

**{services\_list}**

The increase in cyber-attacks has driven companies to rethink their security strategy. Some of your most valuable assets are online and need to be protected against external and internal threats.

Red Team Partners will help you in this ever-changing landscape. With a worldwide team of cyber security experts combined with the latest technology and processes, Red Team Partners will partner with you to make sure your digital assets are protected. We understand how hackers and external threats can harm your organisation; that’s why Red Team Partners will provide you with an insight into how these risks can be remediated.

TABLE OF CONTENTS

[TEST AUTHORISATION & ORDER FORM 11](#_Toc189061633)

[PROJECT SUMMARY 13](#_Toc189061634)

[STATEMENT OF WORKS 14](#_Toc189061635)

[Scope 14](#_Toc189061636)

[Details of Scope 14](#_Toc189061637)

[Tester's Note 16](#_Toc189061638)

[Pre-Test 18](#_Toc189061639)

[Assessment 18](#_Toc189061640)

[Post-Test 18](#_Toc189061641)

[RTP Robin Platform (included in all packages) 19](#_Toc189061642)

[COSTING 20](#_Toc189061643)

[TOOL LIST 23](#_Toc189061644)

[METHODOLOGY 24](#_Toc189061645)

[REPORTING 25](#_Toc189061646)

[DELIVERY STEPS 28](#_Toc189061647)

[TIMESCALES 28](#_Toc189061648)

[WHY CHOOSE RED TEAM PARTNERS? 29](#_Toc189061649)

[OUR QUALIFICATIONS 30](#_Toc189061650)

[Company 30](#_Toc189061651)

[Testers 30](#_Toc189061652)

[OUR SERVICES 31](#_Toc189061653)

[33](#_Toc189061654)

[GET IN TOUCH 33](#_Toc189061655)

# TEST AUTHORISATION & ORDER FORM

|  |  |
| --- | --- |
| **SC** |  |
| **TYPE OF ASSESSMENT(S)** | {#cyberthreatintelligence }  Cyber Threat Intelligence  {/cyberthreatintelligence }  {#iso27001certification}  ISO 27001 Certification  {/iso27001certification}  {#mobileapplicationtesting}  Mobile Application Testing  {/mobileapplicationtesting}  {#phishingsimulation}  Phishing Simulation  {/phishingsimulation}  {#redteamassessment}  Red Team Assessment  {/redteamassessment}  {#securecodereview}  Secure Code Review  {/securecodereview}  {#silversubscription}  Silver Subscription  {/silversubscription}  {#firewallreview}  Firewall Review  {/firewallreview}  {#vulnerabilityassessment}  Vulnerability Assessment  {/vulnerabilityassessment}  {#apipenetrationtesting}  API Penetration Testing  {/apipenetrationtesting}  {#bronzesubscription}  Bronze Subscription  {/bronzesubscription}  {#cloudassessment}  Cloud Assessment  {/cloudassessment}  {#cyberawareness}  Cyber Awareness  {/cyberawareness}  {#cyberessential}  Cyber Essential  {/cyberessential}  {#cyberessentialsplus}  Cyber Essentials Plus  {/cyberessentialsplus}  {#goldsubscription}  Gold Subscription  {/goldsubscription}  {#infrastructuretesting}  Infrastructure Testing  {/infrastructuretesting}  {#wapt}  Web Application Penetration Testing{/wapt} |
| **RECOMMENDED START DATE** |  |

|  |  |
| --- | --- |
| **COMPANY NAME** | Red Team Partners |
| **CONTACT NAME** | {manager\_name} |
| **NUMBER** | {manager\_contact} |
| **EMAIL** | {manager\_email} |

|  |  |
| --- | --- |
| **COMPANY NAME** | {company\_name} |
| **CONTACT NAME** | {client\_name} |
| **NUMBER** | {company\_number} |
| **EMAIL** | {client\_email} |

This proposal has been prepared exclusively for {company\_name} and contains information that should be considered the confidential property of Red Team Partners.

Red Team Partners gives permission to internally and to any other body where Web Application Penetration Testing is required to do so by applicable law or regulation. Other than as permitted by the foregoing, this proposal must not be disclosed to any third party.

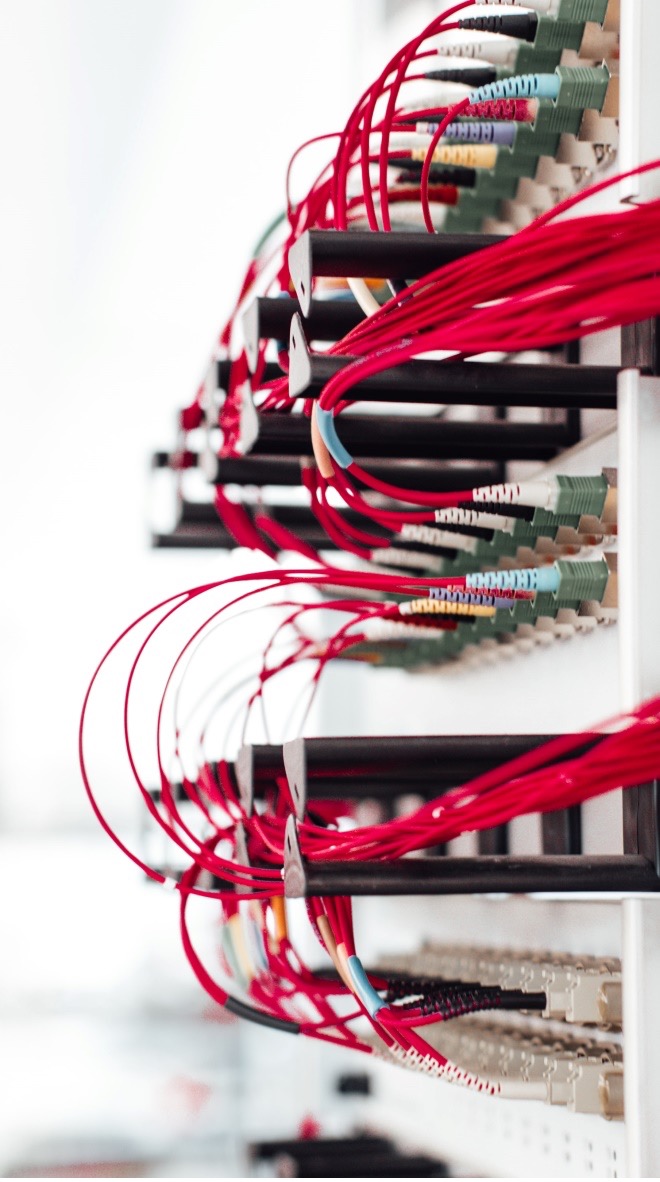
# PROJECT SUMMARY

{company\_name} has requested Red Team Partners to conduct {services\_list} to identify any potential risk and suggested remediations.

Red Team Partners has a team of specialists with rich experience in assessing security postures and finding vulnerabilities in organisations that are driving a cyber security strategy. Red Team Partners' world class team focuses exclusively on some of the most important cyber security movements within an organisation involving implementation, systems, infrastructure, and applications.

Red Team Partners is positioned as a partner of {company\_name} to help work together in assisting the security and maturity of the organisation. Our worldwide team of specialists allows us to work within timeframes that best suit you, including a 24-hour turnaround time for those immediate scenarios.

For {company\_name}, we understand the security of your assets is a vital process in your business. A breach can have a catastrophic impact on your brand reputation and overall revenue. Red Team Partners has been approached to conduct the following service(s) – {services\_list} which will allow {company\_name} to understand vulnerabilities and risks including concise actions and how to address them.



Red Team Partners will act as your partner (It's in the name). Our team of world-class experts will provide a customized test based on your requirements and deliver a clear roadmap of recommendations for a change. We confidently update our world-class methodologies and technologies to combat new threats.

# STATEMENT OF WORKS

Red Team Partners will provide the services described in this scope. A final Statement of Works will be provided by the delivery team once the proposal has been accepted. Understanding Web Application Penetration Testing's environment is key to performing the correct assessment. This section will contain the type of assessment requested.

## Scope

{company\_name} has requested Red Team Partners to conduct cyber security assessment for their company. Red Team Partners and {company\_name} have identified the need the following services: {services\_list}. These services have been based on the discussion conducted with Test.

## Details of Scope

Company has identified the following parameters for the test:

|  |
| --- |
| **Service(s)** |
| * {#cyberthreatintelligence} * Cyber Threat Intelligence * {/cyberthreatintelligence} * {#iso27001certification} * ISO 27001 Certification * {/iso27001certification} * {#mobileapplicationtesting} * Mobile Application Testing * {/mobileapplicationtesting} * {#phishingsimulation} * Phishing Simulation * {/phishingsimulation} * {#redteamassessment} * Red Team Assessment * {/redteamassessment} * {#firewallreview} * Firewall Review * {/firewallreview} * {#securecodereview} * Secure Code Review * {/securecodereview} * {#silversubscription} * Silver Subscription * {/silversubscription} * {#vulnerabilityassessment} * Vulnerability Assessment * {/vulnerabilityassessment} * {#apipenetrationtesting} * API Penetration Testing * {/apipenetrationtesting} * {#bronzesubscription} * Bronze Subscription * {/bronzesubscription} * {#cloudassessment} * Cloud Assessment * {/cloudassessment} * {#cyberawareness} * Cyber Awareness * {/cyberawareness} * {#cyberessential} * Cyber Essential * {/cyberessential} * {#cyberessentialsplus} * Cyber Essentials Plus * {/cyberessentialsplus} * {#goldsubscription} * Gold Subscription * {/goldsubscription} * {#infrastructuretesting} * Infrastructure Testing * {/infrastructuretesting} * {#wapt} * Web Application Penetration Testing * {/wapt} |

***Additional Services:***

{#premium\_service}

* Premium Services/Quick Delivery (within 2 weeks)

{/premium\_service}

{#evening\_test}

* Evening Test (After 6pm)

{/evening\_test}

{#weekend\_holiday}

* Weekend/Holiday

{/weekend\_holiday}

{#onsite\_delivery}

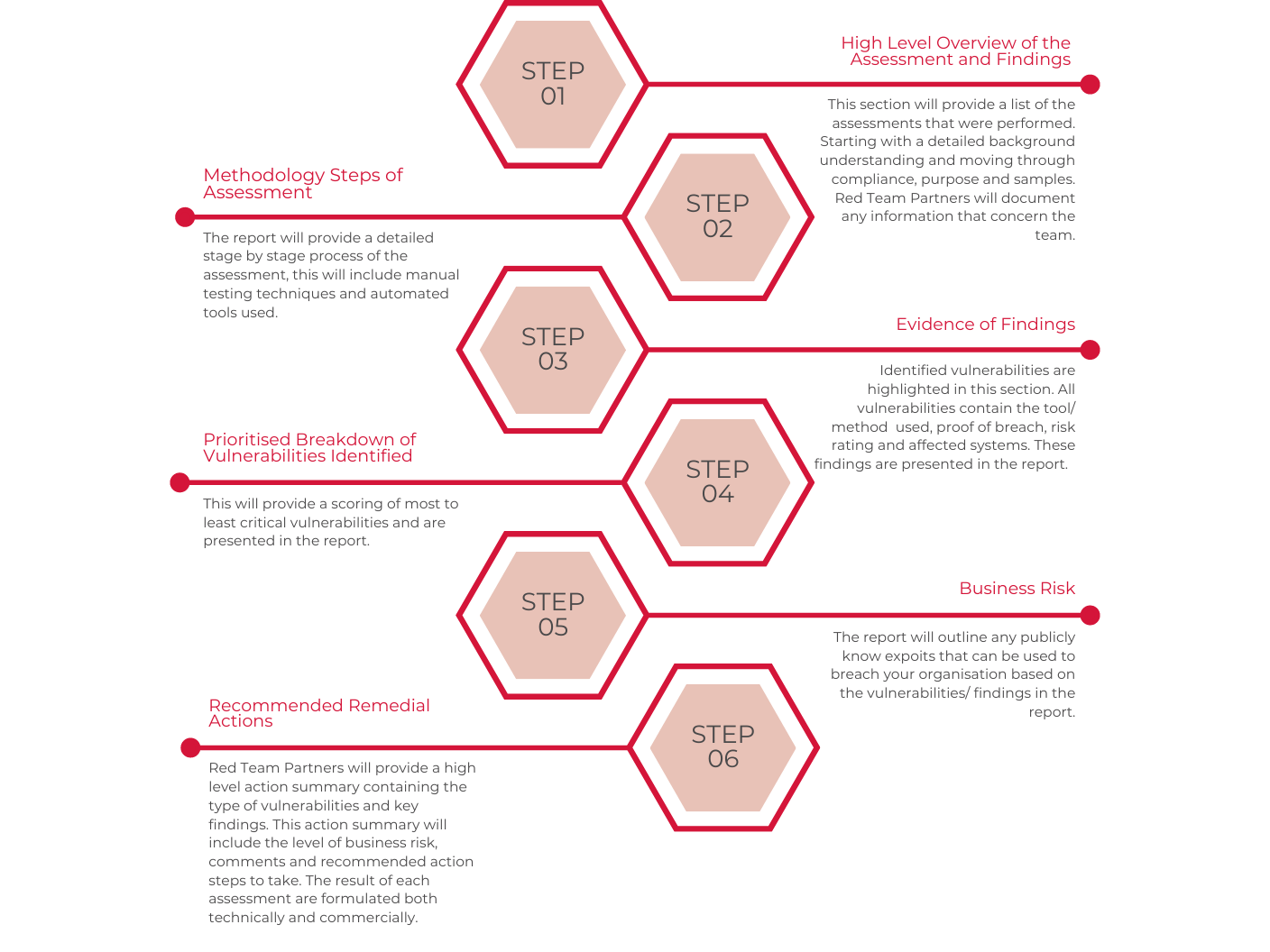
* On-site Delivery

{/onsite\_delivery}

## Tester's Note

|  |
| --- |
|  |

Red Team Partners will use the following stages to undertake the requested service(s)



Our delivery team will work with you before the test to confirm scope and logistics of the service. Rules of engagement will also be discussed at this stage.

