Excelium

Defensive Security

Proactive defence. Measurable resilience delivered.

Introduction

Modern organisations are no longer defending against opportunistic threats alone. Today's adversaries are persistent, adaptive, and capable of operating undetected for extended periods. Effective defensive security is not achieved through tools alone it requires continuous visibility, operational discipline, and the ability to detect, respond and recover under real-world conditions.

Our Defensive Security services are designed to protect, detect, and respond across complex enterprise environments. We focus on ensuring security controls operate effectively in practice, not just in policy or design, providing organisations with confidence that attacks will be identified early, contained swiftly, and remediated decisively.

What we solve

We help organisations move beyond reactive security towards operational resilience. Our defensive operations helps organisations:

- Prevent common and advanced attack techniques through effective control implementation
- Detect malicious activity early across endpoints, identities, networks, and cloud environments
- Respond decisively to incidents, reducing dwell time and business impact
- Validate that people, processes, and technology operate cohesively under pressure
- Build executive confidence through measurable, evidence-based security assurance

Who we help

Defensive Security services are suited to organisations that require continuous protection and assurance, including:

- **Government and regulated entities** protecting sensitive, personal, or classified data.
- **Enterprise and critical infrastructure operators** with complex, hybrid environments.
- **Security and technology leaders** accountable for operational cyber risk
- **Boards and executives** seeking confidence in detection and response capability
- **Organisations undergoing change** such as cloud migration, transformation or uplift programs

Core offensive security capabilities

Security Monitoring & Detection Engineering

We help organisations design, deploy, and optimise monitoring capabilities to identify malicious behaviour early:

- SIEM and log management design and optimisation
- Endpoint, identity, network, and cloud telemetry integration
- Use-case development mapped to real attacker techniques
- Alert tuning to reduce false positives and analyst fatigue
- Detection coverage assessment against threat frameworks

Security Operations & SOC Enablement

Strong detection requires mature operations. We support:

- SOC process design and uplift
- Analyst workflow optimisation and triage procedures
- Incident classification, prioritisation, and escalation models
- Integration between security tools and operational teams
- Metrics and reporting that reflect true defensive effectiveness

Incident Response & Digital Forensics

When incidents occur, rapid, and accurate response is critical:

- Incident response planning and preparedness
- Containment, eradication, and recovery support
- Digital forensics across endpoints, cloud, and identity platforms
- Root cause analysis and attacker activity reconstruction
- Post-incident reporting with actionable remediation guidance.

Prevention Control & Hardening Assurance

We strengthen your security baseline to reduce attack success:

- Identity and access control reviews and hardening
- Endpoint and server security configuration validation
- Network segmentation and exposure reduction
- Cloud security posture and configuration assurance
- Secure logging, backup, and recovery configurations

Defensive Exercises & Validation

We help organisations validate readiness through controlled, realistic scenarios:

- Tabletop incident response exercises
- Technical detection and response simulations
- Purple Team collaboration to improve SOC performance
- Playbook and decision-making validation
- Executive and operational readiness assurance

Our approach, methodology and reporting

We apply a methodical, threat-informed approach aligned to industry frameworks and real-world attacker behaviour.

A structured defence methodology

- Threat & Environment Understanding - Understand business context, critical assets, threat actors, and likely attack paths
- Control Validation & Hardening - Ensure preventative controls are correctly configured, implemented, and maintained across identities, endpoints, networks, and cloud services
- Continuous Monitoring & Detection - Establish and tune logging, alerting, and visibility across security telemetry sources
- Incident Response & Containment - Enable rapid, coordinated response to security incidents using defined playbooks and escalation paths
- Recovery & Resilience Improvement - Support post-incident learning to strengthen controls, processes, and maturity over time

This approach ensures defensive capabilities remain effective, measurable, and sustainable.

Reporting that enables action

Our defensive security reporting is designed to drive improvement, not create noise:

- Executive-level visibility of risk, readiness, and trends
- Clear articulation of detection gaps and operational weaknesses
- Prioritised recommendations aligned to business impact
- Practical, actionable remediation guidance
- Metrics that demonstrate maturity progression over time

No unnecessary alerts. No abstract risk. Just **credible, defensible security insight.**

How we operate

How Defensive Security Fits the lifecycle

Defensive Security operates continously across the security lifecycle:

1. **Prevent** - Reduce exposure and attack surface
2. **Detect** - Identify malicious behavior early
3. **Respond** - Contain and eradicate threats decisively
4. **Recover** - Restore services and confidence
5. **Improve** - Strengthen resilience through learning

This ensures security remains effective as the organisation evolves.

Why Defensive Security Matters

Attackers only need to suceed once. Defencers must be effective every day. Defensive Security provides organisations with:

- Reduced breach impact and recovery time
- Confidence that controls function under real attach conditions
- Measurable improvements in detection and response maturity
- Assurance for executives, regulators, and stakeholders
- A defensible security posture built on evidence, not assumptions

Our experience

Department of Education - Victoria

The Department required independent assurance to understand and reduce its external attack surface. Excelium conducted an Attack Surface Reduction Assessment across the Department's externally exposed digital environment. The assessment identified internet-facing assets, reviewed exposure points, and analysed configurations that could increase susceptibility to compromise. Excelium applied recognised industry standards and threat-led techniques to identify unnecessary exposure, misconfigurations, and opportunities to reduce the overall attack surface. The assessment provided the Department of Education – Victoria with a clear, prioritised view of its external attack surface, highlighting areas where exposure could be reduced to lower the likelihood of successful cyber attack. Excelium delivered a comprehensive report with actionable recommendations to eliminate unnecessary exposure, strengthen security controls, and improve ongoing attack surface management.

Fair Work Ombudsman

Given the breadth of FWO's digital footprint and the sensitivity of information processed, FWO sought independent assurance to better understand and reduce its external attack surface while also improving the effectiveness of its vulnerability management practices. Excelium delivered an Attack Surface Reduction Assessment and Vulnerability Management Optimisation Uplift across FWO's enterprise environment. The engagement provided the Fair Work Ombudsman with a clear, prioritised view of its attack surface and vulnerability risk, enabling targeted reduction of unnecessary exposure and improved focus on high-risk issues. Excelium delivered a comprehensive report outlining actionable recommendations to strengthen attack surface management, enhance vulnerability prioritisation, and uplift ongoing security operations.

Raiders Group

The Raiders Group identified the need to strengthen their vulnerability management capability, with a particular focus on improving patch management practices and reducing risks associated with weak or unmanaged credentials.Excelium conducted a Vulnerability Management Assessment across the Raiders Group and Raiders Clubs enterprise environment, reviewing existing vulnerability identification, prioritisation, and remediation processes. The assessment included a detailed review of patch management practices to identify gaps in coverage, timeliness, and governance across both football and club systems. In addition, Excelium supported password optimisation by assessing credential management practices and assisting with the introduction of a centralised password management system.

They trust us

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