TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GOAA

June 15, 2026

GOAA 06/15/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

This report corresponds to March 2026 and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC`s Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, Cyber Security Validation and Access

ABOUT THIS REPORT

The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

Hosts & Vulnerable Hosts In Last 6 Months

During the March reporting period, the external vulnerability assessment identified 38 externally exposed assets, of which 33 were found to contain at least one vulnerability. The findings were primarily concentrated within the medium severity category, highlighting opportunities to improve the security configuration of Internet-facing services.

The most significant findings included insecure web server configurations, information disclosure through HTTP headers, support for deprecated cryptographic protocols such as TLS 1.0 and TLS 1.1, and the use of weak cipher suites, including RC4 and configurations affected by the SWEET32 vulnerability.

Although no critical or high-severity vulnerabilities were identified during the reporting period, the observed conditions indicate areas where security controls can be further strengthened. Continued remediation and configuration hardening efforts will help reduce the organization's external attack surface and enhance its overall security posture over time.

Total Attacks Successfully Blocked

0

This metric is not available because the corresponding service is not currently included within the contracted scope.

Critical Attacks Successfully Blocked

0

This metric is not available because the corresponding service is not currently included within the contracted scope.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

GOAA 06/15/2026

Vulnerability Metric

5

During March, GOAA maintained a stable external security posture, with no critical or high-severity vulnerabilities identified. All findings were limited to medium-severity issues related to security hardening and configuration improvements.

The most common observations involved legacy cryptographic support, weak cipher suites, information disclosure through HTTP headers, and web server configuration weaknesses. Addressing these findings will help reduce external exposure and further enhance the organization's defensive posture.
Overall, the results demonstrate a controlled risk environment and reflect the value of continuous vulnerability monitoring and remediation activities in maintaining and improving GOAA’s external security posture.

TLP:AMBER = Limited disclosure, restricted to participants’ organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500