1 Executive Security Assessment Report

1.1 Introduction

This report provides an executive-level overview of the security assessment conducted on the domain **plmusc.us.baesystems.com**. The analysis was performed using a Basic scan type, initiated on **April 29th at 22:45** and completed in **00h:09m:37s**. The evaluation focused on identifying High and Medium-risk vulnerabilities within the domain's infrastructure, following OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, with **1 Low-risk** and **17 informational findings**. The most significant concern is the Low-risk issue related to SSL/TLS protocols, where only TLS 1.2 is supported, lacking the more secure TLS 1.3, which could impact data confidentiality. No High or Medium-risk vulnerabilities were detected, indicating a generally secure environment. Key metrics include **100% of servers located in the USA** and **0% unresolved subdomains**, suggesting robust infrastructure management. Actionable insights include upgrading to TLS 1.3 for enhanced security and maintaining regular monitoring of SSL certificate expirations to prevent potential service disruptions.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security	Low

1.3.1 SSL/TLS Protocols Security Assessment

Description The assessment of SSL/TLS protocols revealed that the domain supports only TLS 1.2, which is currently considered an acceptable minimum standard but lacks the enhanced security features and performance improvements offered by TLS 1.3. The absence of support for TLS 1.3 could potentially impact data confidentiality and overall security posture.

Affected Assets

- **1 endpoint** using TLS 1.2

Recommendations It is recommended to upgrade the existing infrastructure to support TLS 1.3 to align with current best practices for security and performance. This upgrade will enhance data confidentiality and provide improved cryptographic algorithms, ensuring a more robust defense against potential threats.

1.4 General Recommendation

To maintain a secure environment, it is crucial to regularly update and patch all systems, conduct periodic security assessments, and ensure compliance with industry standards. Implementing TLS 1.3 across all endpoints will significantly enhance security measures. Additionally, continuous monitoring of SSL certificate expirations and other critical security metrics will help prevent potential service disruptions and maintain a strong security posture.