PURECYBER

G-Cloud 14 - Service Definition Document

Table of Contents

About Us

Founded in 2012, now with a global footprint, PureCyber is an award-winning Cyber Security consultancy making cyber security accessible, understandable, and affordable for any organisation.

Recently named "Most Innovative Cyber Security Company in the UK", "Best International Cyber Security Consultancy Firm in the UK" and the highest placed cyber security organisation within the WalesTech50, the team at PureCyber are specialist security experts with a vast knowledge of the latest trends, technologies, and attack vectors. PureCyber is ISO27001:2013 and ISO9001:2015 certified allowing the provision of cyber security consultancy services to private and public sector clients worldwide.

Acting as a dedicated hybrid team for your business, PureCyber provides support to organisations of all sizes and sectors, developing innovative state of the art services to stay one step ahead of the ever-increasing cyber security threat, protecting processes and data from internal and external cyber security risks.

Offering individual services or the highly regarded Total and Core monthly subscription packages, PureCyber ensures clients are wrapped in a suite of affordable and accessible services to meet their specific needs.

PureCyber is not a solutions provider and as such do not sell hardware/software or provide IT consultancy services, this means they are the perfect trusted partner to advise clients on what is needed for them to become more secure.

With an established reputation for putting the true needs of the customer first, PureCyber prides itself on building a strong relationship of trust and offering highly valued appropriate services and advice to all clients.

Service Document Overview

This document provides a full explanation of the services that PureCyber are providing through G-Cloud and the Digital Framework.

Our approach is simplistic, allowing buyers to match the solutions and price, according to their requirements within the Digital Marketplace.

For every service and engagement, PureCyber will work with the client to produce a scoping document and then provide a complete, and reasonable, statement of work for the required project. All charges are exclusive of VAT and based on PureCyber's terms and conditions.

Penetration Testing

A penetration test or pen test is an exercise where an ethical hacker will try to compromise an organisation (or asset) to identify existing security vulnerabilities for the client. In essence, a penetration test is an authorised simulated cyberattack on a computer system. It is important not to be confused with a vulnerability assessment. When a penetration test is conducted, customers are provided with a precise demonstration of what a hacker would do to their business or asset.

PureCyber provides CREST-certified penetration testing services across multiple penetration testing applications, infrastructures and environments. Our CREST and Offensive Security accredited team use a mixture of automated and manual techniques, to discover all vulnerabilities within the scope.

With years of experience in this scope of work, PureCyber follows a methodology to penetration testing that adheres to industry best practice and is split into several key phases; pre-engagement, intelligence gathering, vulnerability analysis, infrastructure exploitation, application testing, reporting, and deliverables.

On completion, you will be provided with a full, detailed, and understandable report stating all the vulnerabilities that have been identified and their required remediation.

Web Application Penetration Testing

This test aims to identify security vulnerabilities resulting from insecure development practices in the design, coding and publishing of software or a website. Web application penetration testing is a context-based review of the asset to identify and exploit a range of OWASP related issues.

Infrastructure Penetration Testing

The goal is to identify and expose vulnerabilities across an entire network or smaller scope. This type of testing can also be applied to cloud infrastructure, such as AWS, Azure and Microsoft 365.

Mobile Application Penetration Testing

Similar to web application testing, mobile application testing is used to ensure that vulnerabilities are identified and remediated across both iOS and Android mobile applications.

API Penetration Testing

An Application Programming Interface or API is a software component that enables different systems/applications to interact with each other.

Wireless Penetration Testing

Wireless penetration testing involves testing the connections between all devices connected to an organisation's Wi-Fi or wireless network.

Red Teaming Penetration Testing

Red Teaming is a covert engagement designed to identify weaknesses in your cyber preventative controls and staff security awareness. Typically, this involves pretending to be an external attacker, gathering as much open-source intelligence to build a picture of the organisation, and then trying to exploit these by using multiple cyber-attack methods.

