1 Executive Security Assessment Report

1.1 Overview

This report presents the findings from a security assessment conducted on the domain **identity.yoti.com**. The assessment was initiated on March 19th at **21:45** and completed in **12** minutes and **40** seconds. The analysis was performed using a Basic scan type. The scope of the assessment included evaluating the security posture of the web application and its infrastructure, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Summary of Key Issues

The security assessment identified a total of **19** issues, categorized as **1** High-risk, **2** Medium-risk, **2** Low-risk, and **14** informational. The most critical finding is the imminent expiration of an SSL certificate in **24** days, posing a significant risk to secure communications and potentially impacting business continuity. Medium-risk issues include the absence of a Web Application Firewall (WAF), leaving **100%** of hosts vulnerable to injection attacks, and the exposure of HTTP port **80**, which lacks encryption. Immediate action is recommended to renew the SSL certificate and implement a WAF to mitigate these vulnerabilities.

1.3 Issues Table

Title	Risk
SSL Certificate Expiration Analysis	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assess.	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 SSL Certificate Expiration Analysis

Description:

The SSL/TLS certificate for the domain **identity.yoti.com** is set to expire in **24** days, categorizing it as a critical risk that requires immediate action. Failure to renew the certificate could lead to disruptions in secure communications and potential loss of trust from users.

Affected Assets:

- Domain: identity.yoti.com

Recommendations:

Immediate renewal of the SSL certificate is essential to maintain secure communications. Implement automated monitoring for certificate expiration to prevent similar issues in the future.

1.4.2 Absence of WAF

Description:

The absence of a Web Application Firewall (WAF) results in a **100%** vulnerability rate, significantly elevating the risk of successful cyber-attacks, particularly injection-based attacks. This lack of protection increases the risk of unauthorized data access, data breaches, and potential system compromise.

Affected Assets:

- Host: identity.yoti.com

Recommendations:
Deploy a Web Application Firewall to provide an additional layer of security against injection attacks and other web-based threats. Regularly update and configure the WAF to adapt to evolving threats.

1.4.3 Nmap Port Scan Results Analysis

Description:
Port **80** is flagged as potentially insecure due to lack of encryption. It requires verification for HTTPS redirection or HSTS implementation. The HTTP service running on yoti-edge-proxy poses a risk if not properly secured.

Affected Assets:
- IP: **185.116.53.15** - Ports: **80/tcp** (http), **443/tcp** (ssl/http)

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS and that HSTS is enabled to enforce secure connections. Regularly audit open ports and services for potential vulnerabilities.

1.5 General Recommendations

To enhance the security posture of identity.yoti.com, it is recommended to prioritize the renewal of expiring SSL certificates and the implementation of a Web Application Firewall. Additionally, ensure all HTTP traffic is securely redirected to HTTPS, and maintain regular security audits to identify and mitigate emerging threats promptly.