Security Testing

G-Cloud 15 Service Definition

Table of Contents

Introduction

Ekco Cloud & Security is an ideal partner for public sector organisations seeking a **secure, compliant, and scalable provider** via G Cloud 15.

We make it easier for IT teams to innovate, scale, manage, troubleshoot and secure. Across cloud, business continuity, security and workspace solutions, we enable the growth our customers want with the team they already have.

Through our security-first approach, large specialist workforce, AI-enhanced operations, and proven delivery capability, we help organisations:

- Modernise securely
- Strengthen cyber resilience
- Reduce operational risk
- Improve service continuity
- Deliver safer, more reliable digital services for our customers and their stakeholders.

Ekco's end-to-end cloud and cyber services are well matched to **G Cloud purchasing needs and public sector transformation goals**.

Security Testing

Service Overview

Our Security Testing team helps clients in identifying vulnerabilities and security misconfigurations in their cloud based applications, infrastructure, virtual environments, and networks. This enables the identified issues to be triaged, treated and protected before they are potentially targeted by malicious threat actors.

We offer a comprehensive catalogue of security testing services that can be tailored to offer a bespoke security testing package that best suits your needs and risk appetite.

Our highly skilled and experienced team have recognised certifications in various testing disciplines enabling us to deploy the most suited individuals to the particular test.

Features

The key features of the Security Testing Service are:

- Adversary Emulation using Tactics, Techniques and Procedures (TTPs)
- API Security Assessment
- Ethical Hacking as a Service
- Infrastructure Penetration Testing
- Mobile Applications Penetration Testing
- Purple Team Assessment and Red Teaming/TIBER-EU
- Social Engineering & Phishing Assessment
- Static Application Security Testing (SAST)
- Vulnerability Management as a Service
- Web Application Penetration Testing

Benefits

The key benefits of the Security Testing Service are:

- Penetration Testing by certified professionals (CREST, OSCP, eWPT etc.)
- Focused on areas in ISO27001, OWASP Top 10, PCI-DSS
- Follows security standards including OWASP, MASTG and NIST
- Pinpoint and report holistic security weaknesses and associated organisational risks
- Enhances organisation's ongoing efforts in maintaining compliance and assuring security

- Employs Tactics, Techniques and Procedures used by cyber criminals
- Replicates Threat Actor scenarios using MITRE ATT&CK framework
- Targeted phishing campaigns and physical security assessments
- Application source code assessed using white box approach
- Identify critical vulnerabilities and reduce cybersecurity risk

Service Outline

Adversary Emulation

Ekco's Adversary Emulation is carried out by a team of penetration testing experts with extensive experience and certifications in security testing. The objective of this service is to assist the organisation in understanding the operation and effectiveness of their detection capabilities by simulating the activities and Tactics, Techniques and Procedures (TTPs) of a sophisticated threat actor.

Such vulnerabilities could potentially be exploited by attackers to compromise the security and integrity of your organisation and its internal network, its user base, and the sensitive data it contains therein. Key aspects of the assessment include emulating a cyber threat actor including the running of a range of specialised commercial tools and in-house developed test scripts that address security concerns, prominently featuring covert communication, privilege escalation and pivoting/lateral movement within the network and testing for data exfiltration.

Service Offering:

- Penetration Testing is conducted by knowledgeable and experienced security professionals and Active Directory experts
- Pinpoints holistic security weaknesses and associated organisational risks, with a focus on emulating specific scenarios and targeting systems as a real-life attacker would
- Enhances the organisation 's ongoing efforts in maintaining compliance and assuring security
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

API Security Assessment

Ekco's API Security Testing is carried out by a team of penetration testing experts with extensive experience and training in API security testing. The objective of this service is to identify potential security weaknesses and configuration errors in an organisation's external and Internal-facing APIs. Such vulnerabilities could potentially be exploited by attackers to compromise the security and integrity of the application, its user base, and the sensitive data it handles. The service includes a range of tests that address various security concerns, prominently featuring the identification of issues from the OWASP API Top 10 list.

Key aspects of the assessment include the scrutiny of API settings, checking for ways to circumvent user role restrictions, and evaluating the resilience of logical workflows.

