BULLETPROOF

G-CLOUD SERVICE DESCRIPTION

CYBER SECURITY, INFORMATION SECURITY & DATA PROTECTION SERVICE DESCRIPTIONS

ABOUT BULLETPROOF

We are your best defence against cyber threats. We are Bulletproof.

At Bulletproof, security is in our DNA. We're laser-focussed on bringing innovation and simplicity to all areas of cyber security, information security, and data protection. As an established leader in the UK market, we have the expertise and experience to help you through your challenges.

Organisations in all industries trust us to remove the complexities of managing projects in-house, helping SMEs grow and empowering enterprises to work smarter. Combining our years of industry experience with a perfected suite of services, Bulletproof works as an extension of your team to give you full visibility over your threat landscape and proactively manage your risk

PENETRATION TESTING

Our CREST-certified pen testers will evaluate assets, networks, APIs, web applications, mobile applications, cloud infrastructure (and more) for security weaknesses and vulnerabilities.

INTRODUCTION TO CUSTOMER SUCCESS

You'll be designated a Customer Success representative who will work with you throughout the process and answer any questions you have.

GETTING YOU SET UP ON OUR PLATFORM

Your dedicated Customer Success representative will assist with setting you up on our secure threat management platform. Along with access to additional tools to complement your Penetration Test, the platform is used to communicate and share your test report and findings.

Next your Customer Success representative will work with you to secure and schedule the dates for your Penetration Test. You'll then be required to confirm the scope of works and share any additional target information. Dependent on your test type, this will include:

WEB APP

- URL & IP addresses
- Login credentials for all user roles levels (authenticated tests only)

INTERNAL INFRASTRUCTURE

- Internal URLs & IP addresses
- VPN details, including gateway URL and login credentials

EXTERNAL INFRASTRUCTURE

- External URLs & IP addresses

WIRELESS

- SSIDs/APIs
- On-site address

MOBILE

- Two copies of each mobile application files
- One standard copy
- One without root detection mechanisms and certificate pinning

API

- API info such as endpoints or requests
- Relevant API documentation
- Sample API requests

CLOUD

- Web and API credentials
- Appropriate access granted

SOCIAL ENGINEERING

- Target employee details, including name, email address & telephone numbers (if appropriate)

On the day of the Penetration Test your designated tester will be in contact with your chosen point of contact to confirm the test has started. If any critical issues are identified during the course of the test, you will be notified immediately, otherwise you are unlikely to hear from the tester until the conclusion of the test, unless there are any issues.

We recommend that you have a recent backup of your key systems and data prior to your test date, and let the relevant departments within your organisation know when a Penetration Test is being carried out.

AFTER YOUR TEST

REPORT DELIVERY

On completion of the Penetration Test, your report will be written, passed through quality assurance, and be delivered within five working days. You will receive an email notification when your report is ready to be viewed within your secure platform. This will be visible to your Admin and Tech level users.

THREAT DASHBOARD

The risks identified during your Penetration Test will also be added to your Threat Dashboard. This will enable you to prioritise threats in order of criticality and manage remediations.

RETESTS

We will carry out a re-test where requested, either as part of the service if a re-test is listed on the order form, or if you have ordered a re-test within 30 days of the initial Penetration Test. Any re-test must be scheduled within 30 days of completion of the original Penetration Test.

CYBER SECURITY HEALTH CHECK

Our Cyber Security Assessment provides a comprehensive review of the information security measures in place across your organisation, helping you to understand your cyber risks. The assessment is based on the NIST Cyber Security Framework and the ISO 27001 controls to benchmark your business against universally recognised standards.

As part of the service we will provide an experienced Information Security Consultant to conduct an assessment of your organisation's current level of security. Once completed, we will provide you with a comprehensive report detailing any areas of non-compliance and recommendations on how you can improve your information security practices.

