1 Executive Security Assessment Report

1.1 Overview

This report provides a detailed analysis of the security assessment conducted on the domain **p6analytics.mtn.com**. The assessment was initiated on **08-04** at **12:45** and completed in **00h:20m:13s**. The scope of the work included a basic security analysis using OWASP and OSCP methodologies to identify potential vulnerabilities within the web application and infrastructure.

1.2 Summary of Findings

The recent security assessment revealed no High, Medium, or Low-risk issues, with three informational findings. Notably, all scanned ports were filtered, indicating robust perimeter security controls, such as a well-configured firewall and active IPS/IDS systems, with **100%** of ports filtered. The analysis confirmed no shared hosting environments, ensuring dedicated infrastructure for all hosts. Additionally, the geographic distribution of servers showed normal patterns, with no servers located in high-risk areas. These findings suggest a strong security posture, but further manual verification is recommended to ensure comprehensive coverage and address any potential blind spots in automated assessments.

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. The findings were limited to informational observations that highlight the effectiveness of existing security measures. All scanned ports were filtered, which suggests that perimeter defenses are well-configured and actively managed. The absence of shared hosting environments indicates that each host operates on dedicated infrastructure, reducing the risk of cross-contamination from other tenants. Furthermore, the geographic distribution of servers aligns with expected patterns, with no presence in high-risk areas.

1.4.2 Affected Assets

- **Domain:** p6analytics.mtn.com
- **Ports:** **100%** filtered
- **Hosting Environment:** Dedicated infrastructure
- **Server Locations:** No high-risk areas detected

1.4.3 Recommendations

1. **Manual Verification:** Conduct a thorough manual review to complement automated scans and ensure no vulnerabilities are overlooked.
2. **Continuous Monitoring:** Implement continuous monitoring solutions to detect and respond to potential threats in real-time.
3. **Security Audits:** Schedule regular security audits to maintain and improve the current security posture.
4. **Training and Awareness:** Provide ongoing security training for staff to recognize and mitigate potential security threats.

1.5 General Recommendation

While the current security posture appears robust, it is crucial to maintain vigilance through continuous monitoring and regular security audits. Manual verification should be employed to ensure comprehensive coverage beyond automated assessments. Additionally, fostering a culture of security awareness among staff can significantly enhance the organization's ability to prevent and respond to emerging threats.