G-Cloud 15

Ethical Hacking Service

January 2026

Contents

Ethical Hacking

This section describes in more detail the service features and benefits included within this service definition document.

Ethical Hacking

Testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures.

Ethical Hacking Service Features	Ethical Hacking Service Benefits
• IT Health Checks, internal and external security assessments • Cloud assessments including architecture reviews across the full range of PaaS and IaaS solutions • Assessments of cloud first identity services including PAM solutions • Application security reviews including source code analysis • Build configuration reviews, including operating systems, databases and network devices • Network device reviews including wireless and voice networks • Mobile applications and devices security reviews • Red team attacks including phishing, vishing, SMiShing and other social engineering techniques • Cyber threat profiling to identify technical characteristics of potential attacks • Custom malware implementation to evade internal network controls • Stolen laptop assessments to replicate an attacker with physical access • Auditing of previous penetration tests including scope and remediation activities • Connected systems security testing • Electric Vehicle & EVSE systems testing	• Custom methodology, which is aligned with NCSC CHECK and CREST • Fully accredited CHECK reports clearly articulating business risks • Root cause analysis that enables you to fix issues directly and once • Cost effective recommendations for mitigating risks and preventing their proliferation • Expert guidance on understanding risks to systems and data • Reduced delays in project delivery resource can be made available • Identification of robust process controls to improve security posture • Leverage of PwC's extensive experience in providing ITHC testing • Use of highly skilled CHECK team certified technical resources • Access to additional specialists in cyber security and risk consulting.

Our Services

Our Penetration Testing (Ethical Hacking) services apply tailored testing methodologies to identify security vulnerabilities that may be exploited by real world threat actors. We offer several different penetration testing services depending on the technology under test and the attack scenario being emulated.

Red Teaming: Utilising a proprietary and industry approved methodology to deliver real-world and intelligence-led red team exercises. This allows us to offer a full suite of services that can emulate any type of targeted cyber attack.

Web Application Penetration Testing: Combines automated security testing and manual analysis of vulnerabilities at all stages of the software lifecycle, covering the OWASP top ten most critical web application security risks. We test bespoke applications as well as low-code and SaaS solutions such as Microsoft Dynamics and Salesforce.

Software security: Utilises our methodology for evaluating the maturity of software security and compliance efforts covers all phases of the development lifecycle, to allow an organisation to build a highly secure application. This includes deployments on low-code and no-code SAAS solutions.

Mobile App Testing: Security testing and manual analysis of vulnerabilities within mobile applications at all stages of their development, covering the OWASP Mobile top ten most critical app security risks.

Internal Infrastructure Testing: Covering all technologies and operating systems that are likely to be located on an internal network. We can conduct white box penetration tests, limited to defined systems, through to black box penetration tests, that explores the impact of an attacker with logical access to an internal network but no credentials.

External Infrastructure Testing: Simulating tactics used by attackers to probe external systems for any open ports or applications that could be used to gain access to your internal network.

Cloud Platforms: Reviewing cloud systems from an attacker centric view, including the management, architecture and design of a system and the configuration of authentication mechanisms used throughout the solution. These reviews include collaboration platforms such as Microsoft Teams, Slack, Jira, Confluence, as well as file sharing platforms.

Endpoint Security Assessment: Perform user endpoint device build reviews as well as acting as a malicious insider who has access to IT equipment, such as a standard user laptop, but limited knowledge of the internal network.

Network device security: Our methodology combines the use of automated tools, manual verification and interviews with technical stakeholders (such as firewall administrators) to assess the security of each network device. This includes assessing the device/s for misconfigurations, deviation from good practice, outdated software and missing security patches.

Hardware, OT, IIoT, Automotive and IoT security: Utilising our dedicated specialist testing environment: Testing for various types of electronic devices is possible. Such devices can include smart home devices, operational technology and IoT devices.