## Pre-Test

Our delivery team will help schedule your test by providing the following:

* Scheduled Test Plan - When requested we are able to provide scheduled test plans, these include critical requirements, credentials, and test setup.
* Personnel Vetting - Our tester aligns with CREST and OSCP standards, background checks are regularly conducted by Red Team Partners.
* Third Party - All third parties that are affected must be informed prior to the test.
* Confirmation Dates - Dates of the test will be confirmed within the Statement of Works.
* Point of Contact - A designated point of contact will be required to deal with any issues that arise. Your project manager will be your point of contact for Red Team Partners.

## Assessment

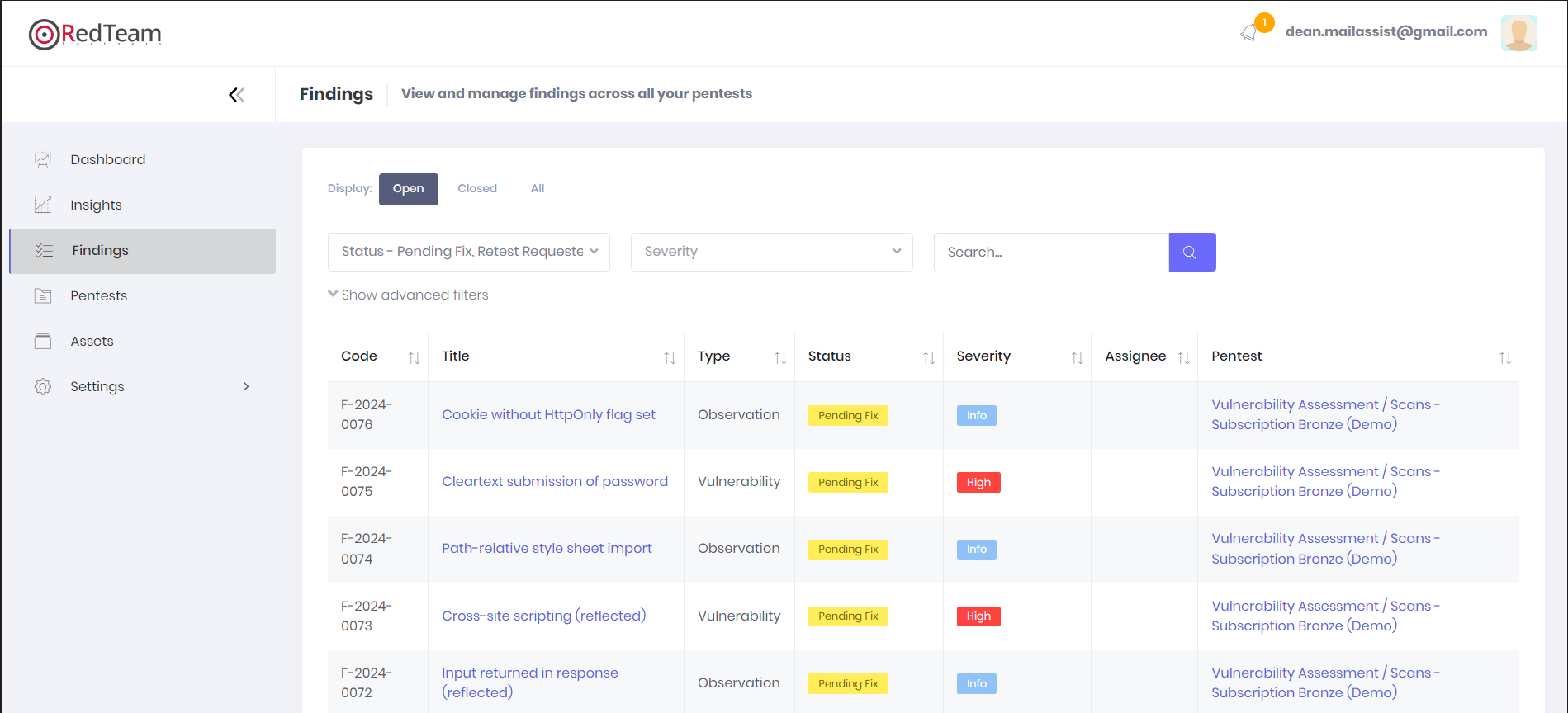
* Test Environment - Red Team Partners is careful to ensure the performance of systems when cyber testing because we understand that systems are vital for the company and ensure measures to keep these systems operating during the testing window.
* Notifications of Vulnerabilities - During the testing window, especially when a critical vulnerability is found, notifications will be sent to your point of contact through our communication platform to ensure remediation action.
* Data Handling - All testing is performed in a secure laboratory adhering to ISO27001 requirements, only our testing personnel will have access to critical information.

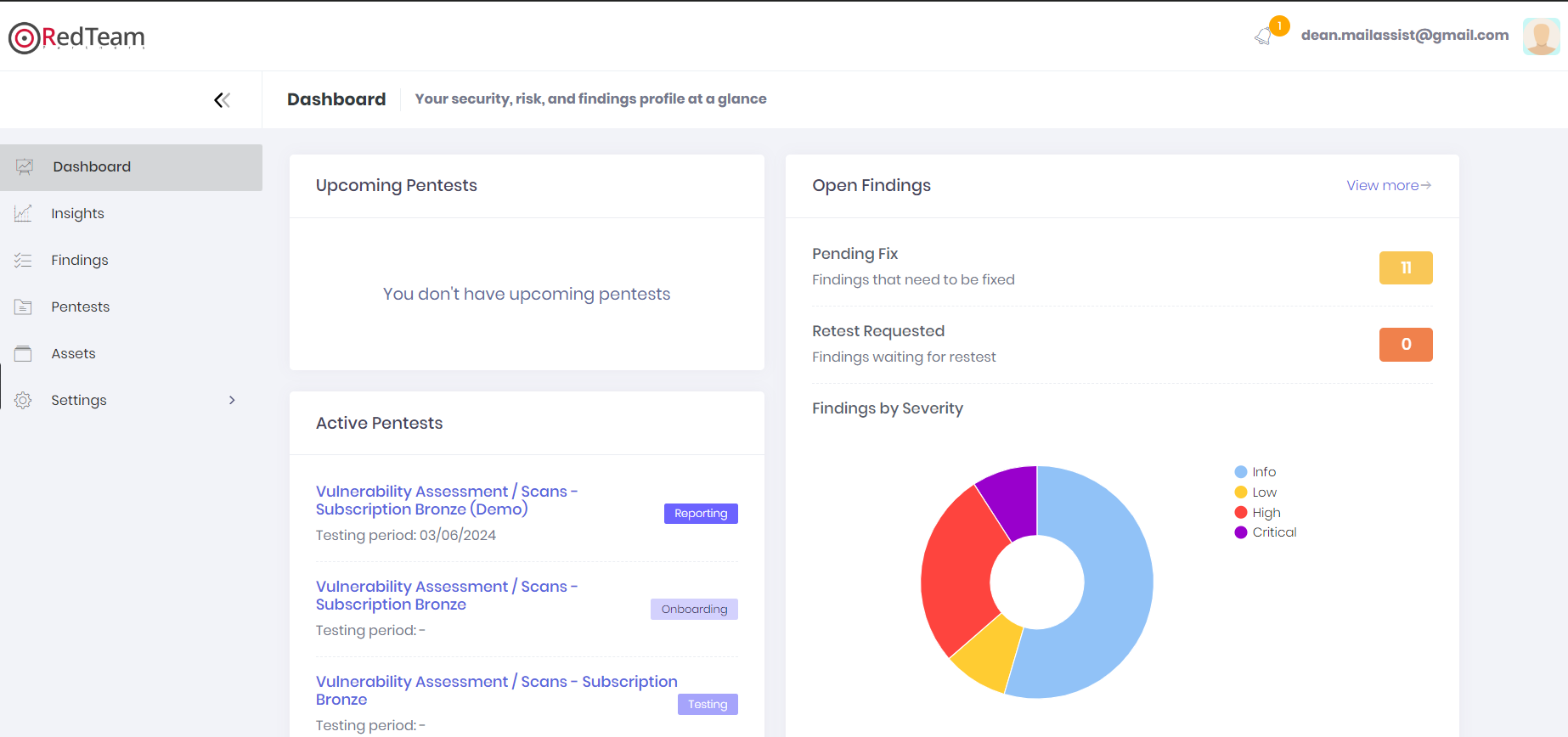
## Post-Test

* Report Delivery - All reports are encrypted from source and are sent to your registered point of contact. Passwords are sent via SMS to ensure maximum security controls.
* Report Results - At the end of the engagement, Red Team Partners will provide a detailed report in which the quality is controlled by certified testers. Using the traffic light system (Red=High, Yellow=Medium, Green=Low), your report will highlight any vulnerabilities/risks from this assessment.
* Data Removal - Once your test has been completed, we dispose all information using CREST approved procedures and handling methods.
* Debrief - Red Team Partner encourages a debrief call with our tester to discuss any risk and remediation steps following the result of the report.

# RTP Robin Platform (included in all packages)

Explore our customer platform equipped with a user-friendly dashboard providing actionable insights, facilitating requests, and accessing findings. Seamlessly navigate through your security landscape, request assessments, and gain valuable insights to fortify your online security effectively.





# COSTING

**Summary**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Service(s)** | **Days** | **Price** |

{#cyberthreatintelligence}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cyber Threat Intelligence |  |  |

{/cyberthreatintelligence}

{#firewallreview}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Firewall Review |  |  |

{/firewallreview}

{#iso27001certification}

|  |  |  |  |
| --- | --- | --- | --- |
|  | ISO 27001 Certification |  |  |

{/iso27001certification}

{#mobileapplicationtesting}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Mobile Application Testing |  |  |

{/mobileapplicationtesting}

{#phishingsimulation}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Phishing Simulation |  |  |

{/phishingsimulation}

{#redteamassessment}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Red Team Assessment |  |  |

{/redteamassessment}

{#securecodereview}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Secure Code Review |  |  |

{/securecodereview}

{#silversubscription}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Silver Subscription |  |  |

{/silversubscription}

{#vulnerabilityassessment}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Vulnerability Assessment |  |  |

{/vulnerabilityassessment}

{#apipenetrationtesting}

|  |  |  |  |
| --- | --- | --- | --- |
|  | API Penetration Testing |  |  |

{/apipenetrationtesting}

{#bronzesubscription}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Bronze Subscription |  |  |

{/bronzesubscription}

{#cloudassessment}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cloud Assessment |  |  |

{/cloudassessment}

{#cyberawareness}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cyber Awareness |  |  |

{/cyberawareness}

{#cyberessential}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cyber Essential |  |  |

{/cyberessential}

{#cyberessentialsplus}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cyber Essentials Plus |  |  |

{/cyberessentialsplus}

{#goldsubscription}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Gold Subscription |  |  |

{/goldsubscription}

{#infrastructuretesting}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Infrastructure Testing |  |  |

{/infrastructuretesting}

{#wapt}

|  |  |  |  |
| --- | --- | --- | --- |
|  | Web Application Penetration Testing |  |  |

{/wapt}

|  |  |  |  |
| --- | --- | --- | --- |
| **TOTAL** |  |  |  |

Cost includes retest on found vulnerabilities, this can be redeemed during or within 90 days after the service completion.

All services are timeboxed based on quoted number of days.

This proposal is valid for **30 days** from the actual date sent.

# TOOL LIST

|  |  |
| --- | --- |
| **Tool Name & Version** | **Description** |
| Nessus (Professional License) | Vulnerability scanner <https://www.tenable.com/products/nessus/nessus-professional> |
| Nmap | Open source port scanning tool <https://nmap.org/download.html> |
| Testssl | Open source SSL/TLS enumeration tool <https://testssl.sh/> |
| Burp Suite (Professional License) | Web Application Proxy and Security Tool <https://portswigger.net/burp> |
| Dirbuster | Directory Brute-Force Tool <https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project> |
| Nikto | Web Server Vulnerability Scanner <https://github.com/sullo/nikto> |

# METHODOLOGY

{#cyberthreatintelligence}

# Cyber Threat Intelligence

## Overview

The investigation uses all available resources, software or data files available on the internet to find out if the target assets are published online.

Our target is to offer our client the best possible overview of his assets, as available to an outside hacker. When doing so we focus exclusively on assets where the client has clear ownership rights (no personal details about the employees are provided).

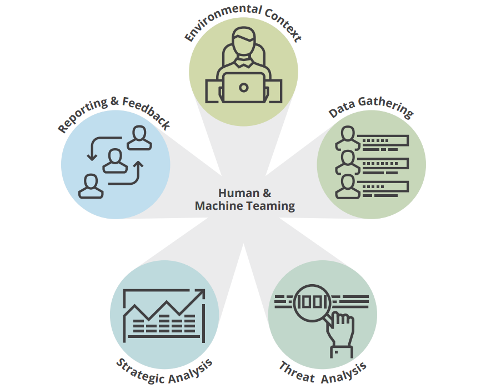
Cyber Threat Intelligence (CTI) can still be described as a nascent and fast-developing field. However, the practice of intelligence itself is historically and commercially a very well-established discipline.

