Quorum Cyber

Service Description Security Assessment (Pen Testing) G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

Quorum Cyber Offensive Security (OffSec) services help organisations understand how vulnerable they really are in the face of today's rapidly evolving cyber threats.

In an increasingly hostile cyber threat landscape, penetration testing is a critical assurance activity that enables organisations to understand and manage their real-world cyber risk. While security controls, policies, and compliance frameworks are essential, they do not confirm whether defences are effective against active, motivated attackers. Penetration testing provides this validation by simulating realistic attack scenarios to identify exploitable weaknesses before they can be leveraged by threat actors.

Our assessment services are designed to give organisations clear, practical insight into where weaknesses exist and how they could be exploited, without requiring technical expertise from the business. By identifying these risks early, organisations can prioritise improvements, reduce the likelihood of disruption, and strengthen overall resilience. Ultimately, the service helps leaders gain confidence that their security investments are effective, their exposure is understood, and their organisation is better prepared to withstand real-world cyber threats.

Quorum Cyber's Solution

At Quorum Cyber, we take a thorough and practical approach to assessing security risk by safely testing systems, applications, and data to identify weaknesses that could be exploited by attackers. These activities are carefully controlled and designed to reveal where unauthorised access could occur, while ensuring minimal disruption to the business. Importantly, findings are never viewed in isolation; each issue is assessed in context to clearly explain the potential business impact and how it can be addressed.

Our focus is on delivering meaningful outcomes rather than simply meeting technical standards or compliance requirements. By combining proven methods with our own expertise and experience, we provide insight that goes beyond surface-level assessments and helps organisations understand their real exposure to cyber risk. This ensures that time and investment are directed toward improvements that genuinely strengthen resilience.

By adopting the mindset of real-world adversaries, we provide a realistic view of how threats could affect your organisation in practice. This approach enables leaders to make informed decisions based on credible risk, rather than checkbox compliance, and helps build confidence that security measures are aligned to protecting the business against modern and evolving threats.

Differentiators

Our offensive security centre of excellence is home to a team of creative CREST-certified professionals who have years of experience testing a huge range of technology to the limits. Working with a cybercriminal's mindset – and with your permission – they work to locate your weaknesses and advise how you can strengthen your security in an affordable way before threat actors take advantage.

Service Features

Active Directory Assessment

Active Directory Assessment evaluates the overall security of your Microsoft Active Directory environment from a real-world threat perspective. This includes a review of key security misconfigurations, account permissions, group policies, domain trusts, and other common areas of weakness.

Breakout Assessment

Breakout Assessment service helps you identify misconfigurations which may otherwise be exploited by an authenticated attacker. They help to assure key controls both locally and within the surrounding environment. We use a blended approach of both manual and automated tooling to provide an in-depth assessment of the targets threat landscape. Our consultants have a shared in-depth knowledge of a wide range of Operating Systems as well as Kiosk/POS and Citrix environments, allowing them to provide hardening recommendations that go beyond the output of traditional automated scanners.

Build Review Assessment

Build Review Assessment service helps identify and remediate security related configuration weaknesses in your endpoints, let it be a gold build for a workstation, server, laptop, or mobile phone. Our consultants have a shared in-depth knowledge of a wide range of Operating Systems, allowing them to provide hardening recommendations that go beyond the output of traditional automated scanners.

Code Review Assessment

Quorum Cyber’s consultants bring extensive application security experience across solutions of all sizes, from individual applications to complex, enterprise-scale environments, ensuring practical, effective guidance tailored to your organisation’s development landscape.

External Infrastructure Assessment

External Infrastructure Assessment helps identify and remediate security issues in your perimeter systems, reducing your business risk, and increasing your customer trust. From small-scale to full enterprise-level solutions, our team of consultants has a wide range of network security experience.

Insider Threat Assessment

Insider Threat Assessment assumes an initial foothold into your corporate environment and measures the impact an active threat actor may have, relative to the objectives of the engagements whilst allowing your defenders to detect and respond to it.

Mobile Application Assessment

Mobile Application Assessment service is designed to identify and address security weaknesses within mobile application design and implementation, helping to reduce business risk and strengthen customer trust. Our consultants bring

extensive experience across a wide range of mobile environments, from individual applications to large-scale, enterprise deployments.

As part of the service, associated application programming interfaces (APIs) can also be assessed to provide a comprehensive view of end-to-end security. Evaluating the supporting web services enables organisations to understand full-stack risk, address issues before deployment, and demonstrate a mature, proactive approach to application security therefore helping to protect both operational integrity and organisational reputation.

Vulnerability Assessment

A Vulnerability Assessment provides a clear, structured view of an organisation's security posture by systematically scanning the IT environment to identify known weaknesses. These assessments highlight potential points of exploitation, giving organisations early visibility of where they may be exposed and enabling informed decision-making before threats can be realised. Regular scanning also supports a consistent, proactive approach to cyber risk management.

Web Application Assessment

Our Web Application Assessment service helps identify and remediate security issues in your applications, reducing your business risk, and increasing your customer trust. From brochureware to full enterprise-level solutions, our team of consultants has a wide range of application security experience.

Web Service Assessment

Our Web Service Assessment service helps identify and remediate security issues in the design and implementation of your web-based Application Programming Interface (API) endpoints, reducing your business risk, and increasing your customer trust. From small-scale to full enterprise-level solutions, our team of consultants has a wide range of web service security experience.

Wireless Assessment

Wireless network assessments allow Quorum Cyber to emulate external and internal attacks which identify threats to the target networks, userbase and attached networks, this includes, but is not limited to, the following strategies:

- Rogue Access Points
- Weak Encryption
- Default Configuration
- Guess Network Attacks
- Wireless Client Base Attacks
- Weak Authentication Configuration

Where advanced authentication, such as WPA Enterprise, is deployed, we also suggest reviewing client configuration.

Service Benefits

- **Early Identification of Security Weaknesses:** Helps organisations uncover vulnerabilities and weaknesses before they can be exploited by attackers, reducing the likelihood of security incidents.
- **Reduced Business and Operational Risk**: Identifies risks that could lead to disruption, data loss, or reputational damage, enabling targeted improvements that lower overall exposure.
- **Improved Resilience to Real-World Attacks**: Security Assessments simulate realistic attack scenarios, providing confidence that security controls can withstand modern threats and adapt where needed.
- **Stronger Compliance and Assurance**: Supports regulatory, customer, and insurer requirements by demonstrating a proactive and structured approach to managing cyber security risk.
- **Informed Investment and Prioritisation**: Provides clear, risk-based insights that help organisations focus time, effort, and budget on the areas that will deliver the greatest security improvement.