CNS
at Six Degrees

RED TEAMING

Gain total visibility of your organisation's vulnerabilities through the eyes of a hacker.

Six Degrees' Red Teaming services take testing your organisation's cyber resilience to a whole new level. Through a range of techniques including phishing, scenario testing, and physical and social security compromise, Red Teaming allows you to gain total visibility of your organisation's vulnerabilities through the eyes of a hacker.

Whether you are looking to understand more about specific risks or want a general view of your organisation's cyber security posture, Red Teaming delivers critical insights by taking a real-world approach to infiltrating your organisation, following the sophisticated methods hackers use every day.

Six Degrees' Red Teaming service is the ultimate test of your organisation's cyber security posture, giving our Security Testing Team free reign to launch customised technical and physical, simulated real-life attacks within any date or time during the testing period. The simulated attack activities performed by the 'Red Team' leverage the full scope of Six Degrees' security testing capabilities.

Once areas of weakness are identified, our expert Penetration Testers provide guidance around how each weakness can be mitigated – delivering a roadmap to enhancing your organisation's cyber security posture.

Our Red Teaming services are provided by some of the most highly experienced and accredited Penetration Testers in the industry. We are members of the National Cyber Security Centre (NCSC) CHECK scheme, and our team members and leaders are certified under CREST and the Cyber Scheme.

"Red Teaming delivers critical insights by taking a real-world approach to infiltrating your organisation..."

Red Teaming Benefits

Understand where you need to invest resource to ensure adherence to compliance and accreditation standards.

Receive clear, easy to understand reports that include remediation advice.

Work with a cyber security partner who can support you through mitigating actions.

Why Choose Six Degrees for Your Red Teaming Testing

20

Over 20 years of cyber security heritage and experience.

SC cleared, UK-based Penetration Testers.

CHECK, CREST and Cyber Scheme certified.

Tailored testing that suits your organisational requirements.

Access to complementary testing, consultancy, and managed security services.

Service Credentials

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CREST

THE CYBER SCHEME
OFFICIAL CYBER SCHEME SPONSOR

Six Degrees Credentials

Member of Microsoft Intelligent Security Association
Microsoft

CERTIFICATION BODY
CYBER ESSENTIALS PLUS

ISO 27001

CNS at Six Degrees

For more information about our Red Teaming services, please contact sales@6dg.co.uk or call 0800 012 8060.

1. Service Overview

The Red Teaming Service is performed by our Offensive Security team, which includes our CHECK Team Members ("CTM") and Leaders ("CTL"), certified under CREST, TigerScheme and Cyberscheme, along with our Threat Intelligence Professionals, Incident Responders and Social Engineers.

As part of the Service, we will perform a Red Team exercise, where we will scope the rules and safeguards that will be applied for you, prepare and complete the exercise, produce a report of the outputs and provide advice to address items in the report.

1.1 The Red Team Exercise

The exercise allows you to interact with our Offensive Security team to build a set of customised, real-life attacks or simulations that are contextual and meaningful to your organisation, as well as the industry vertical that you are working within.

The simulated attack activities performed by the Red Team often involve, but are not limited to, threat intelligence analysis, penetration testing, Malware and Phishing attack execution, hardware hacking or social engineering to identify and assess how the target performs and reacts within the confines of the given situation.

We will agree the Targets with you before any testing commences in accordance with your requirements.

1.2 Report

We will provide you with a report setting out the results of the exercise and what the potential impact of any compromises could have been. The report may also include details of how your defensive solutions mitigated against the attack.

During this stage we will present you the results of the engagement, which you will review in conjunction with your nominated Blue Team and/or stakeholders.

1.3 Advice

The report will include advice on actions and steps you can take to remediate and remove vulnerabilities.

The results and advice will be presented in a workshop where you will have the opportunity to ask questions and clarification on complicated elements of the test.

2. Service Deliverables

Although the nature of the Red Teaming Service is highly customisable, it is designed to work in stages and its length may be configured to meet your requirements.

We will work with you ahead of the engagement to understand and agree the scope of the Red Team exercise and the associated timeframes. These details will be captured in a Terms of Reference ("ToR") document which we will provide you ahead of any part of the engagement.

The Red Team exercise will be limited to the agreed scope detailed in your ToR. If additional time or requirements are identified during the Red Teaming process, we will endeavour to meet your requirements, however the applicable Fees may be adjusted to reflect the increased time and/or resources needed. If additional time or requirements are identified during the Red Teaming exercise, we will discuss these details and the associated applicable Fees to reflect the increased time and/or resources needed before proceeding.

