Luke Andrew Brown

TSPV Clearance | 0439 944 696 | lukeandrewbrown@gmail.com

PROFESSIONAL SUMMARY

Luke is an accomplished and passionate information security specialist with nearly two decades of experience in IT. Throughout his career, he has cultivated exceptional customer service and stakeholder relationship skills, a problem-solving mindset, a stoic attitude under pressure, and an extreme level of adaptability. These skills have been honed through a wide range of unique IT and Cybersecurity experiences that range from solving mid-flight IT issues for the Prime Minister on his RAAF Aircraft to collaborating with the ACSC on purple team operations. Luke is deeply committed to achieving outcomes for the Australian government and believes that ASD is the perfect place to pursue this.

EDUCATION AND CERTIFICATIONS

UNSW Canberra: Master of Cyber Security (Digital Forensics) | Ongoing - Estimated 2024 completion
SANS: GIAC Experienced Incident Handler #346, GCIH, GCED, GSEC, GIAC Advisory Board
Cloud: AZ-104, AZ-500, SC-200
Offensive: EJPTv2
Other: Mental Health First Aid Accredited, ITIL Foundations v3
Studying for: ISC2 CISSP (Exam Booked for Dec 18. 2023), SC-100 Azure Security Architect Expert

WORK EXPERIENCE

Office of National Intelligence **Oct. 2022 – Present**

Cyber Security Officer. SFIA: SCTY 5 (Limited SCTY 6), SCAD 5, VUAS 4, INAS 3

- Designed and led the security assessment activities required as part of the Authority to Operate process in line with NIST 800-37 and the ISM for a complex large scale Azure cloud project. Built rapport with stakeholders such as cloud engineers, project managers, and IT management to foster a collaborative project mindset, and modularised security testing to ensure that the highest and most urgent risks were tested and treated first. The project received ATO for production without security ever being the bottleneck to progress.
- Led threat detection engineering activities during a significant purple team assessment operation in collaboration with ACSC's Cyber Maturity team, recording all malicious activities in a super timeline and ensuring that all findings were mitigated, preventable or detectable. This was achieved with a combination of Sentinel/Defender KQL queries, converting Sigma and Yara rules for ArcSight ESM compatibility.
- Deployed custom honeypots to detect stealthy bloodhound scans, Kerberoasting and DCSync Attacks, and popular windows privilege escalation scripts and techniques such as PowerUp, and designed future strategies for the implementation of canaries.
- Led essential eight assessment and uplift activities including an MFA implementation project that raised ONI to E8 Maturity Level 2. Detailed a strategy with the steps necessary to achieve Level 3.
- Conducted multiple Vulnerability Assessments and assisted with Penetration tests for on-premises and cloud-based networks for both Azure and AWS environments.
- Created a custom RunZero Asset attack surface management API integration with Tenable.SC to ensure that any gaps in our Tenable coverage were visible, and to add extra context for vulnerability management activities.

Department of Prime Minister and Cabinet **Sept. 2013 – Oct. 2022**

IT Support Advisor to the Prime Minister's Office, Acted IT Security Advisor, Acted VIP Support Team Lead SFIA: USUP 5, ITMG 5, RLMT 5, CSMG 5

- While travelling globally with the prime minister's office to more than 50 international summits, planned for and installed temporary office setups in hotels, convention centres, embassies, and even ambassadorial residences. Researched local communications standards and ensured that the PM and travelling party could reliably communicate - even in locations like Myanmar where iPhones were not supported on the 2G only cellular infrastructure. Lent technical expertise to, and cultivated relationships with DFAT, AFP, RAAF, and Hotel staff during the planning and execution phases of these trips.

- As the sole technical operator in country on many of these trips, took direct calls from the Prime Minister at any time of day or night and provided immediate solutions to requests spanning Level 1 helpdesk to network and systems administration tasks.
- Designed and implemented portable packet capture and intruder detection system capabilities based on Security Onion and PFSense that significantly enhanced the security posture of the temporary network setups which, until then, had no threat visibility mechanisms.
- Filled in for the IT Security Adviser on several occasions. Refreshed the departments ICT Security Policy, conducted Insider Threat investigations, managed several incident response activities, and produced GRC documentation.
- Acted as the VIP Support team lead on several occasions and mentored junior staff, especially on how to navigate stressful environments like the Prime Minister's office in a professional manner.
- Developed keen emotional intelligence, situational and political awareness. Extreme circumstances like changes of government meant working closely with staff who had lost their jobs after 6 weeks of gruelling election campaigning. Exemplified the maturity and resilience necessary to maintain both professional boundaries and public service impartiality.

Lockheed Martin Australia **Aug. 2012 – Sept. 2013**

Enterprise Operations Centre Administrator. SFIA: ITOP 4, RLMT 4

- Provided infrastructure and network security and performance administration as part of a rotational watch keeping team that operated 24/7 for the Australian Taxation Office.
- Optimised existing Splunk Dashboards and Rules to lower the false positive alert rate on Severity 1 incidents occurring due to Exchange Server temperature thresholds, which prevented high severity SLA breaches with a large monetary impact.

ASG Group **Feb. 2009 – Aug. 2012**

Service Desk Analyst, Desktop Support Analyst. SFIA: CSMG 3, USUP 3, ITOP 2

- Solved unfamiliar problems and patiently communicated technical solutions to non-technical staff over the phone.
- Talked an 80-year-old ex-governor general through the removal of a virus from his standalone PC with the use of command line tools in windows recovery mode, saving the time and money involved in getting a technician to his remote Queensland farm.
- Promoted into the Level 2 support team, involving Hardware Repair, Fiber Optic Patching, configuring SOE Images, SCCM deployment, Mobile Device Management, VLAN configurations, switch deployments, and secure disposal of hardware.

ACT Government **Nov. 2007 - Feb. 2009**

Project Support Officer - Windows XP SOE Rollout Project. SFIA: PROF 2, ITOP 1

- Part of a SOE Rollout Project Team that upgraded the entirety of the ACT Government from Windows 2000 to Windows XP, at locales such as courts, police stations, hospitals, and prisons, then provided on-site support in the following weeks as part of a 6-week rolling schedule.
- Coordinated and carried out the smooth and successful upgrade of the Emergency Department at Canberra Hospital. Designed a tailored rollout plan that included setting up concurrent workstations with pre-cached credentials and pre-installed software, and rate limited the rollout to 1 PC each weeknight at 0230, statistically the ED's quietest time. All PCs were successfully swapped with zero downtime, and Emergency Department stakeholders provided excellent feedback acknowledging the careful and diligent approach.

AWARDS AND COMMITEES

ONI Wellbeing Committee - 2023
PM&C Secretaries Excellence Award - Excellence in Collaboration - 2021
PM&C Secretaries Excellence Award - Individual Excellence - 2018
PM&C Secretaries Excellence Award - Individual Excellence – 2015
ASG 'In Focus' Award for Superior Customer Service – 2014