CyberProof®
A UST Company

EXPOSURE MANAGEMENT SERVICES: VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Service Definition Document

Approved by: Faizal Ashruf, Head of Exposure Management Services, CyberProof

Contents

Service Definition

Vulnerability Assessment and Penetration Testing (VAPT) is a comprehensive security process designed to identify, analyse, and validate weaknesses within systems, networks, and applications. By integrating automated techniques with manual attack simulations, VAPT reveals real-world risks, enabling organisations to enhance their defences, comply with regulatory requirements, and proactively prevent cyberattacks by addressing identified vulnerabilities.

CyberProof also conducts detailed simulated attacks that allow customers to validate their cyber defences, provide Security Operations Centre (SOC) teams with practical experience managing cyber incidents, and discover opportunities for improvement in team operations, infrastructure, and business processes.

Service Highlights

CyberProof's Penetration Testing service delivers both point-in-time assessments and continuous testing to help organizations proactively identify and secure vulnerable assets. Combining expert-led testing with automation and artificial intelligence, our service uncovers known vulnerabilities, misconfigurations, and enterprise network weaknesses across infrastructure and applications. This blended approach not only supports compliance efforts but also continuously highlights gaps in security coverage, incident response readiness, and the effectiveness of people, processes, and tools thereby enabling organizations to stay ahead of evolving threats.

Service Features

- Web Application Penetration Testing: Comprehensive penetration tests are conducted on web applications to identify vulnerabilities that could be exploited by attackers. The testing simulates real world attack scenarios to evaluate how an attacker could exploit flaws to access sensitive data, manipulate user sessions, escalate privileges, misuse business logic, or compromise the hosting environment. This helps determine not just the presence of vulnerabilities, but their actual exploitability, impact, and the effectiveness of existing security controls.
- Cloud Configuration Review: A comprehensive review of cloud environment configurations is conducted using industry-recognized benchmarks such as the CIS Controls and cloud service provider best-practice frameworks. This ensures alignment with security best practices and enables the identification of misconfigurations that could expose the organisation to security risks.
- Red Teaming/Adversarial Simulation: As part of our goal oriented red teaming activities, CyberProof simulates targeted attacks based on sophisticated and industry specific threat actors to evaluate how well the organisation can withstand realistic adversarial behaviour. These exercises are designed to align with the organisations unique risk profile, and physical security breach attempts are typically excluded from the scope of delivery.

  During the engagement, we conduct realistic attack scenarios including phishing campaigns, Advanced Persistent Threat simulations, ransomware scenarios, and Assumed Breach

operations. These simulations allow us to assess the effectiveness of the current security stack in identifying, containing, and responding to tactics commonly used by known adversaries targeting the organisation or its wider industry. This approach provides a practical and accurate measure of the organisation's real world defensive readiness.

- Mobile Application Penetration Testing: Mobile Application Penetration Testing evaluates the security of applications deployed on Android and iOS, examining client-side behaviour, data storage, communication channels, and platform specific security controls. CyberProof assess both the platform specific security test cases and the application's logical and functional security test cases to ensure thorough coverage. This also includes platform independent mobile applications, such as hybrid apps and PWAs, where execution environments, API interactions, and cross platform security boundaries are analysed. The objective is to identify vulnerabilities, validate real world exploitability, and provide actionable remediation guidance to ensure secure performance across all mobile platforms and development frameworks.
- Network and Infrastructure Penetration Testing: Testing covers both internal and external network and infrastructure components. It involves systematic enumeration of exposed services, identification of outdated or unpatched operating systems and firmware, and evaluation of misconfigurations within network access controls and segmentation policies. The assessment also includes exploitation attempts against insecure protocols, weak authentication mechanisms, legacy services, and improperly hardened network devices. This approach provides a realistic view of potential attack paths, lateral movement opportunities, and the overall resilience of the organisation's network architecture.
- Compliance Specific Vulnerability Assessment Analysis: Beyond the baseline security frameworks CyberProof follows, the assessment scope can be further customized through pre-engagement discussions with the customer to ensure alignment with their unique business, operational, and regulatory requirements. Such assessments are tailored to the organisation's compliance obligations, ensuring alignment with relevant regulatory requirements and industry standards such as **PCI DSS**, **HIPAA**, **ISO/IEC 27001**, **NIST SP 80053**, **SOC 2**, and **GDPR**, where applicable. This ensures that identified vulnerabilities are evaluated in the context of mandated controls, audit expectations, and risk management priorities defined by the chosen compliance frameworks. The outcome supports effective remediation planning and demonstrates the organisation's readiness for external audits or certification processes.

