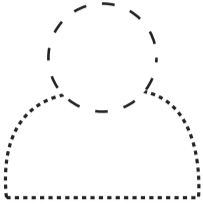## ACSC

Australian Cyber Security Centre

- HuntIR by ACSC
- HuntIR by ACSC

Adrian Justice

Adrian (@zeroedtech) is threat hunter specialising in IIS, webshells and .NET, with a little bit of software development thrown in.

- Bringing Harmony to IIS: Using game mods to protect (or nuke) your web server

AFK Choir

AFK = Geek ∩ Singer

We are a Canberra-based group that enjoys singing about the important things in life, including Star Wars, Star Trek, Lord of the Rings, zombies, and computer games.

- AFK

Amy Nightingale

Hi, I'm Amy - I'm currently the Security Engineer at Cydarm, an incident response startup, working closely with a broad range of teams to develop the core platform. By night, I am an Assistant Lecturer at Sydney University teaching an intensive 26-week cybersecurity bootcamp to educate newcomers and re-skill professionals transitioning into the cybersecurity industry.

I come from a very strong background in SIEM/SOARs (specialising in Splunk), development in a variety of programming languages and applications and fluency in the Japanese language. I regularly apply these skills on personal projects and contributing to the Security community, including hosting workshops, volunteering at events and building out CTF platforms and scenarios.

- RF Demos
- RF Demos
- RF Demos
- RF Demos
- RF Demos
- RF Demos
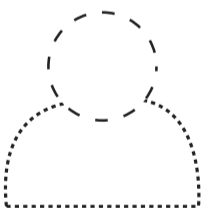
Artemis Calvi

- Careers Village: What is - Application Security
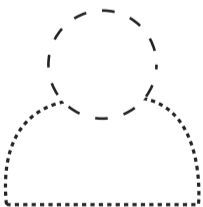
CG

CG (@int3rrupt) is a Principal, cyber espionage focused, Intrusion Analyst and Threat Hunter at CrowdStrike (OverWatch). Formerly, he was a postgraduate course writer and lecturer at the Australian Defence Force Academy, and an employee of the Australian Department of Defence.

- 'Hold Your Horses': Stopping A North Korean Supply Chain Attack Before It Bolts
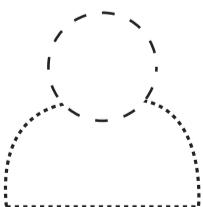
Courtney

Courtney is a Technical Director in a team called Research on Operational, Critical and Emerging Technology. She has worked in cyber security since 2015, and is passionate about securing our critical infrastructure and encouraging diversity in cyber security.

- Hardware in the Loop: Building a Rack for Substation Protection

Cybears

The Cybears are a Canberra based social CTF team consisting of a diverse range of individuals brought together by a passion for cyber security. They play in both local and international CTF competitions and are actively involved in the Australian cyber security community.

- Intro to Capture-the-Flag (CTF) Session 2
- CTF Mayhem Unleashed!
- CTF Mayhem Unleashed!
- Intro to Capture-the-Flag (CTF) Session 1
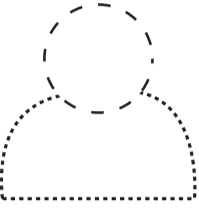
David Collett

David is a Software Developer with the Digital Surveillance Collection branch at the Australian Federal Police and formerly worked for ASD. He has 20yrs experience in the computer security field.

- IoT Malware IRL

David Robinson

Dave/Karit in his time working in various parts of the IT industry has developed a skillset that encompasses various disciplines in the information security domain. Dave currently works as a Penetration Tester at ZX Security in Wellington and runs Kākācon.

Since joining ZX Security Dave has presented at DefCon, Kiwicon, Aerospace Village @ DefCon, BSidesCBR, ChCon, Unrestcon and at numerous local meetups; along with running training at Kiwicon, Syscan, CrikeyCon, ChCon and TuskCon. He also has a keen interest in aerospace, lock-picking and all things wireless.

- A hacker's view of DoS attacks
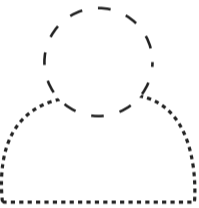
Eldar Marcussen

Eldar is an accomplished practitioner in the security research and penetration testing space. He is a long time bug hunter with a large number of published advisories, exploits and conference presentations at leading security conferences all over the world. In addition to finding vulnerabilities he develops and maintains several open source projects aimed at web application security and penetration testing. His tools and research are featured in most security oriented Linux distros and industry leading books.

