PURECYBER

Service Definition Document

GCloud 15

STRENGTHENING YOUR **CYBER RESILIENCE**

PureCyber Ltd 2026

www.purecyber.com

Table of Contents

About PureCyber

Founded in 2016, PureCyber is an award-winning cyber security company with a mission to make cyber security accessible, understandable, and affordable for organisations of all sizes. We offer a comprehensive, subscription-based service that combines Defensive Security, Offensive Security, and Governance & Compliance. Our all-in-one solution delivers 24/7 protection, proactive threat intelligence, expert consultancy, and real-world attack simulations, simplifying cyber security and eliminating the complexity of managing multiple vendors.

PureCyber has earned industry recognition for its commitment to excellence, being named "Most Innovative Cyber Security Company in the UK" for three consecutive years and ranking as the highest-placed cyber security organisation in the 2024 UK Fast Growth Index. We pride ourselves on our ability to stay ahead of emerging threats, providing clients with cutting-edge solutions to safeguard their operations.

We work with a diverse range of organisations, including universities, colleges, multi-academy trusts, sports organisations, legal firms, financial institutions, and some of the world's largest manufacturing businesses.

Our tailored cyber security solutions are designed to protect data, systems, and processes from evolving cyber risks, ensuring our clients can focus on their core operations with confidence. As a trusted partner, we are dedicated to keeping our clients secure and one step ahead of cyber threats.

ACCREDITED BY

CREST Penetration Testing · CREST Security Operations Centre · CREST Incident Exercising · Cyber Essentials · Cyber Essentials Plus · IASME Cyber Assurance · National Cyber Security Centre · OffSec · CISSP Certified Information Systems Security Professional · HM Government G-Cloud Supplier · Crown Commercial Service Supplier

Service Definition Document

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 Services

Penetration Testing, sometimes referred to as 'pen testing' or 'ethical hacking', is a simulated cyber-attack that aims to identify security vulnerabilities or misconfigurations before they can be exploited by cyber criminals.

PureCyber's CREST-certified penetration testing team consist of Cyber Scheme Team Members, Cyber Scheme Team Leaders and Offensive Security consultants. PureCyber is your trusted cyber security partner to deliver comprehensive network, software, web application & cloud penetration testing.

Using the same tools and techniques as attackers, but in an authorised, controlled environment, Penetration testing can be carried out on an entire organisation, specific computer systems, networks, and applications. It is a proactive approach to uncovering vulnerabilities within your systems and networks before malicious actors can exploit them. Our CREST-certified penetration testing services simulate real-world cyber-attacks, helping you identify weaknesses and strengthen your defences.

We offer the following types of penetration testing:

External Network Penetration Testing:

Simulates attacks from outside your network to identify vulnerabilities in externally-facing assets such as websites, email servers, and public-facing devices.

Internal Network Penetration Testing:

Mimics attacks from within your organisation, identifying weaknesses like unpatched systems or misconfigured devices.

Web Application Testing:

Assesses your web applications to identify vulnerabilities like SQL injection, cross-site scripting (XSS), and insecure session management.

Mobile Application Testing:

Evaluates the security of your mobile apps, uncovering vulnerabilities such as poor encryption practices and improper API usage.

Wireless Network Penetration Testing:

Tests your wireless network security, looking for weaknesses such as rogue access points and weak encryption.

Cloud Security Testing:

Evaluates your cloud infrastructure for misconfigurations, improper permissions, and other vulnerabilities.

IoT (Internet of Things) Security Testing:

Assesses the security of IoT devices to ensure they don't serve as entry points for attackers.

API Security Testing:

Identifies weaknesses in your APIs, such as authentication issues or improper access controls.

Deliverables

- A detailed report with identified vulnerabilities, their risk levels, and remediation recommendations.
- An executive summary with key findings for non-technical stakeholders.
- Re-test services to ensure the effectiveness of remediation efforts.

Why Choose PureCyber Penetration Testing?

- **CREST Certified:** We adhere to the highest industry standards in penetration testing, ensuring quality and professionalism.
- **Proven Expertise:** Our team consists of highly skilled professionals with certifications in ethical hacking, cybersecurity, and threat simulation.
- **Tailored Solutions:** We customise our services to meet the specific needs of your organisation, ensuring relevant and impactful results.
- **Cutting-Edge Tools:** We use a combination of manual testing and automated tools to ensure comprehensive coverage of potential vulnerabilities.
- **Actionable Insights:** Our reports provide clear, actionable recommendations to strengthen your security posture.

Red Teaming

Red teaming goes beyond traditional penetration testing by simulating sophisticated, multi-stage attacks targeting your organisation's systems, people, and processes. Our red team engagements test the resilience of your security measures and evaluate your ability to detect, respond to, and recover from complex threats.

Key services in red teaming include:

Advanced Social Engineering:
Simulates phishing, spear-phishing, vishing, and physical intrusion attempts to assess your employees' susceptibility to social engineering attacks.

Physical Security Testing:
Tests the physical security of your premises, attempting to bypass access controls or steal sensitive materials to identify weaknesses in physical security policies.

Multi-Vector Attack Simulation:
Simulates a real-world attack incorporating various techniques, including phishing, exploiting vulnerabilities, social engineering, and physical access breaches.

Targeted Threat Simulations:
Replicates the tactics of advanced persistent threats (APT), hacktivists, or nation-state actors to test your security readiness against specific adversary profiles.

SOC (Security Operations Centre) Assessment:
Evaluates your SOC's ability to detect, respond to, and escalate incidents in real-time.

Deliverables

- A detailed report with identified vulnerabilities, their risk levels, and remediation recommendations.
- An executive summary with key findings for non-technical stakeholders.
- Re-test services to ensure the effectiveness of remediation efforts.

Why Choose PureCyber Red Teaming?

- **CREST Certified:** We adhere to the highest industry standards in penetration testing, ensuring quality and professionalism.
- **Proven Expertise:** Our team consists of highly skilled professionals with certifications in ethical hacking, cybersecurity, and threat simulation.
- **Tailored Solutions:** We customise our services to meet the specific needs of your organisation, ensuring relevant and impactful results
- **Cutting-Edge Tools:** We use a combination of manual testing and automated tools to ensure comprehensive coverage of potential vulnerabilities.
- **Actionable Insights:** Our reports provide clear, actionable recommendations to strengthen your security posture.

