Capgemini

IT Health Check (ITHC)
G-Cloud 15

Table of Contents

1 Service Overview

An IT Health Check is a penetration test specific to the public sector, often to support PSN Compliance. A reliance on interconnecting networks, cloud, web applications, VPNs, VoIP, BYOD policies and IP-enabled devices creates multiple entry points into a network. The ITHC penetration testing service provides an in-depth technical review of your network, using proven methodologies to identify all weaknesses and vulnerabilities. Penetration testing is effective at preventing unauthorised access by simulating an attack and using active exploitation.

The deliverables for a formal ITHC assessment include completion of a comprehensive penetration testing formal document report and spreadsheet tracker per area of focus.

2 Business Need

In today's digital age, the landscape of cyber threats is not only expanding but also becoming increasingly sophisticated, making traditional reactive security measures insufficient for safeguarding assets. As adversaries employ more advanced techniques to exploit vulnerabilities, the need for proactive security measures has never been more critical. Penetration Testing emerges as an indispensable solution in this context, offering a comprehensive and proactive evaluation of an organization's security posture.

Penetration Testing transcends conventional security assessments by simulating real-world attack scenarios, providing a unique opportunity to identify and address vulnerabilities before they can be exploited by malicious actors. This allows organisations to stay a step ahead of potential threats, ensuring that security measures are not only responsive but also anticipatory.

Capgemini's IT Health Check service not only helps in identifying security gaps but also plays a crucial role in guiding organisations towards industry standards and best practice configuration. By understanding the specific vulnerabilities and threat vectors that could be used organisations can better allocate their resources, prioritising the strengthening of defences where they are most needed.

3 Our Approach

Capgemini will conduct this assessment using our standard methodology. This methodology has been successfully utilised in many similar projects and has been refined to ensure an effective and efficient engagement that results in meeting your overall objectives.

This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

Our standard assessment methodology includes the following stages and are refined to meet customer requirements and objectives:

- Stage One – Scoping Meeting
  - Confirmation of the overall objective(s) of the assessment
  - Understanding of timelines
  - Identification of key personnel
  - Confirmation of the scope (including systems, access, credentials, URLs, IPs)
- Stage Two – Planning and Scheduling
  - Creation of a scope of work document and plan of assessment activities
  - Confirmation and requesting of client dependencies
  - Dissemination of a schedule of activities to key personnel
  - A confirmed schedule for the report creation & QA activities
- Stage Three – Testing
  - Assessment of systems in line with relevant methodologies
  - Technical testing
  - Communication and escalation of any significant vulnerabilities identified to enable swift remediation
  - Verbal summary of the days finding with the primary contact at the end of each day
- Stage Four – Report writing and QA Process
  - Compilation of interim reporting data
  - Early release of draft interim findings to allow early remediation to start
  - Full detailed long form reporting completed

- QA process and final release to customer

- Stage Five – Follow up (if required)
  - Presentation and discussion of findings at high level, or low level with technical personnel
  - Capgemini can provide technical support resources to support in investigating, identifying and implementing suitable remediation(s) for any weaknesses, risks or vulnerabilities
  - Further support for vulnerability and risk management opportunities can be identified, including SOC services, information systems architecture or support services

Scope of Tests

An ITHC may include the following tests

- Cloud Platform Security Configuration Review (access control, storage visibility, attack surface, misconfigurations)
- External Infrastructure Assessment (access control, remote access, VPN Servers, DMZ servers)
- Internal Infrastructure Assessment (internal servers, router and firewall devices, network appliances)
- Operating System Assessment (patching, monitoring, anti-virus, configuration and malware protection)
- Wireless Infrastructure Assessment

Network Device and Firewall, Gateway Device Configuration Reviews

- Application Security Assessment (including websites and Intranets/Extranets)
- Mobile Application Security Assessment
- Vulnerability Scanning
- Scenario Based Penetration Testing
- Security Code Review

Cloud Platform Security Configuration Review

This is a comprehensive review of the configurable options within a cloud platform paying close attention to the responsibilities of customer vs cloud provider with configurable controls. The objective is to examine the key security issues associated with modern cloud platforms and cloud-based applications, focusing on risks from unauthorized users and assessing the potential for legitimate users to misuse their privileges and access rights. Examples include:

