Offensive Security

Offensive testing. Defensive confidence delivered.

Introduction

Modern organisations are no longer breached by chance, they are systematically targeted by motivated, well-resourced adversaries. Excelium's Offensive Security services are designed to replicate real-world attacker behaviour, uncovering weaknesses and misconfigurations before they can be exploited.

Our approach goes beyond compliance-driven testing. We simulate real-world threat actors, tactics, techniques, and procedures, providing actionable insight and recommendations that improves an organisations security posture and provides confidence and resilience under pressure.

What we solve

Excelium helps organisations proactively identify, validate, and reduce real-world cyber risk by simulating how attackers would compromise their environments.

- Expose unknown and exploitable weaknesses before adversaries do
- Validate whether security controls work in practice, not just on paper
- Prioritise remediation by proving real business and operational impact
- Test detection, response, and resilience against realistic attack scenarios
- Build executive confidence through evidence-based security assurance

Who we help

We help organisations that need assurance their security can withstand real-world attacks, not just compliance requirements.

- **Government and regulated entities** responsible for protecting sensitive or classified information
- **Enterprise and critical infrastructure organisations** with complex, high-value environments
- **Security and technology leaders** accountable for cyber risk, resilience, and assurance
- **Boards and executives** seeking evidence-based confidence in defensive capabilities
- **Organisations undergoing change** such as cloud adoption, mergers, or major system uplift

Core offensive security capabilities

Penetration Testing

Our team will identify exploitable weaknesses and misconfigurations across your technical environment using controlled, ethical attack simulations.

Our specialities include

- Remote and on-premises Network and Technology Security Testing
- Cloud and Hybrid (Azure, AWS, Google) Security Testing
- Hosted and Cloud Web Application Security Testing
- API and Microservices Security Testing
- Mobile Application Security Testing
- Wireless Security Testing

All testing is conducted with realistic attacker intent, prioritising exploitability over generic vulnerability listings and automated vulnerability assessments.

Red Team Operations

Our security specialists provide end-to-end adversary attack emulation to measure your organisation's detection, response, and resilience.

What we test

- Initial access threat vectors and attack surface analysis
- Controlled privilege escalation and lateral movement
- Discrete persistence and command-and-control
- Detection and response effectiveness
- Human and process weaknesses

All Red Team engagements deliver board-level clarity on "Would we detect a real attack - and how quickly can we return to normal operations?"

Assumed Breach and Purple Teaming

Our security specialist operates under the assumption that perimeter defences have already failed and your technical environment has been breached.

We work collaboratively with your security teams to:

- Validate detection capabilities
- Improve SOC workflows
- Reduce dwell time
- Strengthen preventative controls

This approach bridges the gap between **offence and defence,** rapidly increasing security maturity.

All testing is conducted with realistic attacker intent, prioritising exploitability over generic vulnerability

Our approach, methodology and reporting

Our team utilises the latest industry standard frameworks, recognised testing methodology and state of the art tolls.

A methodical approach to offensive security

- Targeted Reconnaissance - Understand your attack surface and business context
- Controlled Exploitation - Safety execute realistic attack paths, validating true business impact
- Impact Demonstrations - Show what an attacker could access, manipulate, or steal
- Clear, Actionable Reporting - Executive summary, prioritised, business-aligned findings, technical remediation guidance
- Optional Retesting and Advisory - Validate remediation and improve longer-term resilience

Our tried and tested approach and methodology aligned to strict rules of engagement provides guaranteed results.

Reporting that drives change

Excelium reports are designed to support your organisation and maintain your security baseline:

- Our reports are tailored to be read by executives and engineers alike
- Our testers clearly articulate technical risk, impact, and likelihood
- In depth knowledge provides practical and actionable remediation guidance
- We eliminate noise and false positives so you don't have to

No inflated severity. No checkbox findings. Just credible, defensible reporting.

Our experience

Department of Health, Disability and Ageing

The Department of Health, Disability and Ageing (DHDA) engaged Excelium to assess the security of its Health Business Systems (HBS) Microsoft Azure cloud environment, which underpins critical digital services supporting health, disability, and ageing programs across Australia. The engagement focused on validating the resilience of public-facing applications, workflow automation, identity services, and enterprise integrations, ensuring that sensitive personal and case-related data is protected against real-world cyber threats.

Department of Health, Disability and Ageing

Excelium was engaged to assess the security of the Aged Care Gateway (ACG) a large-scale, enterprise digital platform delivering integrated aged care services to older Australians, their families, carers, and healthcare professionals. The ACG comprises a complex ecosystem of user portals, web and mobile applications, enterprise integration services, customer relationship management systems, data platforms, and external interfaces. Given the sensitivity of personal and health-related information handled across the platform, the engagement focused on validating the resilience of the ACG against real-world attack scenarios spanning applications, integrations, and data layers.