Managed Extended Detection Response (MXDR)

The PureCyber MXDR provides comprehensive, proactive cyber threat detection, investigation, and response. The service enables organisations of every size and sector to strengthen their resilience against constantly evolving cyber risks.

At the core of the service is a CREST-certified, UK-based, 24/7 Security Operations Centre (SOC). Unlike many global providers that outsource or automate critical functions, PureCyber's SOC operates exclusively from the UK. Every security event is handled by trusted cyber security professionals. Our analysts are trained to industry-recognised standards and bring contextual understanding of UK regulatory frameworks, compliance requirements, and threat landscapes.

PureCyber MXDR combines advanced technology, automation, and artificial intelligence with the essential layer of human expertise and evaluation. This hybrid approach ensures rapid, accurate, and contextual response to threats, minimising false positives and delivering actionable intelligence that supports both IT and business decision-making.

The service integrates seamlessly with existing technology investments, avoiding the need for costly or disruptive platform replacements. PureCyber MXDR enhances rather than replaces your current infrastructure and adapts to your operational needs. To provide complete assurance, all MXDR clients benefit from our Unlimited Incident Response Guarantee, giving peace of mind that if a serious incident occurs, our expert responders will act immediately and without limitation.

A Unified, Proactive Defence Model

Traditional cyber security tools are reactive, detecting issues only after they have occurred. PureCyber MXDR takes a different approach. It combines machine-speed detection and response with continuous human-led threat hunting and validation, providing end-to-end visibility and control across:

- Endpoints, servers, and mobile devices
- Cloud workloads and infrastructure
- SaaS applications and collaboration platforms
- Firewalls, gateways, and network telemetry
- Identity and access management systems

By correlating signals across these domains, MXDR detects complex, multi-vector attacks that span devices, users, and networks. These are the types of attacks that often evade siloed or single-source security tools.

Our behavioural analytics and threat intelligence enable early detection of suspicious activity, while automated playbooks trigger containment actions within seconds. When automation acts, a UK-based analyst always validates and enriches the event to ensure accuracy and relevance.

Key Benefits of PureCyber MXDR

CREST-Certified, UK-Based SOC
At the heart of PureCyber MXDR is a fully CREST-accredited Security Operations Centre operating from the UK. The SOC functions 24 hours a day, 365 days a year, providing constant vigilance from experienced analysts who understand the local and sector-specific threat landscape.

Detection and response are never outsourced. Every alert, escalation, and report is managed by UK-based analysts, maintaining full control over data sovereignty, privacy, and assurance.

True 24/7 "Eyes-On-Screen" Coverage
PureCyber's SOC team provides continuous, human-led monitoring. There are no time-zone gaps or "follow-the-sun" handoffs. Analysts are eyes-on-screen at all times, ready to contain, validate, and communicate incidents as they occur. This ensures that no alert is missed, no detection is delayed, and no response is executed without verification.

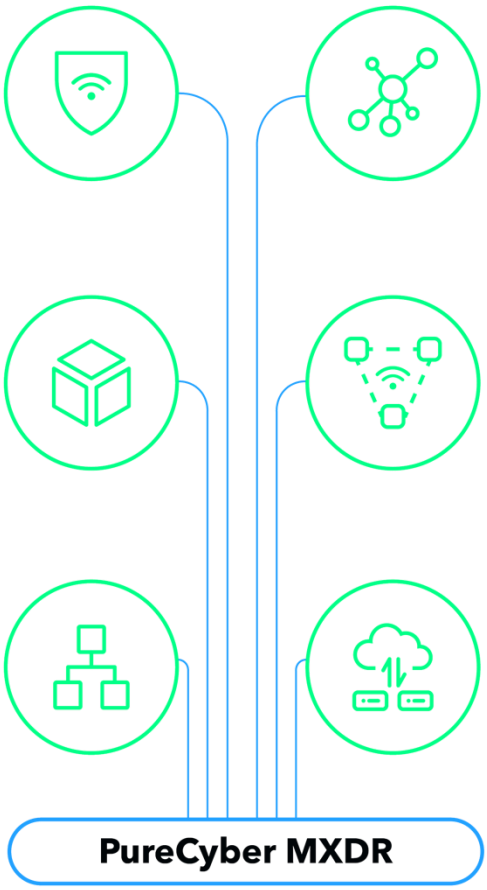
Unlimited Incident Response Guarantee
We are so confident in our ability to detect and respond to threats that we include Unlimited Incident Response as standard with all MXDR services.

If the worst should happen, our incident response team will act immediately to investigate, contain, and recover your environment, without restriction on time or scope. This guarantee gives our clients total peace of mind, knowing that expert responders are on hand around the clock to protect business continuity and minimise impact.

Vendor-Agnostic Flexibility

Many MXDR solutions enforce specific technology stacks or proprietary platforms. PureCyber takes a flexible approach.

Our vendor-agnostic architecture integrates with your existing security tools and infrastructure, providing protection that complements your technology strategy rather than replacing it. This flexibility allows for rapid deployment, reduced disruption, and cost efficiency. Organisations can maintain continuity and gain enhanced analytics, automation, and centralised visibility without the need for wholesale change.



Automation, AI, and Human Context

Automation and artificial intelligence deliver speed and scale, but human judgement adds precision, relevance, and accountability. PureCyber MXDR combines these strengths into a hybrid detection and response model that ensures every action is proportionate and accurate.

- Automation performs data correlation, enrichment, and first-response actions in real time.
- AI-driven analytics detect subtle behavioural anomalies that may indicate insider risk, compromised accounts, or advanced persistent threats.
- Human analysts interpret and validate alerts, adding business and environmental context to ensure responses are aligned with your risk appetite.

This blend of technology and human expertise significantly reduces false positives, enabling IT and security teams to focus on verified, actionable incidents.

Unified Visibility Across All Assets

MXDR consolidates telemetry from across your entire estate into a single, contextual view. This unified visibility provides actionable intelligence across endpoints, cloud workloads, networks, and user accounts.

Through continuous normalisation, enrichment, and correlation, PureCyber MXDR delivers complete situational awareness. This enables rapid identification of lateral movement, privilege escalation, or unusual activity across hybrid and multi-cloud environments.

