TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GOAA

May 16, 2026

GOAA 05/16/2026

TLP AMBER BOARDROOM

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.

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 (MSSEASM) 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 Attacks Successfully Blocked

8882

During the April reporting period, web application protection controls successfully mitigated 8,882 attack events directed at internet-facing services. This sustained activity reflects the continuous presence of automated external reconnaissance and validation attempts targeting publicly exposed resources.

The blocked activity was primarily associated with automated probing, protocol manipulation attempts, unauthorized resource access validation, and reconnaissance patterns aimed at identifying potential weaknesses across published applications. These results continue to demonstrate the effectiveness of the deployed protection layers in preventing hostile interactions from reaching protected services while maintaining visibility into evolving external threat activity.

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

GOAA 05/16/2026

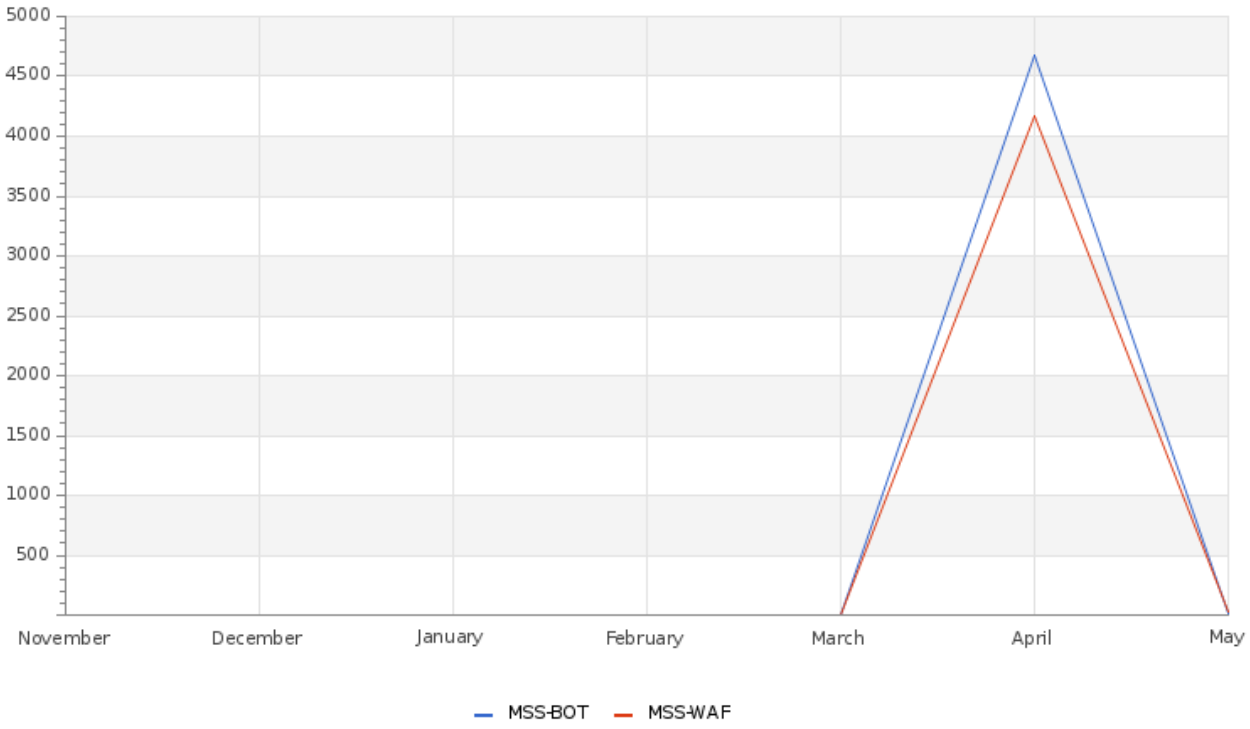
Critical Attacks Successfully Blocked

4192

A total of 4,192 critical attack events were successfully blocked during the reporting period. These detections correspond to higher-priority malicious activity patterns identified and mitigated by the deployed security controls before interaction with protected resources could occur.

The successful prevention of these events highlights the operational effectiveness layered web protection strategy in detecting and blocking higher-risk attack attempts, reinforcing the organization's defensive posture against application-layer threats targeting externally exposed services.

Attacks Successfully Blocked



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.

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.

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