CYBERFORT

G-Cloud 14

Service Description

Security Testing

Table of Contents

1. Security Testing Overview

1.1 Summary of Service

Cyberfort provides reliable independent assurance that applications, databases, and associated infrastructure deployments are protected from security threats.

Using CREST and CHECK ITHC-accredited methodologies, we perform state-of-the-art automated vulnerability scanning and carefully targeted manual testing to deliver an outstanding assessment across internal and external estates.

An application penetration test is an authorised simulated attack on applications and associated infrastructure, performed to identify vulnerabilities and strengths within the environment. We offer black box (unauthenticated) and white box (authenticated) testing of all key application components and their supporting infrastructure. Comprehensive vulnerability reporting clearly communicates threats and risks in their business context. Actionable technical remediation advice and support are provided to help ensure best practice security controls are implemented.

1.2 Service Detail

1.2.1 Service Description

Penetration testing is a key component of security auditing. Scoping, planning, delivering, and reporting on a simulated cyberattack requires meticulous planning and control to ensure all infrastructure and application vulnerabilities are identified while minimising risk and delivering maximum value for money.

Many frameworks exist to help deliver a simulated cyberattack. Cyberfort have adopted the best industry-accepted methodologies including NIST SP 800-115, OSSTMM and OWASP to ensure our scoping is formal and comprehensive, and our testing is extremely thorough. Our reporting exceeds the requirements of CREST, the NCSC Check ITHC scheme and the PCI DSS, and includes innovations based on research which are not seen elsewhere in the industry.

Our penetration test teams are trained in requirements gathering (business and technical) to ensure consistent high-quality scoping can be conducted which reflects real business risk as it applies to the clients. Our testers have undertaken report writing courses accredited by the Plain English Campaign to ensure accurate accessible and concise written communications. Unusually in the industry our testers enjoy conversation which means verbal debriefs and discussions are a key differentiator for us.

We offer the following security testing services:

- **Internal Infrastructure Penetration Testing:** This assessment will offer you an insight into how an attacker will move through the network to steal data or elevate their access. Cyberfort will perform automated and manual penetration testing to identify any flaws in the infrastructure.
- **External Infrastructure Penetration Testing:** This assessment will identify vulnerabilities that are present on your externally facing infrastructure. This engagement will offer you an in-depth view of how a real-world attacker might attempt to compromise your network without prior knowledge of the system.
- **Wi-Fi Penetration Testing:** This assessment will identify flaws in the Wi-Fi networks and determine what level of access an unauthenticated attacker can achieve within proximity of the site and once they compromise a single SSID.
- **Active Directory Configuration Review:** This assessment will review the configuration of the Active Directory domains to ensure the latest security features are in use and provide the best inherent protections to users on the domain. Additionally, we will assess how domain admin accounts and passwords are managed.

- **Patch Management Review:** This assessment will provide a review of the patches across the internal and external infrastructure.
- **Network Design & Segmentation Review:** In this assessment, Cyberfort will review the topology of the network and ensure there is sufficient network segmentation. Segmentation of the network minimises the hosts an attacker can access if they successfully compromise a host.
- **Firewall Ruleset & Configuration Review:** This assessment will provide a detailed review of your firewalls, including the rules themselves and the firewall configurations. This will ensure rules are not overly permissive and the firewalls have been configured securely.
- **Workstation Build Review:** This assessment will identify any vulnerabilities in the standard builds used by you. Cyberfort will attempt to "breakout" of the restricted environment, attempt to elevate privileges and install malware on the build.
- **Office 365 & MEM Configuration Review:** This assessment will review the settings of the Office 365 tenancy to ensure security features are enabled. Cyberfort will base this on the latest industry standards for Office 365.

1.2.2 Features

- As a dedicated Cybersecurity Consultancy, our approach is designed to help organisations to detect, remediate and reduce the risk posed by threat actors.
- Cyberfort prides itself on having the ability to deliver a holistic approach to penetration testing, considering the organisation in its entirety, deconstructing complexities and delivering actionable steps and prioritising Cybersecurity across the whole organisation.
- Clients benefit from a truly independent assessment of application security controls Comprehensive assistance with requirements definition and scoping.
- A clearly defined, systematic, structured approach to penetration testing.
- Clear reporting of threats and risks in their business context, communicating impact analysis and assisting with remediation.
- Supporting clients to build in innovative security underpinned by Cybersecurity best practices.
- Bespoke methodology blending automated and manual testing techniques to deliver comprehensive, cost-effective solution.
- Access to highly skilled Cybersecurity Practitioners and Consultants across multiple disciplines ensures effective programmes and complete governance.