The Red Team exercise will provide standard information around potential vulnerabilities such as outdated software and unpatched systems or security misconfigurations, but may also identify vulnerabilities in your physical security, supply chain, operational processes and your staff. The test will seek out information about your organisation and interrogate the dark web to identify leaked information which could be leveraged and used to infiltrate your organisation and cause operational disruption.

Once the Red Team exercise is completed, the Offensive Security team will provide a report, which we will then review with you to explain how we gathered information, identified a weakness or threat and how we leveraged this to gain access to your systems. Our team will then proceed to advise what could have been carried out from this point and the potential damage that an adversary could have caused.

Although Red Teaming leverages a variety of methods that attackers would use, our team will not compromise your operational ability and will discuss with you any potential risk associated with the test. This Service does utilise the same techniques as a real-life attack would, and therefore, unless otherwise agreed, attacks such as Denial of Service or data manipulation may be utilised in order to further traverse the network.

As a standard, we will perform the initial engagement in accordance with the table below:

Stage	Overview
Pre-Engagement	We will schedule time with you to plan and understand more about the physical Targets, assets of interest and core data. We will work with you to understand and define the boundaries of the Red Teaming engagement and the safeguards that can be put in place to remain within the agreed limits. Our team will walk you through each element of the engagement to ensure these are clearly understood by both parties. In order for the exercise to provide the most accurate results, it is important that details of the Red Teaming exercise are not distributed to the wider business. We recommend that the pre-engagement process is limited to critical, senior stakeholders only.

Setup	This phase will take place over approximately a four (4) week period. Within this period, extensive reconnaissance work will be carried out against Targets of interest (such as websites, buildings, stores, networks, administrative endpoints, VPN endpoints etc.) to determine the most successful strategy for exploitation. During this stage, our Read Team will prepare tool kits, exploits, and physical attack plans. The length and resources used during this phase is dependent on the agreed scope of works and the complexity of the engagement, as documented in your ToR.
Execution	This phase will take place over approximately an eight (8) week period and will involve the targeting of systems identified in the setup stage as well as making use of the strategies and tooling developed during the setup stage. The purpose of the execution stage is to complete the attack strategy resulting in the attainment of access to the assets/data of interest, as agreed with you during the pre-engagement stage. The length and resources used during this phase is dependent on the agreed scope of works and the complexity of the engagement, as documented in your ToR.
Assumed Compromise and Remediation	This phase is reached when the Targets have been compromised or indeed the defensive, protective measures and services employed have protected the Targets from attack within the agreed time and effort. Our Red Team will produce a report detailing the activities they undertook and the outcome of these. As part of this stage, your nominated Blue Team can review the findings and discuss how the compromises were made, what the impact of these compromises could have been and how you can address these issues to mitigate against the risks of the identified vulnerabilities. The workshop is interactive and will give you the opportunity to ask questions about the test and the actions that need to be taken.

2.1 Pre-Engagement

During the pre-engagement stage, we will perform the following activities:

(a) We will define the boundaries of the engagement based on the information provided by you, including:

(i) Who can be targeted within your organisation and whether there are any limits in terms of a subset of employees;

(ii) Where the test should be conducted and whether we can target all sites and locations or limit the test to UK-based sites only or particular sites of interest;

(iii) When the test can be performed and whether there are any time periods during which we should not be conducting reconnaissance or attempting to execute and compromise your environment;

(iv) What do we do to identify ourselves in the event that we are approached or accused of illegally trying to breach your organisation security and what measures will you put in place to safeguard our team.

(b) Defining the scope and identify the primary Targets in scope, which could include:

(i) Accessing buildings, offices or otherwise secure locations;

(ii) Obtaining critical business information (e.g. information about your technical architecture or confidential data);

(iii) Compromising systems, such as your firewalls, active directory, core network, critical databases, websites, applications, email systems or endpoints;

(iv) Manipulation of your staff to understand whether we can socially engineer team members, how susceptible you are to Phishing, and if your employees make mistakes when it comes to good security process.

(c) Defining the context and build an understanding of the value of your assets, systems, resources and data, what are the most critical systems for your organisation, who are the most important people, what would cause the most disruption and have the greatest financial impact if it was compromised or unavailable. This will allow us to put the findings in our report into context for your business.

We will also agree the levels of communications and updates that you will receive during the delivery, which can range from no communication until the execution phase has completed, through to communication ahead of any activity. It is preferable to minimise all communications to simulate as close to a real-world attack as possible.

(d) Defining timeframes by taking into consideration any boundaries that we have identified. The definition of timeframes is a key element of the engagement. Timeframes can be:

(i) Controlled, in which event we will provide a timetable of activities;

(ii) Uncontrolled, in which event we will decide (within the boundaries of the test) when to launch the attacks and conduct the reconnaissance work. Uncontrolled with minimal or no boundaries is preferential as it provides a more accurate and true representation of a real-world attack.