CYBER ESSENTIALS & CYBER ESSENTIALS

We will assist you with achieving certification under the NCSC Cyber Essentials scheme. Support is provided in line with the level of service you have chosen as per the following:

Includes	Cyber Essentials	Cyber Essentials Premium (MOST POPULAR)	Cyber Essentials Plus	Cyber Essentials Plus Premium
Cyber tools required to pass:				
Anti-virus protection	✓	✓	✓	✓
Training	✓	✓	✓	✓
Vulnerability scanning	✓	✓	✓	✓
Phishing simulator	✓	✓	✓	✓
Threat dashboard	✓	✓	✓	✓
Asset tracker	✓	✓	✓	✓
+ more	✓	✓	✓	✓
Cyber Essentials certification	✓	✓	✓	✓
Up to 25k FREE cyber insurance	✓	✓	✓	✓
Cyber Essentials Plus certification	×	×	✓	✓
Tailored policy documents	×	✓	×	✓
Remote support	2 hrs included	4 hrs included	4 hrs included	6 hrs included
Free retest	1 free retest	2 free retests	1 free retest	2 free retests

Free cyber insurance available to UK companies if the basic certification covers the entire organisation. Additional cyber protection and threat management tools for up to 5 users, delivered via the Defense.com SaaS platform.
Remote support is limited via telephone, email or video conferencing. Any additional support time is available at our standard rate.

CERTIFICATION PROCESS

You will need to complete a self-assessment questionnaire which acts as a personal action plan to help you meet the Cyber Essentials requirement. We will then assess your responses against the Cyber Essentials scheme's criteria.

If the completed questionnaire meets the scheme criteria (which is assessed in accordance with the IASME marking scheme), we will notify you in writing and arrange for the issue of your Cyber Essentials certificate. If the questionnaire does not meet the Cyber Essentials scheme criteria (and in accordance with the service level you have selected), we will support you with any areas to address and provide a reassessment.

DATA PROTECTION OFFICER

We will act as the Data Protection Officer (DPO) for your organisation in accordance with the applicable data protection laws and provide the following

- Facilitate your organisation's compliance with the UK/EU GDPR and other applicable data protection legislation by ensuring effective systems and controls are in place to enable you to comply with your legal obligations
- Act as your intermediary between relevant stakeholders, including supervisory authorities, data subjects, and business units
- Inform and advise the board (where appointed to do so) in accordance with our position as DPO of your organisation.

We will provide you with a virtual consultation, information, advice and other related services to ensure that your organisation processes the personal data of its staff, customers, service providers or any other individuals (also referred to as data subjects) in compliance with applicable data protection law and best practice.

SERVICE LEVELS

All service levels apply only from 9:00am to 5:30pm GMT Monday to Friday excluding UK bank holidays. All DPO service requests are handled via email with your allocated DPO and will be prioritised in accordance with the following:

TYPE	DESCRIPTION	RESPONSE TIME
Critical	Scenario which will have serious immediate impact on the protection of personal data	1 hour
Urgent	For advice on GDPR/data protection topics that are subject to time constraints	4 hours
Non-urgent	For advice on GDPR/data protection issues and longer term projects that do not immediately affect your operations	Next business day

GDPR CONSULTANCY SERVICES

We offer a range of GDPR consultancy services to help your organisation achieve and maintain GDPR compliance. One of our GDPR consultants will conduct an initial scoping call to understand your organisation's current level of compliance at a high level. From there, they we will recommend what GDPR services would best fit your needs.

GDPR GAP ANALYSIS

We will provide an experienced GDPR consultant to undertake a Gap Analysis against the requirements of the GDPR. Your Gap Analysis report will then detail the current level of compliance against each of the requirements, along with recommended actions on what needs to be done to achieve compliance. Your Gap Analysis will be conducted via a series of online interviews with key stakeholders, during which your organisation will need to provide documents e.g. policies and procedures that are currently in place for assessment.

GDPR IMPLEMENTATION

A GDPR Implementation project typically follows on from a GDPR Gap Analysis. The purpose of an implementation project is to develop the necessary policies, procedures, processes, and documentation to achieve and maintain GDPR compliance. We take a fully customised approach to GDPR implementations to address your specific business needs.