1.2.3 Benefits

- A reduction in information and communications technology (ICT) costs over the longterm.
- Translate security issues into business language and help focus organisationalpriorities.
- Communicate issues effectively to secure stakeholder and managementendorsement.
- Greater levels of confidence in the security of IT application environments.
- Visibility of risks and prioritised remediation advice.
- Experienced, dedicated technical staff deliver a full range of cost-effective testing.
- Eliminate the need to employ specialist (and expensive) staff, reduce training costs.

2. Our Approach

Testing engagements can vary enormously in size and complexity, and one size does not fit all. Rightsizing our solution for each client is key to our service.

All Penetration Testing is delivered within comprehensive project and service management wrappers ensuring your needs are central to the service delivered. Our processes and methodologies have been audited and approved by CREST and the NCSC Check ITHC Scheme.

Our approach to penetration testing begins with a needs assessment which allows us to capture and understand the purpose of testing, business drivers, cost constraints, success criteria and ground rules. Once we understand your business drivers, we then move on to full scoping and delivery phases.

2.1 Pre-Test Assessment and Discovery

The Pre-Test Assessment and Discovery will deliver guidance, structured questionnaires, and hosted workshops to help you focus on what is required from testing to deliver assurance which meets risk, compliance, and business objectives.

Our team will be on hand to answer questions and explain the pros and cons of different testing strategies and how they can add value within the larger security auditing and governance program. If we can help de-jargonise a problem or clarify objectives in business language, we are always happy to mentor or work as part of a virtual team to ensure expert knowledge is transferred to your teams and decision makers.

2.2 Scoping and Planning

Our team will manage all aspect of the test planning process. We understand that things can change and will work flexibly to accommodate changes to requirements and deadlines. We understand that an extensive program of testing requires more planning and management than a simple single infrastructure test and will ensure we do not overload any test with unnecessary costs allowing us to use the budget on comprehensive testing where it’s needed.

For each test we will ask you to fill out a scoping document detailing all the information needed to scope and cost testing effort. Alongside this a scoping meeting is arranged for each test with at least one senior tester from Cyberfort, to ensure complete understanding of what needs testing, and ideally with a walkthrough of the application.

Our test planning process includes the following steps related to scoping and support during this process:

- Understand your benefits of penetration testing. Ensure the objective of testing and rationale behind this is understood – adapt scoping and pre-test support need as required.
- Agree and document security requirements, ensuring GDPR and other legal requirements are met.
- Understand the functional requirements of software/infrastructure to be assessed. Assess the risk profile of the environment including attack vectors and broader threat environment.
- Work with your technical teams, developers, suppliers to scope the testing requirement and understand how automated and manual testing might be applied during testing.
- Develop and document test strategy to ensure objectives are met and the appropriate tooling is used. Ensure risk mitigation plans are in place, reporting timeframes and mechanisms are agreed.
- Delivery management – agree tooling and platforms required for testing. Ensure resource skills and requirements are matched to meet program deadlines.
- Agree communication plan including updates to scope and delivery timeframes.
- Agree the content, mode, and frequency of reporting. In addition, a daily wash up call will be held. Notification of high and critical vulnerabilities discovered will be immediate. Draft reports will be

delivered within 24 hours of test completion with final reports arriving within 5 days of the end of testing following QA.

Once all agreements and authorisations are in place with you, a pre-test call is made to ensure all requirements are setup correctly and ready to go so that testing can start promptly and run efficiently with minimal impact during the authorisation window.

2.3 Testing

To ensure that our testing covers an array of real threats and to identify all areas of vulnerability we have adopted the best industry-accepted methodologies to ensure our scoping is formal and comprehensive, our testing is extremely thorough, and our reporting exceeds the requirements of CREST, the NCSC Check ITHC scheme and the PCI DSS.

