1 Executive Security Assessment Report

Domain Analyzed: us-sbc2.cbre.com
Tracking ID: 011c16e92a48
Analysis Type: Basic
Date and Time: Initiated on March 18 at 10:00
Duration: 00h:05m:54s

The security assessment was conducted using OWASP and OSCP methodologies. The analysis focused on identifying High and Medium-risk vulnerabilities within the specified domain. The assessment did not reveal any High or Medium-risk issues, highlighting the effectiveness of current security measures.

1.1 Short Summary of Main Issues

The security assessment did not identify any High or Medium-risk issues. The robust perimeter security and dedicated infrastructure use were confirmed, with all servers located in the United States, ensuring a normal risk profile.

1.2 Key Security Issues

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

1.3 Detailed Findings

1.3.1 Description

The security assessment of the domain **us-sbc2.cbre.com** revealed no High or Medium-risk vulnerabilities. The perimeter security was found to be robust, with all **11** scanned ports being filtered, indicating effective firewall and intrusion prevention systems. The infrastructure is dedicated, mitigating potential cross-domain vulnerabilities. All servers are geographically located in the United States, avoiding high-risk areas.

1.3.2 Affected Assets

- Domain: **us-sbc2.cbre.com**
- Scanned Ports: **11**

1.3.3 Recommendations

To maintain the current security posture, it is recommended to continue regular security assessments and manual verifications. This proactive approach will ensure that the infrastructure remains resilient against evolving threats. Additionally, maintaining up-to-date firewall configurations and intrusion prevention systems is crucial for ongoing protection. Regularly reviewing server locations and ensuring they remain in low-risk geographic areas will further mitigate potential risks.

1.4 General Recommendation

It is advised to conduct periodic security assessments and manual verifications to ensure continued protection against evolving threats. Maintaining current security controls, such as firewalls and intrusion prevention systems, is essential for safeguarding the infrastructure. Regular updates and reviews of server locations should be performed to ensure they remain in low-risk geographic areas, thereby minimizing potential exposure to threats.