An experienced GDPR consultant will remotely deliver your implementation project. The service will include the preparation of all required documentation along with advice and support on how to ensure current processes are compliant. Your organisation will need to play an active part in the Implementation through interviews and workshops. An implementation project will also train your staff to ensure data protection becomes second nature throughout your business.

GDPR AUDIT

For organisations that have a good level of GDPR compliance and wish to assess their position to ensure standards are being met. For this service we will provide an experienced GDPR consultant to audit your organisation's current level of compliance against the GDPR. The output of the GDPR Audit will be a report that will outline any non-conformities. During the course of the audit, which will be conducted remotely, your organisation will need to provide access to key staff, documentation and evidence to support the audit.

MANAGED SIEM

Our managed SIEM service combines powerful technology with expert SOC analysts to monitor logs from your applications, systems, networks and users, safeguarding them from cyber threats 24/7/365. Your will receive multi-layered cyber threat intelligence protection that can be deployed anywhere, anytime with smart runbooks and integrated machine learning.

Our Managed SIEM solution has been engineered for fast, seamless integration with your existing infrastructure. Our SaaS delivery model and automated deployment process enables a rapid, low-touch setup for both traditional on-premises infrastructure and modern cloud environments. It features native support for public cloud providers including Azure, AWS and Google and is even designed to work effortlessly with container and serverless technologies.

As part of our Managed SIEM service we provide the following:

LOG INGESTION AND SEARCHING

Our platform supports the ingestion of logs from virtually any source. Search millions of logs in milliseconds, with advanced parsing to help cut through the noise and quickly establish a baseline level of activity. Unlike other providers, we price our service based on the number of nodes that are collecting logs, rather than on a per log basis. This helps to keep costs down, while maintaining a scalable solution that grows with your organisation.

NETWORK & HOST INTRUSION DETECTION (IDS)

Detect and even proactively block malicious traffic and behaviour. Our IDS modules can be host or network based, with our security analysts' expert configuration knowledge and machine learning components combining to deliver a low number of false positives.

FILE INTEGRITY MONITORING (FIM)

Avoid fatigue with an intelligent approach to FIM. Our experienced SOC analysts will fine-tune the configuration to deliver useful alerts on your critical files.

PROCESS MONITORING

We provide a lightweight shipper to install on your servers which audits the activities of users and processes on your systems. For example, you can collect and centralise audit events from the Linux Audit Framework. You can also detect changes to critical files, like binaries and configuration files, and identify potential security policy violations.

WEB APPLICATION FIREWALL (WAF)

Stay protected against common web exploits with our WAF module. By filtering HTTP traffic and watching for potential threats, our solution secures your application against attacks like XSS and SQL injections.

VULNERABILITY SCANNING

Our Managed SIEM solution integrates seamlessly with the Vulnerability Scanning feature within the Defense.com platform, using commercial and in-house built scanning engines.

INTEGRATED MACHINE LEARNING

Our smart machine learning technology detects and analyses suspicious behaviour patterns and automatically creates security events within the SIEM area of Defense.com. It also feeds actionable intelligence to our security analysts, enabling them quick and decisive actions.

RUNBOOKS

Get tailored runbooks to build a profile of what normal behaviour looks like for your business, cutting through noise and reducing false positives. Strong security is not one-size-fits-all, so we offer customised runbooks for all customers.

PROACTIVE THREAT HUNTING

Our team of specially-trained security analysts will proactively hunt for unknown threats in your environment that would otherwise go undetected.

ENDPOINT PROTECTION

Deploy our endpoint protection and anti-virus solution to protect workstations and servers across your organisation. Behavioural analysis and continuous monitoring capabilities allow you to quickly identify and protect against all types of malware, with the capability to isolate compromised devices.

