Capgemini

Red Teaming
G-Cloud 15

Table of Contents

1 Service Overview

The Red Teaming Cloud Service by Capgemini is crafted to replicate the strategies of advanced cyber attackers. Unlike conventional penetration testing, this service offers an aggressive, multi-layered attack simulation, targeting both digital and physical aspects of your organisation's security. Emphasizing real-world attack scenarios, our team assesses the resilience of your cloud infrastructure, applications, and human factors against sophisticated threats.

2 Business Need

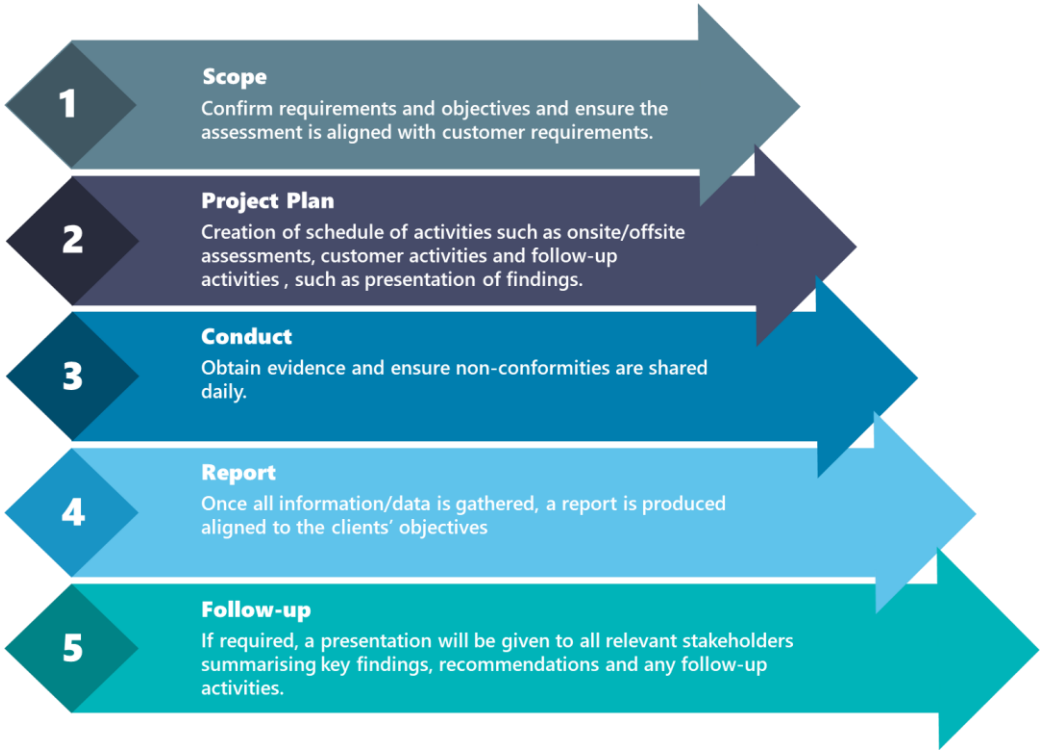
In today's digital landscape, where threat actors continually evolve their methods, the limitations of conventional security strategies are increasingly apparent. Capgemini's Red Teaming Service fills this void by offering an in-depth evaluation of your organisation's readiness against sophisticated cyber threats. This goes beyond standard security checks to test your team's detection and response mechanisms under real attack conditions. Such an assessment is vital for any organisation aiming to protect their assets and maintain operational resilience against external threats.

3 Our Approach

Capgemini’s Red Teaming methodology is a structured, strategic process beginning with a clear definition of objectives to align the exercise with an organisation's specific risk profile. Advanced reconnaissance is undertaken to uncover exploitable vulnerabilities, simulating the initial phases of a cyber-attack. Our team then progresses to the execution phase, actively exploiting these vulnerabilities to gauge the effectiveness of your security measures.

The engagement concludes in a thorough debriefing, providing a detailed analysis of our findings and actionable recommendations for strengthening your defences. This end-to-end approach ensures not only a comprehensive assessment of your current security posture but also a roadmap for continuous improvement.

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 Red Teaming 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
  - Verbal summary of the days finding with the primary contacts only 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

Features and Benefits

Red Teaming simulates 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 organisations to tailortesting to the risks they face. Meeting with business stakeholders to identify objectives for testing and to determine the threat profile of likely attackers. We use this to distinguish specific attack vectors commonly associated with the business and methods noted to be successful in the real world, by real attackers.

- Cloud Platform Attacks
- External Infrastructure (VPNs, remote work solutions)
- Internal Infrastructure Penetration Testing
- Wireless Infrastructure Exploitation
- Web / Mobile Application Exploits (leading to internal / cloud platform attacks)

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 testers will set out and agree scenarios from digital 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 keep organisations informed without inadvertently alerting an organisations internal defender team.

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

4 Buyer Responsibilities

All buyer responsibilities are identified on scope 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 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 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 for customers. Capgemini is an NCSC-approved company. Capgemini and its CHECK Team statuses are listed on the NCSC website for validation purposes.

Capgemini 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
- Sub-contractors

Not applicable.

10 Business Continuity and Disaster Recovery

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

11 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.

12 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.

13 Termination Terms

Please refer to the Supplier Terms for this service.

14 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