Using an intelligence-led approach has long been accepted as best practice in the realm of conventional security. Without it, organisations will invariably defend against too little, because they don’t understand the threats they face, or try to defend against all potential threats – an unsustainable approach that may also impair the organisation’s ability to operate effectively.

For example, a company looking to build a facility in a potentially hostile environment would first seek intelligence on the threat posed by malicious actors in the vicinity before trying to adopt appropriate security controls.

## Cyber Security Assessment Methodology

The Threat Intelligence methodology contains the following phases:



**Environmental Context**

A deep understanding of your organization, including your organization’s entire attack surface; threats, risks, and opportunities targeting your organization and industry; and your organization’s internal and external network and operations. Gaining this understanding is a continuous process and influences what data is needed to perform cyber intelligence.

**Data Gathering**

Through automated and labor-intensive means, data and information is collected from multiple internal and external sources for analysts to analyze to answer organizational intelligence requirements.

**Threat Analysis**

Assessing technical telemetry and non-technical data pertaining to specific threats to your organization and industry to inform cybersecurity operations/actions and Strategic Analysis. Threat Analysis is built on operational and tactical analysis and enhances CSO/CISO and other mid- to senior level decision making.

**Strategic Analysis**

Holistically assessing threats, risks and opportunities to enhance executive decision-making pertaining to organization-wide vital interests such as financial health, brand, stature, and reputation.

**Reporting and feedback**

Communication between analysts and decision makers, peers, and other intelligence consumers regarding their products and work performance. Reporting and feedback help identify intelligence requirements and intelligence gaps.

## The Different Levels of Cyber Threat Intelligence

As with conventional intelligence, there are different levels of cyber threat intelligence: operational, tactical, and strategic. Each level differs in the nature and format of the material conveyed, its intended audience and its application. These are summarised:

**Operational threat intelligence** often relates to details of potential impending operations against an organisation. Although it is not always easy to obtain, by using an all-source approach an intelligence provider will be able to detect, for example, chatter from cyber activists discussing potential targets for an upcoming campaign, or data leaked or sold on a dark web forum that could be used in an operation against the company. Cyber threat intelligence providers will generally supply operational threat intelligence in a combination of human and machine-readable formats.

**Tactical threat intelligence** consists of material relating to the techniques, tactics and procedures (TTP’s) used by threat actors. Indicators of compromise (IOCs) are the main deliverable for tactical threat intelligence providers. These are particularly useful for updating signature-based defense systems to defend against known attack types, but can also prove useful for more proactive measures, such as threat hunting exercises. It is therefore particularly useful to network defenders such as Security Operations Centres (SOCs). CTI providers will generally supply IOCs in machine-readable formats, whereas intelligence on TTPs will be in human-readable formats and will require human assimilation and action.

**Strategic threat intelligence** exists to inform senior decision makers of broader changes in the threat landscape. Because of this intended audience, strategic intelligence products are expressed in plain language and focus on issues of business risk rather than technical terminology. The reporting format of strategic cyber threat intelligence products will reflect this longer-term view – for example it will often be disseminated on a monthly or quarterly basis to assist the formulation of longer-term strategy.

## Sources of Intelligence That We are Searching In

Cyber threat intelligence suppliers should draw from a wide range of different sources to enable them to provide a rounded and holistic understanding of the threats that organisations face. This is particularly true because the range of cyber adversaries most organisations face are disparate, and relevant information sources about those threat actors need to match that challenge. Commonly used sources by cyber threat intelligence providers include:

**Indicators of compromise (IoCs)** associated with malicious activity. Hashes of malware samples, IP addresses and domain names can all be used to update firewalls and detection systems, as well as contribute to an understanding of threat actors’ TTPs. IOCs are their own are more akin to data than processed intelligence, though are still included within the spectrum of cyber threat intelligence.

**Client-derived data,** such as that regarding its infrastructure or extracted from a security information and event management (SIEM) tool or other logs can be correlated with other sources, or for pro-active measures such as threat hunting.

**Deep web,** such as information from member-only hacking forums frequented by cybercriminals. These sources can provide valuable insight into the tools and services advertised and requested by cybercriminals, as well as identifying which exploits are being discussed to enable patch prioritisation.

**Dark web** will include marketplaces and shops that are hosted on anonymity-focused networks such as Tor or I2P which criminals use to purchase goods and services. This will enable consumers to identify if their data – ranging from login credentials to valuable intellectual property – is available or being advertised for sale, or if infrastructure they use may be targeted.

Messaging platforms are also used by threat actors to communicate and can provide intelligence. Rather than relying on semi-public forums, some cybercriminals prefer more direct means of engaging each other to sell their goods and services. Similarly, cyber activists will often use a combination of outmoded Internet Relay Chat (IRC) channels and other messaging platforms to discuss impending operations, which can provide useful insight into potential tactics and targets.

**Social media** can be used by a variety of actors, typically those with low capabilities. Activists may signal their intent to pursue specific targets in advance via social media pages. Criminals may use popular networks as an alternative means of attracting potential customers, particularly in jurisdictions where law enforcement capability is limited, and they do not run the risk of arrest. Social media collection may also include coverage of inadvertent data leaks by employees or potential threats from malicious insiders.

**Human intelligence** can be derived from engagement with individuals via several the above sources. However, threat intelligence providers should only engage in such activity under a strict and defined framework and in pursuit of specific intelligence requirements and in a legal and ethical way. Providers also need to ensure that collection efforts from social media and human sources are compliant with legislation such as the General Data Protection Regulation (GDPR).

**Malware analysis,** which allows analysts to extract information such as indicators of compromise from a sample, which can in turn be used to search the client estate. Analysis also allows providers to better understand the latest tactics, techniques and procedures that are being used by threat actors, with a view to informing network defenders how to better respond.

**Geopolitical developments** can be used to derive an understanding of the intent of nation-state actors. For example, understanding how a state’s strategic development objectives coincide with those of the client organisation, or how potential nation-state rivalries will affect the prospect of disruptive attacks in a region in which it operates, will help it understand the threats it faces.

**Code repositories,** such as exploit databases, can provide insight into which exploits are available for adoption by threat actors, and which vulnerabilities should be prioritised for patching as a result.

**Paste sites** can reveal a wide array of information, including leaked credentials, indications of impending activist operations, code snippets, and evidence of breaches. The example in the image to the right shows a message from a campaign by the Anonymous collective, which goes on to list a series of targets for DDoS attacks.

**Information sharing platforms** can also provide additional context and insight to threat actors’ current activity.

{/cyberthreatintelligence}

{#firewallreview}

# Firewall Review

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. Red Team Partners employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

The RTP Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The RTP Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

RTP follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Technical Summary

**Preventive controls:** These controls prevent any negative incidents to happen. Organizations routinely perform these control procedures including administrative or physical such as segregation of duties. An example of such a control is to have separate individuals write and authorize checks for payments.

**Detective controls:** These are the controls that are utilized after an adverse event to find out the cause, extent of damage, and protective next steps. Internal audits are an example of such controls.

**Corrective controls:** These controls are invoked after the detective controls. Examples of corrective controls are software patches and updates, filing reports, and modifications to the system.

## Phases of a Security Controls Audit

There are four significant phases in an audit:

**Planning Phase**

**Preliminary information gathering and assessment**

Planning is an integral part of any audit. In the beginning, planning is done to create a process flow based on an initial reconnaissance of the entire system. The plan is updated according to the test results of the initial assessment.

**Overall knowledge of the infrastructure**

The auditor is responsible for culminating all technical and non-technical information about the organization and the systems. This helps in scoping out the work and planning the areas to be audited. The following are some aspects of this early-stage information gathering:

* Operating environment and functions of the organization’s systems
* Dependency on the IT infrastructure
* Organizational structure
* Software and hardware information
* Current and past security issues within the organization

This information-gathering step helps in finding potential areas of concern and defining the scope of the audit.

**Assessment scope and objective**

From the above steps, the auditor gains relevant information and details to define the objective and scope of the assessment in a clear and detailed format. The initial risk assessment forms an important part of the process and answers questions pertaining to three primary security goals, confidentiality, integrity, and reliability.

Risk assessment consists of ranking the potential threats from low to high, or other scientific or complex metrics. The ranking depends on the severity of the issue with respect to the extent of damage it can cause or the ease of exploitation. Vulnerabilities that are easy to exploit and those causing a high degree of damage must be ranked comparatively higher. These assessments can also include inputs from the management authorities, questionnaires, reviewing available documents, and a survey of applications.

Below are some common Security Control audit objectives:

* Review existing IT security systems
* Review of specific programs and systems for performance and security
* Analyzing security standards at various development phases

Objectives are not limited to the above-specified ones. Security Control audit can cover all major areas such as security settings, firewalls, physical security, and access rights, to name a few.

**Evaluating collected evidence**

Through rigorous testing and prodding the security infrastructure, various types of evidence are gathered that must be interpreted to compile the results of the audit. There are various techniques to test a system and obtain results. Evidence can be majorly three types:

* Documentary evidence
* System analysis
* Observation of processes

**Documenting audit results**

Proper documentation of the results forms an integral part of IT security audit methodology. The final report cab be in a very consumable format for stakeholders at all levels to understand and interpret. It will contain details such as the audit plan, audit scope, tests carried out, findings and detailed solutions, and next steps to remedy the security issues.

## Type of testing

The type of testing can be divided into five parts:

**IT controls**

The current IT systems need to be tested for both substantive and compliance aspects. Compliance testing is done to assess whether controls are being applied according to the documentation offered by the client. It also checks if IT controls follow the compliance levels in accordance with management procedures and policies. In substantive testing, the adequacy of the controls is substantiated on whether they can protect the organization from cyber threats. These tests need an in-depth understanding of the different kinds of threats such as unauthorized access to assets including data, unusual interactions with the system, data corruption, inaccuracy in information, etc.

**General control audit**

In a summarized form, general controls are concerned with the applications, databases, operating systems, and IT infrastructure support. The purpose of an audit in this area is to check the following points:

* Databases, applications, and infrastructure support having logical access controls
* Management controls for program changes
* Recovery and backup related controls
* Physical security of data centers
* Controls for the system development cycle

**Application control audit**

Application controls are application-specific controls and have a high impact on individual transactions. These controls ensure and verify that all transactions are authorized, safe, and recorded. To proceed with this phase of the audit, there is a need for a deep understanding of the working of the system. For this analysis, a brief description of the application is required, along with details of transactions including volume, involved data, and flow. This audit can be subdivided into:

* Input controls
* Processing controls
* Output controls
* Stationary file control

**Internet and network controls**

Most of the organizations use local area networks for their operations. This leads to the risk of access by unauthorized users if not monitored and protected properly. The fundamental requirement of a network is to be accessible by only authorized users. Controls should be implemented to eliminate issues like data corruption, data loss, or interception while being transmitted.

**IT Audit standards**

The IT audit can comply with the internationally accepted security standards. Some of these are mentioned below:

* **ISO Compliance:** The ISO publishes a slew of guidelines that ensure reliability, quality, and safety. ISO 27001 is suitable for information security requirements
* **PCI DSS Compliance:** These standards apply to any company that is involved with customer payments. This is necessary to ensure that all transactions are secure and protected.

{/firewallreview}

{#wapt}

# Web Application Penetration Testing

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. Red Team Partners employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

The RTP Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The RTP Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

RTP follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Technical Summary

The methodology employed during a Web Application Security Assessment involves the following stages:

A diagram of a workflow

Description automatically generated

The steps are aligned to the in-depth security concepts and are focused on process and technical security controls and their implementation in the various phases of the project delivery. The results provided for each activity will include a detailed and comprehensive assessment of client’s current security posture, expansive recommendations, and tools and knowledge to facilitate the continuous improvement.

**Intelligence Gathering & Workflow Study**

Conduct passive and active information gathering to determine the level of information that can be found about the assets in scope. These actions are conducted to understand what level of exposure the assets have, and how an attacker can use this information to conduct further attacks.

**Vulnerability Assessment & Identification**

Security Engineers investigate for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

**Exploitation**

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level.

**Reporting**

The report will communicate to the reader the specific goals of the Penetration Test and technical details of findings of the assessment exercise. The intended audience will be those who oversee the oversight and strategic vision of the security program as well as any members of the organization, which may be impacted by the identified/confirmed threats.

