1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **monosem-planters.com**. The analysis commenced on **June 5th at 20:00** and concluded in a duration of **00h:05m:12s**. The assessment was identified with tracking ID **155b1525b20b** and was categorized as a **Basic** type scan. The primary objective was to evaluate the security posture of the domain, focusing on identifying High and Medium-risk issues that could impact the business.

1.2 Summary of Key Issues

The security assessment identified one High-risk issue. The critical High-risk finding involves a shared hosting environment with over **16,751** domains sharing the same IP address, posing significant security risks such as potential data breaches and service disruptions. Immediate attention is required to address this High-risk shared hosting vulnerability to mitigate potential threats.

1.3 Issues Table

Title	Risk
Shared Hosting Environment	High

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description

The analysis revealed a High-risk shared hosting environment where the domain **monosem-planters.com** is hosted alongside 16,751 other domains on the same IP address. This configuration significantly increases the risk of data breaches and service disruptions due to shared infrastructure vulnerabilities. The presence of such a large number of shared domains indicates a potential for cross-site contamination and unauthorized access to sensitive data.

Affected Assets

- **Hostname:** monosem-planters.com

Recommendations

It is recommended to migrate the domain to a dedicated hosting environment to mitigate the risks associated with shared hosting. This will reduce the likelihood of cross-site contamination and enhance the overall security posture of the domain. Additionally, implementing strict access controls and regular security audits can further protect against potential threats.

1.5 General Recommendation

To enhance security, it is advisable to conduct regular security assessments and implement a robust monitoring system to detect and respond to threats promptly. Ensuring that all software and systems are up-to-date with the latest security patches will also help in maintaining a secure environment.