Compliance-Ready and Audit-Strong

PureCyber MXDR supports compliance and assurance requirements aligned to:

- ISO 27001 – Information Security Management
- Cyber Essentials Plus – Baseline protection and governance
- NCSC CAF – Cyber Assessment Framework for critical infrastructure
- NIST CSF – International best practice alignment
- GDPR and NIS2 – Data protection and network resilience obligations

Detailed audit trails, evidential logs, and investigation reports provide full transparency for internal governance, regulatory review, and board-level reporting.

These outputs can be directly mapped to compliance controls, supporting assurance and reducing internal workload.

Transparent and Predictable Pricing

PureCyber believes that cyber security should be transparent, predictable, and fair. Our pricing model removes hidden costs such as data ingest, storage, or complex licensing uplifts. Clients pay for protection and service outcomes, not for data volume. This approach simplifies procurement, improves cost predictability, and removes financial barriers to achieving full visibility and protection.

Architecture Overview

Data Ingestion and Normalisation

MXDR collects data from multiple data sources, including:

- Endpoints, firewalls, and network sensors
- Cloud platforms and SaaS applications
- Identity and authentication systems
- Email gateways and collaboration tools
- Legacy or bespoke system

All data is normalised and enriched with contextual information such as user identity, device type, business criticality, and geographic location. This ensures that each signal is analysed within the correct business context, improving detection accuracy.

Detection and Correlation Engine

At the core of PureCyber MXDR is a SIEM-XDR correlation engine aligned to the MITRE ATT&CK framework. It performs continuous detection across multiple threat vectors, supported by:

- Cross-source correlation that identifies patterns across devices, users, and networks
- Threat intelligence enrichment that integrates real-world indicators of compromise
- User and Entity Behaviour Analytics (UEBA) that detect anomalies based on behaviour rather than static rules
- Dynamic rule tuning that adapts continuously to your evolving environment and risk profile

This advanced correlation ensures that even complex or low-and-slow attacks are detected early, before they escalate into major incidents.

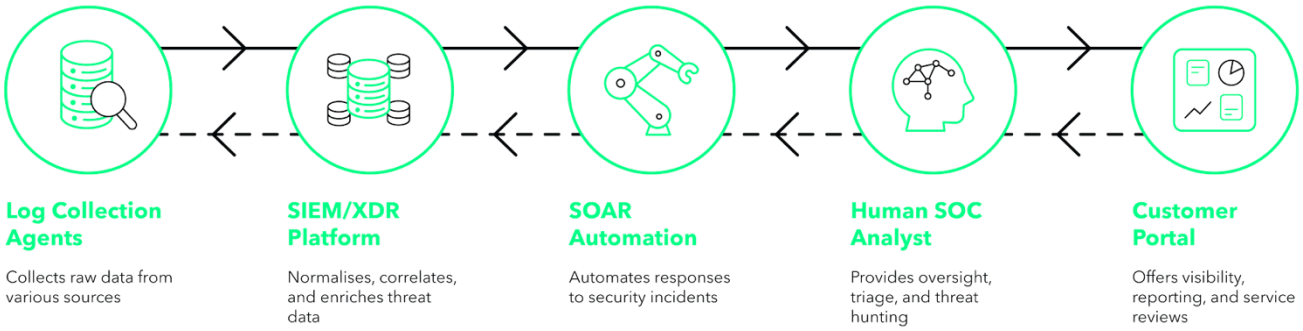
Response Automation and Playbooks

The response automation engine minimises Mean Time to Respond (MTTR) through pre-defined playbooks that trigger containment actions immediately when risk thresholds are met.

Automated actions include:

- Device isolation
- Account suspension
- Domain or IP blocking
- Multi-factor authentication (MFA) enforcement
- Policy reconfiguration

Each playbook includes escalation and approval logic aligned with your organisation's governance model and service levels. Common scenarios such as phishing, credential theft, malware infection, and insider risk are preconfigured for rapid containment.



Example: Credential Compromise

1. Alert received from identity source
2. Login and device fingerprint analysed
3. Account automatically suspended if deviation confirmed
4. Client notified for validation
5. SOC analyst reviews event and provides an incident report

This combination of automation and human validation ensures fast containment without disrupting legitimate users or operations.

What Makes PureCyber MXDR Different?

FEATURE	PURECYBER MXDR	TRADITIONAL MXDR
Vendor-Agnostic	✓ Works with any existing toolset	✗ Locked to proprietary stack
Full SIEM/XDR Correlation	✓ Unified, cross-source visibility	✗ Partial coverage
CREST-Certified, UK-Based SOC	✓ 24/7, in-house "eyes-on-screen"	✗ Offshore or part-time support
Unlimited Incident Response Guarantee	✓ Full response coverage included	✗ Billed separately or capped
Automation + Human Validation	✓ Balanced accuracy and speed	✗ Overreliance on automation
Transparent Pricing	✓ Fixed, predictable costs	✗ Hidden usage or ingest charges

Our MXDR Core Advantages

- **CREST-Certified, UK-Based SOC** – 24/7, never offshored, always eyes-on-screen
- **Unlimited Incident Response Guarantee** – Included as standard for complete peace of mind
- **Co-Managed Flexibility** – Retain as much control as you choose, with full integration into your processes
- **Scalable for All Organisations** – Suitable for businesses, public sector bodies, and charities of any size
- **Transparent Pricing** – Fixed service tiers, no ingest or licence-based billing
- **Actionable Reporting** – Clear, business-focused outputs that drive measurable improvement
- **Continuous Improvement** – Detection logic evolves with your environment and the global threat landscape

PureCyber MXDR enables organisations to anticipate, withstand, and recover from cyber threats with speed, confidence, and clarity. Whether building new detection capabilities, enhancing existing operations, or replacing legacy services, our UK-based, CREST-certified SOC provides the expertise, visibility, and trust to make security an enabler, not a burden.

At PureCyber, we believe the strongest defence is built on partnership, transparency, and trust. Through MXDR and our Unlimited Incident Response Guarantee, we deliver not just protection, but peace of mind.

Incident Response Retainer

Every second counts when faced with a cyber-attack. PureCyber's comprehensive Incident Response Service is designed to provide critical support to organisations when they need it most.