We will determine and provide you details of the estimate amount of time required to complete each stage. Such details will include a minimum and maximum period of time in which the activities can be completed.

2.2 Setup

The setup phase will be tailored to your requirements and customised based on the agreed scope. The activities that the Offensive Security team will undertake may vary and involve the use of new tools or approaches based on the latest attack methods that malicious actors are employing.

Typically, the setup stage includes the activities listed below. Please note that this list is not exhaustive and the activities may vary depending on your requirements.

(a) Fake domain name registration;

(b) SSL certificate registration - allowing a period of time to assure certificate distribution;

(c) Social media account setups - fake accounts, exploratory exercises to support target identification;

(d) Phishing email template construction based on the reconnaissance work to identify systems of shared interest, topics of interest for targeted individuals etc;

(e) Physical attack plans - back story setup, prop setup, building schematic analysis;

(f) Malware creation - bespoke situations or scenarios;

(g) Technical aids - construction/configuration (where applicable) of hardware (e.g. bugs, hardware Key Loggers, Data Miners, remote dial out devices).

The amount of time required to complete the setup stage is dependent on the scope of the test. Typically, around 40-50% of the available resource time is used during this stage. Details of the estimate amount of time required for your test will be included in your ToR.

2.3 Execution

This stage is extended over a greater period of time to allow for typical and known evasion techniques to be used and to mimic real-world attack scenarios.

We will agree with you the duration of this stage. Our Offensive Security team will recommend a suitable timeframe, however this can be reduced if faster results are required or extended to increase the Red Team's opportunities to avoid detection. In either case, we will agree with you the minimum and maximum amount of time allowed for the execution stage during the pre-engagement stage.

The execution stage will be focused on attaining access to the items identified in the pre-engagement and setup stages as test goals, core data and Targets.

Typically, the execution stage includes the activities listed below. Please note that this list is not exhaustive and the activities may vary depending on your requirements:

(a) Physical targeting of client locations (e.g. offices, distribution centres, call centres etc.) using a variety of social engineering attacks;

(b) Adding physical devices to accessible equipment in key areas (e.g. Key Loggers, network packet capture devices, remote access devices etc.);

(c) Phishing emails;

(d) Malware engineering;

(e) Website hacking;

(f) External/internal network infrastructure hacking;

(g) Vishing - social engineering via phone call;

(h) SMSishing - social engineering via SMS messages;

(i) Exploitation of known vulnerabilities on external/internal IT systems;

(j) Exploitation of Zero Day/custom vulnerabilities on external/internal IT systems.

During the execution stage, you have the option to either be informed of the planned activities before execution or assume an entirely reactive role in defence. We recommend the latter approach for Red Teaming engagements. The levels of interaction will be agreed with you during the pre-engagement stage.

The amount of time required to complete the execution stage is dependent on the scope of the test. Typically, around 40-50% of the available resource time is used during this phase. Details of the estimate amount of time required for your test will be included in your ToR.

2.4 Assumed Compromise

Within this phase it is assumed that either the execution stage has been completed successfully, or the pre-agreed timeframes for the execution stage have expired. In either case, we will provide you with a report setting out the results of the compromises, what the potential impact of these compromises could have been and what is needed to remediate and remove vulnerabilities. The report may include information around why the planned compromises failed, and details of how your defensive solutions mitigated against the attack and what an attacker may have attempted to do to get around your solutions if they had more time.

During this stage we will present you the results of the engagement, which you will review in conjunction with your nominated Blue Team and/or stakeholders. The results will be presented in a workshop where you will have the opportunity to ask questions and clarification on complicated elements of the test.

As a standard, the workshops will cover:

(a) Technical detail on how the compromises were made;

(b) Identification of the core issues that lead to the compromises;

(c) Recommendations on eradication and detection of the events that lead to the compromises;

(d) Retesting of the events that lead to the compromises following remediation to ensure the loop is closed between the Blue and Red Teams;

(e) A PDF report of the engagement will be produced and made available during the workshop meeting.