ISO 27001 CONSULTANCY SERVICES

We offer a range of ISO 27001 consultancy services to help your organisation achieve and maintain ISO 27001 certification. One of our ISO consultants will conduct an initial scoping call to understand your organisation's current level of compliance at a high level. From there, they we will recommend what ISO conultancy services would best fit your needs.

Accurate scoping is integral to getting a value-driven, cost-effective project, and Bulletproof take the time to understand your current position and your ISO objectives to create a truly best-fit engagement that delivers real information security benefits, and ISO 27001 certification. Activities can include:

Gap analysis, Implementation activities, internal audits (readiness audits), external audit support and more,

The detailed activities the ISO consultant will do depends on your current compliance status and your available in-house resources.

SOC 2 CONSULTANCY SERVICES

We offer SOC 2 consultancy services to help your organisation achieve and maintain SOC 2 compliance. One of our consultants will conduct an initial scoping call to understand your organisation's current level of compliance at a high level. From there, they we will recommend what SOC 2 consultancy activities would best fit your needs.

Accurate scoping is integral to getting a value-driven, cost-effective project, and Bulletproof take the time to understand your current position and your SOC 2 objectives to create a truly best-fit engagement that delivers real information security benefits, and SOC 2 certification. Activities can include:

Gap analysis, Implementation activities, internal audits (readiness audits), external audit support and more. The detailed activities the consultant will do depends on your current compliance status and your available in-house resources.

NHS DSP TOOLKIT SUPPORT

For organisations needing to complete a NHS Data Security & Protection (DSP) Toolkit submission, Bulletproof provides expert, consultant-led support. One of our data protection consultants will conduct an initial scoping call to understand your organisation's current level of compliance at a high level. From there, they we will recommend what consultancy activities would best fit your needs.

Accurate scoping is integral to getting a value-driven, cost-effective project, and Bulletproof take the time to understand your current position and your DSPT submission scope. The detailed activities the data protection consultant will do depends on your current compliance status, the scope of your submission requirements, and your available in-house resources.

RED TEAMING

Red teaming is an adversarial, threat-led approach to security testing. Red team activities are diverse, which is why Bulletproof take the time to understand your security objectives. We'll create a custom security testing project that will meet your needs, providing insights that are invisible to other types of security testing.

Red Team

Red team penetration testing is the only way to truly gauge how your business' security defences react to a real-world threat. By simulating the resources and tools available to a determined adversary, red teaming reveals security flaws that you didn't know you had. Red teaming is the most comprehensive security test available and demonstrates your commitment to business security.

Purple Team

Purple teaming simulates a wide range of techniques, tactics and procedures in a safe and collaborative way. Both red and blue teams work together to evaluate individual offensive actions commonly taken during a real-world attack, with the goal of remedying any issues. Purple team testing gives you a comprehensive overview of detection and response gaps mapped to industry-standard frameworks, such as MITRE ATT&CK.

Black Team

The aim of black teaming is to gain access to a restricted physical space, such as a particular office or data centre. Bulletproof's skilled back team pen testers will use all tools at their disposal to model a determined, persistent adversary aiming to breach your physical defences. Find out how resistant your people, processes and technology are to social engineering, ethical hacking, tailgating, pretexting and much more.