Fair Work Ombudsman

The Fair Work Ombudsman (FWO) engaged Excelium to assess the security of its Microsoft Azure Environment, which delivers critical public-facing services, case management capabilities, and secure integration workflows. The assessment focused on validating the resilience of FWO's cloud environment against real-world attack scenarios, with particular emphasis on public-facing services, workflow automation, identity controls, and enterprise integrations.

National Disability Insurance Agency

The National Disability Insurance Agency (NDIA) engaged Excelium to assess the security of its Amazon Web Services (AWS) hosted systems, services, and applications that support delivery of the National Disability Insurance Scheme (NDIS). Given the scale of operations and the sensitivity of participant and operational data, the engagement focused on validating the resilience of NDIA's AWS environment against real-world attack scenarios, with particular emphasis on identity, infrastructure configuration, data protection, and event-driven architectures.

They trust us

CANBERRA RAIDERS

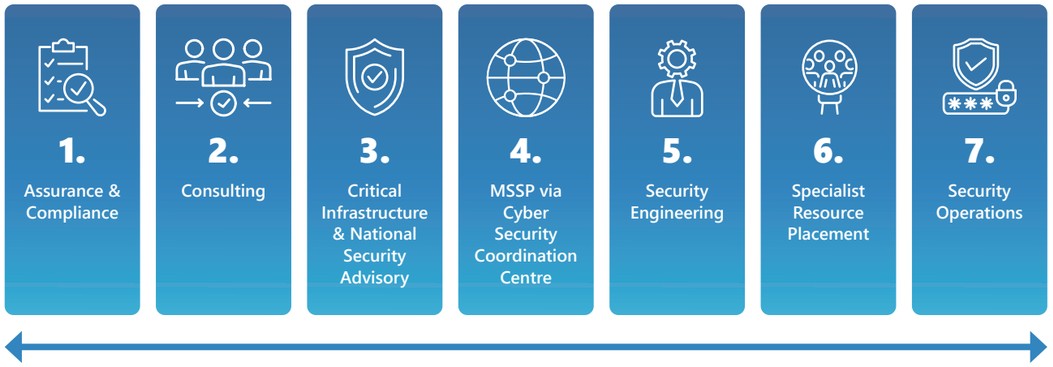
AINSLIE GROUP

SARONIC

FEDERAL GOLF CLUB CANBERRA

How we operate

Excelium's Seven Pillar model positions us as a true full-stack cyber and risk management partner. Our seven service lines combine to deliver end-to-end capability and full solutions across the entire security lifecycle from strategy to assurance, engineering to operations, and compliance to resilience. Each pillar is powerful in its own right and together they form the basis of a service which can provide a holistic resilience framework for our clients.



Excelium's Seven Pillars

- **Assurance & Compliance:** Security framework achievement, certification readiness, and continuous compliance.
- **Consulting:** Strategic cyber advice, regulatory compliance, cyber security maturity assessments, and cyber uplift roadmaps.
- **Critical Infrastructure & National Security Advisory:** *Security of Critical Infrastructure Act 2018* compliance, 'All Hazard' risk assessments, Critical Infrastructure Risk Management Plans, Hosting Certification Framework accreditation, transport security plans and compliance, and national security risk management.
- **Managed Security Services (via CSCC):** Proactive threat monitoring, SOC/SIEM integration, and rapid cyber incident response.
- **Security Engineering:** Secure-by-design architecture, system integration, and security hardening and attack surface reduction.
- **Specialist Cyber Resource Placement:** Embedding skilled professionals (CISO, ITSA, Analyst, Architect and GRC personnel) for immediate impact and long-term capability.
- **Security Operations:** Offensive penetration testing, digital forensics, incident response, operational defence, cybersecurity exercising

Our Cyber Security Coordination Centre (CSCC) underpins the model, acting as a central command hub for managed services and rapid incident response, enabling faster mobilisation, coordinated resourcing, and continuous monitoring tailored to each client's environment - all under a single contract and single account manager.

Get in touch

Mark Farley-Thompson
Security Operations & Engineering Partner
0412883750
Mark.Farley-Thompson@excelium.com.au

ACT – Head Office
Ground Floor
Unit 2,14 Brisbane Avenue
Barton ACT 2600

NSW
Level 11
66 Clarence Street
Sydney, NSW 2000

QLD
167 Eagle Street
Brisbane 4000 QLD