Service Offering:

- Penetration Testing is conducted by knowledgeable and certified security professionals. (CREST, OSCP, eWPT etc.)
- Pinpoints security weaknesses and associated organisational risks, with a focus on areas highlighted in the OWASP API Top 10
- Enhances the organisation 's ongoing efforts in maintaining compliance and assuring security
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Ethical Hacking as a Service

Ekco's Ethical Hacking as a Service is carried out by a team of penetration testing experts with extensive experience and certifications in security testing. The objective of this service is to work collaboratively with the client to provide governance and oversight of your penetration testing programme. This enables a broad range of penetration testing to be performed including external-facing or internal infrastructure, applications, mobile applications, APIs, and other testing scenarios such as Red teaming and Social engineering as applicable. Such vulnerabilities could potentially be exploited by attackers to compromise the security and integrity of the applications, infrastructure, and internal network. The service includes a range of tests that address various security concerns for example, PCI-DSS and ISO-27001 and follows leading security practices and standards from OWASP, NIST etc.

Service Offering:

- Penetration Testing is conducted by knowledgeable and certified security professionals. (holding certifications such as CREST, OSCP, eWPT etc.)
- Aid in the creation or amending of the existing penetration testing programme and implementation of same with a dedicated consultant to act as a Single Point Of Contact (SPOC)
- Identify and document the valid services and applications running both on the Internet Perimeter and Internally
- Analyse the services to determine their risk priority which will be utilised when determining the sequence in which vulnerability scans or penetration testing must be conducted
- Perform vulnerability scanning and penetration testing on the identified services and applications
- Pinpoints security weaknesses and associated organisational risks, with a focus on areas highlighted in PCI-DSS, ISO 27001 by following leading security practices and standards such as OWASP and NIST etc
- Enhances the organisation's ongoing efforts in maintaining compliance and assuring security
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes

- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Infrastructure Penetration Testing

Ekco's Infrastructure Penetration Testing is carried out by a team of penetration testing experts with extensive experience and certifications in security testing several types of IT infrastructure including various servers, endpoints, network devices and cloud systems across numerous operating systems. The objective of this service is to identify potential security weaknesses and configuration errors in an organisation's external or internal infrastructure by enumerating ana analysing the services and open ports available on the target systems. Such vulnerabilities could potentially be exploited by attackers to compromise the security and integrity of the network, its user base, and the sensitive data it handles. The service includes a range of tests that address various security concerns for example, PCI-DSS, ISO 27001, Cyber Essentials etc.

Key aspects of this assessment include network mapping and enumeration, external and internal infrastructure testing including wireless testing. In addition, privilege escalation and pivoting/lateral movement within the network and finally testing for data exfiltration and persistence.

Service Offering:

- Penetration Testing is conducted by knowledgeable and certified security professionals. (holding certifications such as CREST, OSCP, eCCPT etc.)
- Enhances the organisation's ongoing efforts in maintaining compliance and assuring security by following leading security practices and standards such as NIST and utilising tools such as nmap, Nessus Professional and Qualys, among others
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Mobile Applications Penetration Testing

Ekco's Mobile Applications Penetration Testing is carried out by a team of penetration testing experts with extensive experience and certifications in both Android and Apple iOS mobile application security testing. The objective of this service is to identify potential security weaknesses and configuration errors in an organisation's Mobile Applications. Such vulnerabilities could potentially be exploited by attackers to compromise the security and integrity of the application, its user base, and the sensitive data it handles. The service includes a range of tests that address various security concerns, prominently featuring the identification of issues from the OWASP Mobile Top 10 list.

Key aspects of the assessment include Information Gathering and Reconnaissance, Identifying Attack Surfaces and Threat Modelling, Testing for Common Mobile App Vulnerabilities, Code Analysis and Reverse Engineering, Authentication, Authorisation, and Session Management Testing, Data Security and Privacy Testing, Network and Communication Security Testing, Malware Analysis and Detection, Physical Device Security Testing.

Service Offering:

- Penetration Testing is conducted by knowledgeable and certified security professionals. (holding certifications such as CREST, OSCP, eWPT etc.)
- Pinpoints security weaknesses and associated organisational risks by following leading security practices and standards such as OWASP MASTG and NIST
- Enhances the organisation's ongoing efforts in maintaining compliance and assuring security
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Purple Team Assessment

Purple teaming is a specific type of penetration testing that aims to closely simulate a real-life attack on an organisation by a sophisticated cyber threat actor (the Red Team) but work in collaboration with the defending Blue team. Such an exercise is often broader than standard penetration testing and is a more holistic approach to security testing.

The collaborative approach means that the defending team will have more awareness and information on what scenarios are being run/activities are being performed giving them more insight into what security gaps exist and how these attacks could be prevented during the exercise.

