# Vulnerability Assessment and Penetration Testing Services

Onsite | Remote

## Overview of Service

Identify all 'weak points' within your organisation that are exploitable and learn how to remediate them through advanced reporting.

Remediate all 'weak points' with the assistance of penetration testers and other security experts.

## HOW IT WORKS

Utilize our Pentesters as an independent service or an extension of your team - providing Penetration Tests, and Vulnerability Assessments for all of your attack surfaces.

SCOPING FORM

## SCOPE

- Penetration Testing - Whitebox, Blackbox, Greybox Testing
- External Vulnerability Assessments
- Web Application Scanning
- Domain Health Scanning

## BENEFITS OF VAPT SERVICES

Designed to provide businesses with essential cyber security proactive assessment services - regardless of size.

These services aims to bolster security measures, ensure compliance - with a flexible billing model.

## DESIGNED FOR YOUR BUDGET

Vulnerability assessment and penetration testing (VAPT) services can be procured through two primary expenditure models: Capital Expenditure (CAPEX) or Operational Expenditure (OPEX). CAPEX involves an upfront investment in the services, or allow a Once-off fulfillment of the services. OPEX, on the other hand, entails recurring subscription fees for access to VAPT services, including ongoing support, security consultancy and remediation assistance.

## REPORTING

Following a Vulnerability Assessment and Penetration Test (VAPT), comprehensive reports would be provided to the client. These reports would include detailed lists of identified vulnerabilities, their severity levels, and potential impacts on the organization. Each report would offer actionable recommendations for remediation, including specific steps to address each vulnerability. The reports would be presented in a clear and concise manner, making it easy for the client to understand and prioritize their security efforts. Additionally, each report may include an executive summary, a list of test methodologies used, and any relevant supporting documentation.

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com