1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **test.apigee.firstdata.com** using a Basic analysis type. The scan was initiated on **April 30th at 07:00** and completed in **00h:08m:30s**. The tracking ID for this assessment is **1758687f25c5**. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **1 High-risk**, **4 Medium-risk**, **1 Low-risk**, and **13 informational**. The most critical finding is the imminent expiration of an SSL certificate in **26 days**, posing a significant risk to secure communications. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, unusual port assignments, and potentially sensitive subdomains, which could expose the organization to cyber-attacks and unauthorized access. The low-risk finding pertains to the use of TLS 1.2 without TLS 1.3 support, indicating room for improvement in encryption standards. Immediate actions should focus on renewing the SSL certificate and implementing a WAF to mitigate these vulnerabilities.

1.3 Key Security Issues

Title	Risk
SSL Certificate Expiration Analysis	High
Absence of WAF	Medium
Unusual Port Assignments Detected	Medium
Subdomain Naming Security Assessment	Medium
Nmap Port Scan Results Analysis	Medium

1.3.1 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain **test.apigee.firstdata.com** is set to expire in **26 days**, categorizing it as a critical risk. This expiration poses a significant threat to secure communications, potentially leading to service disruptions and loss of trust from users.

Affected Assets:
- HTTPS-enabled subdomain: **test.apigee.firstdata.com**

Recommendations:
Immediate renewal of the SSL certificate is essential to maintain secure communications. Implement an automated monitoring system to alert administrators well in advance of future expirations.

1.3.2 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was detected on **100%** of the analyzed hosts. This lack of protection significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks, which could lead to unauthorized data access and potential system compromise.

Affected Assets:
- Host: **test.apigee.firstdata.com**

Recommendations:
Deploy a robust WAF solution to filter and monitor HTTP traffic between the web application and the internet. Regularly update WAF rules to protect against emerging threats.

1.3.3 Unusual Port Assignments Detected

Description:
Unusual port assignments were identified, with services running on non-standard ports or ports running unexpected services. This may indicate attempts to evade detection or misconfigured applications, increasing the risk of unauthorized access.

Affected Assets:
- Host: **test.apigee.firstdata.com (107.23.127.47)** - Port: **80**

Recommendations:
Conduct a thorough review of port configurations and ensure that services are running on standard ports unless there is a specific business need. Implement strict firewall rules to restrict access to non-standard ports.

1.3.4 Subdomain Naming Security Assessment

Description:
A potentially sensitive subdomain associated with development/staging and API endpoints was identified. Such subdomains may contain unpatched vulnerabilities or debug information, providing access to critical systems and sensitive data.

Affected Assets:
- Subdomain: **test.apigee.firstdata.com**

Recommendations:
Restrict access to development and staging environments, ensuring they are not exposed to the public internet. Regularly audit subdomains for sensitive information and apply necessary security patches.

1.3.5 Nmap Port Scan Results Analysis

Description:
Port 80 is associated with HTTP service, flagged for lacking encryption, necessitating verification for HTTPS redirection or HSTS enablement. This lack of encryption could expose data in transit to interception.

Affected Assets:
- IP Address: **107.23.127.47** - Ports: **80/tcp** (http?), **443/tcp** (ssl/https)

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS and that HSTS is enabled to enforce secure connections. Regularly review and update security configurations for all open ports.

1.4 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network traffic. Additionally, educating staff on cybersecurity best practices will help mitigate risks associated with human error.