Incident Response utilises the PureCyber team to analyse, respond to, and mitigate the effects of a security incident. This involves identifying the scope and origination of the breach, containing the threat, eradicating it from the system, and recovering affected systems and data.

The investigation phase focuses on understanding how the incident occurred, what was impacted, and gathering evidence to prevent similar occurrences in the future. The goal is to minimise damage, restore normal operations, and prevent future.

Why is Incident Response Important?

24/7/365 Incident Response
Unlimited, round-the-clock access to our certified incident responders. Whether day or night, our team is ready to contain, investigate, and remediate cyber incidents.

Rapid Threat Mitigation
Incident response services quickly contain and eliminate cyber threats, minimising damage and downtime from sophisticated attacks.

Expert Knowledge Access
Gain instant access to cybersecurity experts who efficiently manage incidents, alleviating the burden on in-house teams.

Regulatory Compliance Support
Ensure timely and accurate incident reporting, helping to meet regulatory requirements and mitigate legal and reputational risks.

Incident Response Simulations

In today's rapidly evolving cyber threat landscape, organisations are facing increasingly sophisticated cyber-attacks that can have devastating consequences on operations, reputation, and financial stability. As cyber threats grow in both complexity and frequency, it is no longer sufficient to simply have cyber security measures in place; organisations must be fully prepared to respond swiftly and effectively when an incident occurs.

At PureCyber, we understand the importance of robust incident response capabilities in minimising the impact of a cyber-attack. That's why we are pleased to propose our comprehensive Incident Response (IR) Simulation service, designed to equip your organisation with the practical skills and strategic insights needed to respond to cyber security incidents with confidence and precision.

Our Incident Response Simulation programme offers a structured, hands-on training experience that mirrors the high-pressure environment of a real cyber-attack. Leveraging the expertise of our experienced incident response team, the simulation will focus on key areas such as threat detection, incident management, communication strategies, and post-incident recovery.

This experience will improve your organisation's ability to identify potential vulnerabilities, respond rapidly to minimise damage, and recover with minimal operational disruption. By the end of the simulation, your organisation will be better equipped to handle the complexities of a real-world cyber incident, ensuring that your response efforts are both effective and well-coordinated.

Our approach to Incident Response Simulation is designed to drive continuous improvement in your cyber security posture, equipping your team with the tools, knowledge, and experience to respond to a wide range of cyber threats. This simulation will not only highlight strengths within your current incident response procedures but also identify any gaps or areas for improvement, allowing you to strengthen your security defences and improve your resilience to future attacks.

What is PureCyber's Incident Response Simulation and Assessment?

As an assured NCSC Cyber Incident Exercise (CIE) provider, PureCyber measures how well an organisation can respond to cyber-attacks, reviewing both technical and non-technical aspects of your security playbook.

We offer two approaches to cyber incident response simulations:

Table-Top Simulations:
These are discussion-based exercises that focus on the roles, responsibilities, activities, and key decision points in line with your organisation's incident response plan. Table-top exercises are ideal for assessing the strategic and tactical decision-making process.

Live-Play Simulations:
These are real-time sessions where participants execute their roles in response to a particular cyber attack scenario. Live-play simulations provide a hands-on, immersive experience that tests the operational readiness and coordination of your incident response team in a more dynamic environment.

In both types of simulations, our team evaluates the effectiveness of your organisation's response across key areas, including:

- Prevention
- Detection
- Mitigation
- Response
- Impact

Key Objectives

Enhance Incident Detection and Response:
Provide your team with a hands-on, practical exercise that tests their ability to detect and respond to various cyber incidents, from data breaches to ransomware attacks.

Improve Coordination and Communication:
Strengthen internal communication channels and coordination between your security, IT, and executive teams during an incident.

Optimise Incident Handling Protocols:
Assess and refine your incident response plan to ensure it aligns with industry best practices and is tailored to your organisation's unique needs.

Minimise Business Impact:
Equip your organisation with the skills to contain and recover from cyber incidents quickly, reducing potential financial and reputational damage.

Service Overview

Pre-Simulation Planning & Customisation:
We work closely with your team to define the scope and objectives of the simulation. This includes identifying key stakeholders, understanding your organisation's risk profile, and tailoring the simulation scenarios to match your unique threat landscape.

Realistic Simulation Execution:
We deploy a series of highly realistic cyber attack scenarios that simulate real-world threats, such as data breaches, insider threats, ransomware, and denial-of-service (DoS) attacks. During the simulation, your team will work through various stages of the response, including detection, containment, and recovery.

Post-Simulation Review & Analysis:
After the simulation, PureCyber will conduct a comprehensive review session with your team. We analyse the decisions made, highlight strengths, and identify areas for improvement. This debrief is key to enhancing your overall security posture and refining your incident response strategies.

Actionable Recommendations & Reporting: We provide you with a detailed report that includes recommendations for improving your incident response capabilities. This will cover everything from technical adjustments to policy updates, helping you enhance your IR readiness.

Incident Response as a Service

PureCyber's Incident Response as a Service (IRaaS) provides a complete lifecycle approach to cyber incident preparedness and response. Rather than reacting after a breach, IRaaS ensures your organisation is fully prepared to detect, contain, and recover from incidents at any time.

Delivered by our CREST-certified, NCSC Assured for Cyber Incident Exercising, UK-based team, the service combines governance, planning, simulation, and guaranteed access to expert responders. It enables organisations to move from reactive firefighting to proactive readiness, minimising business disruption, financial impact, and reputational damage.

This is not a simple retainer. IRaaS is a continuous readiness and assurance service built on four integrated pillars: Host, Govern, Prepare, and Respond. Each element strengthens resilience and ensures your organisation can act with confidence when it matters most.

The Four Pillars of IRaaS

Host
PureCyber securely hosts your Incident Response Plan (IRP) and all related artefacts within an encrypted cloud environment accessible only to authorised stakeholders and our SOC.

- Secure document vault for IRP, playbooks, contact lists, and escalation flows
- Version control and audit logs for all updates
- 24/7 accessibility for authorised users and SOC personnel during incidents

Govern
We design and maintain a governance framework for your incident response capability aligned with ISO 27001, ISO 22301 and NCSC guidance.

