Service Definition Document

Service Definition Document

For

CREST Accredited Penetration Testing Services

Commercial In Confidence

This document is commercial-in-confidence. The recipient of this document agrees to hold all information presented within as confidential and agree not to use or disclose or allow to use or disclosure of the said information to unauthorised parties, directly or indirectly, irrespective of the acceptance or rejection of the presentation or at any time before, during or after an agreement has been reached, without prior written consent.

Contents

What the service is

Phishing Campaigns: Turn Mistakes into Learning

Through targeted phishing simulations that mimic real-world scenarios and the latest phishing trends – think emails that appear to be from your HR or IT department – you can test your team's alertness without pointing fingers. Instead, it's an invaluable learning opportunity.

Types of testing:

- Internal and External Network
- Web Application
- Social Engineering/Phishing
- Website
- Mobile Application
- Threat Modelling

Unlock Deeper Insights, Defend Against Realistic Attacks

- Our threat-led CREST Penetration Testing Services are designed to go beyond tick-box security assessments.
- Our penetration tests mirror real-world attacks, zeroing in on the systems and risks that matter most to your business.
- To get the most out of your testing budget, we suggest focusing on areas critical to keeping your business running smoothly. This gives you a clear picture of how your defences stack up in real-life situations, helping you invest wisely in security.

We believe that to replicate how real-world attacks unfold, penetration tests must go beyond simply examining the security of your systems and applications. You also need to assess the awareness of the people who operate them, and your wider team.

Real attackers leverage both system vulnerabilities and human factors to find the path of least resistance. Attackers often prefer exploiting human psychology over technical flaws because it can provide an easier entry point. Which is why our testing strategy includes social engineering tactics designed to evaluate how your team responds under conditions that mimic real attacker methods.

For instance, alongside a technical penetration test, we may also conduct targeted phishing campaigns. These might focus on team members with administrative access to privileged accounts, assessing whether they can be manipulated into sharing admin credentials.
Once access is obtained, our tests further probe the depth of your defences. We examine whether your "defence in depth" model prevents further penetration or if it allows us to extend our reach within your systems. If access is achieved, will it trigger alarms from detection systems? This approach ensures that you are not only aware of potential entry points but also have effective layers of security and alert mechanisms in place to stop hackers getting any further if they do find a way in.

This approach prepares you for a wide range of threats by addressing both technical and human vulnerabilities, giving you a clearer picture of your security against real-world attacks.

It enables you to fix technical issues like software flaws and enhance cyber awareness within your team through targeted training.

Why choose us as your penetration testing partner?

- CREST Accredited Penetration Testing Company
- OSCP Certified Penetration Testers
- Our commitment to your security doesn't end with the report. We provide expert guidance to help you level up your security posture.
- Our skilled testers apply real-world hacking techniques to assess your security effectiveness, revealing crucial insights for secure business advancement.

- **Step 1: Baseline Phishing Assessment**

We start by evaluating your team's current ability to identify phishing attempts. This initial assessment helps us understand the level of training needed and track progress throughout the programme.

- **Step 2: Tailoring the Campaign**

We work with senior leaders to ensure our phishing simulations use language and terminology that mirrors your organisation’s communication style, preparing for more sophisticated attacks.

- **Step 3: Phishing Simulation**

We launch the phishing campaign with emails that increase in complexity across three rounds, testing employees’ ability to spot these scams.

- **Step 4: Analysis and Training Focus**

After the simulations, we analyse the results to identify weaknesses and areas where targeted cyber awareness training is most needed throughout the continued programme.

The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans

We host all documentation on MS365. We utilise MS365 backup processes which is supported by an external backup system through which we undertake a fully monthly backup of all sites. For BC and DR we test restoration from backup components on a monthly basis.

We also host some testing services in our co-located data centre location. This is also backed up through the backup regime.

Any onboarding and offboarding support you provide

We have a dedicated project office that undertakes a full client onboarding which incorporates meeting all scoped requirements and a signed Terms of Engagement document for client onboarding. This document details any specific dates for the length of the engagement as well as detailed technical IP address level scope information.

For client offboarding we adhere to our IASME Cyber Assurance Level 2 certification which ensures that we carry out a full deletion of any data no longer required. This is based on the type of data held and any contractual requirements that we may have to retain or delete data as necessary.

Service constraints like maintenance windows or the level of customisation allowed

This service is delivered from a combination of cloud based (MS365) and our own co-located data centre services. If during the period of engagement, in the unlikely event of there being any full maintenance windows that we are not in full control of, we can switch between the cloud and data centre hosted services.

Service levels like performance, availability and support hours

Our availability is 8am – 6pm.

After sales support

We provide full support during the period of engagement.

Any technical requirements

We have a dedicated project office that manages all client pre-requisites which also includes any technical requirements.

All pre-requisite documents will be discussed and provided at the point of engagement.

Outage and maintenance management

This service is delivered from a combination of cloud based (MS365) and our own co-located data centre services. If during the period of engagement, in the unlikely event of there being any full maintenance windows that we are not in full control of, we can switch between the cloud and data centre hosted services.

Hosting options and locations

We host all documentation on MS365.

Our service is delivered through a co-located datacentre where we host additional testing services.

Access to data (upon exit)

We adhere to our IASME Cyber Assurance Level 2 certification which ensures that we carry out a full deletion of any data no longer required. Where the client requires access to the data this will be provided as required.

The deletion or provision of data is based on the type of data held and any contractual requirements that we may have to retain or delete data as necessary.

Security

As a dedicated Cyber Security organisation, we ensure that all the information we create, hold or share is done so securely. We are Cyber Essentials and Cyber Essentials Plus certified as well as being IASME Cyber Assurance Level 1 and 2 certified.

We carry out regular penetration testing and vulnerability scanning.