## Type(s) of Test Performed

Red Team Partners security checklist includes, but is not limited to, identification of the following risks:

|  |  |  |
| --- | --- | --- |
| Application Profiling and Information Disclosure | Platform and Third-Party Misconfiguration | Cookie and Session Handling |
| * Default Banners * Unhandled Error Conditions * HTML/JavaScript Comment Information Leakage * Extraneous Content in Web Root * Source Code Disclosure * Robots.txt Path Disclosure * Content Expiration and Cache Control * Bit Bug/Referrer Header Leakage * Account Enumeration * Backup/Archive Content | * Default Administrative Credentials * Default Content and Scripts * Application Script Engine * Web Server * Weak SSL Implementation * Flawed Use of Cryptography | * Session Fixation/Hijacking * Set-Cookie Weaknesses * Sensitive Information Disclosure * Cookie Poisoning * Multiple Simultaneous Login Allowed * Session Timeout * Explicit/Implicit Logout Failures * Cookie less Sessions * Custom Session Management |

|  |  |  |
| --- | --- | --- |
| Command Injection Flaws | Logic Flaws | Client-Side Flaws |
| * SQL Injection * XXE, XPath, and XML Injection * SSI/OS Command Injection * Server Script Injection/Upload * Cross-Site Scripting (XSS) * Buffer Overflow | * Privilege Escalation * Sensitive Information Disclosure * Data Mining/Inference * Functional Bugs * Application-Specific Control Failures * Cross-Site Tracing (XST) * Weak Data Validation * Race Conditions * CPU-Intensive Functions | * Exposure of Sensitive Business * Logic * Reliance on Client-Side Validation * AJAX/Web Service Flaws * Java Applet/ActiveX * Control/Flash Weaknesses |

|  |
| --- |
| Authentication and Authorization |
| * Unauthenticated Sensitive Content * Poor Separation of Privilege * Brute-Force Login * Weak Password Policy * Account Lockout/Denial of Service * SSO Weaknesses * Security Question Weaknesses * CAPTCHA Flaws |

{/wapt}

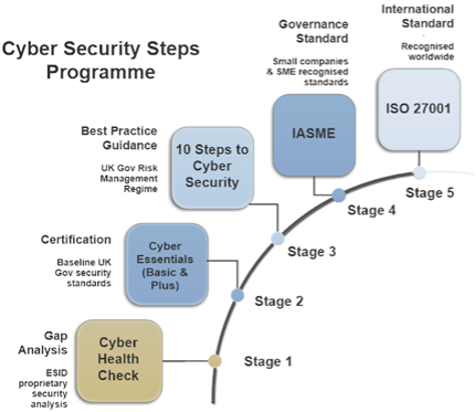
{#iso27001certification}

# ISO 27001 Consultancy

## Overview

Red Team Partners would ensure that your business and the data you hold is protected and secure from the threat of cyber-attack and insider risk, and that your company’s security posture will minimise the possibility of a data breach or information leakage & ensure the continuity of your business in the event of a cyber incident or other disruptive event.

## Goals



## Success Metrics

You will have a clear and independent picture of the current state of cyber and information security provision.

You will know what is required to better secure the information you hold, increase your cyber resilience, and as a result protect your business reputation.

Certification with the key standards (above) are the major milestones against which progress will be measured. Red Team Partners Consulting’s “Cyber Security Steps Programme” is a progressive programme to help you achieve implementation and compliance with those standards as your organisational information security maturity develops.

Our proprietary security analysis is mapped against:

* ISO 27001 for Information Security
* GDPR, NIS and the Cyber Security Directive
* ISO 22301 for Business Continuity
* Insider Threat Management as modelled on the best-practice principles of New Scotland Yard, US Secret Service and reflected in advice from UK Centre for the Protection of National Infrastructure (CPNI)

## Cyber/Information Security Health Check

Our Health Check process involves key person/stakeholder interviews over a period of 1 week to 10 days. Outside of this, Red Team Partners will work from our end on the certification, the analysis and production of findings, which will then be presented to you within 30 days from project commencement. During this process, we will correspond as required to gather information, clarify elements, or to gather supplemental information, and this may include the use of additional scheduled conference calls with key stakeholders.

## Cyber & Information Security Governance

Strengths and weaknesses in your current security and compliance posture will be identified at the Health Check stage. We will then develop with you a project road map to achieve the milestones identified.

Following our Cyber Security Steps Programme, Red Team Partners will then work with you to help build your Cyber Essentials Certification and implement an Information Security Management System (ISMS) to achieve compliance and certification with the UK Government’s “10 Steps to Cyber Security” risk management regime and IASME Governance Standards with support your journey towards achieving ISO 27001 certification.

Guarantee: Red Team Partners Consulting will generate the results agreed by both companies as described in the Goals section of this document.

## Test Area

1. **ISO 27001 Assessment**  
   Review current operational & IT processes  
   Review of existing documentation and interviews with team  
   Review against ISO27001 criteria
2. **ISO 27001 Certification Roadmap**  
   High level plan and outline of path to Certification  
   Agree approach for Critical areas  
   Initial review and discussion with Team
3. **ISO 27001 Remediation**  
   Initial Remediation Steps - e.g., creation of policies  
   Detailed Plan of ISO Controls to address and timeline

{/iso27001certification}

{#mobileapplicationtesting}

# Mobile Application Penetration Testing (iOS/Android)

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. RTP employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

The Red Team Partners Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The Red Team Partners Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

Red Team Partners follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open-Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Technical Summary

A Mobile Application Security Assessment (MASA) is an assessment of the application on the running device as well as the associated back-end components. The objective of the assessment is to identify vulnerabilities within these environments and verify their existence using manual testing techniques. These assessments are most successful when customers share all known information with the tester; however, the customer can elect to share less information.

The MASA is a comprehensive assessment that identifies vulnerabilities ranging from Critical to Informational severity. Red Team Partners’ Application Security Team identifies, verifies, and reports anything that raises the attack surface of the application. We will use multiple techniques to simulate attacks from both an unauthenticated and authenticated attacker perspective, exposing the greatest amount of attack surface and providing the most value from the testing efforts.

After the client provides the initial information and the application, the Red Team Partners Team will run the application and test the credentials taking note of their privilege levels. During the initial review of the application, the consultant will take note of any critical areas of the application and identify potentially sensitive functions to target during the testing efforts.

The Red Team Partners consultant will run and analyze the mobile application on a jailbroken or rooted device, provided by Red Team Partners and connected to a customized assessment environment compromised of wireless access points, proxies, and many other tools. If the consultant does not use a RTP -provided device, the client must supply a suitable test device. Using a jailbroken or rooted device simulates a potential attacker’s approach for attacking an application or accessing sensitive data on users’ mobile devices.

The Red Team Partners team uses a methodology that focuses on real-world scenarios to provide an accurate risk assessment. In some instances, certain mobile security features may limit the application functionality on a testing device. These may include jailbreak or root detection, tamper prevention, device provisioning, or certificate pinning. When such features are present, we recommend providing an alternate build of the application with these features disabled or removed.

The Red Team Partners consultant will validate the strength of the security controls in the original application, but if the consultant cannot defeat these in a reasonable period, the consultant will continue testing with the alternate version. This approach allows for in-depth testing of the application within the time allotted.

The methodology employed during a Mobile Application Security Assessment involves the following stages:

A diagram of a workflow

Description automatically generated

The steps are aligned to the in-depth security concepts and are focused on process and technical security controls and their implementation in the various phases of the project delivery. The results provided for each activity will include a detailed and comprehensive assessment of client’s current security posture, expansive recommendations, and tools and knowledge to facilitate the continuous improvement.

**Intelligence Gathering & Workflow Study**

Conduct passive and active information gathering to determine the level of information that can be found about the assets in scope. These actions are conducted to understand what level of exposure the assets have, and how an attacker can use this information to conduct further attacks.

**Vulnerability Assessment & Identification**

Security Engineers investigate for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

**Exploitation**

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level.

**Reporting**

The Report will communicate to the reader the specific goals of the Penetration Test and technical details of findings of the assessment exercise. The intended audience will be those who oversee the oversight and strategic vision of the security program as well as any members of the organization, which may be impacted by the identified/confirmed threats.

**Testing**

Red Team Partners conducts testing using both automated and manual testing methods. A majority of the testing will focus on manual testing. Red Team Partners uses automated testing, where possible, on back end and web service components, and manually validates identified vulnerabilities. Throughout the assessment, Red Team Partners uses a mixture of commercial, open source, and custom-built tools.

Some examples of tools that Red Team Partners uses include:

* Burp Suite Pro
* Apktool, dex2jar, Android Studio, JD-Gui, Frida
* Hopper App, Xcode, iExplorer, SQLite Studio
* adb, ssh, Cydia, Pangu, TaiG, cycript, and others
* Wireshark

The Red Team Partners Team configures the automated tools using information obtained during the information-gathering phase. This ensures the highest level of success, by removing obstacles that typically hinder their functionality and ability to navigate the application properly.

## Type(s) of Test Performed

Red Team Partners security checklist for Mobile Applications includes, but is not limited to, identification of the following risks:

|  |
| --- |
| OWASP Top 10 Mobile Risks |
| * M1: Improper Platform Usage |
| * M2: Insecure Data Storage |
| * M3: Insecure Communication |
| * M4: Insecure Authentication |
| * M5: Insufficient Cryptography |
| * M6: Insecure Authorization |
| * M7: Client Code Quality |
| * M8: Code Tampering |
| * M9: Reverse Engineering |
| * M10: Extraneous Functionality |

|  |  |  |
| --- | --- | --- |
| Application Profiling and Information Disclosure | Platform and Third-Party Misconfiguration | Cookie and Session Handling |
| * Default Banners * Unhandled Error Conditions * HTML/JavaScript Comment Information Leakage * Extraneous Content in Web Root * Source Code Disclosure * Robots.txt Path Disclosure * Content Expiration and Cache Control * Bit Bug/Referrer Header Leakage * Account Enumeration * Backup/Archive Content | * Default Administrative Credentials * Default Content and Scripts * Application Script Engine * Web Server * Weak SSL Implementation * Flawed Use of Cryptography | * Session Fixation/Hijacking * Set-Cookie Weaknesses * Sensitive Information Disclosure * Cookie Poisoning * Multiple Simultaneous Login Allowed * Session Timeout * Explicit/Implicit Logout Failures * Cookie less Sessions * Custom Session Management |

|  |  |  |
| --- | --- | --- |
| Command Injection Flaws | Logic Flaws | Client-Side Flaws |
| * SQL Injection * XXE, XPath, and XML Injection * SSI/OS Command Injection * Server Script Injection/Upload * Cross-Site Scripting (XSS) * Buffer Overflow | * Privilege Escalation * Sensitive Information Disclosure * Data Mining/Inference * Functional Bugs * Application-Specific Control Failures * Cross-Site Tracing (XST) * Weak Data Validation * Race Conditions * CPU-Intensive Functions | * Exposure of Sensitive Business * Logic * Reliance on Client-Side Validation * AJAX/Web Service Flaws * Java Applet/ActiveX * Control/Flash Weaknesses |

|  |
| --- |
| Authentication and Authorization |
| * Unauthenticated Sensitive Content * Poor Separation of Privilege * Brute-Force Login * Weak Password Policy * Account Lockout/Denial of Service * SSO Weaknesses * Security Question Weaknesses * CAPTCHA Flaws |

TRed Team Partners performs extensive manual testing, which comprises a significant majority of the testing effort. During this portion of the testing, the Red Team Partners consultant executes the application, and analyzes the communication, functions, and the data the application sends and receives. The Red Team Partners Team tests complex interactions, workflows, and business logic. Additionally, the Team manually evaluates areas of the application and specific vulnerabilities that automated tools either have difficulty with or are unable to identify.

Red Team Partners validates any identified communication channels for proper confidentiality and integrity. We monitor the application execution on the device and examine the device from a high-level forensic perspective to identify areas where the application may be storing or caching sensitive information in an insecure manner. After reverse engineering the application binary to the extent possible, we analyze it for information leakage or hard-coded secrets. During testing, we map the back-end environment and test any in-scope components for vulnerabilities.

{/mobileapplicationtesting}

{#phishingsimulation}

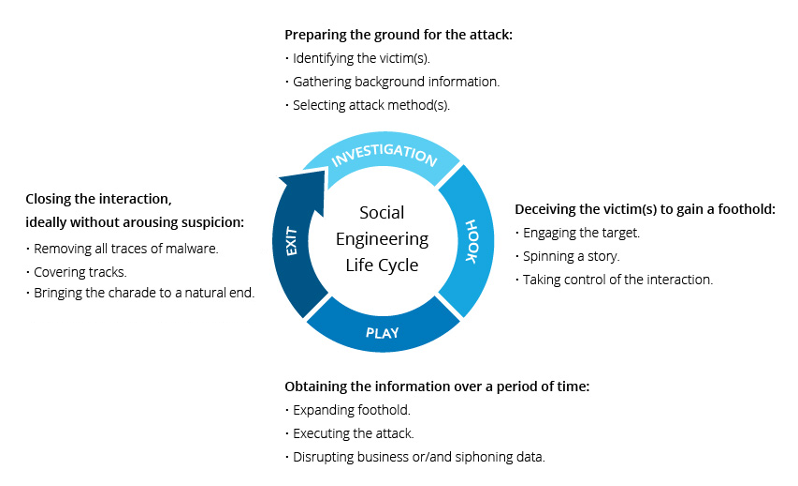
# Phishing Simulation

## Overview

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, credit card details, etc. by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, which matches the look and feel of the legitimate site.

Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social websites, auction sites, banks, online payment processors, or IT administrators.

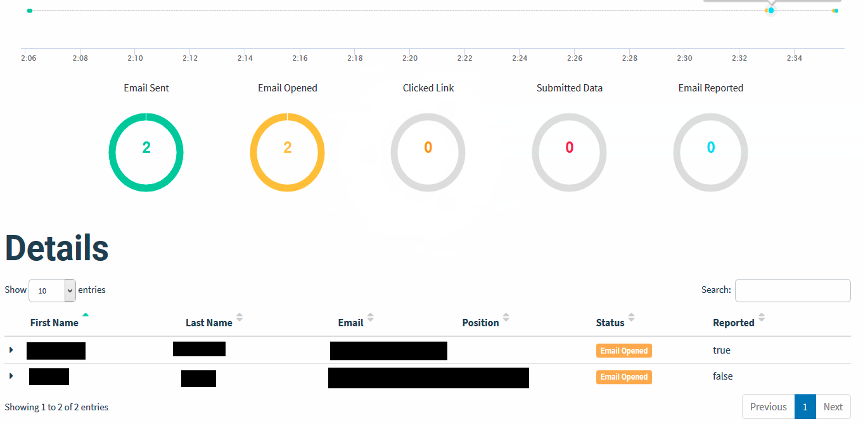
## Social Engineering Process



The security team, based on the client requirements, will try to get the following data:

* How many employees opened the email
* How many employees clicked the received link
* How many employees submitted any data
* How many employees have reported the email

the below diagram, a highlight of the report, which contains all the above information is presented.