SIEM / Purple Team Penetration Testing

This type of testing involves combining both red and blue team activities so that the defensive side of your security team can analyse a simulated attack to identify any potential weaknesses within your current cyber security strategy and SIEM configurations. This type of penetration test allows your internal security team to identify opportunities for improvement within your blue team's training, defensive configurations, technologies utilised and processes.

Device Build, Configuration and Hardening Security Review

A device build and hardening security review allows an organisation to analyse the configuration of all end-user devices, servers and infrastructure to ensure they are protected against a range of cyber security attacks. This typically involves reviewing firewall

rules, assessing anti-virus capabilities as well as potential privilege escalation opportunities an attacker could take if they gained unauthorised access to your internal network.

Active Directory Security Assessment

An active directory security assessment allows an organisation to ensure that all of the technical controls within this system match corporate policies and the wider cyber security strategy of the business. This allows you to assess if user permissions, passwords and accounts are assigned appropriately and configured securely.

Vulnerability Scanning

Vulnerability scanning is completed by a highly specialised software tool that interrogates IT systems to collect data which is then compared to a database of known flaws or vulnerabilities.

Managed vulnerability scanning is a fundamental component of any security testing programme for identifying existing or new vulnerabilities and misconfigurations across your systems. Failing to understand and remediate the vulnerabilities you have within your environment could present an attacker the opportunity they need to gain access to your systems.

Not only does our managed vulnerability scanning service identify the threats your network faces internally it also can look outside and view your system as an external attacker would, highlighting actions that need to be taken to protect your systems.

There are many benefits of having vulnerability management capability in place to help protect your environment and provide a proactive stance against threats to your organisation:

- Improved security and control
- Fast identification of vulnerabilities before external threats can take advantage of them
- Continuous threat visibility and reporting across your environment – all the time
- Eliminate blind spots across your environment
- Contributes to meeting compliance, governance, and data protection requirements
- Operational efficiencies – scanning is repeatable, automated, and efficient meaning you get repeatable results
- Vulnerability prioritisation – know what to remediate first
- Patch management – vulnerability scanning can enhance and evolve your existing patch management program

Internal Vulnerability Scanning

Vulnerability scanning is the examination of an organisation's networks and the devices that use them, such as workstations, servers and printers. The purpose is to identify security weaknesses that can leave an organisation exposed and vulnerable to a cyber-threat.

External Vulnerability Scanning

Some of the devices on your network are accessible through the public internet, introducing vulnerabilities that can allow a cyber-criminal to view parts of your network from anywhere in the world and even gain access to your most important data.

Security Operations Centre

PureCyber Cyber provide a managed Security Operations Centre to companies that don't have an internal function. By monitoring networks, infrastructures and critical services, PureCyber can protect your organisation from multiple cyber security threats and attacks. By monitoring our Security Information & Event Management system in real-time we can quickly identify potential threats and liaise with your internal team to limit potential cyber security attacks against your organisation.

What is a SIEM?

Security Information & Event Management (SIEM) is a platform that provides real-time analysis of security alerts and improves threat detection and response capabilities. For optimal minimization of risk, the SIEM software integrates and combines host-based and network-based security event data and log files into one overview by a powerful correlation engine. It finds weak spots in your infrastructure and detects anomalies on your network so that threats can be prevented or mitigated.

What is a SOC?

Our Security Operations Centre (SOC) consists of a team that monitors networks and systems 24/7 that show your security status, vulnerabilities, intrusions, or anomalous activity. When an incident is detected, the team immediately gives actionable advice to your IT staff, which ensures the quickest response times to mitigate threats.

Managed SIEM deployment and SOC monitoring

PureCyber's managed SIEM solution is deployed via both agent and sensor. The agent is installed to collect vital security detail of devices no matter where they are and provides data such as vulnerabilities, file integrity and security incidents. While the sensor is deployed onto the network to monitor activity at a packet level.

Cloud services such as AWS, Azure and Microsoft 365 are monitored at an API level and fed directly into the SIEM, while instances can also have an additional level of monitoring using the agent deployment as well.

Managed SIEM Capabilities

Syslog monitoring

Syslog is a network-based logging standard used for applications and network devices to send data to a central server, providing information on events, statuses, diagnostics, and more. This powerful tool can be used to manage complex networks with large volumes of data in need of a centralized monitoring solution.