This methodology is tuned to ensure maximum coverage of all assets while using rate limiting and monitoring technology to ensure only minor additional loading on operational services. We ensure that scoping covers all potentially “fragile” services to ensure our testing does not impact services. While the technology and processes being tested will determine the specific tools and techniques employed, our assessments are in-line with recognised methodologies:

ISSAF ISSAF is an Open Source, peer-reviewed, penetration-testing framework created by the Open Information Systems Security Group (OISSG)

OSSTMM OSSTMM is an open-source security testing methodology introduced in 2000 by the Institute for Security and Open Methodologies (ISECOM)

NIST SP 800-115 This standard provides a guide to the technical aspects of conducting information security assessments

OWASP Top 10 Our testing covers all the Open Web Application Security Project’s (OWASP) most common risks

OWASP ASVS The OWASP Application Security Verification Standard (ASVS) Project provides a recognised standard for testing web application technical security controls.

WAHH Our methodology aligns with the techniques in the Web Application Hackers Handbook

For each type of security assessment test, we have a specific methodology which is updated on a regular basis with new hacking techniques and attack paths added. The purpose of the methodology is to be a guide for the tester, ensuring they achieve full testing coverage for the system under test. The testing methodologies ensure the false negative rate remains low and the number of undiscovered vulnerabilities remains low.

We want to ensure that you are involved in the testing process as much as you wish to be. While testing we’ll maintain an open communications channel between the senior consultant leading the test, and yourselves. This is to ensure that should any issues about the underlying technologies arise, we can quickly resolve them through communication. We understand that real attackers are not time-constrained, and as such we leverage the communication channel to bypass tedious enumeration and clarify uncertainties, allowing for direct focus on vulnerability identification and enumeration.

2.4 Reporting

We offer many different report types and channels for report delivery that ensure your objectives and requirements can always be satisfied.

Our reports are produced from a range of standard templates using professional automation toolsets to deliver clear reporting of vulnerabilities, threats, and risks in their business context, communicating impact and delivering prioritised remediation advice. The Common Vulnerability Scoring System (CVSS) is used to provide the risk and attack vector for each finding, and we identify the stage in your systems lifecycle that the threat has crystalised. The real risk to your business is highlighted in business terms. We provide detailed remediation advice for each vulnerability and explain the steps necessary to reproduce our findings alongside background to the vulnerability and its history of exploitation.

All reporting is quality assured by a senior member of the test team to ensure no stone was left unturned during the testing, as well as to ensure the technical content meets our quality assurance requirements as a ISO9001 certificate holder. A further QA of the report is performed by the Head of Offensive Security to ensure the non-technical aspects of the report are understandable by non- technical people and that the presentation of the final report meets yours' and ours' delivery expectations of report quality.

In addition to the required baseline content prescribed by CREST and the NCSC Cyberfort's reports provide:

- A business impact summary concisely explaining the risks to you in plain language.
- An analysis of the root cause of vulnerabilities to help you understand where in the system lifecycle resources should be prioritised to proactively prevent further vulnerabilities.
- At a glance, traffic light scoring of risk.

Our test reports also include:

- Details of each vulnerability uncovered with associated CVSS v3 base score adjusted to reflect the real environmental risk.
- Background information on each vulnerability.
- Classification of vulnerabilities risk – Critical, high, medium. Low, informational.
- Details of test types and detailed instructions on how each vulnerability was exposed.
- Detailed remediation advice prescribing quick fixes if appropriate and permanent fixes.
- General advice on how security might be approved within your department/organisation.
- Advice for further testing.

As standard you will receive the following reporting approach:

Verbal Reporting

At the simplest level reporting is carried out verbally during informal interactions with your teams and during daily wash up calls using various virtual channels such as Slack, Teams and Video Conferencing.

Daily Reporting

During the testing phase, draft reporting is delivered tactically to address your needs. Daily updates will be provided and will include a summary of the day's findings, a risk assessment, discussion of test basis/type and cases employed, and functional areas tested, plus a summary of the next day's testing schedule.

End of Assessment Report

At the end of the final day of the assessment, a draft report containing the findings in a Microsoft Excel sheet can be provided. This will provide details on findings so that your developers may begin to implement remediations at the earliest possible convenience. The findings and their contents may change during the technical review process and therefore these findings may differ from the Final Report.

