DATASHEET

chess® CYBERSECURITY

CyberSecurity Penetration Testing

CREST

CHESS CREST-ACCREDITED PEN TESTS PROVIDE A COMPREHENSIVE REVIEW OF YOUR ORGANISATION'S INFORMATION SECURITY.

Using industry-standard methodologies such as 'The Open Source Security Testing Methodology Manual (OSSTMM)' and 'The Open Web Application Security Project (OWASP)', our engineers will perform an ethical attack simulation which aims to discover areas of concern in your infrastructure, procedures and policies.

Our tailored assessments can cover every aspect of network security from general vulnerability identification to fully exploiting vulnerable web applications.

CYBERSECURITY

SERVICE

Penetration Testing

Contact one of our specialists for more information

Main Switchboard: 01284 788 900 Email: marketing@chessICT.co.uk

“

Our penetration test assists with GDPR compliance.

Article 32 of the General Data Protection Regulation;

"implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing"

What makes our service standout?

We don't outsource assessment work to other countries, we use UK-based engineers who are certified to the highest standards and have proven experience in the field.

Our experience and accreditations and include:

- CREST Approved
- Highly trained Penetration Testers (OSCP, CREST, SANS)
- Field engineers who are experienced and talk your language
- 2 levels of penetration test services to work within your budgets
- Penetration tests follow an established methodology
- Vulnerability Assessments and IT Health Checks

Chess will provide a detailed penetration test report detailing any threats or vulnerabilities found and the recommended remedial actions. Threats and vulnerabilities will be ranked in order of criticality. The report will contain an executive summary explaining the risks in business terms.

Chess is able to offer guidance on remediation of issues and are also provide a number of solutions and services to assist with this.

Business benefits of Chess Penetration Test

- Think like the enemy - identify vulnerabilities from the perspective of a 'black hat' attacker or malicious user
- Improve your business security stance, meet regulatory compliance such as PCI DSS, ISO 27001 and reduce risk of attack and data loss
- Assist with GDPR compliance
- Ensure that due care is demonstrated by your organisation and its directors
- Help to preserve your brand and reputation
- Provide reassurance that your staff are working to best practices
- Help highlight areas that can be improved using your existing security product licenses and technology to achieve return on investment.

Contact one of our specialists for more information

Main Switchboard: 01284 788 900 Email: marketing@chessICT.co.uk

Chess Penetration Testing Methodology

1. PLANNING AND SCOPING
2. RESEARCH, RECONNAISSANCE AND ENUMERATION
3. THREAT ANALYSIS
4. EXPLOITATION
5. REPORTING
6. REMEDIATION

1. Planning and Scoping

Chess will work with your organisation to define the scope of the engagement, if required a certified Chess engineer will work with you to define this scope to ensure that the tests will fulfil your requirements.

2. Research, Reconnaissance and Enumeration

The assigned engineer will attempt to gather information on your organisation. These sources may include the following and will assist in identifying and exploiting any vulnerabilities or weaknesses.

- IP Addresses of Websites and MX Records
- Details of E-mail addresses
- Social Networks
- People Search
- Job Search Websites.

3. Threat Analysis

The objective of this stage is to identify a range of potential vulnerabilities in an organisation's target systems, which will typically involve the Chess Engineer examining:

- Attack avenues, vectors and threat agents
- Results from Research, Reconnaissance and Enumeration
- Technical system/network/application vulnerabilities.

Automated tools and manual testing techniques will be applied at this stage

4. Exploitation

Once vulnerabilities have been identified, Chess Engineers will attempt to exploit them in order to penetrate the targeted system. The phases of this stage are;

Exploit – use vulnerabilities to gain access to a system, e.g. inject commands into an application that provide control over the target.

Escalate – attempt to use the exploited control over the target to increase access or escalate privileges in order to obtain further rights to the system, such as admin privileges.

Advance – attempt to move from the target system across the infrastructure to find other vulnerable systems (lateral movement) potentially using escalated privileges from target systems and attempting to gain further escalated privileges and access to the network.

5. Reporting

Chess will provide a detailed penetration test report, detailing any threats or vulnerabilities found and the recommended remedial actions. Threats and vulnerabilities will be ranked in order of criticality. The report will also contain an executive summary and attack narrative which will explain the risks in business terms. If required, the Chess Engineer can present the report to the key stakeholders within the organisation, this can be covered at the scoping stage.

6. Remediation

The report will provide information on remedial actions required to reduce the threats and vulnerabilities that have been identified. Chess can provide additional consultancy, products and services which can further improve your organisation's overall security stance.

Contact one of our specialists for more information

Main Switchboard: 01284 788 900 Email: marketing@chessICT.co.uk

How much will it cost?

Chess can offer different packages to suit a range of budgets.

Penetration Standard Package

Recommended for organisations where budget is key, we can provide external penetration tests to ensure your external facing infrastructure* is as secure as possible.
**packages based on number of external IP addresses.*

Penetration Advanced Package

Recommended for larger and more complex infrastructures where mission-critical systems are involved, or where a compliance standard is required.

A Chess engineer will fully scope the penetration test which can include every aspect of your infrastructure, including; internal and external penetration testing, web application testing, phishing assessment, patch audit, password audit, firewall audit and physical security/social engineering.

We are also able to offer:

Vulnerability Assessments

An external Vulnerability Assessment is typically used to validate the minimum level of security that should be applied by an organisation. This service can be used as a first step to assess an organisation's security maturity and can be carried out in advance of penetration testing. It does not exploit the vulnerabilities found and does not replicate a real attack. A report will be provided with the vulnerabilities that are found.

IT Health Checks

A limited internal Pen Test, is used to identify vulnerabilities and weaknesses in a limited set of systems. This service can be used as a first step to assess an organisation's security maturity and can be carried out in advance of penetration testing. It does not exploit the vulnerabilities found and does not replicate a real attack. A report will be provided with the vulnerabilities that are found.

Contact one of our specialists for more information
Main Switchboard: 01284 788 900 Email: marketing@chessICT.co.uk

Services Guarantee

All our services come with our unique Services Guarantee:

If you are not satisfied, or if circumstances outside our control prevent the services work being completed, then a Chess engineer will, at no extra charge, complete the work required to your satisfaction or the cost of the service will be refunded.

Chess is a specialist in security solutions, with over **25 years experience**, **33,000 customers** and **3 million licensed users** throughout the UK, all protected by the endpoint security, web security, email security, data security, network security and remote access products and services that we supply.

Chess provides security solutions and services for all sized businesses and public sector organisations and has been Sophos' UK Partner of the Year for ten consecutive years.

Want To Find Out More?

This guide is designed to give general guidance, however EVERY network is unique and we ALWAYS recommend a consultation with a Chess security specialist if you have any concerns or questions.

Contact Us

Main Switchboard
01284 788 900

Website
www.ChessICT.co.uk

Email
marketing@chessICT.co.uk

Head Office
Manor Park, Great Barton
Bury St Edmunds, Suffolk
IP31 2QR, United Kingdom

chess®
CYBERSECURITY