Network Metadata

Unlike signature-based intrusion detection which looks for specific needles in the haystack of data, network metadata provides you with logs of connections and standard protocols like DNS, HTTP, FTP, SMTP, SSH, and SSL. This provides a real depth and visibility into the context of data and events on your network.

Full Packet Capture

Full packet capture is like a video camera for your network, but better because not only can it tell us who came and went, but also exactly where they went and what they brought or took with them (exploit payloads, phishing emails, file exfiltration). There is certainly valuable evidence to be found but evidence at the host can be destroyed or manipulated; the camera doesn't lie, is hard to deceive, and can capture a bullet in transit.

Security Analytics

Security Analytics is an approach to cybersecurity focused on the analysis of data to produce proactive security measures. For example, monitored network traffic could be used to identify indicators of compromise before an actual threat occurs. The agent is used to collect, aggregate, index and analyse security data, helping to detect intrusions, threats, and behavioural anomalies.

As cyber threats are becoming more sophisticated, real-time monitoring and security analysis are needed for fast threat detection and remediation. That is why our lightweight agent provides the necessary monitoring and response capabilities, while our server component provides the security intelligence and performs data analysis.

Intrusion Detection

An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system. The agents scan the monitored systems looking for malware, rootkits and suspicious anomalies. They can detect hidden files, cloaked processes, or unregistered network listeners, as well as inconsistencies in system call responses.

Our solution generates NIDS (Network Intrusion Detection System) alerts by monitoring your network traffic and looking for specific fingerprints and identifiers that match known malicious, anomalous, or otherwise suspicious traffic. This is signature-based detection so you might say that it's similar to antivirus signatures for the network, but it's a bit deeper and more flexible than that.

In addition to agent capabilities, the server component uses a signature-based approach to intrusion detection, using its regular expression engine to analyse collected log data and look for indicators of compromise.

Log Data Analysis

The agents read operating system and application logs and securely forward them to a central manager for rule-based analysis and storage. The rules help make you aware of application or system errors, misconfigurations, attempted and/or successful malicious activities, policy violations and a variety of other security and operational issues.

Our system is also able to ingest logs from agentless devices such as routers, firewalls, all of which can be analysed on the single pane dashboard.

File Integrity Monitoring

File integrity monitoring (FIM) refers to an IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted. FIM, which is a type of change auditing, verifies and validates these files by comparing the latest versions of them to a known, trusted "baseline."

If FIM detects files have been altered, updated, or compromised, FIM can generate alerts to ensure further investigation, and if necessary, remediation, takes place. File integrity monitoring encompasses both reactive (forensic) auditing as well as proactive, rules-based active monitoring.

Each agent monitors the file system, identifying changes in content, permissions, ownership, and attributes of files that you need to keep an eye on. In addition, it natively identifies users and applications used to create or modify files.

File integrity monitoring capabilities can be used in combination with threat intelligence to identify threats or compromised hosts. In addition, several regulatory compliance standards, such as PCI DSS, require it.

Vulnerability Detection

The agents pull software inventory data and send this information to the server, where it is correlated with continuously updated CVE (Common Vulnerabilities and Exposure) databases, to identify well-known vulnerable software.

Automated vulnerability assessment helps you find the weak spots in your critical assets and take corrective action before attackers exploit them to sabotage your business or steal confidential data.

Mitre Framework

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Configuration Assessment

Our system monitor system and application configuration settings to ensure they are compliant with your security policies, standards and/or hardening guides. Agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or insecurely configured.

Additionally, configuration checks can be customised, tailoring them to properly align with your organisation. Alerts include recommendations for better configuration, references, and mapping with regulatory compliance.

Regulatory Compliance

Our system provides some of the necessary security controls to become compliant with industry standards and regulations. These features, combined with its scalability and multi-platform support help organisations meet technical compliance requirements.

The system can be used by payment processing companies and financial institutions to meet PCI DSS (Payment Card Industry Data Security Standard) requirements. Its web user interface provides reports and dashboards that can help with this and other regulations (e.g., GPG13 or GDPR).