Final Report

The Final Report is a comprehensive record of testing including the scope, requirements, methodology followed, vulnerability score and a detailed technical write up including background, findings, steps to reproduce findings and remediation advice. The report also provides a business summary aimed at decision makers and managers to support prioritisation for remediation. We also note general observations made during testing related to areas of security and control improvement we believe will benefit clients.

All reporting is supported by debrief sessions and informal advice from your penetration testers is only a phone call away.

3. Service Management Approach

3.1 Your satisfaction is the heart of our service

We have a proactive, consultative approach that allows us to gain a better understanding of our clients' needs, requirements, objectives and measures of success in order to help you meet your strategic objectives. Ongoing support and management of services under this framework will be based on this approach. From the Service Desk to your dedicated Account Manager, all are in place to manage the relationship across your business and ensure that you receive the right engagement to help drive and deliver a great service.

3.2 Service Delivery Management

Cyberfort's service management model is designed to meet ISO 9001 and ISO 27001 guidelines and has been established in alignment with ITILv3 service management processes. Clients will have a combination of the best people, using the best tools, delivering a 'best-in-class service management' experience. We recognise that to support your business operational requirements we need to have in place the right team structure, governance and engagement processes.

The ultimate responsibility for the achievement and validation of services delivered will be the Service Delivery Management function, which will be led by a dedicated Account Manager and supported by the Service Delivery Manager (SDM). The SDM will be responsible for the delivery of services, ensuring end-to-end service accountability, responsibility and effectiveness. The service structure is ultimately scalable and will be monitored through the Service Governance processes to ensure Cyberfort deliver all in-scope supported services against agreements, expectations, and commitments with the client.

3.3 Service Satisfaction and Improvement

Key to ensuring Client Satisfaction, is the Continuous Improvement of our services. Measurement and validation of service outcomes is therefore a critically important part of the delivery of services. Cyberfort will provide a comprehensive Service Report, tailored to the specifics of each service/project. This report is provided by the SDM to identified client stakeholders who are then invited to a Service Review meeting where the details are discussed, and any follow-on actions are agreed and documented.

3.4 Service Desk Information and Processes

3.4.1 Service Desk Information

Cyberfort's Service Desk operates 24 hours a day 365 days a year and is the primary point of contact for all service requests, incidents, events, or support escalations.

Cyberfort Service Desk can be contacted via:

- Telephone 01304 814890
- Email service@cyberfortgroup.com

The Service Desk will undertake initial triaging of any service requests, incidents, or events directly with the client.

The Service Desk will manage all communications in relation to service requests, incidents, or events for IT infrastructure or managed services hosted within Cyberfort.

For security purposes, client validation will be required by contacts recorded in the Authorised Contacts Form prior to any work being undertaken.

Each inbound query made by the client will be captured by Cyberfort's ticketing system and assigned a unique reference number with an appropriate severity level. This severity level will be calculated using an impact, urgency, and priority matrix.

