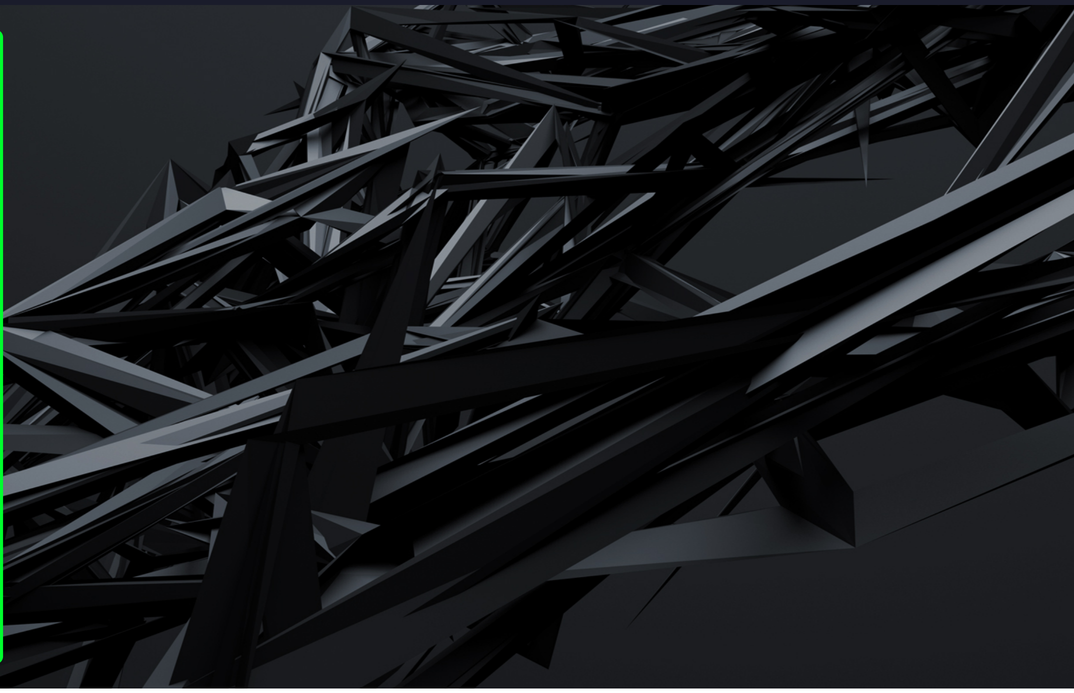
EXPO·e

DATA SHEET

Cyber Security Testing Pack



In an increasingly complex threat landscape, EXPO.e enables your customers and their IT teams to identify and resolve cyber security risks before they affect their core business, boosting their overall cyber resilience. We will provide their organisation with the means to protect against the latest cyber threats, providing monthly external vulnerability scanning, a structured yearly penetration test, testing their users with simulated phishing attacks, and helping them begin the journey to earning Cyber Essentials certification.

EXPO.E'S CYBER SECURITY TESTING INCLUDES:

- Monthly vulnerability scanning of external infrastructure of up to 20 assets – one scan per month, with full reporting for one year
- One-off three-day penetration test
- One-off Phishing Campaign for up to 200 users, with full reporting of results and follow-up training videos
- A one-off Cyber Essentials self-assessment as a baseline certification for architects and consultants. We help secure and protect what your customers value most 24 x 7, allowing them to focus on their core business services.

VULNERABILITY SCAN

Cyber criminals actively seek out exploitable gaps within security, causing substantial damage to brand reputation, finances, and data. It is therefore imperative to conduct regular vulnerability assessments to proactively identify and resolve weaknesses within corporate infrastructure. Our scalable Vulnerability Scanning service examines network perimeters and identifies vulnerabilities by mimicking the actions of the most effective cybercriminals, providing detailed reports and action plans for both management and technical staff.

PHISHING CAMPAIGN

Cyber criminals are becoming increasing aware that humans are the weakest link when it comes to safeguard data. As such, they are employing sophisticated tactics to hit companies' staff via various media. The most common is phishing emails, where they encourage a member of staff to click a bad link which allows them a back door into the company. Phishing Campaign is a flexible service that tests your end users' security awareness, highlighting any areas for improvement and helping foster a cyber security culture at every level of an organisation.

PENETRATION TESTING

Penetration Testing arms your customer with all the information required to optimise their security posture. Our services are tailored to provide comprehensive analysis, advice, and actionable plans, drawing on our consultants' extensive management and business experience that allows them to look at a business as a single entity, instead of a group of disjointed technologies, systems, and departments. Every successful security strategy includes a testing phase to ensure the people, processes and technology deployed are fit for purpose. To assist with this our services include a penetration test which effectively simulates the actions of a threat actor with nefarious motives.

TESTING SERVICE EXAMPLES:

- Penetration Testing of all internal/external infrastructure
- Red Teaming/Brand Damage
- Application Testing
- Mobile App & Device Testing
- Application Code Reviews
- Cloud Testing (AWS, Azure etc.)
- Social Engineering
- API & Web Services Testing
- IoT Security Testing

CYBER ESSENTIALS

Cyber Essentials is a government-enforced industry scheme to help protect against security threats while showing a proactive commitment to cyber security. We can help verify that standards are met and support your customer's accreditation and certification application. This is conducted through the self-assessment included in the pack.

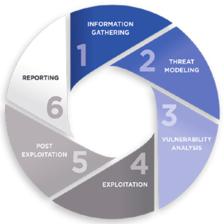
REQUIREMENTS FOR CYBER ESSENTIALS INCLUDE THE FOLLOWING:

- Configuration and firewall protection is used on all devices including those connected to public and untrusted Wi-Fi networks.
- Only software, accounts, and apps that are necessary to the business are used.
- Access is managed efficiently with access and privilege rights given to only those who need it.
- All apps, devices, and software are always kept up to date.
- The scheme addresses and defends against attacks such as hacking, phishing, and password guessing
- All devices which are connected to the internet are ensured that there is protection on confidentially, integrity and availability of data stored on these devices.
- This certification guarantees that a business has put measures in place to protect them from cyber-attacks.

In order to gain a Cyber Essentials certification, an accreditation body will need to be selected. We will help your customer to identify the correct body and verify that all standards are being met. A questionnaire will need to be completed and verified to be awarded with the certificate.

CREST.

CYBER ESSENTIALS PLUS



bsi.

ISO 9001 Quality Management

ISO 27001 Information Security Management

ISO/IEC 20000-1 Information Technology Service Management

CSA STAR Cloud Security

ISO 22301 Business Continuity Management

ISO 50001 Energy Management

ISO 14001 Environmental Management

BS 10012 Data Protection

ISO 27017 Security Controls for Cloud Services

|