1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `oneview.truist.com` using a Basic scan type. The analysis commenced on May 25th at 12:45 and concluded in **00h:16m:06s**. The tracking ID for this assessment is **0d64f0aef7c1**. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized by risk level as follows: **1 High**, **1 Medium**, **1 Low**, and **15 informational**. The most critical finding is the detection of **9 login forms**, classified as High due to potential unauthorized access, which could significantly impact business operations if exploited. Additionally, a Medium issue was identified with open HTTP ports lacking encryption, posing a risk of data interception. The Low finding pertains to SSL/TLS protocols, with all endpoints supporting modern standards like TLS 1.3. Notably, **100%** of servers are located in the USA, with no high-risk geographic locations detected. Immediate actions should focus on securing login interfaces and ensuring HTTP to HTTPS redirection to mitigate potential vulnerabilities.

1.3 Issues Table

Title	Risk
Login Form Detection Analysis	High
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security	Low

1.4 Detailed Findings

1.4.1 Login Form Detection Analysis

Description:
A total of **9 login forms** were detected across the application, posing a High risk due to the potential for unauthorized access. The presence of multiple login interfaces increases the attack surface, making it easier for attackers to exploit weak or improperly secured forms.

Affected Assets:
- URLs associated with detected login forms include: - `https://oneview.truist.com/Content/accounts/mock-data/reports/BG-report-download.json` - `http://oneview.truist.com/Content/accounts/mock-data/reports/BG-report-download.json` - `http://oneview.truist.com/Content/resources/sftp-delivery/getSftpDeliveryDetails.json` - `http://oneview.truist.com/Content/mainapp/mock-data/billing-account.json` - `https://oneview.truist.com/Content/accounts/mock-data/account-details/balances/` - `https://oneview.truist.com/Content/accounts/mock-data/account-details/transactions/` - `http://oneview.truist.com/Content/resources/documentHistory/userList.json` - `https://oneview.truist.com/Content/resources/documentHistory/userList.json` - `https://oneview.truist.com/UI/config/config.json`

Recommendations:
- Implement strong authentication mechanisms such as multi-factor authentication (MFA). - Ensure all login forms are served over HTTPS to protect credentials in transit. - Regularly audit and monitor login attempts for suspicious activities. - Limit the number of login interfaces to reduce the attack surface.

1.4.2 Nmap Port Scan Results Analysis

Description:
The scan identified **2 open ports**, with port **80** running HTTP without encryption. This poses a Medium risk as it allows potential data interception unless there is a redirection to HTTPS or HSTS is enabled.

Affected Assets:
- IP: **13.249.59.21** - Ports: **80/tcp**, **443/tcp**

Recommendations:
- Implement HTTP to HTTPS redirection to ensure all traffic is encrypted. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly review and close unnecessary open ports to minimize exposure.

1.4.3 SSL/TLS Protocols Security Assessment

Description:
The assessment confirmed that all endpoints support modern SSL/TLS protocols, with **4 endpoints** using TLS 1.3 and another **4 using TLS 1.2**. There are no endpoints using deprecated protocols like SSLv3, TLS 1.0, or TLS 1.1, indicating a Low risk in this area.

Affected Assets:
- Endpoints with TLS 1.3: **4** - Endpoints with TLS 1.2: **4**

Recommendations:
- Continue supporting TLS 1.3 as it offers improved security and performance. - Phase out TLS 1.2 where possible and ensure all configurations adhere to best practices. - Regularly update SSL/TLS configurations to protect against emerging threats.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the remediation of High and Medium issues identified in this assessment. Implementing robust authentication mechanisms, ensuring encrypted communications, and maintaining up-to-date security configurations will significantly mitigate potential vulnerabilities. Regular security audits and monitoring should be conducted to detect and respond to any new threats promptly.