



G-Cloud 14

Security Testing & Assurance Rate Card

May 2024

sales@cybercx.com



About Cyber CX

- CyberCX brings together the United Kingdom, the United States, Australia and New Zealand’s most trusted cyber security professionals to create a comprehensive end-to-end cyber security services offering.
- Led by industry experts and delivered by cyber security specialists committed to their craft, CyberCX represents the region’s best cyber security talent, applying unmatched cyber security expertise to protect and defend both local and international organisations from cyber threats.

CyberCX Snapshot

 **1350+**

Cyber security professionals with unique skillsets

 **450+**

Security incidents responded to per year

 **750+**

Cyber security baseline assessments per year

 **20+**

Offices across UK, US, Australia & New Zealand

 **9**

Active Security Operations Centre across UK, US, Australia & New Zealand

 **150+**

Managed Security Services Customers

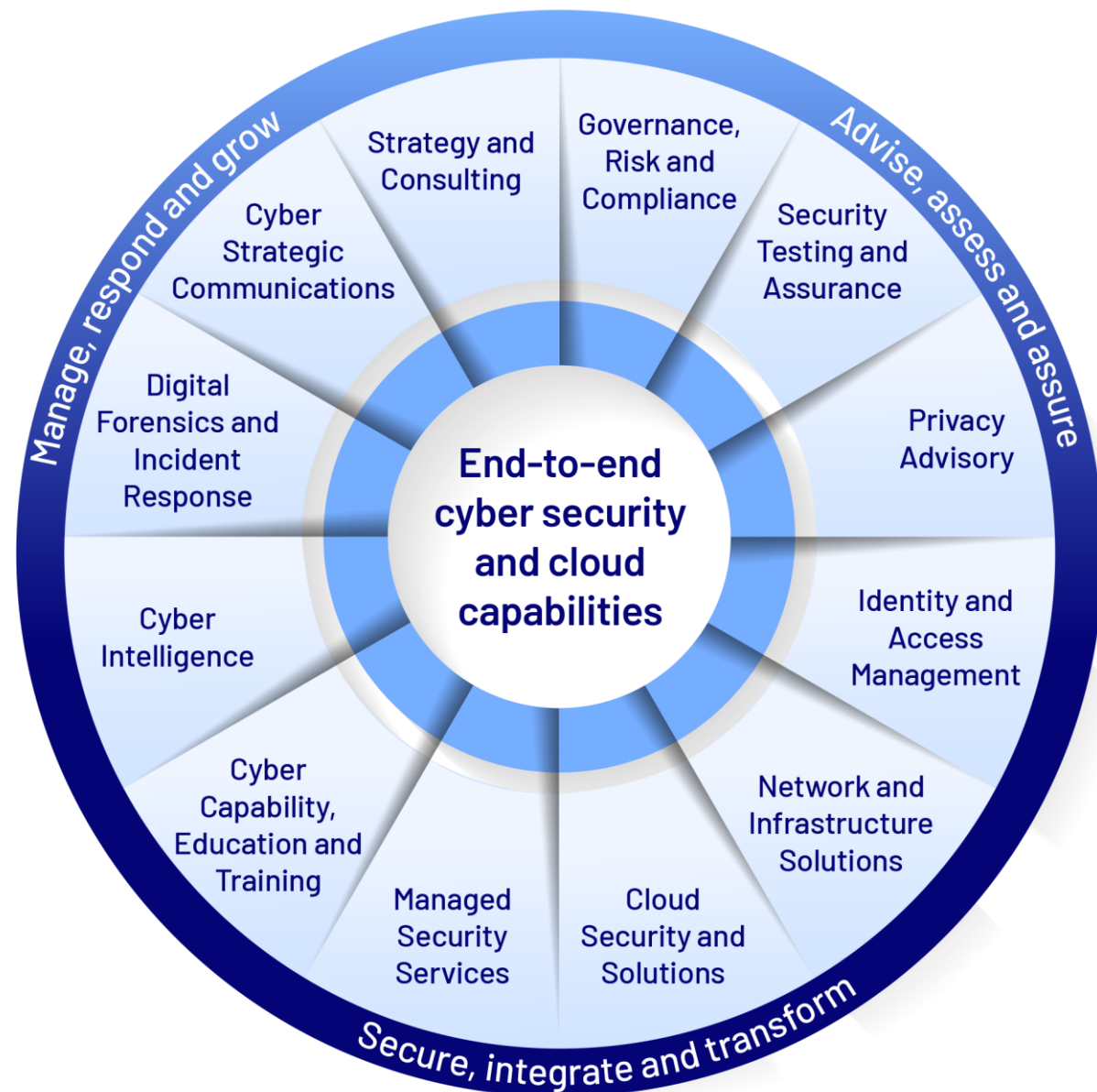
CyberCX Provides Integrated Security Solutions

The breadth of services and capability enables CyberCX to effectively partner with organisations to solve the most complex cybersecurity challenges.

CyberCX unites trusted cybersecurity experts to deliver a comprehensive cybersecurity capability. Every piece of the cybersecurity puzzle matters to the big picture. That's why our security specialists collaborate, so we can deliver true end-to-end cybersecurity results.