Service Offering:

- Employ the Tactics, Techniques and Procedures (TTPs) used by real-world sophisticated cyber criminals to implant malware, communicate with attacker infrastructure, enumerate your environment, bypass host and network defences, move laterally and attempt to access and exfiltrate sensitive data in a simulated attack on your organisation
- Work collaboratively with the Blue team to give additional insight into the testing approach and issues identified
- This testing utilises specialised tooling and can manually replicate elements of specific scenarios employed by Threat Actors and follows the MITRE ATT&CK framework
- A comprehensive report is issued including the attack path and scenarios performed, the security issues identified, the recommended remediation activities and guidance on how to enhance the security posture and resiliency of the organisation

Red Teaming/TIBER-EU

Red teaming is a specific type of penetration testing that aims to closely simulate a real-life attack on an organisation by a sophisticated cyber threat actor. Such an exercise is often broader than standard penetration testing and is a more holistic approach to security testing.

TIBER-EU refers to a European framework for Threat Intelligence Based Ethical Red-teaming and is designed to be followed by entities who provide core services (such as the financial sector) or national authorities who manage critical public infrastructure.

As the name suggests, the scenarios used in a TIBER-EU engagement are derived from the Cyber Threat Intelligence phase, performed at the beginning of the engagement.

This allows the Red team (the simulated attackers) to emulate threat actors applicable to your organisation and employ similar Tactics, Techniques and Procedures (TTPs) that a real cyber-criminal organisation would.

Service Offering:

- Cyber Threat Intelligence:
    - Understanding your organisation and business sector in order to identify the threat actors who may be targeting the organisation (for simulation purposes)
- External Perimeter testing:
    - Perform an assessment of externally facing infrastructure, applications, and services to determine potential security gaps an attacker may seek to exploit to gain a foothold within your organisation
- Social Engineering – Phishing and Physical security testing:
    - Perform a targeted phishing campaign against a representative sample of employees and/or a physical security assessment seeks to bypass physical security controls within your organisation's offices
- Internal Red Teaming
    - Employ the Tactics, Techniques and Procedures (TTPs) used by real-world sophisticated cyber criminals to implant malware, communicate with attacker infrastructure, enumerate your environment, bypass host and network defences, move laterally and attempt to access and exfiltrate sensitive data in a simulated attack on your organisation
    - This testing utilises specialised tooling and can manually replicate elements of specific scenarios employed by Threat Actors and follows the MITRE ATT&CK framework
- Reporting
    - A comprehensive report is issued including the attack path and scenarios performed, the security issues identified, the recommended remediation activities and guidance on how to enhance the security posture and resiliency of the organisation

Social Engineering & Phishing Assessment

Ekco's Social Engineering & Phishing Assessment is carried out by a team of penetration testing experts with extensive experience and certifications in physical security testing and social engineering. The objective of this service is to identify vulnerabilities in human behaviour, processes, and technical controls that could be exploited by malicious actors to gain unauthorised access or sensitive information. Exploiting these issues may give an attacker access to your internal network via phishing or physical premises via social engineering. The service includes a range of tests that address various security concerns.

Key aspects of the assessment include Open-Source Intelligence Gathering (OSINT), testing physical security controls e.g. Assessing Tailgating and Piggybacking Risks, Conducting Phishing, Vishing, and Smishing Campaigns, Evaluating Security Awareness and Training Effectiveness.

Service Offering:

- Testing is conducted by knowledgeable and experienced security professionals
- A targeted phishing campaign is conducted, intended to socially engineer employees of your organisation
- A physical security assessment seeks to bypass physical security controls within your organisations offices in order to gain internal access to the internal corporate network as well as devices, systems, infrastructure, or sensitive data within the physical location itself
- Enhances the organisation's ongoing efforts in maintaining compliance and assuring security
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Static Application Security Testing (SAST)

SAST involves assessing the source code of the target application in order to identify vulnerabilities in an application by performing code analysis, vulnerability identification, configuration review and secure programming review.

Ekco's Static Application Security Testing (SAST) service is carried out by a team of penetration testing experts with extensive experience in both application development and security testing.

This means that we can quickly understand the target application across a wide variety of programming and scripting languages. Combining this knowledge with specific commercial and open-source tools based on the languages used, the Ekco team can quickly and effectively identify vulnerabilities in your application source code but also perform manual verification to help mitigate the reporting of false positives (something many tools struggle with). This hybrid automated and manual approach ensures testing is conducted efficiently but also provides extra assurance on the issues identified.