We also offer advanced penetration testing services tailored for identifying business critical security vulnerabilities in Operational Technology (OT), SCADA, and IoT environments. This includes:

- Automotive and vehicle penetration testing and forensics;
- IoT security evaluations, and
- destructive and non-destructive hardware security testing services.

We have a dedicated lab equipped with the latest technology, as well as a dedicated team with experience conducting security reviews of physical hardware, Operational Technology and IoT environments such as Connected and Autonomous Vehicles (CAV), Industrial Control Systems (ICS) and Connected Devices.

We have one of the largest dedicated warehouse facilities in the UK to allow testing of even the largest platforms including large scale faraday chambers and RF enclosures.

Our hardware security testing methodology covers a full physical analysis of hardware devices, as well as individual components (such as flash memory and processors).

BMS, Access control and HVAC systems are now predominantly online for ease of use, maintenance and reporting, from simply lighting control solutions to complex power switching and security access, such systems are often taken for granted. Our hardware testing services allow the true risks hidden within these components to be made visible so they can be considered and managed appropriately.

Expanded Services Available

Architecture Review: We use a proprietary network architecture security maturity model to provide clients with a current security maturity, target maturity and security roadmap towards achieving this.

Phishing Simulation: We develop realistic phishing emails that are weaponised with custom malware to entice users into following links or opening attachments in order to infect their systems. With the objective to gain a foothold on the internal network by compromising users' systems via targeted phishing emails.

We can also perform open-source intelligence (OSINT) gathering to develop a phishing campaign that targets users en-masse. Using this tailored phishing email designed to trick users into following specially crafted links that leads to disclosing sensitive information, such as credentials. Allowing for a gauge of the overall level of security awareness amongst a target group of users. This can be combined with our cyber

culture and awareness team who can provide user awareness and training courses following on from the phishing results.

(Physical) Social Engineering: Conduct online and physical reconnaissance, develop realistic cover stories and attempt to bypass physical security controls. Facilitating the ability to gain unauthorised access to restricted locations by exploiting physical security weaknesses, procedural weaknesses and user security awareness. Hardware implants can be deployed to provide later remote access if required.

WiFi Security Review and Attack Simulation: Using a rogue WiFi Access Point impersonating a legitimate one and enticing users to connect to it through technical and non-technical means. Allowing for potential capturing of sensitive data or credentials to websites and internal passwords via an interception attack against users when they connect.

Threat Led Penetration Testing: Achieved through an in-depth threat intelligence assessment of an organisation's specific threat profile, followed by the execution of a set of attack scenarios – commonly known as 'red teaming'- designed to mimic the methodologies of real-world threat actors in a safe and controlled manner.

Performed in line with regulatory requirements from the Cabinet Office, the Bank of England, and OFCOM. All scenarios carried out as part of an attack simulation are formed from in-depth threat intelligence assessments that have been crafted into detailed scenarios agreed with the regulator. The attack scenarios are designed to mimic a highly skilled threat actor and identify critical issues.

Software Security Maturity Assessment: We assess your SDLC (software development lifecycle) security and give you the information you need to efficiently and effectively manage your software security risks aligned with your Agile, DevOps or DevSecOps practices.

Application Security Controls Review: Create visibility of the current state of application security and compromise resiliency controls implemented in the application including but not limited to Authentication, Data Protection, Session Management, Access Control and Malicious Input Handling. Also identify effective security controls which can be implemented by application team to increase the cost on the attacker.

Static Application Security Testing: Reviewing the application source code using complementary automated and manual techniques to identify security flaws and analysing embedded open source libraries for publicly known vulnerabilities. This approach provides an efficient combination of scope, coverage and time effective reporting.

Hardware Security Review: Our specialists have experience of conducting destructive and non-destructive firmware extraction, power glitching attacks, in circuit programming and identification and exploitation of debug interface identification. These techniques are combined in our dedicated hardware laboratory with those used in more traditional hardware forensics laboratories such as "chip-off memory extraction" to maximise coverage and identification of vulnerabilities.