CyberCX provides services covering the entire cybersecurity continuum, including:

- **Advise, Assess and Assure:** Cybersecurity to help navigate complexity, minimise risk, improve resilience, and create value for your organisation.
- **Secure, Integrate and Transform:** Plan, design, build and run infrastructure and solutions that deliver tangible business results.
- **Manage, Respond and Grow:** Build security resilience in your organisation and achieve confidence during a crisis, an incident or investigation and quickly and safely restore business operations.



Penetration Testing Services Rate Card

Service	Description	Approximate Duration	Price
Web Application Penetration Testing	Identify vulnerabilities in web applications, which includes any application that is served over HTTP/HTTPS. Broad coverage across web sites with content that is accessed via a web browser, or via computer-to-computer transmissions through web services. e.g. via an API	5 – 10+ Days	£5,250 – £10,500+
Internal & External Network Penetration Testing	Identify vulnerabilities for Internet facing or internal underlying infrastructure, operating systems, applications, and cloud services.	3 – 10+ Days	£3,150 – £10,500+
Mobile Application Penetration Testing	An assessment of Android and iOS mobile applications is performed to identify vulnerabilities and misconfigurations that may lead to compromise. Mobile applications are typically paired with web service or API assessments, as it is often a requirement to test both the application and web service or API together for full coverage. This testing includes automated and manual testing, primarily focusing on manual testing.	5 – 10+ Days	£6,300 – £12,600+
Managed Penetration Testing	<p>A managed penetration testing service that includes, planning, resourcing, scoping, penetration testing, reporting, etc.</p> <p>We would normally run the entire testing program for a single or multi-year program and would include project management and practice delivery services.</p>	Annual or Multi-year commitment, please contact to discuss requirements.	

*The prices shown above are indicative based on a typical engagement. All engagements are scoped individually by a Senior Consultant and final pricing will be included in the statement of work.

Application Security Testing Services Rate Card

Service	Description	Approximate Duration	Price
Source Code Review	Code reviews identify flaws not visible during dynamic testing (Web Application and Web Service), such as authentication, session management, poor cryptographic and secrets practices, outdated and vulnerable internal libraries, and data validation.	5 – 20+ Days	£6,300 – £25,200+
SDLC Security Maturity Review	<p>An analysis of an organisation's software development lifecycle (SDLC) to ensure that security is applied effectively.</p> <p>Using open and industry methodologies, we collaborate with an organisation's software engineering leadership, security leadership and change leadership, to review software workflows from beginning to end, including education and governance, to provide a roadmap of how to uplift their security maturity.</p>	10 – 20+ Days	£12,600 – £25,200+
Threat Modelling	Threat modelling activity develops a sophisticated solution-specific, technical risk assessment which can be used to prioritise the implementation of countermeasures and controls, find security bugs and vulnerabilities early, and to gain an understanding of unique security requirements.	5 – 10+ Days	£6,300 – £12,600+

*The prices shown above are indicative based on a typical engagement. All engagements are scoped individually by a Senior Consultant and final pricing will be included in the statement of work.

Adversary Simulation Services Rate Card

Service	Description	Approximate Duration	Price
Purple Team Exercise	<p>Purple Teaming is a collaboration between our offensive Red Team and your defensive security personnel, or Blue Team.</p> <p>The objective is to uplift your internal security team's readiness to respond to a real-world cyber-attack. Throughout the simulation, the Blue Team will gain experience analysing logs, evaluating attacks, and developing appropriate responses.</p> <p>This enables your internal security team to gain a critical understanding of gaps in your security posture and helps identify areas for capability enhancement.</p>	<p>15 – 25+ Days</p> <p>Dependant on coverage and level of detection engineering during engagement.</p>	<p>£21,750 – £36,250+</p>
Adversary Simulation Exercise (Red Team)	<p>Exercise simulating a realistic intrusion by adversaries within the organisation's threat model to assess and improve their detection, containment, and eviction capabilities.</p> <p>Consultants are free to improvise and try different approaches if the TTPs used could credibly be used by an adversary group.</p> <p>Adopting an adversarial approach, Red Teaming goes beyond standard penetration testing. By simulating the tactics used by real-world attackers, it seeks to identify and exploit any gaps in your defences. Ideal for organisations with a mature security posture, periodic Red Teaming helps further enhance your preparedness to face any determined cyber threat.</p>	<p>External Start: 40 – 60+ Days</p> <p>Assumed Breach Start: 15 – 20+ Days</p>	<p>£21,750 – £87,000+</p>

*The prices shown above are indicative based on a typical engagement. All engagements are scoped individually by a Senior Consultant and final pricing will be included in the statement of work.

Notice To Readers

This document and all written advice and materials provided by CyberCX Pty Ltd ("CyberCX") are the intellectual property of CyberCX. Clients may use these materials freely for their own business purposes, but may not distribute or reproduce this document, in whole or in part, or otherwise supply it for use by any third party, without the prior written consent of CyberCX. CyberCX owns all intellectual property rights, including copyright, trade secrets, know-how and methodologies, in everything developed by CyberCX for clients, in whatever form and regardless of when such rights come into existence. CyberCX appreciates your co-operation in protecting its intellectual property.