Key aspects of the assessment include gaining an understanding of the application source code, its functionality, dependencies, inputs, and outputs and use cases. Assess the code for common vulnerabilities and/or insecure programming patterns or configurations, and manually reviewing potential high-risk areas of code as well as performing false-positive elimination where possible.

Service Offering:

- SAST is conducted by individuals with both software development and security testing experience knowledgeable and certified security professionals
- Testing is conducted from a white-box approach where the target application source code is provided to the testing team (along with any other relevant configuration files or associated information)
- Is used to identify vulnerabilities early in the software development process as well as those which may not be applicable/obvious during penetration testing
- Can be conducted at regular intervals in the software development lifecycle (SDLC) and often used in conjunction with standard vulnerability scanning and penetration testing following standards such as OWASP and NIST
- Specific commercial and open-source tools are used as part of the testing such as SonarQube, Checkmarx, Veracode, among others
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in priortising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Vulnerability Management as a Service

Ekco's Vulnerability Management as a Service is carried out through a network of local teams in thirteen locations across Europe, based in UK, Ireland, and Netherlands our approach helps us be proactive and respond faster to your needs. We offer integrated vulnerability management program based on using the Qualys VMDR (Vulnerability Management Detect and Respond) solution to provide you with greater visibility and insight into cyber risk exposure - making it easy to prioritise vulnerabilities, assets, or groups of assets based on business risk. Quays VMDR is a solution to Discover, assess, prioritise, and patch critical vulnerabilities and reduce cybersecurity risk in real time and across your global hybrid IT, OT, and IoT landscape.

Key aspects of Qualys VMDR covers all of an organisation's rapid remediation needs, leveraging risk-based VM and easy-to-use no-code workflows:

- Qualys Cloud Platform, combined with its powerful lightweight Cloud Agent, Virtual Scanners, and Network Analysis (passive scanning) capabilities bring together all four key elements of an effective vulnerability management program into a single app unified by powerful out-of-the-box orchestration workflows

- Qualys VMDR enables the organisation to automatically discover every asset in their environment, including unmanaged assets appearing on the network, inventory all hardware and software, and classify and tag critical assets. VMDR continuously assesses these assets for the latest vulnerabilities and applies the latest threat intel analysis to prioritise actively exploitable vulnerabilities
- VMDR automatically detects the latest superseding patch for the vulnerable asset and easily deploys it for remediation. By delivering all this in a single app workflow, VMDR automates the entire process and significantly accelerates an organisation's ability to respond to threats, thus preventing possible exploitation

Service Offering:

- Vulnerability Scanning: Identification of vulnerabilities based on cloud agent and appliance-based scanning, for internal networks
- Remediation Policy Management: Creation of remediation policies to generate internal Qualys tickets as required by client
- Vulnerability management service –Triage of discovered vulnerabilities according to asset criticality, threat indications, vulnerability severity and company's policy, and prioritisation based on VMDR prioritisation and client requirements
- Patch management – (for assets in scope of the Qualys Patch Management license) our service will use Qualys PM to install security patches to assets

Web Application Penetration Testing

Ekco's Web Application Security Testing is carried out by a team of penetration testing experts with extensive experience and certifications in the security testing of applications. The objective of this service is to identify potential security weaknesses and configuration errors in an organisation's web applications. Such vulnerabilities could potentially be exploited by attackers to compromise the security and integrity of the application, its user base, and the sensitive data it handles. The service includes a range of tests that address various security concerns, prominently featuring the identification of issues from the OWASP Top 10 list.

Key aspects of the assessment include mapping the attack surface and testing for common web vulnerabilities, testing for implementation and business logic flaws, authentication, and authorisation testing. In addition, testing for configuration and deployment misconfiguration and insecure communication.

Service Offering:

- Penetration Testing is conducted by knowledgeable and certified security professionals (holding certifications such as CREST, OSCP, eWPT etc.)
- Pinpoints security weaknesses and associated organisational risks by following leading security practices and standards such as OWASP and NIST and utilising tools such as Burp Suite Professional

- Enhances the organisation's ongoing efforts in maintaining compliance and assuring security
- Offers a severity-based categorisation of identified risks and vulnerabilities, aiding in prioritising fixes
- Delivers an in-depth report that includes both a high-level overview for executives and detailed technical insights for IT teams, complete with strategic recommendations for addressing identified issues

Project Implementation

Onboarding a client into their new contracted services requires a structured process to ensure a smooth transition and clear expectations. The following process provides a high-level overview of our bespoke implementation plan.