- Inadequate Security Strategy and Monitoring – reviews of monitoring systems and application of best practise controls
- Insecure APIs – modern mobile and web applications use APIs for data, which are frequently incorrectly secured, or secret keys leaked leading to data exfiltration or system access
- Data Breaches – weak authentication measures or unsecured data stores can lead to leaks of sensitive information
- Permanent Data Loss – should malicious actors gain access, data can be deleted in a non-recoverable manner

Account Hijacking – attackers steal personal logon credentials to gain access, mitigations such as MFA are key to help secure access

Insufficient Access Controls – APIs are constantly attacked and malicious actors probe any accessible data, without strict access management, overly permissive access can leak sensitive or personally identifiable information

- Misconfigured Controls – proper configuration of resources and regular audits help to identify misconfigurations of storage blobs and buckets that could expose sensitive data

External Infrastructure Assessment

This will be conducted from Capgemini systems, accessing the organisations internet facing network. The intention is to assess the vulnerabilities which an unauthenticated attacker could use to penetrate the network. This will normally be internet-facing systems such as web servers, remote access gateways and wireless networks.

Internal Infrastructure Assessment

This is a comprehensive review of device and server configurations to identify issues within a client organisation's internal network and is typically conducted from consultants present on a customer site, or remotely via a testing appliance. It will incorporate manual and automated security testing tools and techniques to identify vulnerabilities within desktops, servers and network infrastructure, which could be exploited from within the organisation.

Server / Desktop Security Assessment

The Server / Desktop Security Assessment will provide information as to the resilience of a server or workstation system to withstand attack from unauthorised users and the potential for valid users to abuse their privileges and access rights. This will also include the configuration and patching regime.

- Host Build - reveals flaws in the build process, or weaknesses existing in the accepted build standard
- Firewall Configuration - highlights deficiencies in the firewall configuration security
- Network Device Configuration - uncovers weaknesses that could lead to unauthorised access to network devices

IDS / IPS Configuration - highlights areas of deficient configuration that could lead to unnoticed attacks

- Utilises a tried, tested and proven methodology to conduct a comprehensive Infrastructure Assessment based on open standards such as PTES and OSSTMM and the CHECK scheme
- Achieves incredibly high levels of business value by focusing on areas that, if compromised, would pose the highest risk to your business
- Expert CHECK and CREST certified consultants perform the assessment through a combination of automated toolsets and manual audits

Minimal impact caused to your staff and their productivity.

Wireless Security Assessment

This will assess the organisations network's wireless infrastructure to identify potential vulnerabilities within the wireless network, and therefore any internal wired networks, against unauthorised access, whilst maintaining appropriate access control for authorised users.

Web and Mobile Application Security Assessment

A Web Application Security Test provides an in-depth technical coverage of an application's ability to withstand attack from unauthorised users and the potential for valid users to abuse their privileges and access rights.

A Mobile Application Security test will assess the mobile application security and its resilience to local on-device attacks and data leaks and how the mobile application interacts with its application program interface (API) to

understand how it can withstand attack from unauthorised users and the potential for valid users to abuse their privileges and access rights.

- Understands real world attack techniques and vulnerabilities, as applicable to your business
- Protects your business from unwanted intrusions
- Helps ensure the security of your web applications
- Utilises sophisticated intrusion detection using traditional approaches, public and proprietary signatures, heuristic techniques and manual analysis methodologies
- Comprehensively tests using Open Web Application Security Project (OWASP) methodologies for Web and Mobile testing
- Helps reduce unauthorised or unlawful activity on your applications in accordance with Data Protection Act principles
- Certified CHECK service - compliant with HMG standards

Vulnerability Scanning

Inside the organisations network or outside the organisations network this service aims to provide information on the assets contactable and their susceptibility to attack by enumerating known and unknown vulnerabilities. Can be used at scale to assess vast numbers of systems for one-off or regular scanning for remediation support over a long term

- One off or fully managed service tailored to your needs
- Internal or external (internet facing) assets scanning
- Industry leading vulnerability scanning tools
- Manual validation and testing of identified issues, eliminating false positives
- Non-disruptive testing, specifically no denial-of-service testing unless separately discussed and agreed

Helpful to monitor security baseline between penetration tests

Network Device and Firewall, Gateway Device Configuration Reviews

Configuration reviews of network devices are a critical component of maintaining a secure and resilient infrastructure. These reviews typically combine automated and manual processes to identify vulnerabilities and ensure compliance with best practices. Automated tools, such as Nipper, analyse running configurations to detect deviations from security standards and provide actionable recommendations. This output is then supplemented by manual assessments, which validate findings and evaluate network flows against business requirements. The review process often includes verifying firewall rules, password strength, and permitted traffic flows, while ensuring adherence to recognised frameworks like the Centre for Internet Security (CIS) benchmarks. By systematically assessing device configurations, organisations can reduce risk exposure, maintain regulatory compliance, and strengthen their overall security posture.