Assumed Breach

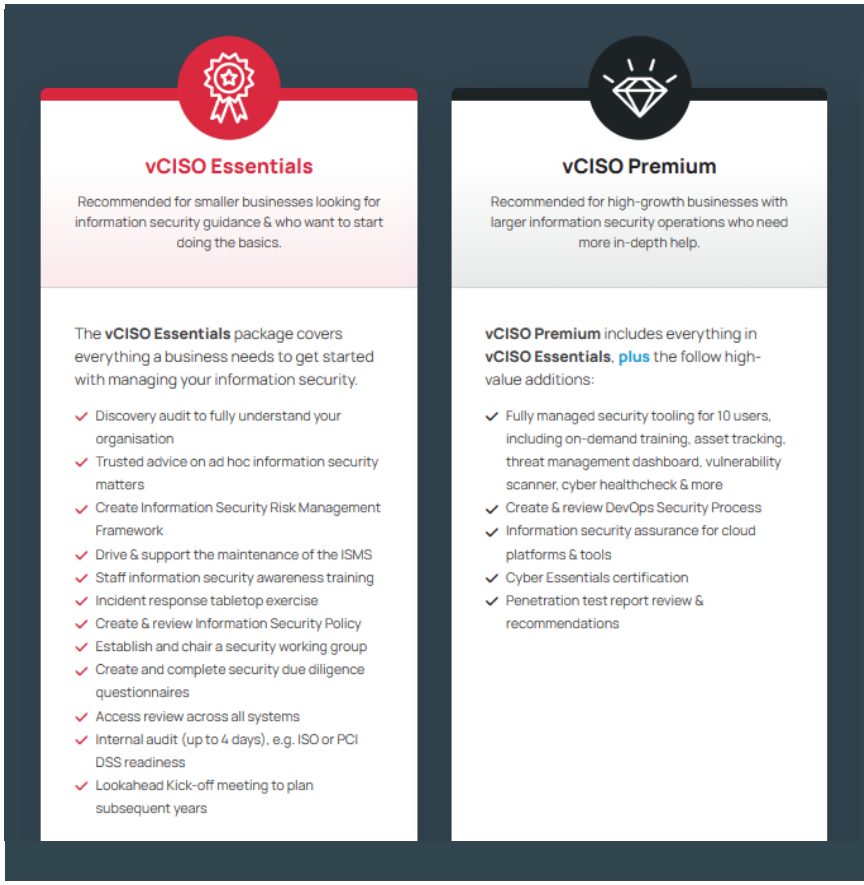
Assumed breach testing operates under the simple principle that a breach can and will happen. It is designed to identify how well your defence in depth would limit a real-world attacker and the effectiveness of protecting your critical business functions. Testing is objective driven and uncovers what an attacker can achieve via device compromise or other attack vector.

EDR/XDR Evaluation

Put your EDR/XDR to the test and determine its efficacy with an expert evaluation from Bulletproof. In-depth configuration and effectiveness reviews of your chosen platforms and technology uncovers weaknesses and help you maximise the effectiveness of EDR/XDR systems. Bulletproof use a test, evaluate & improve approach to put your chosen provider to the test against commodity and bespoke threats.

VIRTUAL CISO

We will provide an experienced, dedicated consultant to act as your vCISO and provide your organisation with ongoing cyber security and information security support. Your vCISO will operate on a retainer basis, meaning as well as providing informative security advice, they will oversee the implementation of projects and maintenance. Bulletproof has flexible packages that deliver effective information security improvements at competitive pricepoints.



vCISO Essentials

Recommended for smaller businesses looking for information security guidance & who want to start doing the basics.

The **vCISO Essentials** package covers everything a business needs to get started with managing your information security.

- Discovery audit to fully understand your organisation
- Trusted advice on ad hoc information security matters
- Create Information Security Risk Management Framework
- Drive & support the maintenance of the ISMS
- Staff information security awareness training
- Incident response tabletop exercise
- Create & review Information Security Policy
- Establish and chair a security working group
- Create and complete security due diligence questionnaires
- Access review across all systems
- Internal audit (up to 4 days), e.g. ISO or PCI DSS readiness
- Lookahead Kick-off meeting to plan subsequent years

vCISO Premium

Recommended for high-growth businesses with larger information security operations who need more in-depth help.

vCISO Premium includes everything in **vCISO Essentials**, plus the follow high-value additions:

- Fully managed security tooling for 10 users, including on-demand training, asset tracking, threat management dashboard, vulnerability scanner, cyber healthcheck & more
- Create & review DevOps Security Process
- Information security assurance for cloud platforms & tools
- Cyber Essentials certification
- Penetration test report review & recommendations

Get in touch

+44 1438 500 500 contact@bulletproof.co.uk