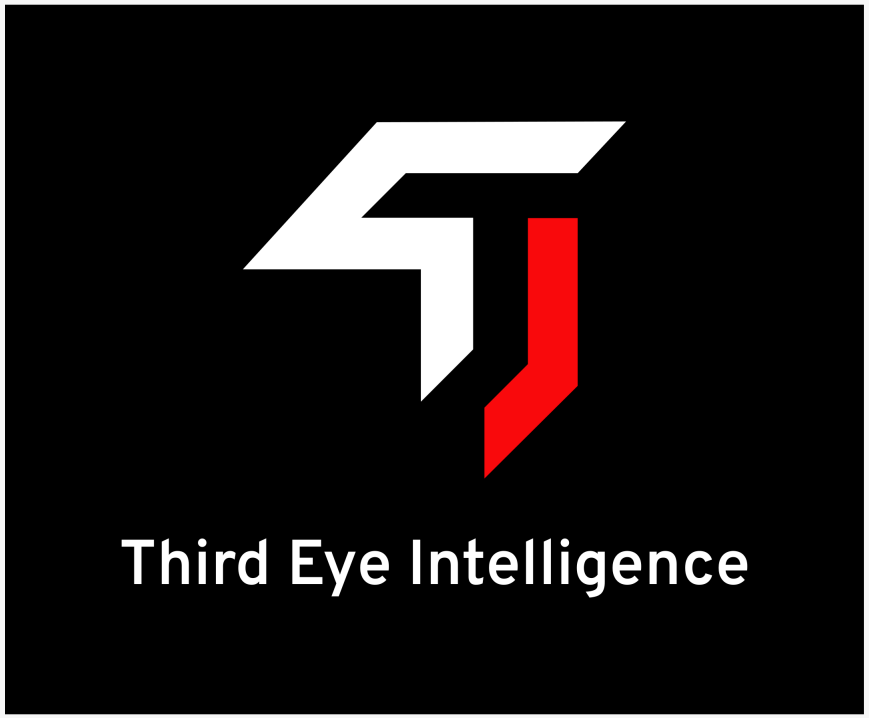
About Third Eye



- Founded in Australia, Third Eye Intelligence is a boutique consultancy firm with capabilities to provide contextual and actional intelligence.
- Third Eye Intelligence was created with aim to protect the community and organisations by providing best possible intelligence on opportunistic to nation state cyber criminals.
- Third Eye Intelligence provides consultancy on
  - Threat Intelligence Framework
  - Intelligence-Led Security Strategy
  - Malware Analysis and Research
  - Threat actor TTP's analysis and attribution
- Following slides contains high level of suggestions or improvement opportunities based on my experience. Would intend to discuss this further and assist in creating Cyber Security strategy.
- Contact Third Eye Intelligence
  - [redacted]

About Owner

Kunal Makwana

- Kunal Makwana (aka beardedavenger) has recently joined Macquarie Telecom as Threat Intelligence Lead in their fight against criminals using cyber as a means to accomplish their illusive motives.

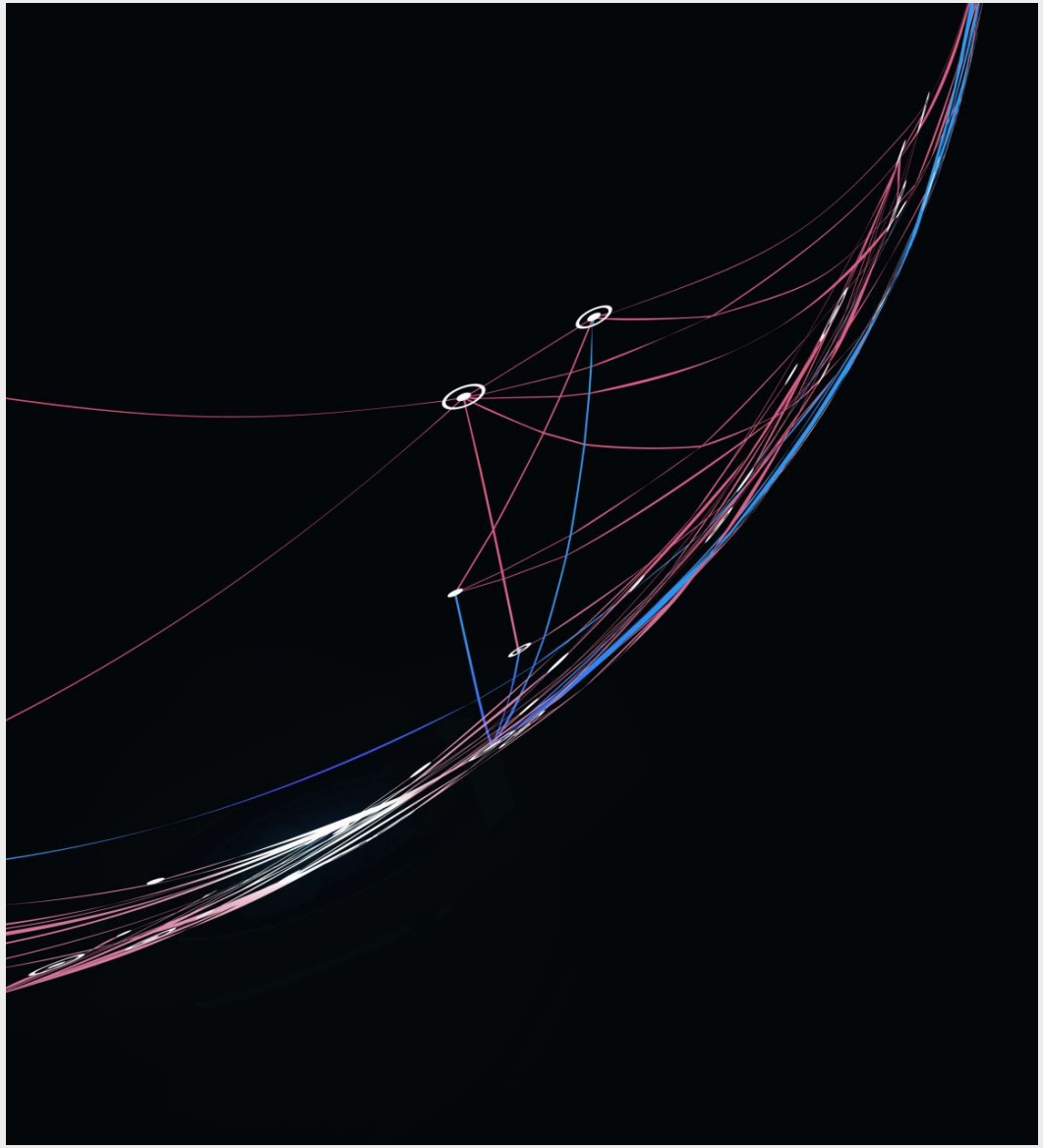
- His friends and colleagues consider him a passionate, highly intelligent, highly driven and charming individual. Kunal is one of the fortunate ones who did not steer away in career paths and has always stayed within fields where intelligence can be provided with information that was not there before and will be obsolete tomorrow.