- Locks on the wire
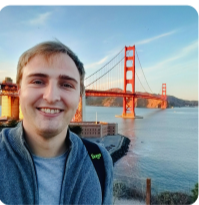
Javan Rasokat

Javan works as a Senior Application Security Specialist at Sage and supports software development teams in securing the software development life cycle. On the side he is lecturing Secure Coding at DHBW University, Germany. His journey as an ethical hacker began at an early age, where he began to automate online games using bots and identified security bugs, which he then reported to the game operators. He later turned his interests into his profession and became a security consultant. He brings experience as a penetration tester and holds certifications, such as GXPN, CISSP, CCSP and CSSLP, as well as a Master's degree in IT Security Management. Javan has presented before at conferences such as OWASP AppSec SanFran, Ekoparty, and HITB Singapore.

- The Dark Side of Large Language Models: Uncovering and Overcoming of Vulnerabilities
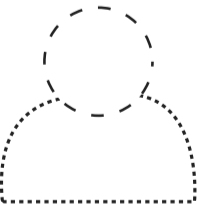
Jayden Caelli

I am a penetration tester at SilentGrid. My main focus during this position is a focus on malware development.

- Introduction to Malware Development in C#

John Gerardos

John Gerardos is an enterprise security architect and penetration tester with over 15 years' experience who loves to make, break, and fix stuff. John can usually be found researching the latest security topics, playing with ham radios, tinkering with random objects or roaming around security conferences. As well as his day job, John actively participates within the information security community. He regularly mentors students and Cyber Security professionals, attends security conferences, and runs several security training sessions.
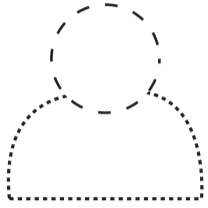
- RF Demos
- RF Demos

- RF Demos
- RF Demos
- RF Demos
- RF Demos

John Uhlmann

John (he/him) is a Security Research Engineer at Elastic, where he focuses on scalable Windows in-memory malware detection. Prior to this he did similar work at the Australian Cyber Security Centre.
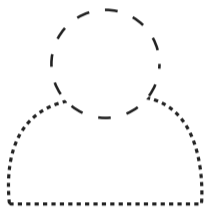
- GetInjectedThreadEx - improved heuristics for suspicious thread creations

Josh Johnson

Josh spends far too much time designing electronics, building robots, and blinking LEDs in overly complex ways than is healthy.

- Designing a Badge Add-on in KiCad Day 3
- Designing a Badge Add-on in KiCad Day 1
- Designing a Badge Add-on in KiCad Day 2

Julian Abrahams

- Black Bag
- Black Bag
- Black Bag

Leo Adrien

Leo Adrien is an independent security researcher, postgraduate Computer Science student at Monash University, and recovering "security consultant". He primarily focuses on finding bugs in Windows, but somehow still spends an inordinate amount of time reading Linux kernel code. He often thinks about creating static analysis tools, but always ends up writing another fuzzer.

- Don't Lookaside or you'll miss it: Turning a Hyper-V cache miss into 200k cash

Lina Lau (@inversecos)

Lina is the Founder of XINTRA, a platform providing advanced cybersecurity training focused on APT techniques and detections. She has an extensive background in incident response, where she was formerly the Principal IR Consultant at Secureworks APJ and the AAPAC Incident Response lead for Accenture ANZ. She has worked in Incident Response for multiple years leading complex international cases covering sectors such as national defence, banking, energy, and manufacturing.

Lina is also a Black Hat trainer, SANS advisory board member and has presented at several international conferences and authored a book on cybersecurity. She currently holds the following certifications: GXPN, GASF, GREM, GCFA and OSCP.

- APT Attack Techniques in Azure Cloud

Louis Nyffenegger

Louis Nyffenegger is a seasoned security engineer and the founder of PentesterLab, a platform dedicated to teaching web penetration testing. With over a decade of experience in cybersecurity, Louis has focused on penetration testing, architecture analysis, and code reviews. He recently launched a YouTube channel, AppSecSchool, further extending his passion for education in application security.

- Keynote Session: The Journey to Mastery

Maddie Stone

Maddie Stone (@maddiestone) is a Security Researcher and leads the Exploits team within Google's Threat Analysis Group (TAG). For the past four years she's focused on 0-days that are actively exploited in-the-wild, first at Google Project Zero and now TAG. She has found vulnerabilities in many major platforms including Safari, Chrome, Android, and Windows. Previously, she was a reverse engineer focused on malware on the Android Security team.