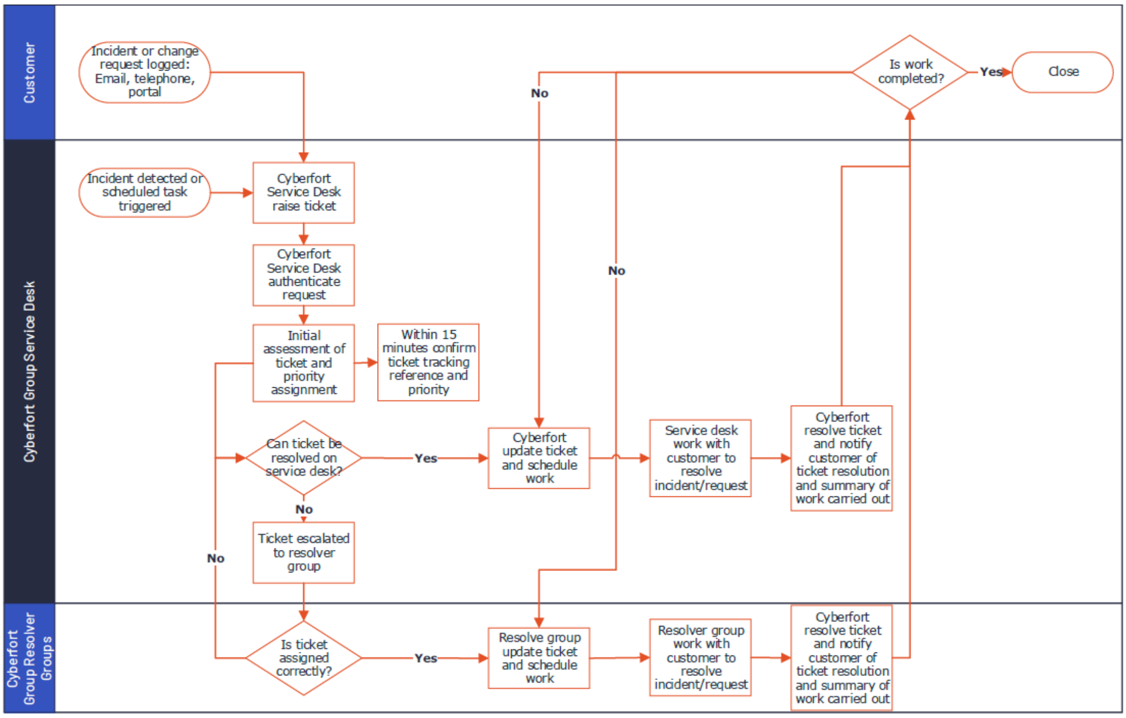
A ticket number will be issued with an initial response within the first fifteen minutes of logging a query. Resolution time goals will be calculated in accordance with a priority matrix. If a client would like to discuss assigned resolution times, they should contact the Service Desk.

Throughout the ticket lifecycle the Service Desk or technical owners will:

- Function as the first point of contact for tickets relating to the provisioned service.
- Ensure tickets are correctly logged, categorised, and prioritised.
- Conduct investigation and diagnosis where appropriate.
- Ensure that all tickets are assigned to the correct analyst or support partners for investigation.
- Manage tickets throughout their lifecycle, escalating where appropriate.
- Keep the client informed of the status of tickets, using ticket updates, telephone communication or emails as appropriate.

3.4.2 Call Handling Process Flow

All tickets logged through the Service Desk will be processed as shown in the figure below.


Customer
Cyberfort Group Service Desk
Cyberfort Group Resolver Groups
Incident or change request logged: Email, telephone, portal
Is work completed?
Yes
Close
No
No
Incident detected or scheduled task triggered
Cyberfort Service Desk raise ticket
Cyberfort Service Desk authenticate request
Initial assessment of ticket and priority assignment
Within 15 minutes confirm ticket tracking reference and priority
Can ticket be resolved on service desk?
Yes
Cyberfort update ticket and schedule work
Service desk work with customer to resolve incident/request
Cyberfort resolve ticket and notify customer of ticket resolution and summary of work carried out
No
Ticket escalated to resolver group
No
Is ticket assigned correctly?
Yes
Resolve group update ticket and schedule work
Resolver group work with customer to resolve incident/request
Cyberfort resolve ticket and notify customer of ticket resolution and summary of work carried out

3.4.3 Client Escalations

In the event that a client is dissatisfied with the progress of their support ticket, they are entitled to request its escalation. Upon such a request, our Service Desk will promptly elevate the matter through our specialised service support engineering team for in-depth analysis and potential solutions. Should the situation necessitate further expertise, it will be advanced to our technical consultancy team to ensure a comprehensive approach to resolution. Recognising the importance of timely and effective responses, escalation to the client's account manager, and depending on the severity, to senior management, will be undertaken to guarantee that all necessary resources are mobilised to meet resolution targets and uphold the highest level of client satisfaction.

4. Commercials & Pricing

4.1 Ordering & Invoicing Process

Please contact us for a quote via email (bidmanagement@cyberfortgroup.com)

Orders are processed on receipt of a purchase order.

Prior to commencement of any work ordered via the G-Cloud framework, Cyberfort requires client acceptance of the order and also completion of a Call-Off Contract.

Clients are invoiced on a monthly basis or according to agreed milestones.