- Kunal has almost 15+ years of experience in cyber, Fraud/Financial Crime and physical security. He has worked and managed multiple units such as Security Operations Centre, Threat Intelligence centres and operations, Incident Response teams, Red team operations and Vulnerability management, to improve organisational defences against threats and reduce overall risk posture.

- Kunal is also very active in consulting and assisting Law enforcement and government entities on local cyber threats. He has participated in AFP-led operations such as Operation DOLOS (BEC taskforce), Operation CAPERTEE (GOZI taskforce), and Operations RUTHVEN (U-Admin taskforce), assisting in takedown and attribution extending to information/intelligence exchange globally and locally related to financial crimes, terrorism, cybercrimes, nation-state threats and human trafficking.

- Community contribution and awareness blog (https://thatintel.blog) and creator of Bob and Chip, two imaginary characters discussing Cyber related topics, on LinkedIn.

2023-2030 Australian Cyber Security Strategy



Key Improvement opportunities

- Legislative, regulatory and legal reforms
- Intelligence Sharing improvements at Local Level
- Regional Cyber Security Resilience
- Security Awareness
- Response and Offensive capabilities
- Improvements in workforce and skills

Legislative, Regulatory and Legal reforms

Improvement opportunities

- Enhancing current cybersecurity frameworks, including Cyber Security Act and SOCI Act.
- All current frameworks are heavily towards compliance, and companies only tend to fulfil when it is due rather than ensuring all year-round controls are implemented as part of compliance.
- Evidence of compliance should also be beyond screenshots and must sign off on implementation.
- Clause to include legislative or regulatory compliance failure should or must be reported to the authorised body with a treatment plan within 72 hours of findings. This could be specific to those systems that hold or interprets customer data.
- Introducing Third Party engagement framework or regulation organisations must adhere to before and after the third parties are engaged. The framework/regulation should extend to notification if a breach occurs.
- Reducing mandatory incident reports to within 24 hours.

Intelligence Sharing improvements at Local Level

Improvement opportunities

- Recommendation to significantly improve cyber security-related articles currently being published by ACSC. The information is basic and on an ad-hoc basis. Usually, the trigger is media attention or attention from the United States. A report on threat actors that are known to target Australia should be a priority as well.
- ACSC provides sharing mechanisms via threat feeds and over the SLACK channel, usually without proper context and analysis. Good examples that follow are reports from CISA, FBI and especially NCFTA.
- In comparison to information shared by the ACSC/ASD on a given cyber threat, external public and vendor articles has more information. To build more robust and actionable deliverables for readers to consume, we can either leave it to organisations (small or big) to get vendor reports or try and improve in that aspect. A threat intelligence portal/platform with combined analysis, research articles, and sharing mechanisms is recommended.
- Sharing mechanisms also require threat intelligence platforms and a good understanding of the information being shared. However, many organisations do not have the ability to implement such platforms nor have the skills to manage it. In such cases, government agencies should have a program to assist in ensuring information can be received regardless of the capabilities.

Local workforce and skills including gov agencies

Improvement opportunities

- A good volume of talent has chosen to move to the private sector instead of working with gov agencies where one of the main motivations is pay difference. As a result, Gov agencies must re-think pay-grade policies to attract and retain talented individuals by matching market rates.

- Hiring fresh graduates is understandable as we must create employment opportunities; however, we should also prioritise hiring subject matter experts with actual field experience.

Regional awareness and support

Improvement opportunities

- Gov-supported incident response services. Many organisations, especially small to medium businesses, do not have an Incident Response or even cyber security function and, during an incident, usually engage local IT or a vendor. Each major city should also have walk-ins to get assistance during an incident.

- The ability to report incidents over a mobile phone and an app would be good.

- More marketing with podcasts, ACSC-sponsored conferences, advertisements, school and university guest lectures etc.

Other suggestions

- Monitoring and blocking of virtual numbers known for sending phishing SMS.

- Involvement of subject matter experts
  - In intelligence-gathering activities
  - Technical assistance during investigations
  - Undercover work to support threat actor actions and attribution. This is usually if they have access to the group or not.
  - Offensive capabilities.

- A known Eg. FBI-led task force in hunting down Trickbot operators had multiple security researchers on it who supported investigation on the technical side of things for malware analysis and offensive capabilities.