McGrathNicol

CYBER DEFENCE & VULNERABILITY MANAGEMENT

Offensive security domains

Offensive security is much more than penetration testing and vulnerability assessments of an organisation's cyber assets. At the core, its purpose is to challenge the security assumptions across the Physical, Human and Cyber domains of an organisation. Offensive security assessments are effective in building an organisation's cyber preparedness, and proactively identifying and understanding the weaknesses that threat actors may exploit. Understanding your cyber risk across all aspects of your organisation can enhance system and service integrity, availability and stability for current use and against future cyber threats.

Following industry standard lifecycles, our skilled practitioners follow the offensive security lifecycle, from gathering reconnaissance information, planning, identifying vulnerabilities, exploitation, and documentation. We have wide security testing experiences in multiple domains, applications, and infrastructure, as well as broad experience across varying industries including government, private and critical services.

Our 2021 analysis of offensive security assessments performed by McGrathNicol showed that:

60%

of findings identified from our practitioners were due to Security Misconfigurations. These misconfigurations can lead to critical findings that can impact an organisations core business.

13,000

credentials and passwords recovered from objective based assessments, including 42 Domain Administrator account credentials over multiple domains.

35mins

The quickest time to achieve final objectives in a security assessment (i.e Compromising highest privileged domain accounts and full compromise of the organisation).

> *"Offensive security assessments are effective in building an organisation's cyber preparedness, and proactively identifying and understanding the weaknesses that threat actors may exploit."*

Organisational security domains

Organisation

Human

People play an important role in the security of any organisation. However, they are just as susceptible to exploitation by threat actors in an attempt to gain access to the organisation.

- User Awareness
- Education
- Social Engineering

Physical

The buildings, facilities and locations of an organisation are important in the offensive security domain. Remote, or less secure locations may enable a threat actor access to sensitive data and networks.

- Building Access
- Geographical Locations
- Security Measures

Cyber

Cyber was traditionally seen as the Information Technology-side of an organisation. But today it includes cloud services, applications and even operational technology assets.

- Infrastructure
- Applications

Incident Response

The capability and readiness of an organisation to respond to a security event in any of the three domains. The nature of the breach is quickly established, understood and further attacks are prevented.

- Forensics
- Post Breach Vulnerability Assessment

Offensive security lifecycle

Threat Landscape Assessment

Threat Landscape Assessments identify and document any publicly available information available through open-source intelligence.

Our experience includes performing open source intelligence gathering on senior executives of an organisation, to help them understand the risks and exposures of their leadership team.

Vulnerability Assessment

Organisations need to continually assess their environments to identify new weaknesses and vulnerabilities among their critical assets. This allows them to focus their efforts on assets or systems that are high risk target for cyber attacks, based on the dynamic cyber threat landscape.

Our experience includes performing vulnerability assessments on organisations from various industries from medical, retail, and critical infrastructure. This helps organisations understand weaknesses in their infrastructure and applications to better guide them on their cyber preparedness.

Penetration Testing

After identifying vulnerabilities and establishing a security baseline, exploitation of these vulnerabilities provides understanding of the potential impact. Penetration testing of infrastructure or applications focuses on root causes, which may be a result of security misconfigurations, patch management, architectural or development practices.

Our experience includes performing objective based testing with specific goals and key objectives on organisations that operate at a global scale. This helps organisations understand the critical information and systems in their organisation, as well as realising the potential impact that a threat actor could inflict.

Red Team Assessment

Combining the three domains to test specific targets and key objectives using reconnaissance, vulnerability identification and exploitation. They provide organisations with a picture of how well they can predict, prevent and respond (security posture) to the dynamic security threats across all domains.

Our experience includes performing assessments in all three domains. Our practitioners have diverse backgrounds from law enforcement to ethical hacking, these assessments help organisations identify and understand the risk exposure from all domains, allowing for a cohesive and strategic preparedness on all fronts.

Incident Response

The increasing number of cyber threats requires organisations to be prepared and act immediately. Whether this be as an actual live fast and decisive response as a result of a breach, or as part of a Red Team exercise, the nature of the breach is established, understood and further attacks are prevented in an incident response.

Our experience from managing many incidents for other organisations, gives us the ability to assist in managing the uncertainty, particularly through all stages such as Containment, Incident Monitoring, Stakeholder Management, Evidence Preservation, Forensic Analysis and Recovery and Remediation Support.

Post-Breach Vulnerability Assessment

A Post-Breach Vulnerability Assessment can be used after a compromise to re-establish a security baseline. Breaches may have a broad impact on an environment, but the threat actor may have used a narrow window for the initial entry vector. Conducting a vulnerability assessment can also assist with validating that similar entry vectors are not present in other systems and hosts.

Our experience includes helping multiple organisations re-establish a known security baseline after an incident to help provide confidence that post incident remediation activities have been strategic and effective and securing the organisation.

Meet the Partners

Darren Hopkins
Partner, Brisbane
M +61 416 151 419
E dhopkins

Darren advises businesses on both proactive and reactive uses of technology in cybersecurity, privacy, digital forensics and technology-led investigations. He regularly works with boards, executives and senior business leaders.

Joss Howard
Partner, Sydney
M +61 460 972 700
E jhoward

Joss specialises in technical, information security and cyber resilience. She advises global businesses across sectors including aerospace, defence, finance, government, healthcare, leisure and retail, transport, telecommunication and utilities.

Jamie Norton
Partner, Canberra
M +61 438 643 170
E jnorton

Jamie specialises in cybersecurity strategy, program development, governance, risk, and operations. He has 20 years experience in managing security resilience for State and Federal Government agencies and commercial organisations.

Blare Sutton
Partner, Melbourne
M +61 417 252 739
E bsutton

Blare is a highly regarded forensic expert with more than 20 years of experience in technology and cyber. He manages highly sensitive engagements involving internal and external actors, law enforcement, financial institutions and civil remedies.

Trent Whitbourn
Partner, Sydney
M +61 407 578 086
E twhitbourn

Trent is a forensic and technology specialist in digital forensics, cyber security and information risk, end-to-end electronic discovery and data analytics. He has worked across different jurisdictions, Government projects and local and US regulators.