4.2 Service pricing model

Cyberfort's pricing for Security Testing links clearly to Resources Based Pricing detailed in our SFIA rate card framework. Please refer to our Pricing document for more details.

4.3 Minimum contract period

Contract terms will be provided at the time of quotation, based on specification. These will not exceed the maximum contract constraints of the G-Cloud framework.

5. About Cyberfort

As one of the leading cyber security organisations in the UK, Cyberfort is an SME with over thirty years' experience in the market, offering end-to-end cyber security solutions from Consulting to Secure Cloud and Data Centre Services. Security is in the DNA of Cyberfort and our company culture and it's this culture that shapes our approach to ensuring we continue to innovate, improve, develop, and share in the ever-changing world of security.

5.1 Our Values

One Team

We put ourselves in our client's shoes and work together to deliver the best solution. This symbiotic relationship leads to successful outcomes. We are on the same team, our diversity makes us strong; when we collaborate and play to these strengths, we become even more formidable. We respect each other's differences, we give honest feedback and by being accountable for our actions, we act positively to grow and develop.

Curious

We are inquisitive and looking to find the best solution, technology and approach for our clients' requirements. Our approach allows us to unpick and probe every avenue with a focus on successful outcomes. Striving for knowledge and driving our own development with energy and enthusiasm, we are constantly questioning how to improve and innovate; by learning from others we will thrive and grown.

Transparent

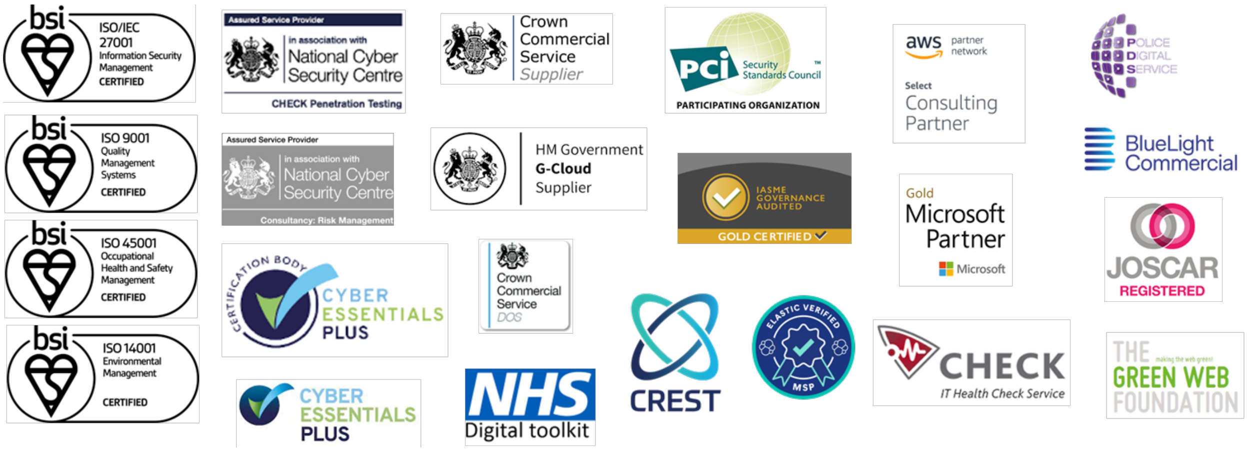
We are responsible for ensuring strong and clear communication with our client; Our bedrocks of trust and professionalism are demonstrated in all that we do. As colleagues, we are open and honest with each other, we share opinions, ideas are sought and given due consideration; we act upon decisions and feedback on outcomes. We trust each other to do the right thing, take pride in our actions and celebrate our successes.