Closed or Open Book Security Reviews: Our methodologies allow for a variety of styles to be taken during the assessment – in the form of tests which provide increasingly more information and access to the systems to allow for a more in-depth analysis over a shorter period of time. Using provided materials subject to the area of interest. A more focused and thorough review of security can be conducted.

IoT Device Testing: Each IoT device is unique thus a mixture of methodologies is required to effectively assess their security. This includes but is not limited to linked mobile app testing, backend web application API testing. Firmware Analysis, testing and network packet analysis. All services offered allowing for a bespoke targeted testing to be provided.

OT/Scada/ICS Device Testing: Using simulated implementations of the environment they would exist within, Allowing for safe testing of all aspects of the device, firmware and overall security. Carried out as part of a security review allows for potential business critical issues to be identified that would otherwise be missed or untestable.

Firmware Analysis: Firmware access can be achieved via multiple potential routes. Once extracted, the firmware can then be examined and reverse engineered by specialists to either identify new potential issues or verify a third-party firmware has all the expected functionality.

Microsoft Software: Based on Microsoft security guidelines we will conduct a review of the underlying Windows server, core security configurations, user accounts and permissions, password policies and auditing policies to identify gaps and potential weaknesses. This will determine if the deployment aligns to Microsoft's security guidelines. We also review cloud-based deployments such as Microsoft Dynamics 365, SharePoint, Azure AD (Entra ID), where the backend is not available for review, so the focus is on the configuration as well as the user permissions within the system.

Guidewire Security Assessment: We conduct a review of the Guidewire configuration and the underlying system it is running on. This will include core security configurations, user accounts and permissions, password policies and auditing policies to identify gaps and potential weaknesses.

Atlassian Security Assessment – Jira and Confluence: We conduct a review of the Atlassian configuration and the underlying system it is running on. This will include core security configurations, user accounts and permissions, password policies and auditing policies to identify gaps and potential weaknesses.

Salesforce Security Assessment: Our Salesforce reviews comprise four key elements:

- **Workshop:** To understand your Salesforce Implementation and configuration, including an customisation you may have performed

- **Security Implementation Review:** We conduct a review of core security configurations, user accounts and permissions, password policies and auditing policies to identify gaps and potential weaknesses. This will determine if the Salesforce deployment aligns to the Salesforce security guidelines

- **Salesforce custom application penetration test:** We perform testing specifically on the custom areas of development deployed and developed by yourself. All manual testing conforms to our internal PwC web application testing methodology to ensure coverage of key security areas, including those outlined by OWASP

- **Targeted Apex Code Review:** We will identify security vulnerabilities in targeted areas of the customer Salesforce applications source code and any third-party dependencies with associated risks and vulnerabilities, determine if these are inline with Security Guidelines for Apex and Visualforce Development and controls needed to prevent recurring security issues.

Workday Assessment: We will conduct a review of core security configurations, user accounts and permissions, password policies and auditing policies to identify gaps and potential weaknesses. This will determine if the Workday deployment aligns to the Workday security guidelines.

Swift Security Assessment: We have developed a SWIFT testing methodology which aligns with Customer Security Program (CSP) SWIFT Customer Security Controls Framework (CSCF). This custom methodology allows us to perform detailed reviews of your SWIFT infrastructure as well as a review of the SWIFT applications in line with SWIFT guidelines.

Active Directory: An Active Directory review of operational processes, as well as the privileged accounts and groups membership. Looking at configuration options applied to the domain through group policy and review of the forest and domain trusts. The output is compared against the current Microsoft best practices – for example Red Forest.

Vulnerability Research: Researching weaknesses within a product or application from a hands on perspective, including fuzzing products, reverse engineering them to perform code reviews. Reviewing network traffic and any custom protocols used by the application or service.

Reverse Engineering: Reverse engineered by specialists to either identify new potential issues or verify a third-party firmware has all the expected functionality.