Simulated Targeted Attack (“Red Teaming”)

Service Definition for the G-Cloud 10 Framework

Overview

We are a supplier of Simulated Targeted Attacks (“Red Team” exercises) under the CREST STAR scheme. A Simulated Targeted Attack is guided by relevant threat intelligence and aims to emulate a real-world attack using the same tactics, techniques and procedures as your adversaries.

Each Simulated Targeted Attack is tailored to the threat profile of your business, and the risks that you face specifically. We target people, process and technologies to gain a holistic picture of your resistance to attack. A key benefit of a Simulated Targeted Attack is that it will allow you to assess your incident detection and response capabilities in a realistic setting – identifying gaps in technical control coverage and highlighting training and development needs for your teams.

Personnel

Our consultancy team is highly-qualified and very experienced, holding certifications including CREST Simulated Attack Specialist and CREST Simulated Attack Manager. Each Simulated Targeted Attack engagement will be overseen in full by a certified Simulated Attack Manager.

Tests are undertaken by experienced CHECK/CREST accredited staff, with HMG SC Clearance.

We have considerable experience working on Simulated Targeted Attack engagements across a wide variety of industry sectors.

Simulated Targeted Attack Engagement Model

Our Simulated Targeted Attack engagements are tailored to the unique requirements of the prevailing threat environment, the organisation and/or the Accreditor, and other related stakeholders. During an initial scoping meeting, we will discuss the engagement objectives, the scenarios and threats of particular interest and the types of attack that may be considered.

Following this initial scoping meeting, we will produce a formal Scope of Work within a commercial proposal which will be subject to customer review and acceptance. Engagements are priced on a day rate basis – see the Pricing document for more information.

The first stage of a Simulated Targeted Attack is generally a detailed attack specification process, which will commence once our commercial proposal has been accepted. Threat intelligence will be reviewed where available, and different approaches towards meeting the business objectives of the exercise will be discussed with relevant stakeholders.

By the end of this exercise, the rules of engagement will be established, together with details of the exercises that will be performed, the targets that will be used and the reporting mechanisms which will be in place. Criteria for ‘success’ or ‘failure’ of the exercise will also be determined at this point, along with break points where appropriate for review and repositioning. We will also conduct a risk assessment of the agreed attack plan and advise of any risk mitigation measures which should be enacted.

Once an agreed attack plan is in place, our simulated attack team will enact the plan according to the agreed rules of engagement and in accordance with the risk assessment conducted.

Activities during a Simulated Targeted Attack vary, but a typical Simulated Targeted Attack may involve some or all of the following activities:

- Penetration testing and targeted exploitation of perimeter network devices
- Exploitation of web application vulnerabilities
- Generic phishing attacks or spear phishing attacks against staff
- Physical building intrusions and the introduction of physical implants
- Targeting of customer-facing people and processes, such as sales functions or online portals

- Targeting of business operation functions such as Finance and HR departments
- Exploitation of workstation misconfigurations and/or software vulnerabilities
- Privilege escalation
- Lateral movement through an internal network
- Data exfiltration and action on agreed objectives

The results of a Simulated Targeted Attack can be fed into your organisation's risk management process and can help to shape your organisation's information security strategy. A full review of activities and control points following a Simulated Targeted Attack can be extremely helpful to internal technical teams tasked with incident response activities.

Our consultants have many years of experience working with industry and government, and will help you contextualise the risks identified, offering constructive and pragmatic remediation advice.

Service Management

We operate a service management process that is integrated with our ISO 9001 quality management system.

All projects are assigned a lead consultant and a project manager throughout delivery of the testing. We operate an escalation procedure in the event of unresolved client dissatisfaction; at the time of G-Cloud 10 submission, this procedure has never been used.

Service Constraints and Levels

We do not have service constraints and levels, other than those specifically tailored and agreed in each 'Scope of Work' within a proposal.

Financial Recompense

We do not have a formal recompense model; as part of our ISO 9001 certification and commitment to customer service, we monitor the quality and delivery of all testing services very carefully.

Training

Training is offered in several of the testing service disciplines we offer; we are happy to discuss training options with our customers.

Ordering and Invoicing Process

Our normal process is to produce a 'Scope of Work' within a commercial proposal and once acceptance is given (through a signed order form or purchase order) we will commence the scheduling process.

Fixed price projects are invoiced on acceptance of the deliverables of each work task. Projects undertaken on a time and materials basis are invoiced monthly in arrears. We are happy to discuss the ordering and invoicing process with our customers.

Termination Terms

Refer to the separate 'Terms and Conditions' document.

Data Restoration / Service Migration

Data restoration and service migration is not included in our price.

Customer Responsibilities

All customer responsibilities will be defined in the 'Scope of Work' for each engagement/project.

Technical Requirements

All technical requirements and service dependencies are discussed with the client during scoping, as in most cases each project has different requirements. Technical requirements and testing pre-requisites will be documented in the 'Scope of Work' within the proposal.