{/phishingsimulation}

{#redteamassessment}

# Red Team Assessment

## Overview

The role of the Red Team is to provide an attacker-like approach to the organisation, this approach consists of network detection and system vulnerabilities. The overall aim of the red team is to gain system/network/data access. Organisations wanting to increase their security strategy throughout the year can view the Red Team as a specialist extension of their own IT team.

During red team exercises, our security experts will launch a realistic attempt to exploit your environment to gain access to systems that would enable us to impact the critical functions necessary for your operations. This simulated attack is carried out in a controlled manner to ensure that your operations are not adversely affected, while still providing valuable information regarding gaps in your preventive or detective controls that could allow an adversary to harm your organization. The attacks utilize real-world adversary tactics, techniques, and procedures (TTPs) that represent a genuine threat to the critical functions of your organization.

The attack scenarios will recognize that a dedicated adversary would leverage a broad targeting profile to gain a foothold within the organization. From this broad attack surface, additional focused attacks on critical functions will be launched in accordance with predefined rules of engagement. The goal of each attack scenario will be to achieve a level of compromise that could then be leveraged by an attacker to impact the associated critical function.

## Methodology

* Red Team Partners will use open-source intelligence tools to collect and identify a target profile of your organisation.
* We will conduct social engineering attacks against your employees to elicit further targeting information including company credentials.
* Based on available threat intelligence gathered, Red Team Partners will devise a series of attack scenarios against the critical functions and key data to simulate real-world threats to your organisation
* Red Team Partners will conduct an offensive campaign against the identified critical functions of your organisation to gain a foothold within the organisation.
* We will be continuing to focus attacks on critical functions to achieve a level of compromise that could then be leveraged by an attacker to impact the associated critical function.

These exercises proved a valuable insight into improving the visibility and capability of your network defenders. At the end of each adversary emulation, our team will work with yours to ensure that all attack techniques leveraged against your organization are clearly explained, evidence that may have been left behind is identified, and suggestions for improving controls to prevent or detect similar attacks in the future are provided.

Critical functions include the people, process, and technology underpinning the ongoing successful operation of your organization, and threats to any of these functions could negatively impact your operations. Based on available threat intelligence, our team will devise a series of attack scenarios against your critical functions. Since a real-world adversary could employ illegal or unethical methods not available to our team, and since the time and effort allocated to this phase of the test will be fixed, this portion of the assessment is conducted in a gray box manner to ensure the completeness of the results.

The attacks will be conducted without detailed coordination with your network defenders to ensure that an accurate picture of your organization’s ability to prevent or detect targeted attacks is achieved. To minimize disruption to your operations, senior management members of your organization will be notified of the details of the attacks, including the timing of the attacks, in accordance with a predefined risk management plan.

## Type(s) of Test Performed

Virtual Assessment:

1. **Reconnaissance/OSINT -** Crawling of online sources to locate employee names, e-mail format and compile a list of employees for further targeting. – organisation will be providing a list of e-mail addresses here.
2. **Enumeration -** Identification of externally facing assets and basic web application tests such as default password checks.
3. **Phishing -** Targeted Phishing campaigns if access has not already been gained.
4. **Password Spraying -** A brute-force style attack against all identified e-mail addresses to attempt to access e-mail and other sensitive applications.
5. **Redundancy -** If Phishing / Physical does not provide network access, organisation will install a network device to allow external access to the Red Team Partners consultants to continue testing.
6. **Network Mapping -** Mapping of organisations internal network to identify key assets and for use in further attacks.
7. **Persistence -** Achieve persistence on the organisations network to access it externally.
8. **Lateral Movement -** Silently move around the organisations network, further identifying key assets and employees.
9. **Escalation of Privileges -** Achieve Domain Administrator permissions within the domain.
10. **Completion of Goals -** Achieve pre-set goals, such as; access to customer PII information, access to source code.

{/redteamassessment}

{#securecodereview}

# Secure Code Review

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. Red Team Partners employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

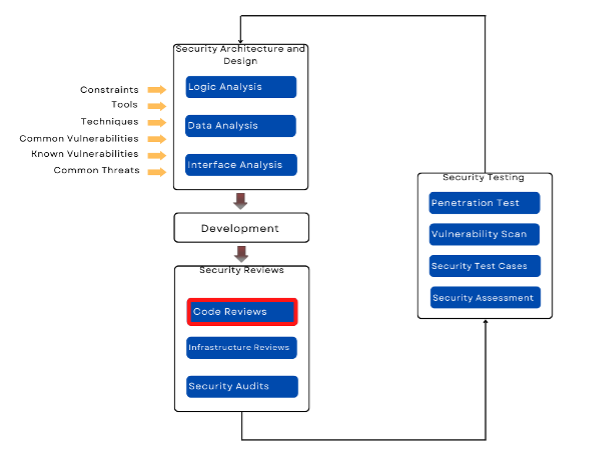
The RTP Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The RTP Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

RTP follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Technical Summary

Code Review is a systematic examination (sometimes referred to as peer review) of computer source code. It is intended to find mistakes overlooked in software development, improving the overall quality of software. Reviews are done in various forms such as pair programming, informal walkthroughs and formal inspections.



**Introduction**

Code review is probably the single-most effective technique for identifying security flaws. When used together with automated tools and manual penetration testing, code review can significantly increase the cost effectiveness of an application security verification effort.

This methodology describes the mechanics of reviewing code vulnerabilities and provides limited guidance on how the effort should be structured and executed.

Manual security code review provides insight into the “real risk” associated with insecure code. A human reviewer can understand the context coding practices, and make a serious risk estimate that accounts for both the likelihood of attack and the business impact of a breach.

## Type(s) of Test Performed

|  |  |  |
| --- | --- | --- |
| Design | Information Gathering | Configuration |
| * Architecture and design documentation is complete * User and role based privileges are documented * Site is well partitioned into public and restricted pages * Security is layered each layer assumes other layers may have been compromised * Security design covers all 8 principles of web security: authentication, authorization, * Confidentiality, message integrity, data integrity, availability, non-repudiation * Sensitive data has been identified | * Get a copy of the code * Manually explore the file structure of the code * Look for any missing pieces of code * Check for frameworks / libraries / dependencies * Check for application routes and their inputs | * Get a copy of the code * Manually explore the file structure of the code * Look for any missing pieces of code * Check for frameworks / libraries / dependencies * Check for application routes and their inputs * Sensitive data is not hard-coded in configuration files * Develop and test code are properly segregated from production * Dependencies are up to date |

|  |  |  |
| --- | --- | --- |
| Secure Transmission | Authentication and User Management | Authorization |
| * Sensitive data is only transmitted over an SSL connection * Site is partitioned into private and public URLs * Sensitive data has been secured in memory, storage and transit * Sensitive data doesn’t leak to non-private channels | * Sensitive data is only transmitted over an SSL connection * User credentials are encrypted in the data store * Security policies are configurable (not hardcoded) * Standard security frameworks are used (instead of custom code) * SSL is used to protect user credentials and authentication tokens * Authentication cookies are not persisted * Authentication cookies are encrypted * Cookie names and paths are used * Application handles user management events such as authentication failure, password reset password change, account lockout and cancel account * Application handles suspicious events such as multiple failed logon attempts, session replay and attempted access to restricted resources * Strong passwords policies are enforced * Authentication credentials are not passed by HTTP GET | * Authentication and authorization should be the first logic executed for each request * Authorization checks are granular (page and directory level) * Deny access to pages and data by default * Re-authenticate for requests that have side-effects * ACLs are configured for all files * Authorization based on clearly defined roles * Authorization works properly and cannot be circumvented by parameter manipulation * Authorization cannot be bypassed by cookie manipulation |

|  |  |  |
| --- | --- | --- |
| Input Validation | Cryptography | Exception Handling |
| * All external input is validated without exception * Where possible input is restricted to known good chars * Data is validated server side (security should not rely on client-side validations) * Application validates numerical input and rejects unexpected input * Application efficiently evaluates input length * Strong separation between data and commands * Strong separation between data and client side scripts * Data should be checked for special characters before being passed to SQL, LDAP, OS and third party commands * http headers are validated for each request (e.g. referrer) | * Sensitive data has been secured in memory, storage and transit * Restricted areas require SSL * Sensitive information not passed to/from non-SSL pages * Proper SSL set up * SSL provider supports only strong algorithms * Web based admin tools require SSL * Decryption services protected by authentication/authorization * Require SSL for login page * Securely store cryptographic keys | * When exceptions occur the application fails securely * Error messages do not reveal sensitive information * System errors are never shown to users * Resources are released and transactions rolled back when there is an error |

|  |  |
| --- | --- |
| Auditing and Logging | General |
| * All user / system actions are logged * Sensitive information is not logged (e.g. passwords) * Logging for user management events (e.g. password reset) * Unusual activity such as multiple login attempts are logged * Logs have enough detail to reconstruct events for audit purposes * Logging is highly configurable (logging levels) | * Proper configuration of frameworks such as Spring, Struts, DOT NET etc. * Libraries are up-to-date * System calls have their return status checked * Efficient memory usage * No exposures to buffer overruns * Code, services, commands and processes are executed using minimal privileges (least privileges) * Code has no back doors * Debugging code and test harnesses have been removed |

{/securecodereview}

{#silversubscription}

# SILVER SUBSCRIPTION

# Overview

Red Team Partners will conduct the Pentest as a Service Silver Subscription using a robust methodology to provide a secure, comprehensive, and effective evaluation. Our team of skilled professionals will perform a thorough analysis of your web application, network, and any other assets that may be exposed on the dark web, identifying weaknesses that could compromise security. Subsequently, we will provide detailed recommendations and actionable steps to help enhance your company’s infrastructure against potential threats.

A diagram of a workflow

Description automatically generated

**Step 1 – Information Gathering & Workflow Study**

We will gather information about the web application, network, company profile, and emails. This helps identify potential vulnerabilities and attack vectors.

**Step 2 – Vulnerability Identification**

In this step we will perform both manual and automated scanning techniques.

We will ensure that the automated vulnerability scanning is conducted in accordance with the customer's agreement and any legal or ethical considerations.

Manual testing is an essential step in testing as it helps to identify vulnerabilities and weaknesses that may have been missed by automated tools. Our team of skilled professionals will perform manual and automatic testing by using various techniques, including:

1. Vulnerability Scanning: This involves scanning the web application and network for known vulnerabilities. We will identify weaknesses in the web application’s configuration, and components, as well as potential network security issues such as open ports, outdated software, and misconfigurations.
2. Vulnerability Assessment: This process involves a detailed analysis of the identified vulnerabilities in both the web application and network. We will evaluate the severity and potential impact of each vulnerability, prioritizing them based on the risk they pose to the organization.
3. Phishing Threat Analysis: This involves identifying possible web domains that may be used to target the company. We will analyze these domains for signs of phishing activities, such as suspicious URLs, cloned websites, and domains that closely resemble the company’s official site.
4. Dark Web Analysis: This involves searching for leaked credentials on the dark web and identifying any company-related information being discussed or sold on dark web forums and marketplaces.

**Step 3 – Reporting**

After the completion of the analysis, a detailed report will be prepared on dashboard that outlines all the vulnerabilities discovered during the assessment, along with recommendations for remediation.

The report typically includes the following information:

1. Management Summary: The report typically includes a management summary that provides an overview of the findings, including the number and severity of findings discovered.
2. Summary of Finding: Each vulnerability is given a severity rating based on the likelihood of it being exploited and the potential impact if exploited.
3. Vulnerability Findings & Technical Details: Each vulnerability discovered during the penetration testing is documented in detail, including the type of findings, the attack vector used to exploit it, and the potential impact of the findings.
4. Recommendations: The report includes recommendations for remediation of the identified vulnerabilities. These recommendations may include specific steps to be taken to address the findings.

{/silversubscription}

{#vulnerabilityassessment}

# Vulnerability Assessment

## Overview

Red Team Partners offers Vulnerability Assessments. Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions.

Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. Red Team Partners employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

The RTP Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The RTP Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

RTP follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

{/vulnerabilityassessment}

{#apipenetrationtesting}

# API Penetration Testing

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. RTP employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

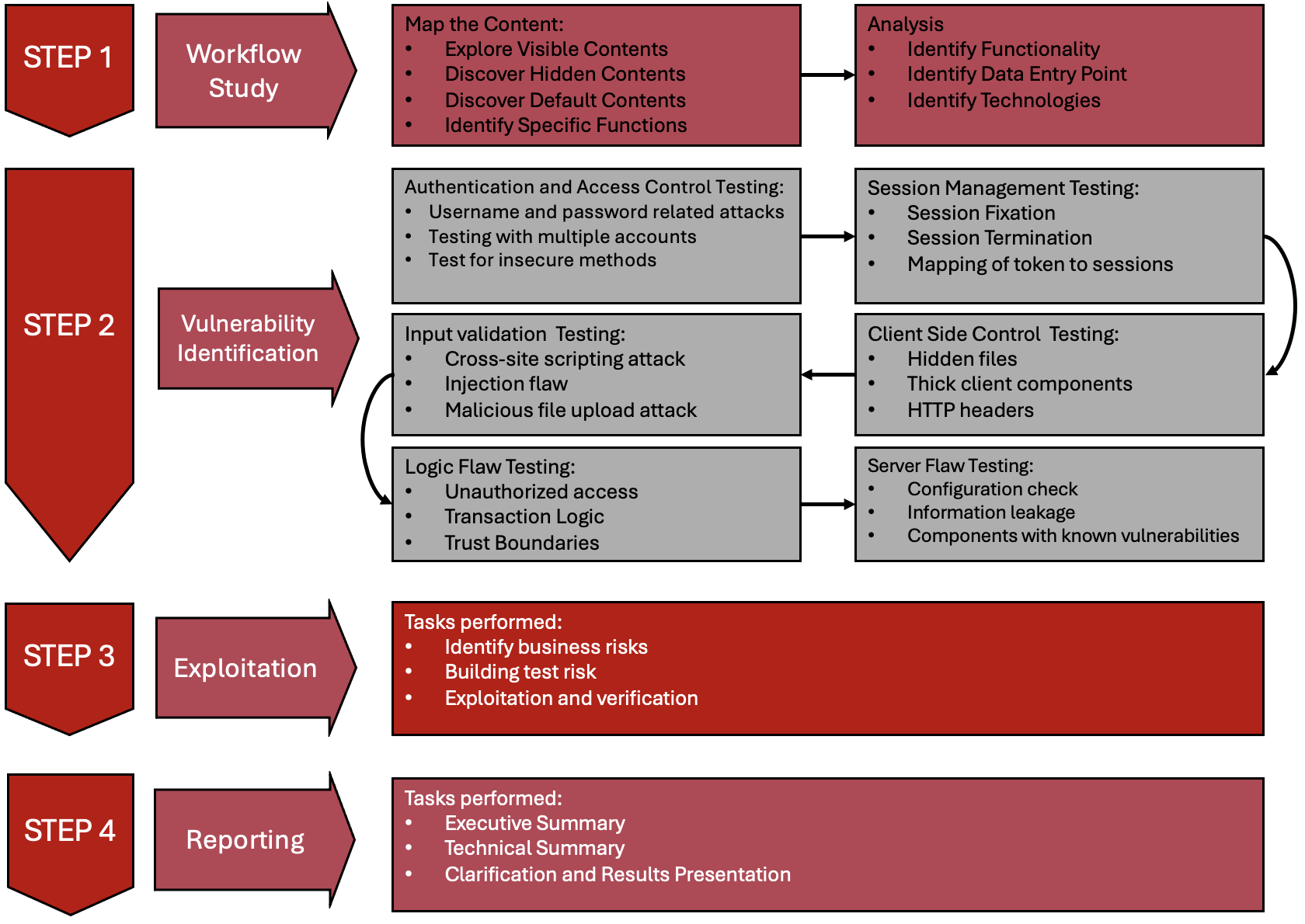
The Red Team Partners Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The Red Team Partners Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client's organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

Red Team Partners follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open-Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Cyber Security Assessment Methodology

The methodology employed during a Cyber Security Assessment involves the following stages:



The steps are aligned to the in-depth security concepts and are focused on process and technical security controls and their implementation in the various phases of the project delivery. The results provided for each activity will include a detailed and comprehensive assessment of client’s current security posture, expansive recommendations, and tools and knowledge to facilitate the continuous improvement.

**Intelligence Gathering & Workflow Study**

Conduct passive and active information gathering to determine the level of information that can be found about the assets in scope. These actions are conducted to understand what level of exposure the assets have, and how an attacker can use this information to conduct further attacks.

**Vulnerability Assessment & Identification**

Security Engineers investigate for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

**Exploitation**

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level.

**Reporting**

The report will communicate to the reader the specific goals of the Penetration Test and technical details of findings of the assessment exercise. The intended audience will be those who oversee the oversight and strategic vision of the security program as well as any members of the organization, which may be impacted by the identified/confirmed threats.

## Type(s) of Test Performed

Red Team Partners security checklist includes, but is not limited to, identification of the following risks:

|  |  |  |
| --- | --- | --- |
| Application Profiling and Information Disclosure | Platform and Third-Party Misconfiguration | Cookie and Session Handling |
| * Default Banners * Unhandled Error Conditions * HTML/JavaScript Comment Information Leakage * Extraneous Content in Web Root * Source Code Disclosure * Robots.txt Path Disclosure * Content Expiration and Cache Control * Bit Bug/Referrer Header Leakage * Account Enumeration * Backup/Archive Content | * Default Administrative Credentials * Default Content and Scripts * Application Script Engine * Web Server * Weak SSL Implementation * Flawed Use of Cryptography | * Session Fixation/Hijacking * Set-Cookie Weaknesses * Sensitive Information Disclosure * Cookie Poisoning * Multiple Simultaneous Login Allowed * Session Timeout * Explicit/Implicit Logout Failures * Cookie less Sessions * Custom Session Management |

|  |  |  |
| --- | --- | --- |
| Command Injection Flaws | Logic Flaws | Client-Side Flaws |
| * SQL Injection * XXE, XPath, and XML Injection * SSI/OS Command Injection * Server Script Injection/Upload * Cross-Site Scripting (XSS) * Buffer Overflow | * Privilege Escalation * Sensitive Information Disclosure * Data Mining/Inference * Functional Bugs * Application-Specific Control Failures * Cross-Site Tracing (XST) * Weak Data Validation * Race Conditions * CPU-Intensive Functions | * Exposure of Sensitive Business * Logic * Reliance on Client-Side Validation * AJAX/Web Service Flaws * Java Applet/ActiveX * Control/Flash Weaknesses |

|  |
| --- |
| Authentication and Authorization |
| * Unauthenticated Sensitive Content * Poor Separation of Privilege * Brute-Force Login * Weak Password Policy * Account Lockout/Denial of Service * SSO Weaknesses * Security Question Weaknesses * CAPTCHA Flaws |

{/apipenetrationtesting}

{#bronzesubscription}

# BRONZE SUBSCRIPTION

# Overview

Red Team Partners will conduct the Pentest as a Service Bronze Subscription using a robust methodology to provide a secure, comprehensive, and effective evaluation. Our team of skilled professionals will perform a thorough analysis of your web application and network. Subsequently, we will provide detailed recommendations and actionable steps to help enhance your company’s infrastructure against potential threats.

A diagram of a workflow

Description automatically generated

**Step 1 – Information Gathering & Workflow Study**

We will gather information about the web application, and network. This helps identify potential vulnerabilities and attack vectors.

**Step 2 – Vulnerability Identification**

In this step, we will perform both manual and automated scanning techniques.

We will ensure that the automated vulnerability scanning is conducted in accordance with the customer's agreement and any legal or ethical considerations.

Manual testing is an essential step in testing as it helps to identify vulnerabilities and weaknesses that may have been missed by automated tools. Our team of skilled professionals will perform manual and automatic testing by using various techniques, including:

1. Vulnerability Scanning: This involves scanning the web application and network for known vulnerabilities. We will identify weaknesses in the web application’s configuration, and components, as well as potential network security issues such as open ports, outdated software, and misconfigurations.
2. Vulnerability Assessment: This process involves a detailed analysis of the identified vulnerabilities in both the web application and network. We will evaluate the severity and potential impact of each vulnerability, prioritizing them based on the risk they pose to the organization.

**Step 3 – Reporting**

After the completion of the analysis, a detailed report will be prepared on dashboard that outlines all the vulnerabilities discovered during the assessment, along with recommendations for remediation.

The report typically includes the following information:

1. Management Summary: The report typically includes a management summary that provides an overview of the findings, including the number and severity of findings discovered.
2. Summary of Finding: Each vulnerability is given a severity rating based on the likelihood of it being exploited and the potential impact if exploited.
3. Vulnerability Findings & Technical Details: Each vulnerability discovered during the penetration testing is documented in detail, including the type of findings, the attack vector used to exploit it, and the potential impact of the findings.
4. Recommendations: The report includes recommendations for remediation of the identified vulnerabilities. These recommendations may include specific steps to be taken to address the findings.

{/bronzesubscription}

{#cloudassessment}

# Cloud Assessment/Review (O365)

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

RTP follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. RTP employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, RTP shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

The RTP Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The RTP Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

RTP follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* hreat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Technical Summary

Any organization needs to implement and operate policies, standards, procedures, guidelines, and controls to assure the security of cloud computing. Cloud security assessment and monitoring will:

* assures the necessary security controls are integrated into the design and implementation of a cloud-based service
* identifies gaps between security control requirements and their actual implementation
* validates that cloud security controls operate and function effectively and
* Serves as the basis for risk acceptance, avoidance, or mitigation decisions.

**Shared Responsibilities and Security Assessment**

Cloud security assessment and monitoring is a shared responsibility. Responsibility for assessment of security controls will vary based on the chosen cloud deployment and service model. In the Infrastructure as a Service (IaaS) model, your organization is responsible for direct assessment of more components and controls, while in the PaaS and SaaS models, your organization must leverage formal certifications or attestations from independent third- parties to assure that the security controls are implemented and functioning effectively.

This assessment aims to highlight any vulnerabilities and misconfigurations in your cloud environment. The assessment combines best practice guidelines and security testing for each type of cloud type.

The controls framework covers fundamental security principles across the following 16 domains, based on CAIQ standard:

|  |
| --- |
| Cloud Security Controls Domains |
| * Application and interface security |
| * Audit assurance and compliance |
| * Business continuity management and operational resilience |
| * Change control and configuration management |
| * Data center processes and operations |
| * Data security and information lifecycle management |
| * Encryption and key management |
| * Governance and risk management |
| * Human resources |
| * Identity and access management |
| * Infrastructure and virtualization security |
| * Interoperability and portability |
| * Mobile security |
| * Security incident management, e-discovery, and cloud forensics |
| * Supply chain management, transparency, and accountability |
| * Threat and vulnerability management |

## Type(s) of Test Performed

* Identifying cloud security risks.
* Performing a cloud security audit to document current controls and provide visibility into the strengths and weaknesses of current systems.
* Assessing gaps in current capabilities that may weaken cloud security in recommending technology and services to address them.
* Assessing security maturity by benchmarking current controls and practices against leading methods and standards.
* Performing a cloud security assessment of the effectiveness of current policies and their alignment with business goals.

{/cloudassessment}

{#cyberawareness}

# Cyber Awareness Training

## Overview

Cyber Awareness Training helps you manage the ongoing problem of social engineering. Discover how you can enable your users to make smarter security decisions.

## Process

**Baseline Testing**

We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

**Train Your Users**

The world’s largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

**Phish Your Users**

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

**See the Results**

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

{/cyberawareness}

{#cyberessential}

# Cyber Essentials Basic (UK Accreditations)

## Overview

Cyber Essentials helps prevent the vast majority of cyber-attacks. Even a simple virus or piece of malware could result in loss of company and client data, disrupt your cash flow, and take up staff time. An attack could also dissatisfy your customers, stop you from trading and damaging your hard-earned reputation. It could also be reported in the local media. Loss of data could breach the Data Protection Act and lead to fines or prosecution.

**Having a Cyber Essentials badge will:**

* Protect your organisation against common cyber threats
* Show your customers this issue matters to you
* Enable you to bid for Government contracts.

## Test Areas

**Step 1: We Identify**

Scanning for vulnerabilities enables the capability to identify all issues which are not in line with the HMG Cyber Essentials scheme. We use technology to automate the search for weaknesses in your system, so you don’t need any prior technical knowledge.

**Step 2: We Fix**

Provided with a list of all devices and their respective issues, the admin can either manually attend to each machine or, can fix issues with one click in the dashboard. For admins with limited cyber security know-how the platform is written in plain English, using smart questions. It offers step-by-step guides and live online support. Our technology ensures good security practices stay in place after certification.

**Step 3: We Certify**

Being secure is only one side of the coin. It is equally important to demonstrate to clients, suppliers and partners, that data protection is a serious matter, and they are in safe hands. It can result in instilling trust and limit liability in case of a breach. You also receive an official Cyber Essentials badge to use online and a physical certificate.

## Result

Cyber Essentials helps prevent the vast majority of cyber-data threats. It is not a one-off exercise but an on-going process. Security standards threats change continuously; for that reason, the software is ideally kept passively running in the background, which allows us to provide you with real-time threat information and security updates. All our offers include one year of on-going support, £25K of free cyber security insurance, and an online support chat. Additional protection and proactive personal support are available upon request.

{/cyberessential}

{#cyberessentialsplus}

# Cyber Essentials Plus (UK Accreditations)

## Overview

Cyber Essentials Plus must be conducted 3 months after Cyber Essentials Basic has been completed.

Cyber Essentials Plus requires an independent assessment of your security controls. This can be provided remotely, the assessment involves a vulnerability scan, which will identify unpatched, or unsupported software, open ports, incorrect firewall configuration. Obtaining Cyber Essentials Plus will verify your company has the correct security controls in place, this certification can only be achieved through the correct preparation and assessments. Cyber Essentials Plus has become a highly regarded certification due its results in improving security controls.

## How Can We Help

Red Team Partners helps companies become Cyber Essentials Plus certified. We provide a pre-audit checklist that contains the correct measures to be taken in order to obtain the Cyber Essentials Plus certification. Once you have completed your pre-audit checklist Red Team Partners certified internal experts will provide any feedback to confirm if any other changes are needed before the audit date.

## How your business benefits:

It is equally important to demonstrate to clients, suppliers and partners that their data is secure. You can add your Cyber Essentials Badge to show businesses that your company is aligned with the UK government cyber standards. As a certified business the steps conduct to achieve this badge can help businesses with their cyber security strategy.

## Result

Once your business has achieved the Cyber Essentials Certification you have the FREE option to have a call with one of our senior consultants to discuss remediations and recommendations. We understand Cyber can be challenging and we are here to help.

All our offers include one year of on-going support and £25K of free cyber security insurance.