Service Benefits

- Proactive Detection and Validation of Vulnerabilities: Early identification and thorough validation of vulnerabilities within customer environments ensure that weaknesses are detected before they can be exploited by an adversary.
- Expertise Across Multiple Sectors: CyberProof possesses extensive experience delivering penetration testing services tailored to the unique needs and threat landscapes of various industries. Our methodologies are designed to be adaptable across diverse operational landscapes and are informed by extensive experience working with industries such as BFSI,

Telecom, and Retail, ensuring relevance regardless of operational sectors or environmental complexity.

- Risk Scoring Aligned with Organisational Environment and Exposure: Vulnerabilities are evaluated and mapped using an industry-recognised risk scoring methodology that reflects the organisation's distinct environment and exposure profile, ensuring prioritisation of the most pertinent threats.
- Prioritisation of High-Impact and High-Exposure Assets: The assessment process focuses on assets with the greatest impact and exposure, ensuring critical systems and data receive attention within the defined scope of engagement.
- Assessment of Significant and Chained Exploitation Risks: Vulnerabilities are evaluated not only individually but also in combination (chained attacks), offering a robust understanding of potential threat vectors.
- Structured Categorisation and Prioritisation: Identified vulnerabilities are systematically categorised and prioritised based on impact, exploitability, and alignment with the MITRE framework, enabling informed remediation decisions.
- Actionable Reporting: Assessment findings are clearly documented, outlining vulnerabilities and their practical implications within the organisation's context. Stakeholders receive prioritised insights and actionable recommendations, supporting immediate remediation and long-term resilience. The reporting process bridges communication between technical teams and management, promoting informed decision-making and continuous improvement in security practices.
- **Certified, Expert Global Offensive Security Team** CyberProof team comprises certified professionals empanelled by CREST, ensuring adherence to global best practices and industry standards. The team consists of **highly certified professionals who operate according to globally recognised methodologies** and industry best practices. Our experts are spread across the globe, enabling around the clock coverage, diverse threat perspectives, and deep familiarity with regional threat landscapes. The team includes accomplished bug bounty researchers with proven success on major platforms, bringing real world offensive insight into every engagement. We also have CVE authors who have identified and responsibly disclosed vulnerabilities in widely used technologies, backed by advanced certifications from Certification bodies such as Off Sec, CREST etc, and more, ensuring research driven, high quality security assessments.
- CyberProof provides clear visibility into the organisation's most significant security risks by identifying and validating vulnerabilities early. Our reporting highlights the issues that matter most to the business, focusing leadership attention on high impact assets and services.
- Findings are prioritised using recognised risk models and aligned with the organisation's environment and exposure, giving a clear view of where action is most urgently needed. Guidance is provided directly to asset and service owners to support rapid remediation and strengthen overall resilience.
- Drawing on broad sector experience, our assessments translate technical risks into business level insights, helping leadership shape security strategy, allocate resources effectively, and improve long term operational readiness and managing risk from exposures.

Service Delivery and Engagement Model

CyberProof's VAPT team delivers services through a globally distributed workforce, ensuring around-the-clock coverage, rapid responsiveness, and access to diverse technical expertise. Each engagement requires a minimum lead time of two weeks following the finalisation of scope and completion of all pre-engagement prerequisites. These pre-engagement interactions include scope discussions, walkthroughs where necessary, validation of asset/ environment readiness, access provisioning requirements, and alignment on testing constraints or business critical blackout windows. The engagement will commence only after the scope, objectives, and system boundaries are clearly defined, documented, and formally approved by both parties, ensuring transparency, controlled execution, and alignment with organisational expectations.