Cloud Security

Our system helps monitoring cloud infrastructure at an API level, using integration modules that can pull security data from well-known cloud providers, such as Amazon AWS, Azure or Google Cloud. In addition, the system provides rules to assess the configuration of your cloud environment, easily spotting weaknesses.

In addition, the lightweight and multi-platform agents are commonly used to monitor cloud environments at the instance level

Information Security Governance

PureCyber is an IASME-accredited Cyber Essentials and Cyber Essentials Plus certification body. Our team can provide consultancy services to prepare the organisation for Cyber Essentials and Cyber Essentials Plus accreditation and as a certified governing body for the accreditation, we are also able to help administer, manage and renew licenses for this government standard.

Cyber Essentials

For the Cyber Essentials Standard certification process, PureCyber offers three services for customers; dependent on their organisation's needs and requirements.

Self-Assessment

The self-assessment is the most minimal service and allows PureCyber to provide the certification once your organisation has completed the Cyber Essentials assessment process. PureCyber is the accreditation body therefore if you are looking for additional guidance on setting up a security strategy our other packages may be more suitable.

Managed Service

For this service, PureCyber will issue the Cyber Essentials certification once organisations have met the criteria needed however, they will also offer advice and guidance throughout the process; helping companies to establish a strong security strategy that is aligning with the Cyber Essentials programme.

Onsite Service

The onsite service delivers the same level of consultancy as the managed service, however, will be priced differently if consultants are required on site.

Cyber Essentials Plus

To achieve Cyber Essentials Plus, the assessment must be completed by a certified Cyber Essentials governing body; therefore there is no option available for self-assessment.

Most certification bodies will often have to visit the organisation to carry out the required tests for Plus, but PureCyber has developed our black box technology that allows us to remotely test the organisation's network. This provides a quick and extremely convenient way to test and retest the applicants' networks at a time that suits them.

Remote Service

The testing of the five key security controls within the Cyber Essentials Plus programme can be completed remotely (with access authorised for PureCyber) and therefore is the preferable option as it is typically cheaper for the organisation.

Onsite Service

If remote testing is not possible or available due to the scope of work, then onsite testing will be available for all customers but will be more expensive than the remote service.

IASME Governance

For the IASME Governance self-assessment certification process, PureCyber offers three services for customers; dependent on their organisation's needs and requirements.

Self-Assessment

The self-assessment is the most minimal service and allows PureCyber to provide the certification once your organisation has completed the IASME Governance self-assessment process. PureCyber is the accreditation body therefore if you are looking for additional guidance on setting up a security strategy our other packages may be more suitable.

Managed Service

For this service, PureCyber will issue the IASME Governance self-assessment certification once organisations have met the criteria needed however, they will also offer advice and guidance throughout the process; helping companies to establish a strong security strategy that is aligning with the IASME Governance programme.

Onsite Service

The onsite service delivers the same level of consultancy as the managed service, however, will be priced differently if consultants are required on site.

IASME Governance Audited

To achieve IASME Governance Audited, the assessment must be completed by a certified IASME governing body; therefore, there is no option available for self-assessment.

Remote Service

The auditing of the IASME Governance self-assessment answers can be completed remotely by our PureCyber assessors and therefore is the preferable option as it is typically cheaper for the organisation.

Onsite Service

If remote auditing is not possible or available due to the scope of work, then onsite testing will be available for all customers but will be more expensive than the remote service.

Information Assurance Consultancy

At PureCyber, our consultants have experience across multiple cyber security frameworks. As an IASME Gold certified and Cyber Essentials / Cyber Essentials Plus certification body, as well as having achieved ISO27001:2013 as a consultancy, we have a good level of experience across multiple information security governance standards.

We have assisted many organisations in achieving compliance with ISO27001, IASME, PCI-DSS, NIST, FISMA, SOC and GDPR.

ISO27001 Consultancy Services

PureCyber employs experienced ISO27001 Lead Auditors who can help you through the process of achieving your own ISO27001 compliance. These projects are set against achievable milestones and work in tandem with your standard business responsibilities so that the company, or individual department, is not overwhelmed with strict deadlines.