- Creation of governance policies and playbooks focused around incident response
- Defined roles, responsibilities, and escalation procedures
- Annual review of incident response policies and associated risks
- Reporting templates for the Board, DPO, and regulators

Prepare

Preparation is the foundation of effective response. We ensure your organisation has the knowledge, tools, and confidence to respond effectively.

- Creation or enhancement of a bespoke Incident Response Plan
- Annual NCSC-Assured Incident Response Simulation or Tabletop Exercise tailored to your threat profile
- Incident playbook development for scenarios such as ransomware, phishing, insider threat, and data exfiltration
- Integration with existing monitoring, SOC, and communication systems

Respond

When an incident occurs, you have guaranteed access to PureCyber's 24/7 CREST-certified SOC and Incident Response team. Our experts investigate, contain, and offer support to recover your environment with precision and speed.

- 24/7 access to UK-based responders
- Forensic investigation, containment, eradication, and recovery support
- Root cause analysis and comprehensive incident reporting
- Post-incident review and lessons learned
- Liaison support with insurers, regulators, or law enforcement

FEATURE	DESCRIPTION
Governance and Policy Framework	Establish and maintain incident response governance, including defined roles, responsibilities, and escalation procedures.
Incident Response Plan Creation	Development and continual improvement of a bespoke IRP aligned with ISO 22301, NCSC guidance, and relevant regulatory frameworks.
Secure Vault Hosting	Secure encrypted storage for all response documentation, contacts, and audit trails, accessible to both client and SOC.
NCSC-Assured Annual Simulation Exercise	Realistic incident simulation or tabletop scenario engaging executive and technical teams, aligned with NCSC Assured Cyber Incident Exercising standards.
24/7 Retained Incident Response Team	Guaranteed access to UK-based, CREST-certified responders available at all times.
Post-Incident Forensics and Reporting	Full forensic investigation, detailed reporting, and recommendations to prevent recurrence.

Key Benefits of PureCyber IRaaS

Full Lifecycle Protection Comprehensive management of the incident response process from governance to recovery.

Guaranteed 24/7 Support Immediate access to our UK-based, CREST-certified incident responders at any time.

NCSC-Assured Exercising All simulations and exercises are conducted under the NCSC Cyber Incident Exercising (CIE) Assured Service, providing recognised, independently validated assurance of quality and rigour.

Regulatory Confidence Alignment with ISO 27035, NCSC guidance, and Cyber Essentials Plus ensures a defensible and auditable response posture.

Board-Level Assurance Annual exercising and governance reports demonstrate measurable maturity and readiness to executive and regulatory stakeholders.

Operational Efficiency Removes the need to source emergency response support at short notice, reducing cost and uncertainty during a crisis.

Deliverables
Each year, PureCyber delivers:

- Full NCSC-Assured Incident Response Simulation Exercise
- Updated Incident Response Plan and Governance Pack
- Executive report with lessons learned and recommendations for improvement

Reporting and Continuous Improvement
Each engagement with IRaaS produces actionable intelligence that strengthens organisational readiness. Reports track governance maturity, incident preparedness, and response performance against defined benchmarks.

Every incident or simulation outcome feeds into a continuous improvement cycle that refines procedures, playbooks, and communication flows to ensure long-term resilience and readiness.

Managed Vulnerability Scanning

Our Vulnerability Scanning service provides comprehensive, accurate, and actionable insights into your security environment by assessing both internal and external surfaces. Leveraging industry-leading technology, we identify vulnerabilities in your infrastructure to ensure no security gap goes unnoticed.

External Vulnerability Scan

We assess externally facing assets (websites, email servers, etc.) to identify potential attack surfaces, misconfigurations, and outdated software that could be exploited by external threats.

Internal Vulnerability Scan

We scan your internal network and systems, detecting vulnerabilities that could be exploited by attackers with internal access (e.g., through phishing or compromised endpoints).

Key Benefits

Comprehensive Coverage:
Both external and internal infrastructure are thoroughly assessed, providing a full-view of the security posture.

Accurate Results:
Using advanced tools, we deliver reliable, actionable intelligence with minimal false positives.

Prioritised Risk Assessment:
Results are risk-scored, enabling you to address the most critical vulnerabilities first.

Detailed Reporting:
You receive a report with identified vulnerabilities, their severity, and actionable remediation steps.

Regulatory Compliance Support:
Regular scanning helps maintain compliance with regulations like Cyber Essentials, GDPR, and PCI-DSS.

Scalable & Customisable:
Our service adapts to networks of any size, allowing tailored scans based on your needs.

Fast Deployment:
Quick and easy to implement with minimal disruption, delivering fast insights into security posture.

By using our Vulnerability Scanning service, you can proactively identify and address risks to reduce exposure and strengthen your security environment.

Phishing Simulations

Phishing attacks are a major cyber security threat, manipulating users into opening malicious documents or clicking harmful links to steal credentials or implant malware.

A phishing simulation is a cyber security exercise designed to test an organisation's ability to recognise and respond to a phishing attack.

PureCyber's phishing simulation allows your organisation to create realistic, bespoke campaigns that closely mimic real attacks. Employees receive fraudulent emails, texts, or calls, using social engineering tactics to gain trust and prompt ill-advised actions. Those who fall for the simulation are alerted to their mistake and directed to educational resources on recognising phishing scams. Post-simulation, organisations receive detailed metrics on employee click rates, helping to identify susceptible users.

Key Benefits

Easy to Administer
Straightforward setup and execution require minimal IT involvement, allowing you to launch simulations quickly and efficiently.

Customisable
Customise scenarios and parameters to address specific organisational needs and unique threat landscapes, maximising the effectiveness of your phishing simulations.

Complementary to Training
Integrates effortlessly with existing cyber security training initiatives, reinforcing awareness and response strategies against phishing attacks.

Real-World Attack Simulations
We simulate tactics like spear-phishing and social engineering to help employees spot different types of threats.

Cyber Awareness Training

In today's digital age, cyber threats are constantly evolving, posing significant risks to organisations of all sizes. At PureCyber, we offer comprehensive Cyber Awareness Training that can be delivered either onsite, online or through our education platform, tailored to meet the unique needs of your organisation. Our training is designed to equip your employees with the knowledge and skills necessary to protect your organisation from cyber threats. The content covers essential areas for maintaining strong cyber security practices, and can be adapted to best suit your team's needs for either in-person or virtual engagement.