We usually deliver one (1) day engagement for the assumed compromise stage, however the relevant timeframe will be agreed with you based on your requirements and documented in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
Stage 1: Pre-Engagement		
Setup pre-engagement meetings to agree the scope of the Service.	●	
Prepare and define acceptable physical Targets, assets of interest and core data. These will be used within the scope as measurements of successful compromise.		●
Stage 2: Setup		
Subject to successful completion of the pre-engagement stage, we will commence reconnaissance on the agreed Targets.	●	
Upon target identification, we will identify the appropriate methods of exploitation and plans of attack.	●	
We will assemble any tooling (bespoke or off the shelf) required during the execution stage, such as software and certificates, in line with the agreed attack plan.	●	
Stage 3: Execution		
You will ensure escalation paths are clearly defined and permission letters are signed off by the relevant authority within your organisation before the attack execution.		●
We will execute each attack as agreed in the attack plan.	●	
We will notify you without undue delay should an attack be successful. In such event, we will provide you remediation advice to mitigate the risk of exposure to an exploitable threat.	●	
Stage 4: Assumed Compromise		
You will define the members of your Blue Team and ensure their time is cleared for attending the assumed compromise workshop. We will schedule the workshop meeting at a mutually agreeable time.	●	●
We will provide you the PDF report of the engagement, which will include details of the compromises identified and suggested remediation actions.	●	
Workshop meeting between the Blue Team and the Red Team.	●	●

All service delivery work will be carried out during Business Hours, unless otherwise agreed with you in your ToR. We will invoice additional Fees for any work requested to be undertaken out of hours. We reserve the right to charge additional Fees for any change in your requirements occurring during or after the implementation of the Service and outside the scope of the contract (as described in the MSA).

4. Billing

Each stage of your Service will be billed as a Non-Recurring Fee as described in our Billing Guide and as indicated in your Order Form and/or SOW. Such Fees will be defined based on the scope of the Service, the size of your environment, and the relevant timeframes agreed with you.

4.1 Additional Fees

We reserve the right to charge additional Fees in the following situations:

(a) Any work carried out outside business hours; and

(b) Any change in your requirements occurring during or after the implementation of the Service and outside the scope of the contract (as described in your MSA).

5. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

6. Dependencies

We provide the Read Teaming Service subject to the following dependencies:

6.1 Client Obligations

(a) You will provide us details of your Targets and any required information around scope (*e.g.* scope boundaries, date Targets, stakeholder/employee Targets, intellectual property Targets, etc.);

(b) You will provide us written authority and approval to carry out the tests, which may be presented to authorities both within your organisation and publicly, in the event that any of our team members are question around the operations that we are carrying out;

(c) You will assure the safety of our operatives at all times.

6.2 Service Dependencies

(a) The Service and the accuracy of the Red Team exercise is dependent on the level of details provided by you during the pre-engagement stage.

7. Exclusions

(a) The excluded items described below are outside the scope of this Service Description: The Service provides an overview of the security and resilience of your environment and your response capabilities. The Service is not designed to provide a comprehensive threat and breach prevention solution and should be used as part of a wider approach to risk mitigation.

(b) You acknowledge that we have no control over the resilience and the security of your environment and, therefore, we shall not be liable for any events, security issues, data

losses, compliance issues or performance degradation resulting from or in connection with the activities carried out by our Red Teaming as part of this Service

8. Definitions and Acronyms

8.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client. The terms listed have the following meanings:

Term	Meaning
Blue Team	A defensive, protective team, responsible for the identification of potential attackers and indicators of compromise.
CHECK	NCSC approved penetration test companies and methodology used to conduct penetration tests.
CREST	Internationally recognised certification body that provides the professional level examinations and certifications for our Cyber Security professionals.
CyberScheme	The Cyber Scheme is one of only three organisations accredited by GCHQ/NCSC to offer examinations that meet UK Government Standards in penetration testing.
Data Miners	Tools that extract and discover patterns in large data sets that can be used to extract critical and useful information.
Key Loggers	Hardware or software devices that record a user’s keystrokes, often used to record and steal user credentials.
Malware	Software specifically designed to disrupt, damage or gain unauthorised access to computer systems.
Phishing	Attempt to extract information and/or credentials from individuals/employees via email campaigns.
Red Team	An offensive, attacking team, looking for weaknesses or vulnerabilities to leverage through various methods and tools.
SMSishing	Attempt to extract information and/or credentials from individuals/employees via SMS/text message campaigns.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines.
Targets	People, data, systems, applications, buildings, assets or any other item that is considered valuable, confidential or essential for business operations.
Tigerscheme	Commercial certification scheme for technical security specialists.
Vishing	Attempt to extract information and/or credentials from individuals/employees via telephone/voice call campaigns.
Zero Day	A yet to be executed attack derived from a previous method or leveraging a new approach never seen before.

8.2 Acronyms

Acronym	Meaning
IT	Information Technology
MSA	Master Services Agreement
PDF	Portable Document Format (Accessible with Adobe Reader)
SMS	Short Message Service (text message)

Acronym	Meaning
SSL	Secure Sockets Layer
SoW	Statement of Work
ToR	Terms of Reference
VPN	Virtual Private Network

9. Operational Targets

N/A