PureCyber breaks this consultancy service into several key stages including the initial scoping of your ISMS processes/strategy, gap analysis, ISMS development, remediation guidance and maintenance. Working as an extension of your internal governance departments, PureCyber aims to operate as a strategic partner, helping to achieve your compliance requirements and shaping your compliance programme.

Cyber Security Audit

The goal of the audit is to provide an overview of the organisation's current security posture. It is an objective review of existing plans, technical capabilities, and a guide to strategic planning. The goal of the audit is to provide the organisation with a clear tactical and strategic direction to further mature and strengthen its cyber defences.

The process

Working with the organisation the process is a mixture of technical (penetration tests, phishing simulations, vulnerability scans etc) and a governance audit that is conducted as a combination of interviews, workshops, policy, and process reviews. The audit can take between 4 – 12 weeks to complete and is dependent on the size and complexity of the organisation.

Technical review

The technology an organisation uses to function can be split into two areas, the first being the technology used for day-to-day user activities such as workstations, printers, and servers. While the second is the technology used to protect them, firewalls, antivirus etc. These provide layers of defence but, any misconfiguration or error in any layer can expose those below to attack.

As a simplistic example, a firewall which is used to secure an organisation's internet access is misconfigured, this could allow an external attacker in another building or even another country to gain access to the servers, workstations and thus the data without anyone noticing.

The purpose of the technical review is to evaluate each layer to ensure they are configured correctly, functioning as expected and do not create an open window into the organisation's defences.

Governance review

Governance is an often overlooked but vital element of a strong cyber defence, it describes the policies, procedures and processes that determine how an organisation

detects, prevents, and responds to cyber events. The cyber audit examines the organisations existing systems and scores them against current industry standards.

Deliverables

Once the technical and governance reviews are completed several reports will be created, each reflecting the findings of each exercise. This information will be summarised in an executive report that will analyse the findings highlighting key tactical and strategic recommendations that align the organisation to industry standards.

What's included in a standard Cyber Audit:

- Full external vulnerability scan
- Full internal vulnerability scan
- Real-world phishing attack simulation
- Dark web audit
- Penetration test of 'most important' assets
- Governance policy review
- Governance interviews

Phishing Simulation

Cyber-attacks are increasingly being launched through phishing campaigns, where users are manipulated into opening a document or clicking a malicious link. The goal of this attack is to obtain credentials or implant malware that gives the criminals a hook into the network.

PureCyber's phishing simulation allows organisations to create bespoke campaigns, designed to be as close as possible to a real attack. Based on the results of the test, we can offer further guidance including user awareness training seminars and additional simulations.

PureCyber offers comprehensive phishing training and engagement materials to provide the reinforcement and remediation suited to your organisation needs. Make employees aware of the methods cyber-attackers use to get information. Through tiered link or attachment-based, data entry, or reply-to phishing simulations, your employees will be able to identify, report, and prevent phishing attacks.

Identifying which users are susceptible to phishing emails is an excellent indicator of the level of threat your company faces from the most prevalent form of cyber-attack.

PureCyber will run bespoke and relevant simulations to fully test your users. This gives you a true reflection of the effects of phishing on your organisation, unlike templated off-the-shelf phishing simulations. On average, 14% of users click on links during these exercises, demonstrating just how effective these attacks are.

Ransomware Consultancy and Training Services

Preparing for Ransomware

The Ransomware Defence Assessment was developed based on extensive experience responding to ransomware incidents and gathering threat intelligence on emerging ransomware.

The PureCyber Ransomware Defence Assessment evaluates the effectiveness of an organisation's ability to prevent, detect, contain and remediate a ransomware attack. Our experts assess technical and non-technical elements of your security playbook to determine how your team will respond to a ransomware attack.

Our experts evaluate the technical impact a ransomware attack could have on your internal network, discover what data could be jeopardized or lost and test the strengths and weaknesses of your security controls' ability to detect and respond to a ransomware attack. Within our preparation consultancy services, we provide companies with Phishing simulation exercises, awareness training, process evaluations, and roadmaps to help organisations improve their defence systems.