Training Overview

Our Cyber Awareness Training is structured to address critical aspects of cyber security, ensuring that your employees understand and can mitigate risks associated with cyber threats. The key training modules include:

Creating Strong and Secure Passwords

- Importance of strong passwords and password managers
- Common password pitfalls and how to avoid them
- Practical tips for creating secure, memorable passwords
- Role of multi-factor authentication in enhancing security

Recognising and Avoiding Digital Traps

- Identifying and avoiding email phishing attacks
- Risks associated with SMS-based phishing (Smishing)
- How attackers use voice phishing (Vishing) to manipulate employees
- QR code-based phishing (Quishing) and emerging threats
- Psychological manipulation tactics used by cyber criminals
- Real-life case studies of social engineering attacks
- Preventative measures to mitigate social engineering threats
- Strategies for verifying legitimate communications

The Dark Web: Protecting Your Company's Data

- Understanding the dark web and its impact on organisations
- How stolen credentials are traded and used against organisations
- Steps to monitor and reduce company exposure on the dark web

Staying Ahead of Emerging Cyber Threats

- The latest cyber security trends affecting organisations
- Real-world examples of recent cyber attacks
- Strategies to stay ahead of evolving threats
- Importance of continuous employee training and awareness
- The role of regular security updates and patch management

Understanding Your Cyber Adversaries

- Overview of cyber criminals, hacktivists, nation-state actors, and insider threats
- Motivations behind different cyber attacks
- How organisations can identify and mitigate risks posed by threat actors
- Tools and techniques used by cyber criminals and how to defend against them

Delivery Method

Our training can be delivered either onsite or online, ensuring that it fits seamlessly into your organisation's workflow and logistical needs. Whether in person or remotely, the training will be highly interactive, engaging your employees in a variety of learning methods including:

- Interactive sessions with live demonstrations
- Hands-on exercises to reinforce key cyber security principles
- Customised content tailored to your organisation's specific risks and needs
- Real-time Q&A with expert trainers to address individual concerns

Our Cyber Awareness Training provides a comprehensive and flexible solution to safeguard your organisation from the growing range of cyber threats. Let us help you build a more resilient, secure, and informed workforce.

Cyber Audit

Cyber security is a process, not a product. Preparation is key; without the correct controls in place, a cyber-attack can have devastating effects on any organisation. It's not a matter of if, but when a cyber-attack will happen.

Understanding the threats is crucial to defending against them. The key is to identify what data is being held, how the data is used, and what current controls are in place around it. This is why we recommend that any organisation wanting to truly understand the threat landscape should undertake a Cyber Security Audit.

A cyber audit offers a clear assessment and overview of your organisation's current security posture, reviewing existing plans and technical capabilities. It provides actionable insights and strategic guidance/direction to strengthen and mature your cyber defences.

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

Key Themes

A cyber security audit helps by evaluating the current threat landscape and assessing the effectiveness of existing security measures. This allows businesses to update their defences and stay ahead of emerging threats.

An audit ensures that the business's security practices align with relevant regulations and standards. It helps identify gaps in compliance and provides recommendations for remediation, reducing the risk of legal issues and fines.

An audit identifies internal vulnerabilities and assesses the effectiveness of existing security controls. It provides actionable insights and recommendations to address these weaknesses, strengthening the overall security posture of your organisation.

Cyber Essentials and Cyber Essentials Plus

Cyber Essentials provides a basic level of cyber security assurance. The certification covers five key areas:

- Secure configuration
- Boundary firewalls and internet gateways
- Access control
- Patch management
- Malware protection

Cyber Essentials is a UK Government-backed scheme aiming to provide a baseline of cyber security through a standard set of technical controls organisations *should* have in place to protect themselves against the most common security threats.

Cyber Essentials Plus is an independent, technical audit that verifies the answers provided within the Cyber Essentials accreditation to ensure the organisation is compliant with the standard.

The process involves auditing against the **5 key controls** of Cyber Essentials by;

- Conducting vulnerability scans against systems to make sure applicable patches have been applied within 14 days
- Checking the malware protection in place is sufficient and working effectively
- Checking for account segregation across permissions
- Reviewing MFA controls against cloud applications.

Cyber Essentials, backed by UK Government, is a set of standard technical controls organisations *should* have in place as a baseline to protect themselves against the most common security threats. By conducting the Cyber Essentials Plus audit, your organisation is demonstrating its commitment to implementing these controls.

Key Benefits

Expert Guidance
As an NCSC Assured Cyber Advisor, PureCyber will provide assistance throughout the accreditation process with tailored advice to suit your organisation.

User-Friendly Process
PureCyber's approach to the accreditation is a streamlined process, designed to limit the disruption and resources required.

Proven Track Record
As one of IASME's longest serving certification bodies, having adopted the Cyber Essentials Plus scheme in its infancy, PureCyber is aware of all the standard requirements and has a history of delivering these services for a huge variety of companies.

Increased Assurance
Independent testing for Cyber Essentials Plus, by certified testers, offers greater confidence in your cyber security practices.

Cost-Effective Packages
Competitive pricing for comprehensive services aligned with IASME prices for different-sized organisations.

Cyber Essentials as a Service

PureCyber's Cyber Essentials as a Service (CEaaS) transforms traditional Cyber Essentials (CE) and Cyber Essentials Plus (CE+) certification into a continuous assurance model. Rather than a once-a-year compliance exercise, CEaaS provides ongoing validation, visibility, and improvement, ensuring your organisation remains compliant, protected, and audit-ready throughout the year.

By combining monthly vulnerability scanning, configuration reviews, benchmarking, and IASME-aligned guidance, CEaaS maintains your Cyber Essentials posture dynamically. This reduces risk exposure, supports CE+ readiness, and prevents compliance drift between annual renewals.

PureCyber's CEaaS service is delivered by IASME-accredited Cyber Advisors, ensuring that every review and recommendation aligns with recognised best practice and the latest threat landscape.

Continuous Compliance, Continuous Protection

Annual certification alone cannot keep pace with daily cyber threats and evolving IT environments. CEaaS provides a proactive approach by embedding monthly assessment and improvement cycles across the five Cyber Essentials technical areas:

- Firewalls and Internet Gateways
- Secure Configuration
- User Access Control
- Malware Protection
- Patch Management

This continuous monitoring and remediation process ensures your organisation maintains Cyber Essentials-level assurance every month, not just at renewal time.

