TLP:AMBER

CISO EXECUTIVE REPORT

GOAA

May 16, 2026

GOAA 05/16/2026

TLP AMBER CISO
EXECUTIVE REPORT

This report corresponds to APRIL 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 month of April,
the Managed External Attack Surface Monitoring, Network and Application Vulnerability Testing and External Pentest (MSS-EASM) service identified 47 externally exposed hosts, of which 38 were found to present vulnerabilities, representing an increase compared to the 33 vulnerable hosts identified in March. This variation reflects changes in the externally visible attack surface and reinforces the importance of maintaining continuous visibility over internet-facing assets.

The vulnerability distribution for April remained primarily concentrated within the medium severity range, consistent with previously observed trends. The most relevant findings continue to be associated with insecure web server configurations, internal information disclosure through HTTP headers, the absence of HTTP Strict Transport Security (HSTS), deprecated cryptographic protocol support such as TLS 1.0 and TLS 1.1, and certificate trust and configuration weaknesses.

While no critical or high severity vulnerabilities were identified during the period, the increase in vulnerable hosts observed during April highlights the need to sustain remediation efforts and reinforce secure configuration practices across exposed services. Maintaining focus on these areas will support the continued reduction external attack surface and strengthen the overall resilience of internet-facing systems.

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 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 reporting period, the continued presence and increase of these findings reinforces the value of continuous external assessment, as these conditions may contribute to expanded attack surface visibility and create opportunities for adversaries to perform reconnaissance or leverage chained exploitation techniques.

The increase observed during April was primarily driven by recurring findings related to cryptographic protocol obsolescence, certificate configuration inconsistencies, and missing security controls affecting externally published services. These conditions continue to highlight areas where strengthened remediation efforts would further enhance the resilience internet-facing infrastructure.

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

THREATS

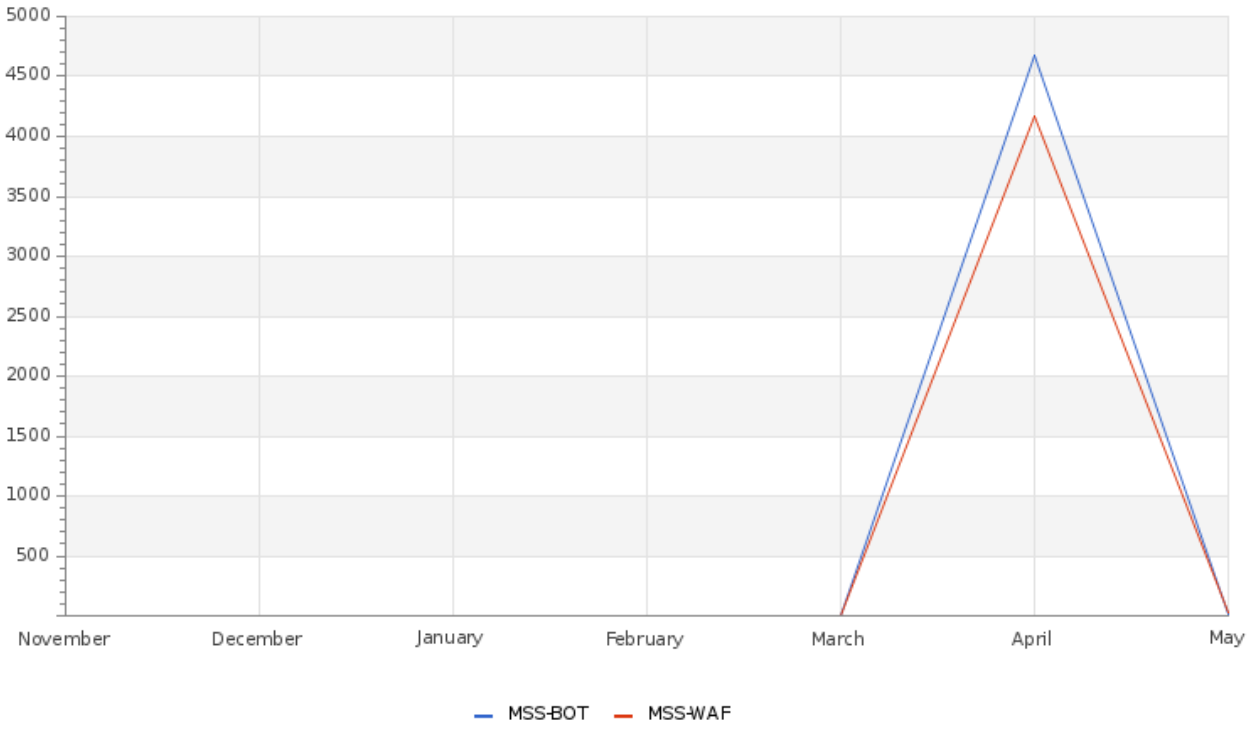
Total Number of Successful MFA authentications per application

During the April, authentication activity monitored through the Managed Trusted Access Service (MSS-TAS) reflected successful multi-factor authentication events associated with three active users, with access concentrated on the Skywatch application.