1. Pre-Implementation Preparation

Initiate internal communications with internal stakeholders, confirming contracted deliverables, and bespoke scope of works. Confirm dedicated resource across the business depending on function.

2. Client Engagement

Initiate communication with the customer's key stakeholders to discuss the onboarding process, timescales (including support go live date), expectations, and roles.

3. Business Intelligence Discovery

Conduct a thorough assessment of the client's internal processes, gather key information regarding end users, business requirements, 3rd party data, user account management and operational workflows.

4. Technical Deliverables

Complete a detailed assessment of the customer's existing IT infrastructure, cloud, network, applications, and systems. Identify different user roles and access requirements. Deploy and document toolsets. Develop a comprehensive knowledge base containing FAQs, troubleshooting guides, and best practices based on their current environment.

5. NOC and SOC Deliverables

Configure and deploy and contracted NOC and SOC toolsets, complete basic security checks such as MFA and password policies.

6. Points of Attention

Based on technical audits and client concerns, create a Points of Attention document with the assigned account manager to review with the client

7. Acceptance into Service

Schedule and complete the acceptance into service with the required internal departments.

8. "Go Live"

Handover to our required internal stakeholders and departments to take on the clients contracted deliverables. Implementation team to provide 2 weeks of enhanced support to our internal teams and the client, ensuring support, access and processes are running smoothly.

Why Ekco

Why UK Public Sector Organisations benefit when they Partner with Ekco Cloud & Security

Security-First Cloud Services Aligned to Government Standards
Ekco Cloud & Security is a leading UK and European **security-first managed cloud provider**, delivering deep expertise across cyber security, identity, and cloud. Our services align with **NCSC guidance, the Cyber Assessment Framework (CAF), NHS DSPT**, and wider public sector assurance requirements.

Our proven **Assess → Protect → Detect → Respond** model supports secure-by-design digital transformation across hybrid and distributed environments—directly addressing public sector risk and resilience priorities.

End-to-End Capabilities Mapped to G Cloud 15
Public sector buyers need suppliers that can deliver migration, protection, management, and optimisation through a single, accountable partner. We provide a **fully integrated cloud and security portfolio**, including:

- Cloud migration and managed cloud operations
- Security and infrastructure management
- Identity security and privileged access management
- Secure modern architecture design
- Real-time threat detection and incident response

These services align directly with **G Cloud 15 lots and purchasing criteria**, enabling organisations to modernise securely while managing complex legacy estates.

Scalable Expertise and Sovereign Delivery
With **1,000+ cloud and security specialists across the UK and Europe**, we offer the scale, depth, and resilience required to support mission-critical public services. A dedicated **identity security practice** provides mature capability for access control and Zero Trust adoption—an increasingly critical requirement across government organisations.

Tailored Solutions for Resource-Constrained Organisations
Recognising the challenges faced by councils, NHS trusts, education, and blue-light services, we offer **cost-effective, scalable cloud and cyber security solutions** designed for organisations with limited internal capacity.

These services protect against phishing, ransomware, and social engineering while meeting G Cloud's expectations for solutions that are secure by default, rapidly deployable, and low overhead.
AI-Enhanced Security Operations
We embed **AI into daily security operations**, improving analyst productivity and response effectiveness. AI-assisted services accelerate:

- Incident triage and prioritisation
- Threat analysis and vulnerability summarisation
- Reporting accuracy and audit readiness

This enables faster outcomes and stronger protection for public bodies operating with limited staffing.

Public Sector-Focused Engagement Model

Our partnership-led approach aligns with government procurement expectations, offering:

- Dedicated, accountable delivery teams
- Transparent SLAs and service reporting
- 24/7 support with local expertise
- Predictable commercial and contract models

This ensures we act as a **strategic long-term partner**, not a transactional supplier.

Global Recognition and Strategic partnerships

These global accreditations partnerships show our commitment to customer satisfaction, data safety, security and overall quality. We're independently audited every year to give our customers confidence in our approach.

From agile managed cloud platforms to next-gen security services that supercharge defences, our local team of specialists provide proactive, round-the-clock management. With one Ekco Cloud & Security team delivering a combination of services, our customers quickly gain control and visibility over their technology.