- Keynote: When Exploits Aren't Binary
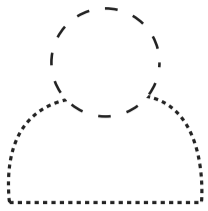
Matt Kurz

- Modern LInux Kernel Mitigations
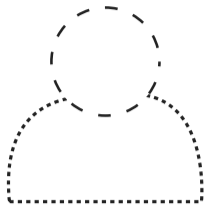
Peter

Peter Rankin is a secure software developer and vulnerability researcher for InfoSect. Outside of work he enjoys making devices do things they shouldn't and then never using them. Peter has previously worked as a vulnerability researcher at Azimuth Security, Penten and Australian Department of Defence.

He has volunteered for the BSides Canberra security conference for the last 5 years and has developed badge firmware include the 2019 "Nopia 1337". He is volunteering again this year and is developing the 2023 badge.
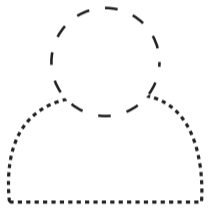
- Introducing the new bPod

phish

Principal Security Consultant at Aura Information Security. Enjoy hacking things and being a father ✌ @dunderhay on twitter

- Fan-Tastic RFID Thief: Revamping an old weaponised RFID reader tool

Ray Veldkamp

- Modern LInux Kernel Mitigations

Redacted

Redacted Information Security is a bespoke sovereign information security consulting firm based in Canberra, providing services to government and private sector industries at all classification levels.

```
Systems security planning, including strategic guidance and policy, procedure, and guideline development
IRAP assessments
Cybersecurity training
General consulting
```

Redacted can help organisations in uplifting their security posture, gaining regulatory compliance, and preparing for or conducting IRAP assessments. Get in touch at info@redacted.au.

- Black Bag
- Black Bag
- Black Bag

Ricki Burke

Ricki Burke is the founder of CyberSec People, helping organisations hire and scale security teams.

As a keen contributor to the infosec community, Ricki is involved as a co-organiser of BSides Gold Coast, SecTalks Gold Coast, host of the Hacking into Security podcast, ran career villages at AISA CyberCon and BSides Melbourne and presented at several conferences, including AusCERT, BSides Canberra, BSides Perth and BSides Melbourne and CHCon.

- Careers Panel: Neurodiversity
- Careers Panel - How to Build Your Brand and Career in Cyber
- Career Village: What Is - Red teaming
- Careers Village: What is - Application Security
- Careers Panel: CISO
- Careers: What is - Incident Response
- Careers: I'm hiring/networking
- CV Workshop

Rohan McLure

Rohan is an open-source hacker at IBM, working on enhancing security and performance on Linux on the Power processor architecture. He contributes to modernising and hardening the Linux kernel, as well as tuning performance in OpenSSL and other cryptographic libraries.

- Going out on a Limb: Accelerating Elliptic Curve Cryptography

Russell Currey

Russell is a vulnerability researcher at InfoSect, and a former Linux kernel developer focused on memory protections and microarchitectural security.

- An abridged history of Linux kernel hardening

Steven Coomber

Steven Coomber is an intelligence professional who has previously worked inside the National intelligence Community across counter-terrorism, counter-espionage and technical capabilities. He has advised government services in South-East Asia and delivered a variety of human-led data driven capability building programs to Five-Eyes and partner intelligence services in the Asia-Pacific, Middle East and African regions.

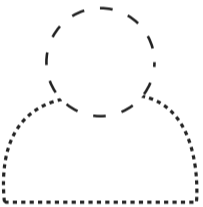- Comprehending Kayfabe: a lens for dealing with cognitive hacking, online influence and layered deception

Tim Noise

Tim is a professional Silvio Cesare impersonator

Bryce is an internet musician

- Ethan Hunt on a Budget

Ty Ridgeway

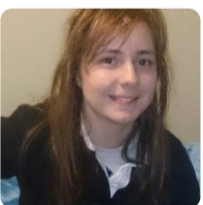- Black Bag
- Black Bag
- Black Bag

Zac Ecob

Second year computer science student @ UNSW. Binary nerd. Occasionally play CTFs for teams like Blitzkreig and Water Paddler. Have previously talked at conferences such as Bsides Sydney and Scones, mainly revolving around kernel exploitation.

- Scudo Allocator exploitation

Zoi Petroulias

Zoi is a Managing Consultant (Penetration Tester) at NCC Group. She has been working in the cyber security field as a Penetration Tester since 2016, particularly in consulting and financial services. Prior to this, Zoi has worked as a firmware engineer and continues to enjoy tinkering with hardware in her spare time.

- Case Studies in Point of Sale Hardware Hacking