From a geographic perspective, all recorded authentication activity originated from the United States, with a total of 7 successful authentication events observed during the month. This consistency supports visibility into trusted access behavior and reinforces the value of continuous authentication monitoring to validate legitimate access patterns and support early identification of deviations that may require further review.

Total Attacks Successfully Blocked Per Service

GOAA 05/16/2026



During the April, web application protection controls recorded sustained activity directed at internet-facing services, with 4,800 attack events mitigated through MSS-BOT and 3,951 attack events successfully blocked through MSS-WAF-CLOUD. These figures reflect the constant level of automated external activity targeting publicly accessible resources and reinforce the importance of maintaining layered application-layer protection mechanisms.

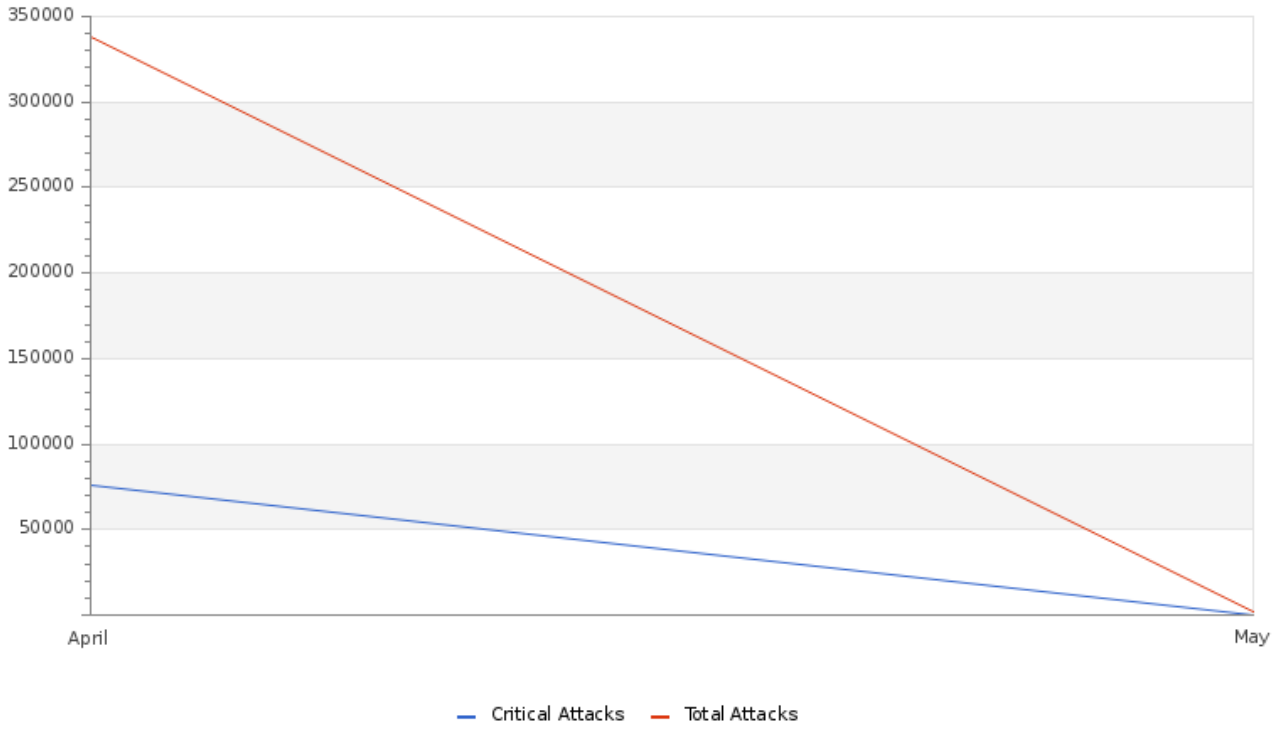
The blocked activity primarily consisted of automated reconnaissance, validation attempts, and malicious interaction patterns designed to identify exposed resources, enumerate accessible application paths, and test application behavior for potential weaknesses. The most recurrent activity types remained associated with HTTP protocol anomalies, unauthorized resource access attempts, predictable resource location probing, and input validation manipulation attempts.