Over the past decade, we have developed a custom knowledge library informed by our experience across diverse industries. Our team of penetration testers, holding industry-recognized credentials and backed by this extensive knowledge base, delivers services designed to reduce exposure and minimize risk.

CyberProof also collaborates with trusted industry partners such as Wiz and Horizon3.ai, and is supported by our in-house automation framework, we ensure timely project delivery while maintaining the highest standards of quality and risk control.

Following the completion of testing activities and delivery of the final report, CyberProof conducts a post engagement lesson learned workshop with key stakeholders. This session provides a structured walkthrough of findings, exploitation paths, risk interpretations, and recommended remediation strategies, ensuring clarity and shared understanding across technical and business teams. The workshop also addresses defensive control gaps observed during testing, trends or patterns identified relevant to business priorities, and quick-wins or security enhancements to application, infrastructure, or cloud security architecture. Additionally, the session incorporates feedback from both sides to refine future testing approaches, strengthen collaboration, and ensure continuous maturity of the organisation's security posture.

Deliverables

As part of the engagement, key deliverables will be shared with the customer across different phases. These deliverables are designed to provide actionable recommendations and strategic guidance, ensuring a clear understanding of security posture and empowering informed decision-making at all levels.

After completing the security assessment, CyberProof delivers a comprehensive report detailing the tests performed and the vulnerabilities identified. These reports will include in-depth findings from the testing process, tailored insights for leadership, and a summary of key security risks and mitigations.

The following reports (as deliverables) are provided to the Customer by CyberProof as part of this service.

- **Interim Report:**

Any critical or high-risk vulnerabilities found in the customer environment are effectively communicated to the customer within one business day.

- **Executive Summary Report:**

Provides a concise summary of key vulnerabilities, highlighting critical security issues and their impact on the organization's systems, along with observable patterns or trends of concern. This is suitable for the leadership and executive team.

- **Comprehensive Technical Report:**

This report will contain: -

  - Detailed Findings: Outline the vulnerabilities discovered including severity, exploitability, and proof-of-concept, and provide clear evidence through screenshots and references to active CVEs and / or EPSS and / or KVEs.
  - Actionable Remediation Guidelines: Provide actionable remediation guidelines, offering recommendations to mitigate or remediate vulnerabilities to enhance security posture.
  - Summary of activities carried out during the Security Assessment Services.

- **One-time Revalidation Report**

  - Thorough Revalidation: Ensure that the issues identified in the initial assessments are properly addressed, going beyond just confirming the replication of initial proof of concepts.
  - Root Cause Focus: Evaluate whether the root cause of vulnerabilities has been properly addressed.

Governance Model

For each engagement, a designated Point of Contact will be appointed, serving as the Program Manager or Technical Account Manager (TAM) for that engagement. Delivery teams, formed based on project requirements, will include a Lead and an appropriate number of analysts aligned to the defined scope and estimated duration.

The assigned Project Manager or TAM will be the primary point of contact who will interface with customers for all aspects of service delivery and operations during the engagement term from updates to the Final Report.

The Project Manager/ TAM will: -

- Serve as a primary point of contact to Customer for ongoing operational activities.
- Establish and maintain communications through the Customer point of contact.
- Communicate material risks to the project and propose remediation plans if applicable.

- Provide governance, oversight, and leadership for project activities and processes, as required.
- Monitor SOW or other agreement compliance by both parties as applicable.

All deliverables, including engagement reports, will undergo a mandatory two-level review process to ensure accuracy, completeness, and alignment with agreed objectives. If high or critical risks are identified, relevant teams will be notified within one business day. Reports are shared only after successful completion of both review stages and formal approval.