Service Features

FEATURE	DESCRIPTION
Cyber Essentials (CE) & Guidance	Monthly review of CE controls across all five technical areas, including remediation recommendations to address identified gaps.
Cyber Essentials Plus (CE+) & Guidance	Ongoing advisory support and readiness assessments to maintain CE+ alignment, with simulated audit checks to detect potential fail points early.
IASME Certification Management	End-to-end management of IASME certification and re-certification processes, including evidence gathering, submission, and assessor liaison.
Monthly Internal & External Vulnerability Scans	Automated and analyst-reviewed scanning of both internal networks and public-facing assets to detect vulnerabilities and prioritise remediation.
Monthly Benchmarking & Reporting	CE+ benchmarking and maturity reports showing month-on-month progress, trends, and recommendations for continuous improvement, suitable for IT Governance or Board reporting.
Dedicated Cyber Advisor	Direct access to an IASME-accredited Cyber Advisor for technical queries, control reviews, and ongoing compliance guidance.

Key Benefits of PureCyber CEaaS

Continuous Compliance
Maintain your Cyber Essentials posture year-round, avoiding last-minute renewal stress or compliance drift.

Reduced Risk Exposure
Monthly vulnerability scanning and benchmarking identify weaknesses early, enabling proactive remediation before attackers can exploit them.

CE+ Ready, Always
Stay aligned with CE+ technical controls and evidence requirements, simplifying annual re-certification and assessor engagement.

Board-Level Assurance
Regular reports provide clear evidence of improvement, control maturity, and risk reduction, supporting governance and insurer assurance.

Predictable Compliance Management
A structured, ongoing service model delivers clarity, consistency, and accountability, reducing administrative overheads and ensuring readiness for renewal at all times.

PureCyber Cyber Essentials as a Service (CEaaS) turns annual compliance into a living, measurable part of your organisation's cyber defence strategy.

Through continuous monitoring, monthly benchmarking, and expert advisory support, CEaaS provides the assurance and visibility needed to stay certified, stay protected, and stay ahead all year long.

IASME Cyber Assurance Level 1 and Level 2

Many organisations choose the IASME Cyber Assurance standard as a more cost-effective certification and stepping stone to achieving the ISO27001 at a later stage, if required. IASME Cyber Assurance (Level 1) is a self-assessment that enables you to demonstrate your overall maturity level for good security and data privacy practices, whilst Level 2 audits the previously completed self-assessment.

The standard focuses on the following key aspects of cyber security governance:

Planning Information Security
Physical and Informational Asset Registers
Access Management
Backup and Business Continuity
Supply Chain Management
Vulnerability Management
Monitoring
Risk Management
Incident Management
People Management
Regularity Compliance

Key Benefits

Expert Guidance
As an NCSC Assured Cyber Advisor, PureCyber will assist you throughout the accreditation process with tailored advice to suit your organisation.

User-Friendly Process
PureCyber's approach to the accreditation is a streamlined process, designed to limit the disruption and resource required.

Proven Track Record
As one of IASME's longest serving certification bodies, after adopting the IASME Cyber Assurance scheme in its infancy, PureCyber is well-versed in the standard requirements and has a history of delivering these services for a huge variety of companies.

Increased Assurance
Independent auditing by certified auditors offers greater confidence in your cyber security practices.

ISO 27001 Consultancy

At PureCyber, we understand that achieving ISO 27001 certification is a critical step in enhancing your organisation's information security management. As specialists in ISO 27001 compliance, we provide comprehensive consultancy services to guide you through every stage of the process, making it manageable and aligned with your day-to-day business activities.

Our experienced ISO 27001 Lead Auditors and Lead Implementers act as an extension of your internal governance departments, ensuring your path to certification is smooth and effective without overwhelming your teams with strict deadlines.

Key Services

ISMS Strategy and Programme Development:
We assist in creating your Information Security Management System (ISMS) strategy, ensuring it aligns with business objectives while meeting ISO 27001 requirements.

Risk-based Approach:
We implement a risk-based approach to developing your ISMS, ensuring your policies are practical and effective in mitigating security risks.

Bespoke or Templated Policies:
Whether you prefer bespoke policies tailored to your business or utilise our templates, we provide the right documentation to support your compliance.

Gap Analysis:
A thorough gap analysis of ISO 27001 controls and associated policies helps you identify areas that require attention before proceeding with certification.

Guidance on Statement of Applicability (SOA):
We guide you in completing your bespoke SOA, ensuring that your security measures are appropriately documented and aligned with ISO 27001 requirements.

Qualified ISO 27001 Auditor Expertise:
Our consultants bring their experience as certified ISO 27001 Lead Auditors, ensuring you receive expert guidance throughout the process.

Multi-Staged Project:
The process is broken into manageable stages, allowing us to work seamlessly alongside your internal teams without disrupting your business operations.

What's Included in the Consultation?

Our ISO 27001 consultancy covers the following key areas:

- Organisational and Operational Security Evaluations
- Information Security Policies Development
- Remote Working Security Measures
- Human Resources Security Processes (Starters/Leavers)
- Asset Management & Data Classification
- Access Control & Physical Security
- Risk Assessments & Incident Management
- Business Continuity & Disaster Recovery
- Compliance & Supply Chain Management
- System Development & Maintenance Security

End-to-End ISO 27001 Support:
While PureCyber does not perform the final audit, we provide full support throughout the process, guiding you every step of the way to ensure you are ready for certification.

Internal Audits:
We conduct internal audits to identify areas for improvement, ensuring you meet the certification requirements and continuously improve your information security posture.

Full Consultancy Process:
Our fully managed service provides an easy path to ISO 27001 certification without requiring additional internal resources. We integrate our consultancy seamlessly into your organisation's information security governance programme.

ISO 22301 Consultancy

At PureCyber, we understand that achieving ISO 22301 certification is a crucial step in strengthening your organisation's business continuity capability. ISO 22301 provides a structured framework for preparing, responding, and recovering from disruptive incidents, ensuring that critical operations can continue even during unexpected events.

