TLP:AMBER

CISO EXECUTIVE REPORT

GOAA

May 16, 2026

GOAA 05/16/2026

TLP AMBER CISO
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.

VULNERABILITY

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 Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	198.136.190.71	0
Current	6	

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.

THREATS

Total Number of Successful MFA authentications per application

During the March reporting period, authentication activity monitored through the Managed Trusted Access Service (MSS-TAS) reflected successful multi-factor authentication activity associated with one active user, with access concentrated on the Skywatch application.

The recorded authentication activity was observed from the source IP address 198.136.190.254.
No authentication failures or anomalous access patterns were identified within the observed activity.

These results reflect normal trusted access behavior during the period and reinforce the value of continuous authentication monitoring in maintaining visibility over access patterns, validating legitimate user activity, and supporting early detection of deviations that may require further review.

Attacks Successfully Blocked by Severity

GOAA 05/16/2026

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	1	2
Critical Device Outages	0	0

During the March reporting period, system availability monitoring recorded 1 device outage. No critical device outages were identified during the period.

The detected event was identified as a momentary availability fluctuation, and validation performed at the time of review did not confirm an active service interruption or sustained impact affecting the monitored asset.

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Probe Device	System Health	MSS-CSME-GOAA	Warning		53	2026-03-05 13:52:34	2026-04-01 08:10:43
goaanet	Ping v2	MSS-CSME-GOAA	Down		1	2026-03-18 21:18:08	2026-03-18 21:18:08
goaanet	HTTPS v2	MSS-CSME-GOAA	Down		1	2026-03-05 08:42:18	2026-03-05 08:42:18
goaanet	HTTP Advanced	MSS-CSME-GOAA	Down		1	2026-03-05 08:42:15	2026-03-05 08:42:15

During the March reporting period, availability monitoring identified isolated and momentary events ,primarily associated with goaanet and routine probe health warnings. No critical outages were recorded during the period.

Validation performed at the time of detection confirmed that these events were temporary fluctuations, and no sustained service interruption was observed across the affected monitored assets.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	0	0	0	0	0

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

GOAA 05/16/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in External High or Critical Vulnerabilities	476
Non Baselined Discovered System	82
Monitoring for open ports	39
High Persistency Detection	15
BAS Immediate Threat	5
Change in Systems Performance	1
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8

During the March reporting period, several notable events were identified across GOAA's monitored environment. The highest volume of activity was observed within the Change in External High or Critical Vulnerabilities monitoring category. Following validation, these events were confirmed to correspond primarily to tracked changes associated with externally exposed assets, with identified findings remaining concentrated within the medium and low severity ranges.

As part of the established monitoring process, once these events were validated, the corresponding cases were created and notified for follow-up, allowing continued tracking and visibility over the identified conditions as remediation and review activities progressed throughout the period.

Additional relevant activity included 82 Non-Baselined Discovered System events and 39 Monitoring for Open Ports detections, providing continued visibility into asset exposure changes and externally accessible services requiring validation

---

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.**

TLP:AMBER

CISO 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