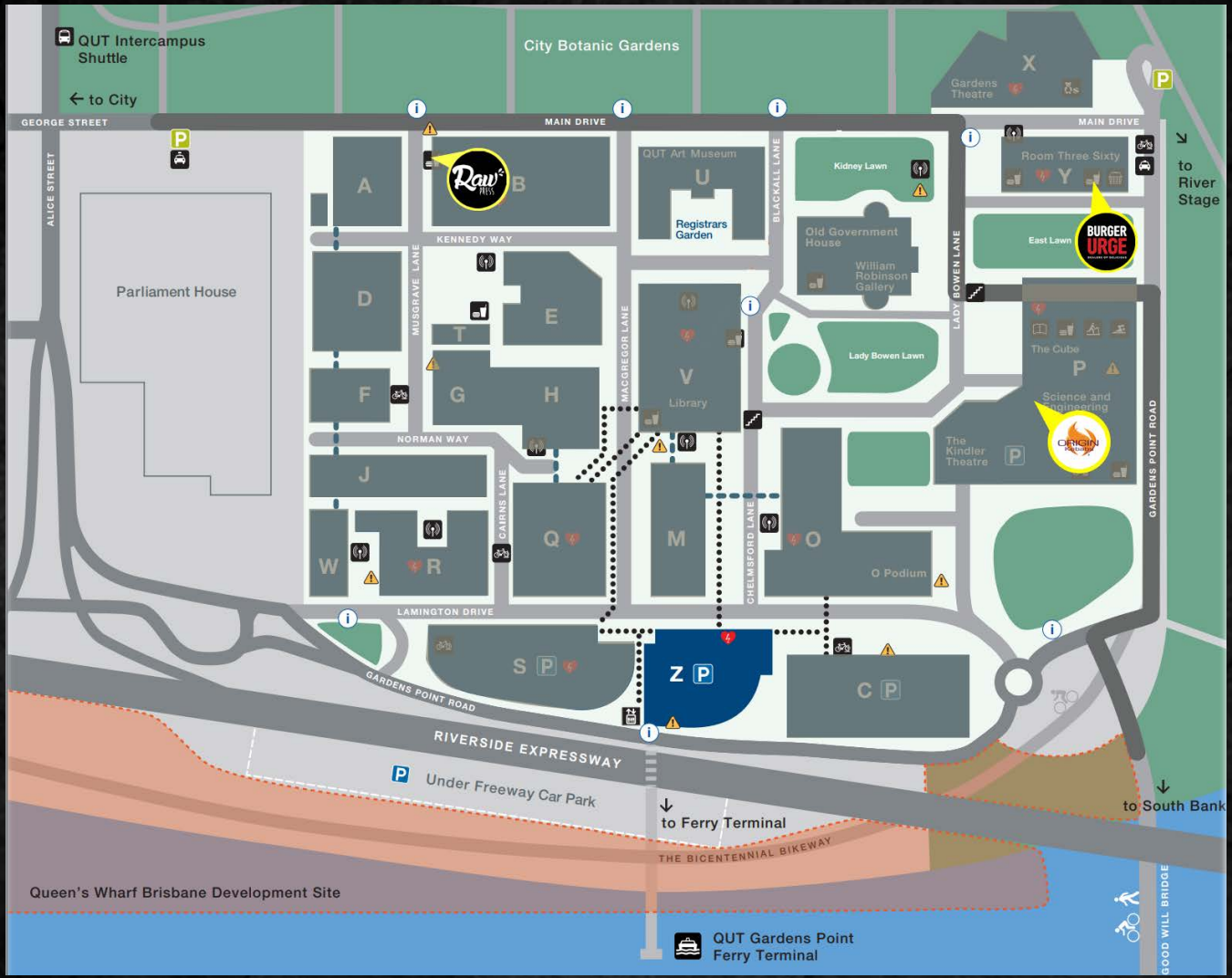
Where to get caffeine

Raw Press (8:00am – 3:00pm)
Located B Block; Corner of B Block off Main Drive

