

**COMPANY XYZ**

**This is a Test Service Name**

**06/30/2021**

**V1.0**



[Introduction](#_Toc3)

[Executive Summary](#_Toc4)

[Technical Summary](#_Toc5)

[Red Team Partners Recommended Next Steps](#_Toc6)

[Appendix - Audit Checklist](#_Toc7)

# Introduction

Red Team Partners services provide a comprehensive review of your organisation's information security. Using industry standard methodologies our consultants have performed a series of assessments designed to discover areas of concern in your business. Conducting a This is a Test Service Name is a process of identifying flaws in business which may be exploited by an attacker. During the engagement, any entry that may be exploited is considered a vulnerability, and the severity of each vulnerability is measured using the latest CVSSv3 scoring system. We categorise all our findings so it’s easy for you to identify root causes and work on solving issues at their core.

Vulnerabilities may be caused by anything from incorrect configuration to out-of-date software or the use of weak authentication. As well as identifying technical vulnerabilities, you may need to review your policies and procedures to ensure that working practices are not vulnerable to other forms of attack. For example, we may identify weak password use or lapses in physical security, which may result or assist in a successful attack. By identifying possible attack vectors from the perspective of an attacker and rating the severity of each vulnerability, we are able to report on how intruders would most likely attempt to gain unauthorised access to your systems.

The purpose of this document is to summarise the findings of the This is a Test Service Name.

# Executive Summary

Red Team Partners has performed a This is a Test Service Name for COMPANY XYZ against its environment. The assessment was carried out between 06/30/2021 - 07/30/2021. In performing a detailed This is a Test Service Name against COMPANY XYZ's environment, Red Team Partners identified (1) Critical and (2) High areas of concern, but overall found This is something about overall security.. Throughout this report we provide brief descriptions of each finding and how it could affect your business.

Overall, Red Team Partners was able to achieve the goals of the (service) and there was a total of 12 findings during the assessment. These where categorised into (1) Critical, (2) High, (3) Medium, (4) Low, (2) Informational.

The key findings during this assessment were:

* Key Findings 01
* Key Findings 02
* Key Findings 03
* Key Findings 04
* Key Findings 05

# Technical Summary

The most important objective of the assessment was to identify any vulnerabilities or potential issues that could affect the systems in scope, in case of a cyber-attack. The security team has conducted the assessment based on the agreed scope to determine the security posture of your organisation.

In order to improve the security of the environment COMPANY XYZ should apply the fixes mentioned in the main report in order of category. We have provided some suggestions below should be reviewed and fixed according to the risk posed to your business model.

Our suggestions for the short-term goals are:

* Short Term 01
* Short Term 02
* Short Term 03
* Short Term 04
* Short Term 05

Medium-Term Goals:

* Medium Term 01
* Medium Term 02
* Medium Term 03
* Medium Term 04
* Medium Term 05

With the identified vulnerabilities, an attacker can abuse the confidentiality, integrity and availability of the system and its components. The overall security posture of the environment presents impactful risks.

The security team recommends that you should conduct a session for planning the remediation of the above-mentioned risks, starting with the highest rated vulnerability.

*For full details on each finding and how to remediate them, your team can refer to the main report. If there are any questions, we can arrange a call with our tester to discuss any part of the report in detail.*

**DISCLAIMERS:** The information presented in this document is provided as is and without warranty. Vulnerability assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks, and applications

# Red Team Partners Recommended Next Steps

Alongside addressing the risks identified, RTP also suggests the following:

* Quarterly Vulnerability Scan and a minimum of an annual Penetration Test.
  + This will ensure the security posture does not regress.
  + Any remediations can be verified in next quarter of testing.
  + Ensure any modifications or application developments do not introduce additional security risks.
* Phishing
  + Regular phishing attacks will ensure staff are reminded of their responsibilities around safeguarding their access and be aware of suspicious activities.
* Longer-term
  + Annual Red Team to ensure the security risks are not just focused on the application or specific environment.
  + Threat Intelligence – security monitoring for pro-active warning of potential risks and attacks.

# Appendix - Audit Checklist

To make remediation more organized, you can use the following checklist:

\*\*\* INSERT TABLE AUDIT CHECKLIST HERE \*\*\*