Ransomware Recovery

PureCyber realises that sometimes it's too late to prepare. As an experienced consultancy, we can offer reactive services to help you respond to an attack, and navigate your way out with as little impact as possible.

We can work with your organisation to conduct forensics, assess the encrypted files/data, analyse specific Malware, conduct negotiations, dark web monitoring, provide incident reports, produce impact evaluations and create a strategy to get your organisation back on track.

Cyber Security Subscription Packages

Managed Cyber Security Services (Core)

A well-protected business has the potential to be confident and the most innovative. The smartest businesses don't just manage cyber risk, they use it as a source of growth and market edge. Technology makes many things possible, but possible doesn't always mean safe. As cyber threats grow in volume and sophistication and technology becomes essential for meeting the needs of your customers, employees, suppliers and society, your cyber security must build resilience and trust.

PureCyber helps you create a resilient and trusted digital world – even in the face of evolving threats. That's because we bring a combination of technological expertise, deep business knowledge, and creative professionals who are passionate about protecting and building your business. Together, let's create a trusted digital world, so you can push the limits of what's possible.

The Core subscription includes everything needed to ensure they are best placed to defend against and survive a cyber event. The standard package includes:

- Monthly internal & external vulnerability scans
- An annual full Cyber Audit
- Annual penetration testing
- Endpoint detection and response
- Awareness training
- Cyber essentials certifications
- Governance
- Phishing tests
- Dark web monitoring

Organisations face increasing pressures when it comes to security and compliance. Whether that be protecting their important assets or ensuring that they are compliant with standards and regulations. It can be costly to have a full-time Information Security Officer to manage these challenges.

The challenge an organisation faces to create a complete internal cyber-service can be unwieldy, the cost of finding the appropriate team, purchasing the tools, and training they require can be incredibly costly. Our hybrid service fills in the gaps that the organisation either does not have the capability or resources to provide.

PureCyber's hybrid service provides an organisation with expert on-call security guidance and assistance when needed. With a global footprint and a highly regarded team of experienced security experts that are available on demand.

Our team offers direction and services from penetration testing right through to security awareness programmes. We have the expertise to ensure that the organisation's security challenges are met whatever they may be.

The complexity of addressing cyber security-related issues, such as staying on top of vulnerabilities, identifying, and responding to threats, and meeting compliance requirements, means that a greater number of organisations are choosing to outsource security requirements.

Key reasons to outsource cyber security include

- Reduced strain on in-house teams
- More affordable security compared with in-house investment
- Access to a broader range of skills and experience
- Greater value from detection technology
- Greater flexibility

PureCyber helps the organisation understand the threats they face and support them through the journey of improvement.

PureCyber assist with:

- Impartial advice regarding process and technology
- Monthly, quarterly, annual meetings to discuss cyber issues
- Support your organisation's teams
- Provide incident response and forensic support in case of misuse or breach.

Managed Cyber Security Services (Total)

Following on from the success of our Total subscription, PureCyber has created a higher level of subscription package for companies who are looking to outsource their cyber security capabilities.

The Total subscription package includes everything within the Core package, with the addition of a managed SIEM solution operating out of our Security Operations Centre.

The Total package includes the following services;

- Monthly internal & external vulnerability scans
- An annual full Cyber Audit
- Annual penetration testing
- Endpoint detection and response
- Awareness training
- Cyber essentials certifications
- Governance
- Phishing tests
- Dark web monitoring
- Managed SIEM solution through our SOC-as-a-Service functionality.

PureCyber's hybrid service provides an organisation with expert on-call security guidance and assistance when needed. With a global footprint and a highly regarded team of experienced security experts that are available on demand. With the addition of our SOC-as-a-Service in the Total subscription package, organisations can be confident that a team of PureCyber analysts are monitoring their endpoints to be the quick detection they need to identify, and help to mitigate, a potential cyber security attack.

Contact Us

info@purecyber.com
@PureCyberLtd
purecyber.com