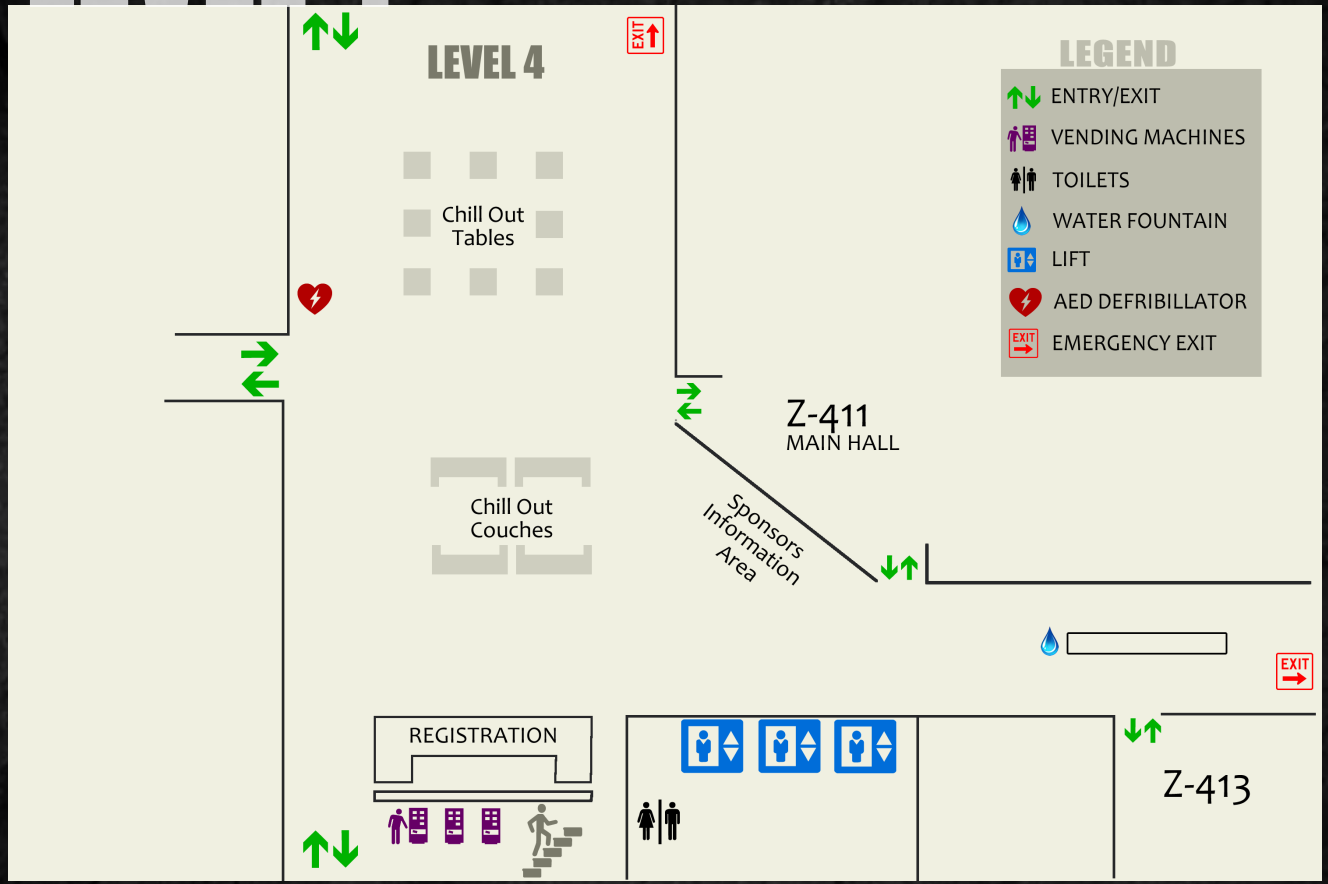
Where to seek HELP

For **Emergencies**, call 000 (then call +61 7 3138 8888)
QUT Security - +61 7 3138 5585 1800 065 585 (freecall)