Owners

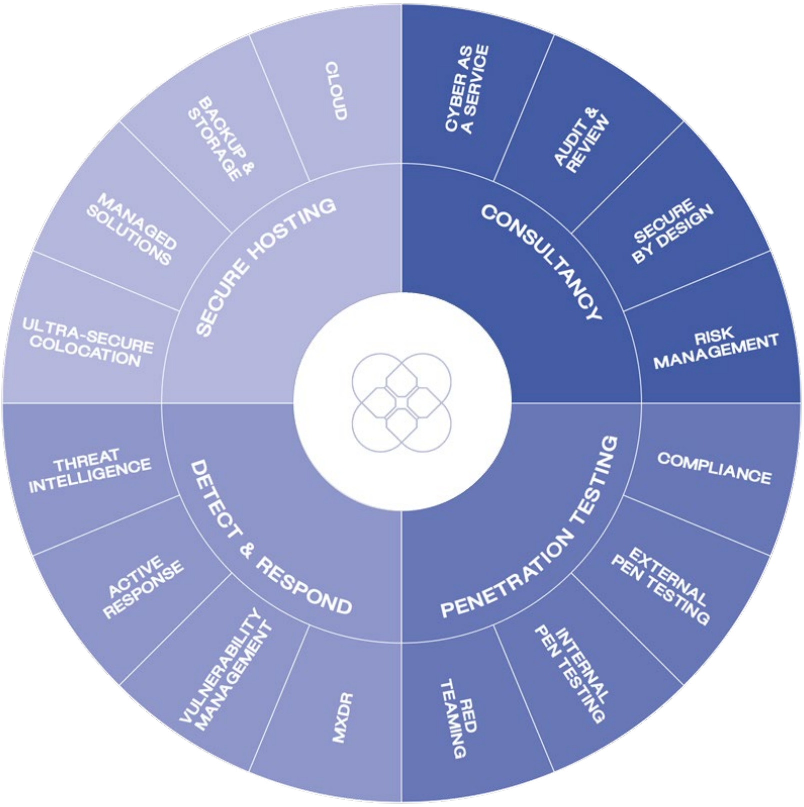
Providing the best solution and support is not always the easiest path; we proactively support our clients, are empowered to make a difference and take accountability to ensure we do what is right. We step up and do not wait for others to act, we care about the outcome and showing others that they can trust us to do the right thing.

5.2 Our Accreditations

We're proud of the extensive list of industry and government accreditations we hold. We understand the need for independent validation when entrusting the security of valuable or sensitive data to a third party.


bsi ISO/IEC 27001 Information Security Management CERTIFIED
bsi ISO 9001 Quality Management Systems CERTIFIED
bsi ISO 45001 Occupational Health and Safety Management CERTIFIED
bsi ISO 14001 Environmental Management CERTIFIED
Assured Service Provider in association with National Cyber Security Centre CHECK Penetration Testing
Assured Service Provider in association with National Cyber Security Centre Consultancy: Risk Management
CERTIFICATION BODY CYBER ESSENTIALS PLUS
CYBER ESSENTIALS PLUS
Crown Commercial Service Supplier
HM Government G-Cloud Supplier
Crown Commercial Service DOS
NHS Digital toolkit
PCI Security Standards Council PARTICIPATING ORGANIZATION
IASME GOVERNANCE AUDITED GOLD CERTIFIED
CREST
ELASTIC VERIFIED MSP
aws partner network Select Consulting Partner
Gold Microsoft Partner Microsoft
CHECK IT Health Check Service
POLICE DIGITAL SERVICE
BlueLight Commercial
JOSCAR REGISTERED
THE GREEN WEB FOUNDATION

5.3 Our Services



Consultancy

Cyberfort understands risk and our consultancy services provide you with a realistic view of the risks your business faces and we do this in quantifiable and objective terms. Managing risk is a balancing act between avoiding threats and missing out on positive opportunities; and our consultants are experts in helping organisations achieve this. Our consultants will work closely with you to help you understand your business, cyber and data related risks and where you should focus your available resources. We provide practical advice, helping you implement pragmatic solutions that will help your organisation run smoothly, while keeping risk at a level you're comfortable with.

Detect & Respond

Cyberfort's MXDR services defends clients and pervasively monitors your network. We combine organisational context with security expertise to detect, correlate analyse and respond across the multiple sites, devices and environments that you and your clients depends on. We understand the criticality of the services provided to often vulnerable individuals, and as such our service defends you with a focus on availability, and effective and appropriate defences.

Cyberfort's SOC operates as an extension of your own team, monitoring your environments 24x7x365, detecting, correlating and analysing events, and providing both guided response and active defences for your environment under your predefined governance.

