TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GOAA

May 16, 2026

GOAA 05/16/2026

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 hosts, of which 33 were found to present vulnerabilities across monitored environment. The findings remained concentrated within the medium severity range, reflecting continued exposure primarily associated with configuration weaknesses affecting externally accessible services.
The most relevant findings identified during the period were related to insecure web server configurations, internal information disclosure through HTTP headers, deprecated cryptographic protocol support such as TLS 1.0 and TLS 1.1, and weak cipher suite configurations including RC4 and SWEET32.
Although no critical or high severity vulnerabilities were confirmed during the reporting period, the identified exposure conditions continue to highlight opportunities to strengthen externally published services and further reduce the organization’s external attack surface through ongoing remediation and configuration hardening efforts.

Total Attacks Successfully Blocked

0

Critical Attacks Successfully Blocked

0

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

GOAA 05/16/2026

Vulnerability Metric

5

The overall vulnerability profile during the March reporting period remained predominantly concentrated within the medium severity range, reflecting persistent security conditions associated with configuration weaknesses and hardening opportunities across externally exposed assets. While no critical or high-severity findings were identified during the assessment period, the continued presence of these findings reinforces the value of continuous external assessment, as these conditions may contribute to increased attack surface visibility and create opportunities for external reconnaissance activity.

The findings observed during March were primarily driven by recurring conditions related to deprecated cryptographic protocol support, weak cipher suite configurations, internal information disclosure through HTTP headers, and insecure web server configurations affecting externally published services. These conditions continue to highlight areas where focused remediation efforts would further strengthen the resilience infrastructure.

This metric underscores the importance of maintaining proactive vulnerability monitoring and remediation activities to sustain visibility over external exposures, reduce potential attack paths, and progressively strengthen GOAA's overall external security posture over time.

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