QUT Gardens Point Campus Map



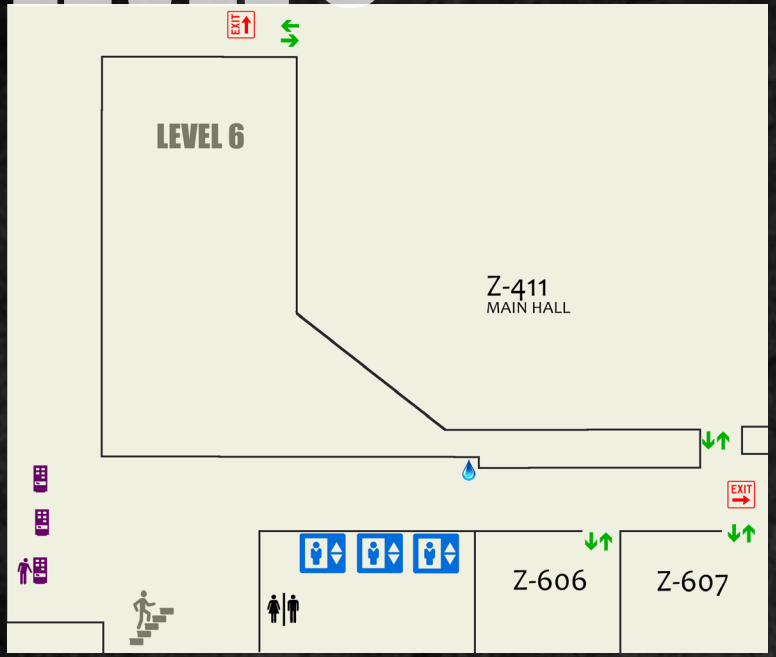
LEVEL 4



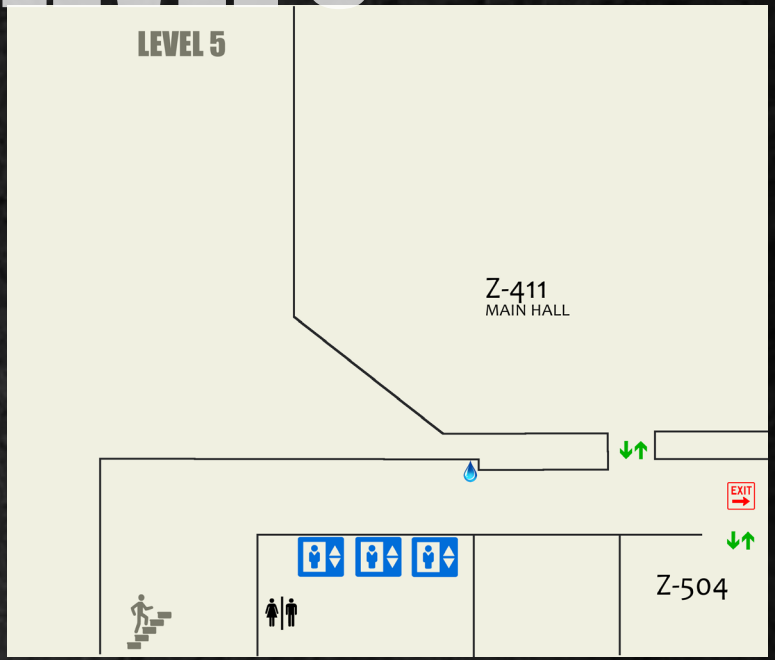
Map of Z Block

LEVEL 6

These maps are only a guide, please refer to venue signage for exact locations.



LEVEL 5




Hardware Hacker Village
Featuring:
Hack-A-Bomb
PLC Skilltester
Turnstile Hacker
Lockbox
City Power Grid
MACY'S

See you next year!

BSIDES BRISBANE 2019