\*\*This service does not include any remediation work highlighted from the Pre-audit; this remediation must be carried out inhouse.

{/cyberessentialsplus}

{#goldsubscription}

# Gold Subscription

# Overview

Red Team Partners will conduct the Pentest as a Service Gold Subscription using a robust methodology to provide a secure, comprehensive, and effective evaluation. Our team of skilled professionals will perform a thorough analysis of your web application, network, and any other assets that may be leaked on the dark web, identifying weaknesses that could compromise security. We will then provide detailed recommendations and actionable steps to help you enhance your company’s infrastructure against potential threats.

A diagram of a workflow

Description automatically generated

**Step 1 – Information Gathering & Workflow Study**

We will gather information about the web application, network, company profile, and emails. This helps identify potential vulnerabilities and attack vectors.

**Step 2 – Vulnerability Identification**

In this step we will perform both manual and automated scanning techniques.

We will ensure that the automated vulnerability scanning is conducted in accordance with the customer's agreement and any legal or ethical considerations.

Manual testing is an essential step in testing as it helps to identify vulnerabilities and weaknesses that may have been missed by automated tools. Our team of skilled professionals will perform manual and automatic testing by using various techniques, including:

1. Vulnerability Scanning: This involves scanning the web application and network for known vulnerabilities. We will identify weaknesses in the web application’s configuration, and components, as well as potential network security issues such as open ports, outdated software, and misconfigurations.
2. Vulnerability Assessment: This process involves a detailed analysis of the identified vulnerabilities in both the web application and network. We will evaluate the severity and potential impact of each vulnerability, prioritizing them based on the risk they pose to the organization.
3. Phishing Threat Analysis: This involves identifying possible web domains that may be used to target the company. We will analyze these domains for signs of phishing activities, such as suspicious URLs, cloned websites, and domains that closely resemble the company’s official site.
4. Dark Web Analysis: This involves searching for leaked credentials on the dark web and identifying any company-related information being discussed or sold on dark web forums and marketplaces.
5. Malware Threat Analysis: This involves identifying any malware discussed or sold that could specifically target the company. The analysis focuses on detecting mentions or advertisements of malware designed to exploit vulnerabilities within the company's systems or infrastructure.
6. Social Engineering Threat Analysis: This involves evaluating potential social engineering threats, focusing on the analysis of communication channels and employee interactions.

**Step 3 – Reporting**

After the completion of the analysis, a detailed report will be prepared on dashboard that outlines all the vulnerabilities discovered during the assessment, along with recommendations for remediation.

The report typically includes the following information:

1. Management Summary: The report typically includes a management summary that provides an overview of the findings, including the number and severity of findings discovered.
2. Summary of Finding: Each vulnerability is given a severity rating based on the likelihood of it being exploited and the potential impact if exploited.
3. Vulnerability Findings & Technical Details: Each vulnerability discovered during the penetration testing is documented in detail, including the type of findings, the attack vector used to exploit it, and the potential impact of the findings.

Recommendations: The report includes recommendations for remediation of the identified vulnerabilities. These recommendations may include specific steps to be taken to address the findings.

{/goldsubscription}

{#infrastructuretesting}

# Infrastructure Penetration Testing

## Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of several different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Red Team Partners follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. Red Team Partners employs a comprehensive and careful methodology to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Red Team Partners shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

The RTP Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The RTP Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client’s organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

RTP follows industry best practice standards and methodologies when performing security- assessment activities. Such methodologies include:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Penetration Testing Execution Standard (PTES)
* Open Web Application Security Project (OWASP) Testing Guide
* The National Institute of Standards and Technology (NIST)
* PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
* The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
* OWASP Mobile Security Testing Guide (MSTG)
* Penetration Testing Framework for IoT (PTFIoT)
* PCI DSS ATM Security Guidelines
* CIS Cloud Foundations Benchmark Standard
* OWASP Code Review Guide
* Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
* Application Security and Development Security Technical Implementation Guide
* Social Engineering Attack Framework and Toolkit (SET)
* Digital Forensics Framework (DFF)
* Incident Response Framework (NIST)
* Secure Controls Framework (SCF)
* CREST Penetration Testing Guide
* CSA STAR Self-Assessment / CAIQ
* CIS Secure Platforms Benchmarks (CIS Security)
* Application Security Verification Standard (ASVS)

## Technical Summary

The methodology employed during an Internal and/or External Network Security Assessment involves the following stages:

A diagram of a workflow

Description automatically generated

The steps are aligned to the in-depth security concepts and are focused on process and technical security controls and their implementation in the various phases of the project delivery. The results provided for each activity will include a detailed and comprehensive assessment of client’s current security posture, expansive recommendations, and tools and knowledge to facilitate the continuous improvement.

**Intelligence Gathering & Workflow Study**

Conduct passive and active information gathering to determine the level of information that can be found about the assets in scope. These actions are conducted to understand what level of exposure the assets have, and how an attacker can use this information to conduct further attacks.

**Vulnerability Assessment & Identification**

Security Engineers investigate for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

**Exploitation**

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level.

**Reporting**

The Report will communicate to the reader the specific goals of the Penetration Test and technical details of findings of the assessment exercise. The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization, which may be impacted by the identified/confirmed threats.

## Type(s) of Test Performed

Red Team Partners security checklist includes, but is not limited to, identification of the following risks:

|  |  |  |
| --- | --- | --- |
| Application Profiling and Information Disclosure | Platform and Third-Party Misconfiguration | Cookie and Session Handling |
| * Default Banners * Unhandled Error Conditions * HTML/JavaScript Comment Information Leakage * Extraneous Content in Web Root * Source Code Disclosure * Robots.txt Path Disclosure * Content Expiration and Cache Control * Bit Bug/Referrer Header Leakage * Account Enumeration * Backup/Archive Content | * Default Administrative Credentials * Default Content and Scripts * Application Script Engine * Web Server * Weak SSL Implementation * Flawed Use of Cryptography | * Session Fixation/Hijacking * Set-Cookie Weaknesses * Sensitive Information Disclosure * Cookie Poisoning * Multiple Simultaneous Login Allowed * Session Timeout * Explicit/Implicit Logout Failures * Cookie less Sessions * Custom Session Management |

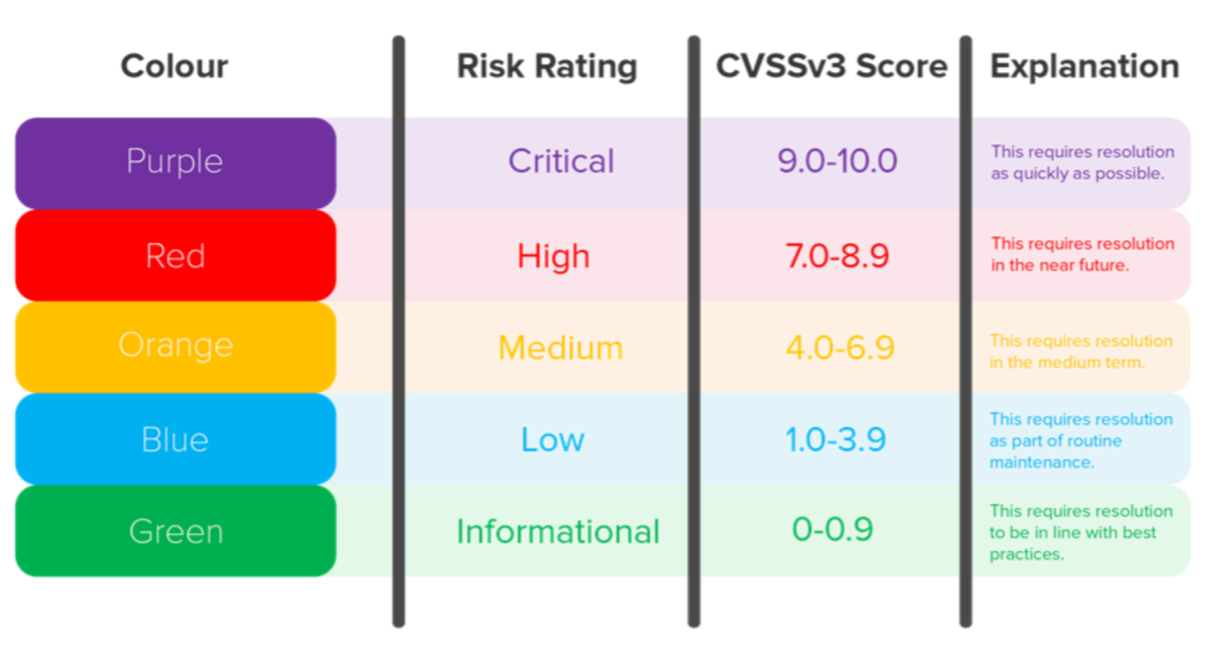
|  |  |  |
| --- | --- | --- |
| Command Injection Flaws | Logic Flaws | Client-Side Flaws |
| * SQL Injection * XXE, XPath, and XML Injection * SSI/OS Command Injection * Server Script Injection/Upload * Cross-Site Scripting (XSS) * Buffer Overflow | * Privilege Escalation * Sensitive Information Disclosure * Data Mining/Inference * Functional Bugs * Application-Specific Control Failures * Cross-Site Tracing (XST) * Weak Data Validation * Race Conditions * CPU-Intensive Functions | * Exposure of Sensitive Business * Logic * Reliance on Client-Side Validation * AJAX/Web Service Flaws * Java Applet/ActiveX * Control/Flash Weaknesses |

|  |
| --- |
| Authentication and Authorization |
| * Unauthenticated Sensitive Content * Poor Separation of Privilege * Brute-Force Login * Weak Password Policy * Account Lockout/Denial of Service * SSO Weaknesses * Security Question Weaknesses * CAPTCHA Flaws |

{/infrastructuretesting}

# REPORTING

After the assessment has been completed, Red Team Partners will evaluate any vulnerabilities detected and evaluate their risk rating. These vulnerabilities will be formulated and presented with next-step actions to mitigate the risks linked to the final report.

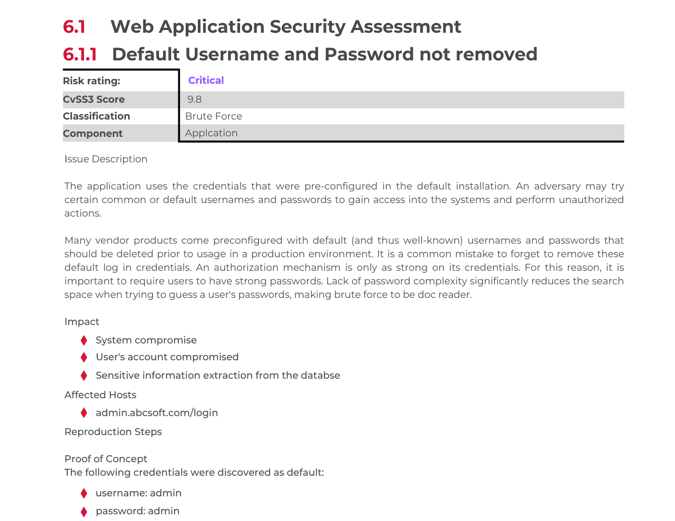


Our reports are presented for management and technical personnel.

**Management Summary** - a high level summary of results including recommendations and overall security posture. This summary is simple and easy to understand it included with critical issues found and it allows non-technical executives to understand the issues.

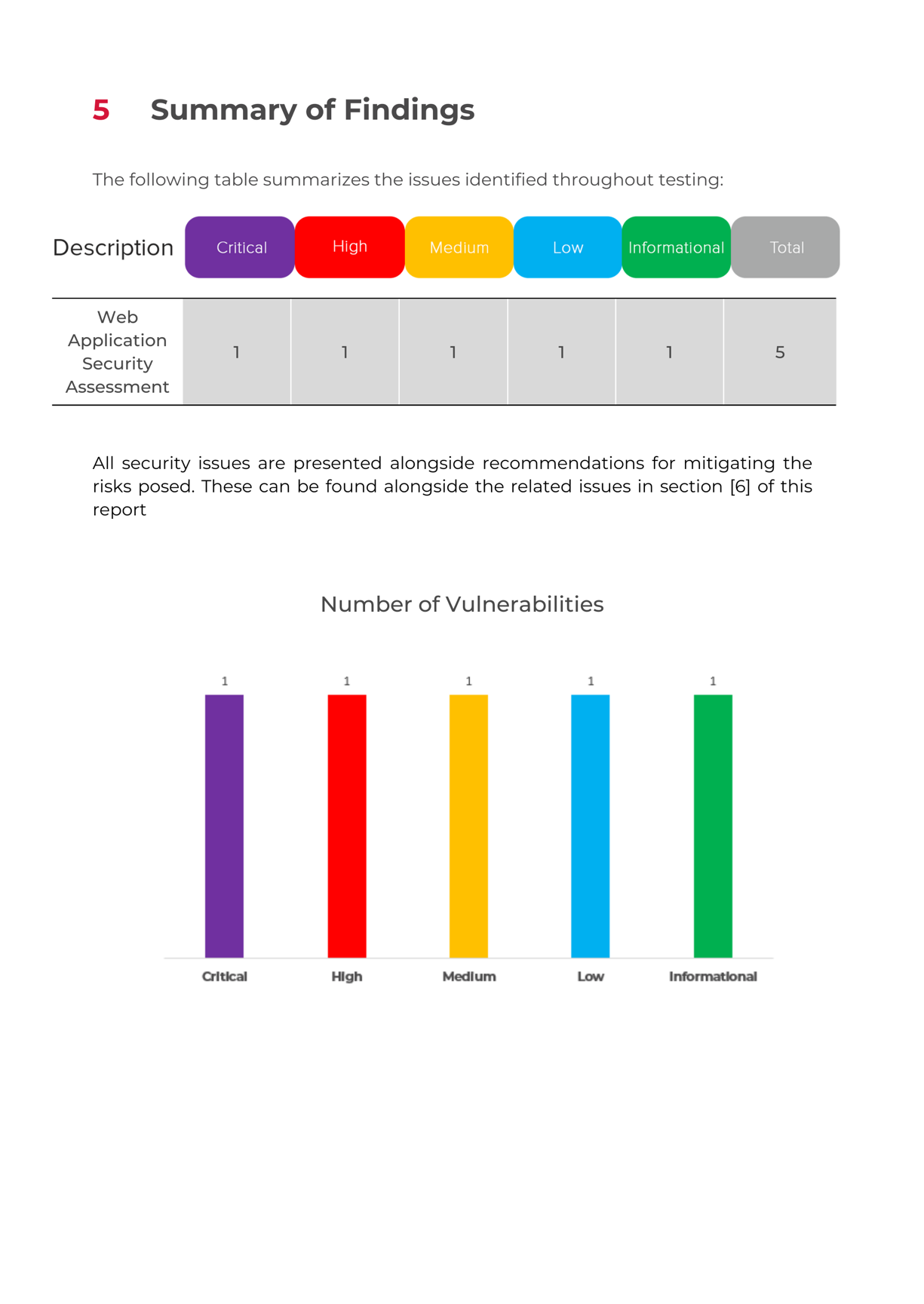


**Technical Findings** - breakdown of vulnerabilities found during testing phase including exploitation probability, technical fix and risk mitigation advice. Prioritised risks are provided to deal with most actionable suggestions.



