



Catalyst
— OFFENSIVE —

Services Summary





CATALYST OFFENSIVE

The quality of offensive security testing directly determines its value. Skilled offensive practitioners understand your environment's nuances, identify and exploit attack chains that bypass modern defences, and provide the strategic context you need to make informed risk decisions.

Testing windows are measured in days or weeks, but real attackers operate without such constraints. That asymmetry makes offensive assurance capability critical - when time is limited, you need to cut through the noise, understand your specific risk landscape, and identify the exposures that genuinely matter to your organisation.

Catalyst Offensive was built differently from the ground up. We're a team of hand-picked senior consultants with specialised experience in advanced offensive testing, intent on delivering the level of capability and client experience that sets the standard for excellence in our industry.

Our team focuses on uncovering the attack paths that matter, providing the strategic and technical context that informs real business decisions, and the advanced technical tradecraft that reflects how sophisticated adversaries actually think and operate across today's threat landscape.

Our team has operated at senior levels within Australia's leading boutique cyber security firms, delivering high-impact engagements across a range of industry sectors including national critical infrastructure, government, telecommunications, finance, healthcare, aviation, mining and resources, transport and logistics, and professional services.



As a **true** sovereign capability, Catalyst Offensive is your trusted partner for modern and comprehensive offensive security services, and we'd love the opportunity to connect with you to chat about your needs and discuss our offensive service offerings and capability in more detail.

THE CATALYST DIFFERENCE

The real difference between offensive security providers is in their depth of expertise. Catalyst Offensive engagements are structured to deliver maximum value – you know exactly what you're paying for, and you get the full capability of our skilled consultants from start to finish in a true partnership model.

Handpicked consultants

Our team is deliberately small and highly selective as we only engage consultants who operate at the highest level of capability to deliver our offensive security services.

No hidden costs

Unlike many other offensive security providers, we don't charge extra for meetings, project management, or any other essential components of our comprehensive services.

Retesting included

Retesting of Medium and above findings is included in our engagement pricing, so there are no separate quotes or additional charges to validate your remediation activities.

Source code assistance

We'd love access to source code where available to deliver the most thorough assessment possible. This isn't at your cost – we just want the best possible result for you.

Responsible AI usage

We leverage carefully selected AI tools to enhance our efficiency and coverage, and client data is never shared with, or used to train, any third-party AI services.

Real sovereign capability

Catalyst Offensive consultants hold current AGSVA security clearances, all operate onshore, and all testing and reporting infrastructure is hosted within Australia.

Our team has demonstrated proficiency in modern offensive tradecraft and has achieved a wide range of industry-recognised security certifications.



OUR OFFENSIVE SERVICES

Catalyst Offensive help organisations of all sizes and industries identify and address vulnerabilities before adversaries exploit them. Our core capabilities span from traditional vulnerability assessments through to sophisticated red team operations, with each engagement tailored to your specific threat landscape and security maturity.

Red Team

Realistic, multi-phase attacks simulating real-world adversary tradecraft to test organisational detection and response capabilities end-to-end.

Purple Team

Collaborative attack-and-defend scenarios working alongside security teams to rapidly improve detection, identify blind spots, and sharpen responses.

Physical

Testing physical controls through social engineering, control bypass, and facility breaches to identify weaknesses in human and physical defences.

Network Infrastructure

Attacking network perimeters and internal digital ecosystems to find viable attack paths, sensitive data exposures, and lateral movement opportunities.

Web Application and API

Finding flaws in applications and APIs through testing of authentication, business logic, and data handling across the entire attack surface.

Cloud Security

Offensive testing against cloud platforms like Azure, AWS, and CCP for privilege escalation paths, identity weaknesses, and security gaps that expose data.

Build Hardening

Offensive evaluation of standard operating environments and system builds against security best practices and industry hardening benchmarks.

Secure Code Review

Deep human-led source code analysis to identify security vulnerabilities, coding flaws, and logic errors that traditional testing methods fail to identify.

Vulnerability Assessment

Automated and manual scanning to identify known vulnerabilities, misconfigurations, and security weaknesses across systems and applications.

Wireless Infrastructure

Assessing WiFi networks for rogue access points, weak encryption, segmentation issues, and flaws that can result in unauthorised network access.

Our experience extends beyond these core service offerings to meet unique client requirements across various offensive security domains. If your offensive security testing needs don't fit neatly into these categories or require a specialised approach, contact us to explore how we can help to address your specific challenges and get the right result.

OUR LEADERSHIP TEAM



Silas Barnes

Partner | Catalyst Offensive

Co-founder of Catalyst Cyber and leader of the offensive security division, Silas brings over 20 years of experience spanning both sides of the cyber security equation. As a three-time CISO - including five years as Group CISO for Virgin Australia - he's defended some of Australia's most complex enterprises across aviation, critical infrastructure, and healthcare sectors against the same advanced attacker tradecraft Catalyst's offensive security team simulates for their clients.

This unique combination of executive security leadership and deep offensive expertise means Catalyst engagements are informed by real-world defensive priorities, not just theoretical risks. Silas maintains active technical certifications and regularly invests in advanced offensive training, ensuring his strategic perspective is grounded in current attack methodologies and the practical realities of enterprise security.



Rick Oates

Head of Offensive Security

Head of Offensive Security at Catalyst, Rick brings over a decade of hands-on experience in adversary simulation and security testing, built on a foundation of defensive security operations and leadership experience that shaped his collaborative, outcomes-focused approach. Battle-tested across numerous red and purple team operations, assumed breach scenarios, and physical security assessments, Rick has led and executed engagements spanning diverse threat vectors and environments throughout his career. He leads Catalyst's offensive security capability as both technical authority and active operator - setting standards based on what actually works in the field, not from the sidelines.

Rick's strength lies in translating complex technical findings into clear, actionable improvements. He maintains cutting-edge offensive security certifications and continuously refines his tradecraft, ensuring Catalyst's testing methodologies reflect current attacker techniques. Under his leadership, the offensive security team has rapidly built a reputation for creative problem-solving and technical rigour in the Australian market.



offensive@catalystsec.com.au

<https://www.catalystsec.com.au>