From an executive security perspective, these results demonstrate the continued operational effectiveness of GOAA’s proactive defensive controls in preventing automated threat activity from interacting successfully with protected applications, while maintaining visibility into evolving attack patterns directed at the organization’s external web infrastructure.

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

GOAA 05/16/2026

Attacks Successfully Blocked by Severity



System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	7	0
Critical Device Outages	0	0

During the April reporting period, system availability monitoring recorded 7 total device outages. Despite this increase in availability-related events, no critical device outages were identified, indicating that none of the observed interruptions resulted in high-impact disruption to monitored critical infrastructure.

Continuous visibility over device availability remains essential for identifying operational anomalies in a timely manner and supporting appropriate response actions when service interruptions are detected.

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

GOAA 05/16/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
iprotestapi.goaa.org/	iprotestapi.goaa.org/	MSS-CSME-GOAA	Down		391	2026-04-14 23:01:08	2026-04-30 17:06:22
iproapi.goaa.org/	iproapi.goaa.org/	MSS-CSME-GOAA	Down		129	2026-04-08 23:11:57	2026-05-01 09:13:24
Probe Device	System Health	MSS-CSME-GOAA	Warning		49	2026-04-01 08:10:43	2026-04-29 15:08:05
iprotest.goaa.org/#/loginDevice	iprotest.goaa.org/#/login	MSS-CSME-GOAA	Down, Warning		21	2026-04-14 22:50:45	2026-04-15 00:30:45
iprodev.goaa.org/#/login	iprodev.goaa.org/#/login	MSS-CSME-GOAA	Down		19	2026-04-14 23:00:49	2026-04-15 00:30:49
mcotaxidispatch.goaa.org/userlogin	mcotaxidispatch.goaa.org/userlogin	MSS-CSME-GOAA	Down		5	2026-04-23 11:02:32	2026-04-23 11:22:32
Probe Device	Probe Health	MSS-CSME-GOAA	Down		2	2026-04-17 02:16:41	2026-04-20 17:26:01
Flymco	HTTP Advanced	MSS-CSME-GOAA	Warning		1	2026-04-24 23:38:29	2026-04-24 23:38:29
ipro.goaa.org/#/login	ipro.goaa.org/#/login	MSS-CSME-GOAA	Warning		1	2026-04-08 23:06:56	2026-04-08 23:06:56
Flymco	flymco.com	MSS-CSME-GOAA	Down		1	2026-04-02 19:54:09	2026-04-02 19:54:09

During the April, availability monitoring identified intermittent service interruptions primarily affecting iprotestapi.goaa.org and iproapi.goaa.org, along with isolated events impacting additional monitored assets within the GOAA environment. No critical outage events were recorded during the period.

All detected interruptions were reported and notified at the time of occurrence in accordance with established monitoring and escalation procedures, ensuring timely visibility for review and validation by the corresponding operational teams.

From an operational monitoring perspective, these events highlight the continued value of real-time availability oversight in supporting prompt visibility into service disruptions and maintaining awareness of infrastructure performance across monitored services.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	4,690	0	0	0	1,646

During the April, layered web protection controls continued to demonstrate effective defensive performance, with 4,690 attack events mitigated by MSS-BOT and 1,646 events successfully blocked through MSS-WAF-CLOUD.

This activity reflects continued automated threat targeting against internet-facing services, including bot-driven interactions, reconnaissance attempts, and application-layer validation activity directed at externally exposed resources.

The distribution of blocked events across both security layers highlights the effectiveness of GOAA’s multi-layered protection strategy, where MSS-BOT provides mitigation against automated abusive traffic patterns while MSS-WAF-CLOUD delivers inspection and blocking capabilities against application-layer exploitation attempts.

From an executive security perspective, these results reinforce the operational effectiveness of the deployed security controls in maintaining protection coverage and reducing exposure to automated external threats targeting services.

GOAA 05/16/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in External High or Critical Vulnerabilities	115
Monitoring for open ports	39
Non Baselined Discovered System	53
High Persistency Detection	15
BAS Immediate Threat	5
Change in Systems Performance	1
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8

During the April, several notable events were identified across monitored environment. The highest number of events was observed under the Change in External High or Critical Vulnerabilities category, with 115 detections. It is important to note that, following validation, the findings associated with these alerts were confirmed to correspond primarily to medium and low severity vulnerabilities.

Additional notable activity included 53 Non-Baselined Discovered System events and 39 Monitoring for Open Ports detections, providing visibility into changes across externally exposed assets and services requiring review. Other relevant activity included 15 High Persistency Detection events, 2 Targeted Campaign Alignment alerts, and 5 BAS Immediate Threat notifications.

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