



CYBERMERC GUARD

Consulting services from experts in Cyber Threat Intelligence and Threat Hunt.

Suite 2, 31-37
Townshend St, Philip ACT 2606

info@cybermerc.com
www.cybermerc.com

ABOUT CYBERMERC

Cybermerc is an Australian-owned cyber security company, founded in 2016 by two brothers with backgrounds in law enforcement and national security. Cybermerc's services, training programmes and cyber security solutions are designed to forge collaborations across industry, government and academia, for collective defence of our Digital Borders.

Cybermerc's flagship solution, **AUSHIELD**, has been successfully deployed across Federal and State Government, Defence, Energy, Law Enforcement, Education and Health sectors. Cybermerc has trained hundreds of students, elevating their cyber skills and defensive capabilities.

"We can meet the challenge of cyber security as a nation. Through partnership and common purpose, we can be *secure together*."

Cybermerc was founded on the principle that we must build a collective defence to meet the challenges of cyber security and protect our Digital Borders.

We leverage our combined expertise across various technology sectors to improve the cyber capability of our clients. Along with our cutting-edge detection and protection solutions, our team of cyber and intelligence experts offer consulting services and training programmes to empower and enable cyber security for Australian businesses at all levels.

SERVICES

Cybermerc is able to offer the following services through individual engagements, as ongoing consultancies, or bundled to a package with our product offerings.

THREAT HUNT

We are experts in, and passionate about, finding evidence of malicious actors. Our Threat Hunting services can be delivered remotely or in person. Our preferred approach is to leverage our **AUSHIELD PROTECT** and **DETECT** technologies which provide full visibility of the network traffic and real time correlation with Cyber Threat Intelligence. Where needed, we can utilise your existing tools to perform threat hunting.

This service includes Incident Triage as needed and collaboration with the Incident Response team.



An avenue to reinforce good cyber security messaging is to provide regular reporting to a domestic and overseas audience. The reporting will come from open and closed sources, analysing new Tactics, Techniques and Procedures from campaigns aimed at our firewalls and sensors, located throughout the world. Cybermerc is currently investigating a number of new domestic incidents and is focused on identifying threats targeting supply chain companies.

Cybermerc can produce dangles (fake online personas) so the community can understand how cyber criminals and state actors are targeting industry and Government employees. This tactic has been very successful in the past when Cybermerc conducted the same exercise for private industry, and can aid in pre-empting cyber threats.

TARGETED ASSESSMENT

ONGOING MONITORING

For our clients with high value information to protect, such as Personally Identifiable Information or Intellectual Property, we offer a continuous monitoring service to give greater peace of mind and reduce the time to detect any data compromise. We monitor the Internet, the Deep Web and the Dark Web including both open and closed sources to identify if malicious actors are attempting to sell your data or access to your network.



Cybermerc is regularly engaged by clients and third parties on behalf of their clients to perform ad hoc investigations across the Internet. Using our experience and access we can perform investigations across the Internet, the Deep Web and the Dark Web including both open and closed sources to identify malicious activity.

PERSONAL BACKGROUND CHECKS

Employers are increasingly looking to potential employees' social media accounts in order to vet their suitability and the insider threat is becoming the biggest threat to businesses and governments. Cybermerc can provide a competitive, discreet online and social media investigation service to help employers make the right decisions when choosing candidates.



AD HOC INVESTIGATIONS





CONSULTANTS

The Cybermerc team are hand-picked experts, drawn from multiple domains of cyber security practice and intelligence operations. All Cybermerc staff hold high-level Australian Federal Government security clearances.

MATTHEW NEVIN

CISSP, LLB

Chief Executive Officer & Co-founder



Matthew leads Cybermerc's business development and enterprise strategy. With 18 years of cyber security experience drawn from law enforcement and industry, Matthew is accountable for all aspects of corporate strategy and development.

Matthew brings extensive knowledge of cyber security challenges from his experience in government and multiple market sectors. Previously, he was a Senior Technical Analyst for the Australian Federal Police and a Director of Strategic Intelligence at the Australian Tax Office.

Matthew is a qualified solicitor, and holds CISSP and a range of SANS Security and Forensic qualifications.

SERVICES

- Cyber Strategy Management
- Cyber Risk Management
- Executive Strategy & Cyber Leadership
- Cybercrime
- Cyber Threat Intelligence Analysis
- Computer and Network Forensics
- Legal, Policy and Compliance
- Government Engagement



PAUL NEVIN

CISSP

Chief Technology Officer & Co-founder



Paul co-founded Cybermerc in 2016, bringing his experience as an expert and highly-regarded cyber security professional. Through his career, Paul has focused on developing solutions within the national security and intelligence agencies, to combat the rising threat of cybercrime and cyber espionage.

An inventor of intrusion detection technologies, Paul is passionate about teaching effective investigative techniques to a new generation of cyber intelligence analysts. Paul holds a range of qualifications including CISSP and a Masters in Cyber Security.

SERVICES

- Cyber Threat Intelligence Analysis
- Cyber Security Technology Architecture and Design
- Cyber Incident Management
- Computer Network Operations
- Intelligence Analysis
- Cyber Risk Management
- Information Security Management
- Government Engagement



ANDREW SLATER

CISSP

Director,
Strategy & Partnerships



A keen and passionate technologist, Andrew has spent over two decades designing and delivering secure solutions across Defence and Federal Government clients. Andrew now brings that knowledge and experience to leading Strategy and Partnerships for Cybermerc.

Andrew has extensive experience in Information Communication Technology and Security, with a focus on security operations, packet analysis and incident response. He is passionate about securing client environments proactively through design and training as well as reactively by investigations. Among his many qualifications, Andrew is also a CISSP.

SERVICES

- Solution Architecture
- Network & Solution Design
- Threat Hunting (Windows Endpoints & Packet Analysis)
- Cyber Threat Intelligence Analysis
- Technical Documentation
- Training Delivery
- Integration



NATHAN HERBERT Chief Security Officer



Nathan is the Chief Security Officer and Senior Intelligence Analyst for Cybermerc. Nathan spent three decades in the military and corporate world, leading teams to identify threats to protect assets and people here and abroad. He is passionate about the defence of Australia, drawing on years in military intelligence, multiple deployments and experience as Security Manager in the corporate world to deliver expert security advice to clients and executives.

Nathan holds multiple qualifications including Masters in Terrorism and Security, Bachelors in Organisational Leadership and Certificate IV in Training and Assessing.

SERVICES

- Threat Analysis and Management
- Information Operations
- Intelligence Collection Management
- Training Development and Delivery
- Intelligence and Security Training
- Security Risk Management
- Leadership development
- Stakeholder Liaison



CHAKRI CASTILLO

Chief Experience Officer & Operations Manager



A skilled communications and operations professional, Chakri brings internal and external communications perspectives to cyber strategy. In her experience in communications and marketing, she has provided strategy and implementation for government, enterprise and non-profit organisations. Chakri specialises in change management, and has overseen corporate cyber transformations from an operational level.

Currently completing a Juris Doctor with an interest in cyber law, Chakri is passionate about ensuring individual, organisational and sovereign cyber security. Her knowledge includes Cybercrime, Privacy and Intellectual Property Law.

SERVICES

- Communications Strategy (Internal & External)
- Public Relations & Social Media Management
- Brand Management & Awareness
- Digital Content Production
- Cyber Transformation Management
- Legal, Policy and Compliance
- Stakeholder Liaison





Suite 2, 31-37
Townshend St
Philip
ACT 2606

info@cybermerc.com
www.cybermerc.com