TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GOAA

June 15, 2026

GOAA 06/15/2026

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 (MSS-EASM) service identified 47 externally exposed hosts, of which 38 were found to contain vulnerabilities. This represents an increase compared to the 33 vulnerable hosts identified in March. The 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 category, consistent with trends observed in previous reporting periods. The most significant findings continued to be related to insecure web server configurations, information disclosure through HTTP headers, the absence of HTTP Strict Transport Security (HSTS), support for deprecated cryptographic protocols such as TLS 1.0 and TLS 1.1, and certificate trust and configuration weaknesses.

Although no critical or high-severity vulnerabilities were identified during the reporting period, the increase in the number of vulnerable hosts highlights the importance of maintaining remediation efforts and reinforcing secure configuration practices across exposed services. Continued focus on these areas will help reduce the external attack surface and strengthen the overall resilience of Internet-facing systems.

Total Attacks Successfully Blocked

8882

During the April reporting period, activity targeting Internet-facing services was observed and mitigated by the web application protection controls deployed within the environment. As the service is currently operating under a Proof of Value (PoV) phase, final metrics and validated figures are not yet available. However, preliminary observations indicate the continued presence of automated activity directed at publicly exposed resources.
>
> The observed activity was primarily associated with reconnaissance attempts, resource validation requests, and automated probing intended to identify potential weaknesses in published applications. These preliminary results demonstrate the effectiveness of the deployed protection mechanisms and provide visibility into external activity targeting the monitored services.

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

GOAA 06/15/2026

Critical Attacks Successfully Blocked

4192

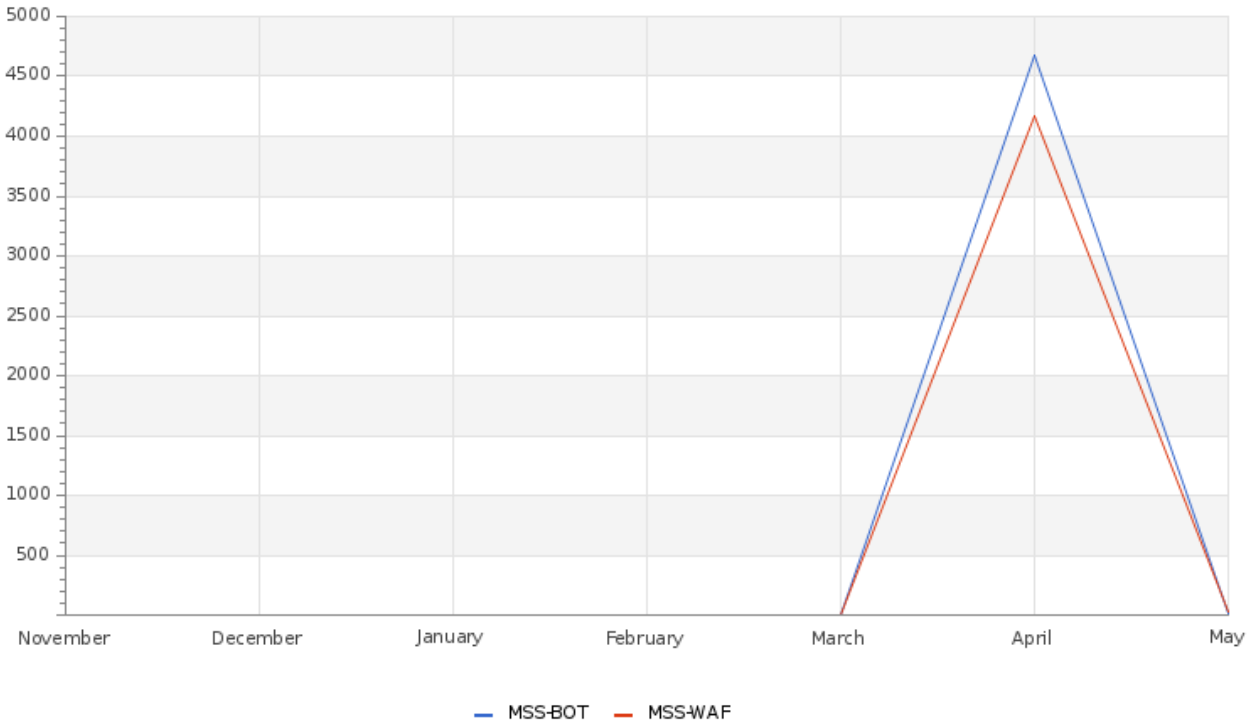
A total of 4,192 critical attack events were successfully blocked during the reporting period. These detections correspond to higher-priority malicious activity patterns identified and mitigated by the deployed security controls before interaction with protected resources could occur.

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.

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

GOAA 06/15/2026

Attacks Successfully Blocked



During April, web application protection controls recorded sustained activity targeting Internet-facing services, with 4,800 attack events mitigated through MSS-BOT and 3,951 attack events successfully blocked by MSS-WAF-CLOUD. These results highlight the continuous level of automated external activity directed at publicly exposed resources and reinforce the value of maintaining multiple layers of application security controls.

The observed activity was primarily associated with automated reconnaissance, resource enumeration, unauthorized access attempts, and malicious requests designed to identify potential weaknesses within exposed applications. Recurring attack patterns included HTTP protocol anomalies, predictable resource discovery, application behavior validation, and input manipulation attempts.

From a security and risk management perspective, these results demonstrate the effectiveness of GOAA web application protection capabilities in detecting and mitigating automated threats before they can interact with protected services. The visibility provided by these controls also supports ongoing monitoring of evolving attack patterns targeting the organization's external web infrastructure.

GOAA 06/15/2026

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