G-Cloud 15 Service Description

Offensive Security Service

January 2026

CONTENTS

1 SERVICE OVERVIEW

1.1 Service Summary

The CYPFER Offensive Security service offers a comprehensive suite of capabilities that are tailored to identify vulnerabilities, assess system defences, and enhance the overall security posture of your Cloud infrastructure.

In today's rapidly evolving digital landscape, safeguarding your organization's assets against cyber threats is paramount. Traditional defensive measures are not enough, and so proactive offensive security testing is essential to uncover vulnerabilities before malicious actors exploit them.

1.2 Key Features

The key features of the CYPFER Offensive Security service are:

- Vulnerability Assessment leveraging industry-leading automated scanning tools
- Detection of missing security patches, misconfigurations and outdated software
- Automated and manual Penetration Testing from certified offensive security experts
- Detection Capability Assessment (DCA) of SIEM security monitoring capabilities
- DCA Endpoint Detection and Response (EDR), Intrusion Detection Systems (IDS/IPS)
- Red Teaming engagements in a stealthy, multi-phase operation
- External intelligence capture of employee, infrastructure and supply-chain weakness
- Phishing and social engineering campaigns to assess employee security awareness
- Internal network exploitation to evaluate detection and response to threats
- Purple teaming to collaborate with the defensive (Blue) team

1.3 Key Benefits

The key benefits of the CYPFER Offensive Security service are:

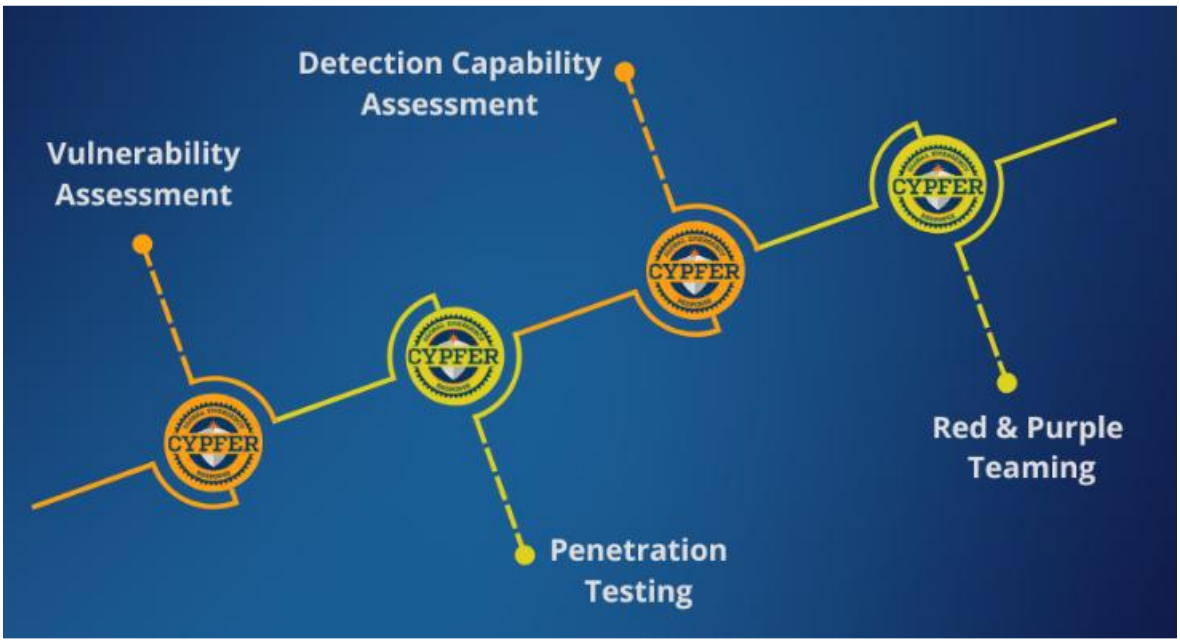
- Uncover, validate, and exploit potential weaknesses in your network
- Identify and prioritize vulnerabilities within your IT infrastructure
- Simulate real-world attacks to evaluate security of systems and applications
- Demonstrate potential real-world impacts under controlled conditions
- Evaluate effectiveness of organisation security controls against cyber threats

- Emulate sophisticated threat actors to test detection and response capabilities
- Improve sharing of insights on tactics, techniques, and procedures (TTPs)
- Foster collaboration between offensive and defensive teams

2 SERVICE DESCRIPTION

2.1 Service Outline

CYPFER offers a comprehensive suite of offensive security services tailored to identify vulnerabilities, assess system defences, and enhance your overall security posture.



This is achieved by the provision by CYPFER of:

- **Industry Expertise:** Our team comprises seasoned cybersecurity professionals with backgrounds in ethical hacking, incident response, and red teaming
- **Comprehensive Approach:** We offer a full spectrum of services, from foundational vulnerability assessments to advanced adversarial attack simulations
- **Tailored Solutions:** Our assessments are customized to meet the unique needs and risk profiles of your organization, whether you are a startup or a Fortune 500 enterprise
- **Actionable Insights:** We provide clear, prioritized recommendations and technical guidance to ensure you can effectively mitigate identified risks
- **Regulatory Compliance Support:** Our services align with industry regulations and best practices, helping organizations maintain compliance with standards such as NIST, GDPR, PCI DSS, ISO 27001, and more