As specialists in business continuity and operational resilience, our consultants guide you through every stage of ISO 22301 implementation. We make the process manageable, aligned to your day-to-day activities, and fully integrated with your wider governance and risk programmes.

Our experienced business continuity specialists act as an extension of your internal teams, ensuring a smooth journey toward a resilient and fully compliant Business Continuity Management System (BCMS).

Key Services

BCMS Strategy & Programme Development
We help you establish a BCMS strategy that aligns with your organisational objectives while meeting ISO 22301 requirements. This includes defining context, leadership responsibilities, planning, operational processes, and continual improvement activities.

Risk Based & Impact Driven Approach
Our team helps you identify critical processes, downtime tolerances, and risks through structured Business Impact Analysis (BIA) and risk assessment, ensuring continuity measures are proportionate and effective.

Policies, Procedures & Continuity Documentation
We support the development and refinement of business continuity policies, recovery strategies, roles and responsibilities, incident response structures, and crisis communication processes. These documents form the backbone of a compliant BCMS.

Gap Analysis
Our consultants perform a detailed gap analysis against ISO 22301 requirements, helping you identify areas for improvement before progressing to formal certification preparation.

Continuity Strategy & Recovery Planning
We assist in developing recovery strategies and operational plans that ensure essential services remain available during disruptions—whether caused by IT outages, cyber incidents, supply chain failures, or internal process breakdowns.

ISO 22301 Implementer Level Expertise
PureCyber consultants bring deep expertise in business continuity and ISO frameworks, ensuring you receive accurate and practical guidance throughout the process.

Multi Staged Project Delivery
Your BCMS implementation is delivered in manageable phases, allowing our team to work seamlessly with your internal resources without disrupting ongoing operations.

What's Included in the Consultation?

- Identification of threats and potential business disruptions
- Business Impact Analysis & continuity requirements definition
- Development of continuity and recovery strategies
- Incident response planning
- Crisis management structures
- Documentation and governance support
- Alignment with regulatory and client resilience expectations

End to End ISO 22301 Support
While PureCyber does not perform the final certification audit, we provide full support throughout the implementation process and ensure you are fully prepared for Stage 1 and Stage 2 assessment. We help you embed resilience into your organisation's culture, demonstrating to customers, regulators, and stakeholders that you can maintain critical operations under pressure.

Internal Audits & Readiness Assessments
Our specialists conduct internal audits to validate that your BCMS meets ISO 22301 requirements, identify gaps, and improve your overall resilience posture. This ensures continuous improvement and prepares you for successful certification.

Full Consultancy Process
PureCyber offers a fully managed ISO 22301 consultancy service, integrating seamlessly into your organisation's continuity and resilience programme. From initial scoping and planning through to documentation, testing, and audit readiness, we provide a clear and structured path to certification—without requiring additional internal resources.

Governance Consultancy

Governance consultancy provides independent expertise to help organisations align with recognised frameworks and standards, identify weaknesses, and develop a roadmap to achieve compliance or best practice maturity.

Our governance consultancy support includes:

- Conducting structured assessments against governance and regulatory frameworks
- Reviewing and developing policies, procedures, and controls tailored to your organisation
- Assessing supplier and third-party governance through due diligence exercises
- Providing outsourced expertise to embed governance best practices into day-to-day operations

Effective governance gives your organisation a strong foundation for risk management, compliance, and operational resilience. By working with a governance consultancy, you demonstrate your commitment to robust oversight and accountability, while ensuring your organisation can meet both current and emerging obligations.

Key Benefits

Expert Guidance
With vast experience across multiple governance frameworks, PureCyber can support you through different disciplines and help provide valuable advice to improve your governance standards.

Policy & Process Development
Our consultants work with you to design and refine governance policies, procedures, and reporting structures that embed compliance into business-as-usual operations.

Supply Chain Confidence
Through supplier due diligence and third-party risk assessments, we give you visibility and assurance across your supply chain, strengthening resilience and meeting regulatory expectations.

Ongoing Governance Support

Whether as a retained partner or outsourced governance function, PureCyber provides ongoing expertise to monitor compliance, manage audits, and keep pace with evolving standards and regulatory requirements.

Supply Chain Risk Management

Effective supply chain governance is essential for managing third party risks, meeting regulatory expectations, and ensuring operational resilience. Our Supply Chain Governance & Risk Consultancy provides independent expertise to help organisations strengthen oversight of suppliers, align with recognised standards, and build a robust framework for managing dependencies across your entire supply chain.

Our consultancy support includes:

- Assessing suppliers against governance, risk, and regulatory frameworks to identify weaknesses and prioritise remediation.
- Reviewing and developing policies, procedures, and controls tailored specifically to third party and outsourced service management.
- Conducting detailed supplier due diligence and third party risk assessments, giving you visibility of vulnerabilities across your supply chain.
- Providing outsourced governance expertise to embed strong oversight into everyday procurement, contracting, and supplier management activities.

Strong supply chain governance enhances your organisation's ability to anticipate and manage risks, maintain compliance, and demonstrate clear accountability over third party operations. By working with a specialist consultancy, you strengthen your resilience and ensure suppliers meet both current and emerging obligations.

Key Benefits

Targeted Supply Chain Expertise
With extensive experience across governance and supply chain risk frameworks, PureCyber helps you understand third-party exposure, evaluate supplier maturity, assess security risk and strengthen end-to-end oversight.

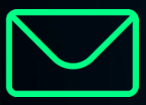
Policies & Processes Built Around Third-Party Risk
We design and refine supplier specific policies, onboarding procedures, due diligence workflows, and reporting structures that embed third-party risk management into business-as-usual operations.

Enhanced Supplier Visibility & Assurance
Through in-depth due diligence, risk scoring, and third-party assessments, we provide clarity and reassurance across your supply chain supporting resilience, regulatory compliance, and informed decision-making.

Ongoing Supply Chain Governance Support
As a retained partner or outsourced governance function, PureCyber delivers continuous monitoring, audit preparation, supplier performance oversight, and ongoing alignment to evolving standards and regulations.

PURECYBER

Get in **Contact** Today



info@purecyber.com

0800 3689397

https://purecyber.com

STRENGTHENING YOUR **CYBER RESILIENCE**

PureCyber Ltd 2026