1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **host.twistlock.gcso.cbre.com**. The analysis commenced on **July 6th** at **15:01** and concluded in a duration of **00h:06m:58s**. The assessment was identified by tracking ID **0e69977e6f18** and classified as a “Basic” type scan. The scope of the work included a comprehensive evaluation of the domain’s security posture, focusing on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies.

1.2 Short Summary

The recent security assessment revealed no High, Medium, or Low-risk issues, with **three** informational findings. Notably, all scanned ports are filtered, indicating robust perimeter security controls such as well-configured firewalls and active IPS/IDS systems. The analysis confirmed no shared hosting environments, with all hosts on dedicated infrastructure, minimizing potential cross-domain vulnerabilities. Additionally, all servers are located in the United States, with no presence in high-risk locations, ensuring a normal geographic distribution. These findings suggest a strong security posture, but continuous monitoring and manual verification are recommended to maintain this status.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues Found	N/A

1.4 Detailed Findings

1.4.1 Description

The security assessment did not identify any High or Medium-risk issues. This indicates that the domain **host.twistlock.gcso.cbre.com** maintains a strong security posture with effective perimeter defenses. The absence of critical vulnerabilities suggests that the current security measures are adequate in protecting against common threats.

1.4.2 Affected Assets

- Domain: **host.twistlock.gcso.cbre.com**

1.4.3 Recommendations

Despite the absence of High or Medium-risk vulnerabilities, it is recommended to continue regular security assessments to ensure ongoing protection against emerging threats. Implementing a robust patch management process and conducting periodic manual reviews can further enhance the security posture. Additionally, maintaining up-to-date firewall configurations and monitoring for any unusual activity will help sustain the current level of security.

1.5 General Recommendation

To maintain and improve the current security posture, it is advised to implement continuous monitoring solutions and conduct regular penetration testing exercises. This proactive approach will help in identifying potential vulnerabilities before they can be exploited by malicious actors. Furthermore, fostering a culture of security awareness among employees can significantly reduce the risk of human error leading to security breaches.