Penetration Testing

Cyberfort's Penetration Testing and Offensive Security will give you the confidence that the technology you are using or developing is as secure as it possibly can be, and if it isn't - what you need to do. Whether you are developing internal software solutions, or you want to ensure your own infrastructure is secure, you need to test your technology for vulnerabilities. This is done by carrying out a penetration or 'pen test' of your IT infrastructure. Cyberfort pen testers are renowned for finding system vulnerabilities other pen testers just haven't dug deep enough to uncover. We tell you what you don't know, not what you know already, allowing you to make informed decisions about where best to invest your resources and budget.

Secure Hosting

Our cloud services are designed to enable your organisation to deliver hosted cloud services in a secure way. We ensure your mission-critical data is always secure and available within our ultra-secure, UK-based data centres. We partnerwith you, becoming a trusted extension of your team and designing bespoke solutions that enable you to grow and meet your business objectives. Our cloud services include public cloud and bespoke technical solution architecture, managed public and private clouds, hosting, colocation services includingsecure and managed suites.

6. Our Experience

Our clients range from the largest of HMG departments, to non-departmental public bodies including projects of critical national infrastructure status. Our private sector work is equally wide-ranging, including blue-chip and FTSE companies, SMEs and agile technology start-ups.

6.1 Case Study Example

APPLICATION & NETWORK INFRASTRUCTURE CHECK IT HEALTH CHECK

The Challenge

The client is responsible for operating and responding to urgent and emergency medical situations within the UK’s capital, they needed to perform a comprehensive test of their infrastructure as part of their Data Security and Privacy Toolkit (DSPT) requirements.

The Solution

Cyberfort provided a comprehensive internal and external test of the clients infrastructure. The Firewall Configuration review was conducted to certify the ruleset. We ensured the relevant skilled consultants were assigned to the delivery of the assessments.

The Outcome

With clear open communication channels between our teams the delivery of the testing was seamless and painless. The interaction between the clients Cyber Team and Cyberfort enabled fixes to be applied and retested, for conformation that the vulnerabilities highlighted were closed.

SOLUTION PROVIDED

- Gold Build Review.
- Firewall Config Review.
- Wi-Fi Security Review.
- Web Application.
- VPN Review.
- Internal infrastructure
- External infrastructure

BUSINESS RESULTS

- Enhanced security of applications and infrastructure.
- Evidence of rigorous testing for clients and prospects.
- Actionable plan for the next 12 months.

7. Governance Compliance

Cyberfort confirm that we will deliver our services to clients in line with all industry and Government recognised standards, best practice and legal regulations, including but not limited to the following:

7.1 GDPR

We adhere to the legal and statutory requirements outlined in the UK Data Protection Act 2018 and the General Data Protection Regulations (GDPR). Our organisation has a current registered Information Commissioners Office (ICO) certificate for Data Protection.

7.2 Government and industry standards

Throughout the life of any contract, our consultants will ensure that all service standard principles are adhered to so that clients can be assured that all delivered outcomes conform with Government and industry standards and expectations. Our teams are deeply experienced in operating services, to deliver outcomes and outputs that fully comply with:

- The principles defined in the Government's Service Standard and Technology Code of Practice (TCoP).
- The Government Functional Standard (GovS 007: Security), ensuring that the stated principles (for example security objectives are aligned to government policy and organisational objectives) are applied to all projects.
- Open standards supported include TOGAF, NIST-CSF, ISO/IEC27000, SANS and OWASP.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).
- As an NCSC assured Cyber Security Consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing) platform.

7.3 Quality Management

Further, we have a fully implemented Quality Management System (QMS) and are certified to ISO 9001:2015 International Standard, which details our policy, objectives and processes, as well as demonstrating how our QMS framework enhances client satisfaction whilst ensuring consistent delivery of product and services is maintained to meet client, statutory and regulatory requirements.

Our delivery is underpinned by certifications and associated management systems including :

ISO:27001,

ISO:14001,

ISO:9001,

ISO: 45001

PCI DSS,

DSPT,

NCSC Cyber Security Consultancy,

NCSC CHECK ITHC,

Cyber Essentials Plus,

CREST Certified Body CE,

CREST Penetration testing

NHS Digital Toolbox.

CYBERFORT

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com