Scenario Based Penetration Testing

Scenario based penetration testing is simulating attacks against an organisation with a focus on testing their detection and response capability. Capgemini simulate the tools techniques and procedures of real-world threat actors.

- Comprehensive detailed reporting and timeline of activities to match up with security operations logs
- Clear concise remediation advice at a technical and strategic level
- Review of people and processes as well as technical security controls

- Security cleared personnel holding SC and DV clearances
- Consultants from networking, systems support and physical security backgrounds complementing each other's skills and experiences to form a strong team

Capgemini work with our organisations to tailor the testing to the risks they face. Meeting with business stakeholders to identify objectives for testing and to identify the threat profile of likely attackers. We use this to identify specific attack vectors commonly associated with the organisations business and methods noted to be successful in the real world, by real attackers.

Planning the assessment and looping in the Capgemini Threat Intelligence team to bring real world data to the table shapes the engagement based on facts and observations.

The team of expert highly qualified testers will set out and agree scenarios from email phishing to physical entry and device implantation to web based internet side application attacks. We follow guidance and methodology from the Mitre Attack Framework to simulate and emulate industry known attacks which have been broken down step by step. Known as the Tools, Techniques and Procedures (TTPs) we map our work to the framework allowing us to give clear mitigation and remediation in the reporting

Reports contain engagement summaries suitable for the executive audience as well as timelines and technical descriptions of issues with evidence and summary risks from each weakness, exposure or vulnerability.

Constant communication via out-of-band secure (non-corporate) methods keeps organisations informed without inadvertently alerting a organisations internal defender team.

Additional training and learning opportunities for organisations may follow, with workshops and meetings with security defender 'blue teams' as appropriate

Security Code Review

A Security Code Review will provide information on the resilience of application code to handle malicious input in a safe manner. Code should be designed to withstand attack from unauthorised and authorised users who may abuse their privileges.

- Key code areas examined in detail
- Large code bases reviewed at high / medium / low level as required
- Reviews of code and its compliance to industry best practise for design and trust boundaries
- Can be combined with active application testing to validate findings, especially with regards to authentication, authorisation and cryptography
- Ensure modern best practises for secrets handling such as credentials or other sensitive information

4 Buyer Responsibilities

All buyer responsibilities are identified on Sales Proposal and detailed in any project plans and statement of works.

Standard responsibilities include:

- Providing points of contact throughout the engagement
- Adherence to all requests for information, including written (hard copy\electronic) and verbal
- Access to appropriate facilities, technologies and individuals

5 Service Management

Capgemini will allocate suitably qualified and certified penetration testing consultants for the assessment.

Dependant on the scope, location, and complexity of the assessment, the consultants may be supported by additional resources as required to complete the assessment.

This may include specialist technical and non-technical resources and may be provided from Capgemini's onshore resource pools as appropriate.

The use of any additional resource will be agreed with the primary contact prior to any commencement, and with full oversight by the dedicated project lead.

Points of escalation will be communicated prior to commencement of any activities to ensure swift resolution of any issues.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and the individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Vendor Accreditations/Awards

For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

CHECK Green Light companies are security organizations that have been evaluated by the NCSC and deemed capable of delivering CHECK services to customers. Capgemini is an NCSC-approved company.

Capgemini and its CHECK Team statuses are listed on the NCSC website for validation purposes and is a partner with Microsoft, Amazon Web Services and Google for all cloud services.

Capgemini can provide security delivery professionals with the following industry certifications:

- Cyber Scheme Team Leader (CSTL)
- Cyber Scheme Team Member (CSTM)
- Offensive Security Certified Professional (OSCP)
- CREST CPSA
- CREST CRT
- CREST CCT
- CompTIA Pentest+
- CompTIA Security+
- AWS Certified Security Specialist
- Microsoft Azure Security Engineer

10 Sub-contractors

Subcontractors may be used under schedule 4 of the CHECK IT Health Check Service Contract between CHECK Green Light companies and NCSC.

11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of this service.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Projects can be priced either on a Time & Materials or Fixed Price basis.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

15 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com