Service Description

What the platform does, and what a subscription includes.

1. Overview

superhack provides a software-as-a-service platform designed to identify, prioritize, and help remediate security vulnerabilities across the Customer's authorized systems, applications, and infrastructure.

The platform uses specialized AI agents to autonomously perform reconnaissance, attack-surface mapping, and penetration testing against the Customer's authorized targets, analyzing and contextualizing data related to discovered assets, hosts, services, endpoints, configurations, and vulnerabilities.

superhack is intended to support IT, cyber information security, and risk management teams in discovering, understanding, and remediating security weaknesses across the vulnerability lifecycle, including identification, validation, prioritization, and remediation tracking. The Services support security, risk management, and operational decision-making, but do not replace Customer's own security controls, monitoring, or compliance obligations.

---

2. Functional Scope

The Services may include, without limitation, functionality in the following areas:

a) Security Posture Analysis

Autonomous analysis of the Customer's authorized attack surface — including exposed services, endpoints, configurations, and security-relevant signals — in order to assess overall security posture and identify exploitable weaknesses.

b) Risk Detection and Findings

Identification and surfacing of potential security risks, misconfigurations, policy violations, or hygiene issues, presented as findings with contextual information and remediation guidance.

c) Attack Surface Mapping

Discovery, visualization, and assessment of the Customer's assets, services, and their exposure across the authorized environment to support attack-surface reviews, audits, and remediation prioritization.

d) Operational Workflows

Case-based workflows supporting security-relevant operational processes, such as user offboarding, access changes, or incident-related reviews, including tracking of remediation activities.

e) Inventory and Visibility

Structured views of discovered assets, hosts, services, endpoints, and identified vulnerabilities to enable exploration, filtering, and reporting.

f) Administrative Configuration and Reporting

Administrative configuration of rules, thresholds, and settings, as well as reporting and audit-supporting capabilities.

---

3. Nature of the Services

The Services provide analytical insights, prioritization, and recommendations based on data gathered from the Customer's authorized targets and observed signals. Outputs are informational in nature and do not constitute legal, compliance, or security guarantees.

The Services do not guarantee the detection or prevention of all security issues, vulnerabilities, or incidents within the Customer’s environment.

---

4. Evolution of the Services

superhack may modify, enhance, or remove functionality from time to time as part of the normal evolution of the Services. Descriptions in this Exhibit are for informational purposes only and do not constitute a binding commitment, feature guarantee, or roadmap representation.

---

5. Beta and Experimental Features

Certain functionality described in this Exhibit may be designated by superhack as Beta or Experimental Features. Any such features are governed exclusively by the Beta & Experimental Features Terms and are not part of the generally available Services.