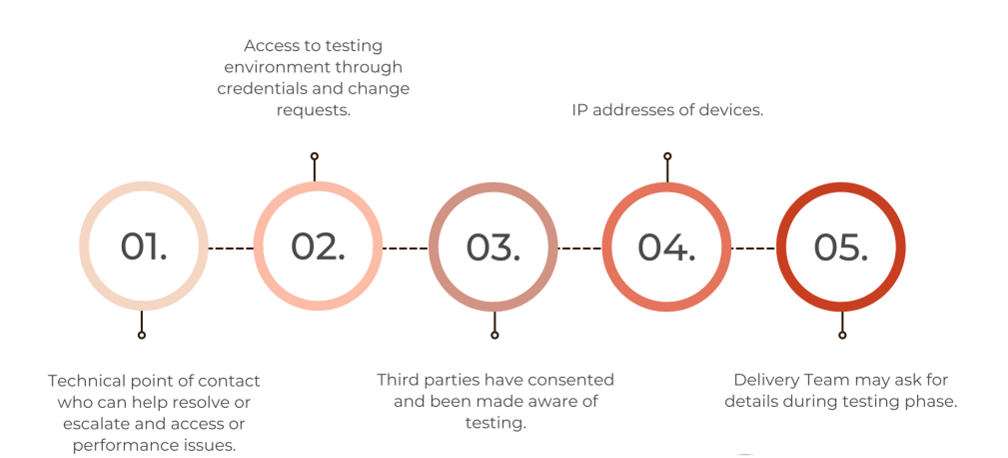
**Evidence** - Evidence of vulnerabilities will be provided within the report, which will include findings of critical flaws and high-risk vulnerabilities. Vulnerabilities are reported in detail showing the depth of our testing, screenshots and examples are provided.

**Recommendations and Remediations** - Based on the discovered findings, our cyber experts provide an in-depth remediation summary based on industry best practice. Samples and screenshots will also be provided within your report.



# DELIVERY STEPS

Red Team Partners delivery team will require the following information before the testing is conducted



# TIMESCALES

Once the dates have been confirmed by our delivery team and a full Statement of Works has been issued, we are able to start conducting testing.

You will be allocated by a project manager as your point of contact. In addition, you will also have access to your lead consultant through our communication platform throughout your testing window. They will be responsible for successfully managing and controlling your project. They will help manage any project issues and track the progress of your project. Meanwhile, the delivery team is accountable for the delivery of the full project and will ensure that it is completed at the expected standard and agreed timescales. All reports are internally reviewed and quality assessed before being released.

# WHY CHOOSE RED TEAM PARTNERS?

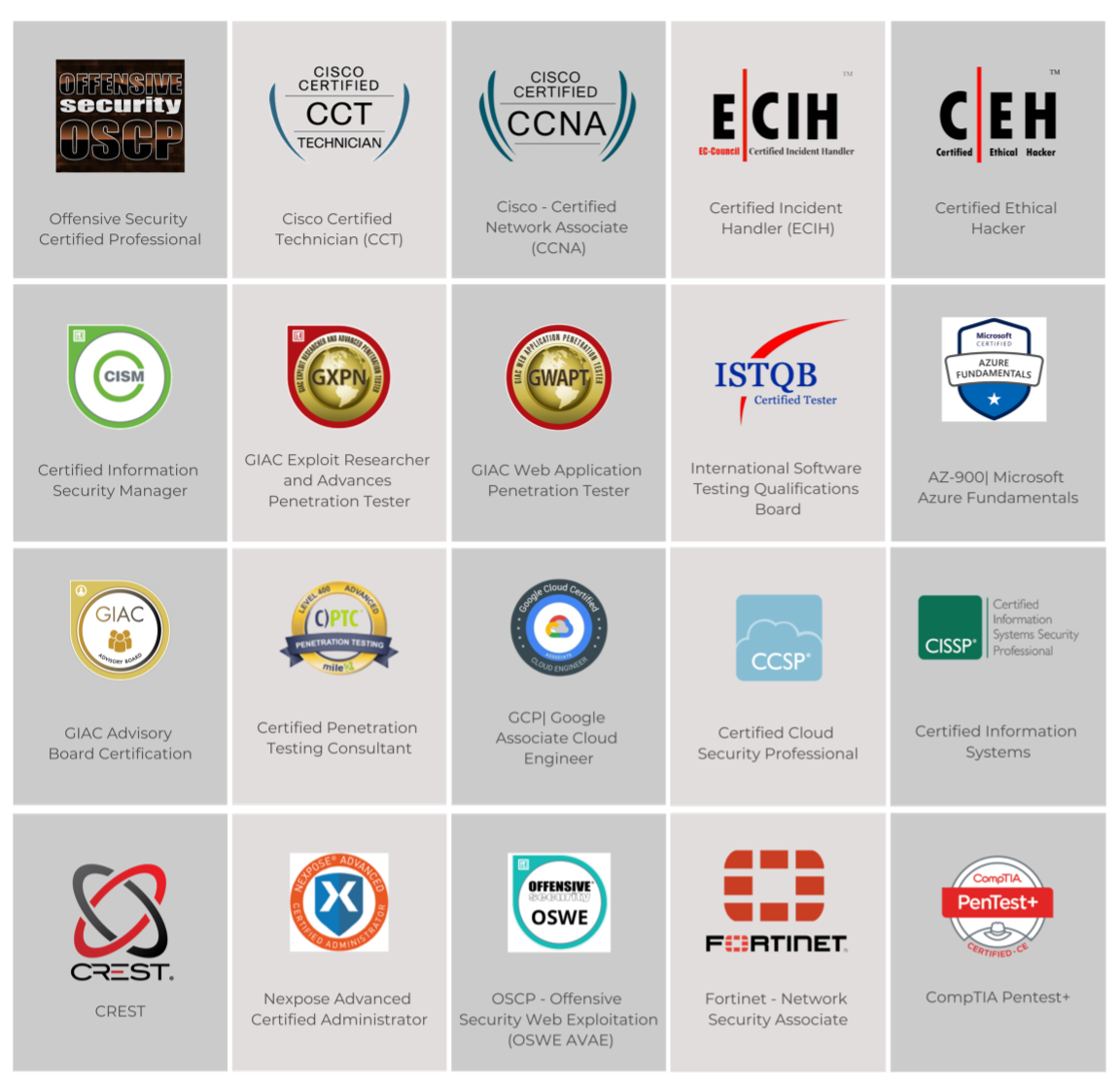
|  |  |
| --- | --- |
| Red Team Partners Experience | Red Team Partners has provided cyber security services on a global scale from small-medium business to enterprise clients. Our speed, quality and customer experience have been a major factor of successful growth and continued success. |
| Red Team Partners Strength | Within the cyber security industry, we have a reputation for fast delivery, excellent quality of service and affordable pricing worldwide. Our team consists of highly renowned experts in the field of cyber security and hold a vast amount of experience by working with cyber strategic intelligence services. Our customers noticeably experience Red Team Partners’ values in our service. |
| Vulnerability Detection | Our teams research through new methods and technologies to identify the most accurate vulnerabilities within your security posture. These accurate findings will provide quantified data to allow actions against findings. |
| Manual Testing | Our tests are conducted manually rather than using automated scanning tools. These techniques are specialised and can often outperform hackers' techniques. Using the manual testing eradicates false positive which are common in scanning tools. |
| Remediations | Our recommendations are provided by cyber experts who can identify real actionable results. Our customers trust these recommendations making sure that these are for the best benefits of the client's security posture. |
| Scalable | We have the capacity to deliver from small to enterprises business worldwide and respond to immediate time scales. |
| Experts in the Field | Our team consists of cyber experts worldwide and are dedicated to helping customers stay secure with years of practical experience in the field. Our team includes experts with CREST, OSCP, CISSP and GWAPT, and CISM. Our certified testers ensure quality of testing and continually research new techniques and technologies. |
| Long Term Vision | One of the main pillars of Red Team Partners is understanding the long-term partnership with organisations. Our purpose is to provide an outstanding service to develop a long-term relationship with our customers. Our customers are confident in our ability to deliver their requirements and they often use us for future projects. |

# OUR QUALIFICATIONS

## Company



## Testers



# OUR SERVICES

**API Penetration Testing**

Test to ensure that the APIs are functioning correctly, are reliable, and perform well. API testing can also help to improve security.

**Web Application Penetration Testing**

Web testing is a process of verifying the functionality of a web application. This can be done prior to a release, or on a day-to-day basis to ensure quality. Web testing allows you to find bugs in the software, which can then be fixed prior to a release.

**Cyber Awareness Training**

Cyber Awareness Training for your workforce. Our training can be customized to your needs. It will educate your employees about cyber threats, policies, and legal compliance, and standard operating procedures in addressing the issue to help produce better service and attract customers.

**Cyber Essentials Basic (UK Accreditation)**

Cyber Essentials Basic provides a range of benefits and is something anyone can use to protect themselves from cyber threats. Whether you have a small business or work for an enterprise, it's easy to get Cyber Essentials certification through Red Team Partners. This will help you to protect your business against a whole range of the most common cyberattacks.

**Cyber Essentials Plus (UK Accreditation)**

Cyber Essential Plus is a step up from the standard. With it, you'll get the same simplicity of approach and the same traditional controls to put in place, but this version adds a hands-on technical verification on top of everything else. Meeting compliance standards can be a tedious and time-consuming process but with our team of experts, we can help you get your certification in less than 24 hours. We make it easy by guiding you through a short questionnaire, matching your needs with the appropriate security requirements, and providing remote CE+ audits.

**Cyber Threat Intelligence**

Security is one of your top priorities and the dark web is the new frontier. Our Cyber Threat Intelligence service provides actionable intelligence to help you navigate this new landscape. We have developed an assessment that identifies dark web-based emerging threats and vulnerabilities to protect your company's most valuable assets and confidential data.

**Cloud Assessment/Review (AWS/Azure/O365)**

Deep dive into your cloud environment and provides an assessment of where your company stands and what you need to do to improve security.

**Firewall Review**

A poorly configured firewall can allow for trivial network compromise by malicious actors. Red Team Partners firewall assessment will test the integrity of your current firewall rules and implementations to ensure nothing has been overlooked.

**Infrastructure Penetration Testing**

This is an effective process of identifying vulnerabilities and weaknesses within your organization’s network infrastructure. It prevents malicious access or loss of confidential data due to IP/ server attacks or internal attacks (servers, workstations, network devices).

**Infrastructure Vulnerability Assessment**

A vulnerability assessment is a systematic review of your company's Internet-facing systems, checking for potential security weaknesses. It is important that you're aware of these issues – misconfigurations and outdated software could put your systems and data at risk. This assessment will help you find, prioritize, and fix these weaknesses before they can be exploited.

**ISO 27001 Consultancy (Global Accreditation)**

Providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

**Mobile Application Testing (IOS/Android)**

Mobile application testing is just one of the many processes involved to make sure an app is successful from end-to-end. It helps you avoid releasing a substandard product to the market.

**Phishing Simulation**

Phishing is one of the most common paths to compromise utilized by attackers in real-world attacks. Phishing Simulation aims to highlight weak security controls and susceptible employees to target for further in-depth phishing awareness training.

**Red Team Assessment**

A thorough investigation of the organization’s security in order to identify and weaknesses that could be exploited by a skilled illegal cyber hacker.

**Secure Code Review**

This code review is a systematic examination (sometimes referred to as peer review) of computer source code. It is intended to find mistakes overlooked in software development, improving the overall quality of software.

**Application Vulnerability Assessment (Black Box / Without Credentials)**

A vulnerability assessment is a systematic review of your company's Internet-facing systems, checking for potential security weaknesses. It is important that you're aware of these issues - misconfigurations and outdated software could put your systems and data at risk. This assessment will help you find, prioritize, and fix these weaknesses before they can be exploited.

# A close-up of a person's face Description automatically generated

# GET IN TOUCH