TLP:AMBER

CISO EXECUTIVE REPORT

OCFL

September 25, 2023

OCFL 09/25/2023

TLP AMBER CISO
EXECUTIVE REPORT

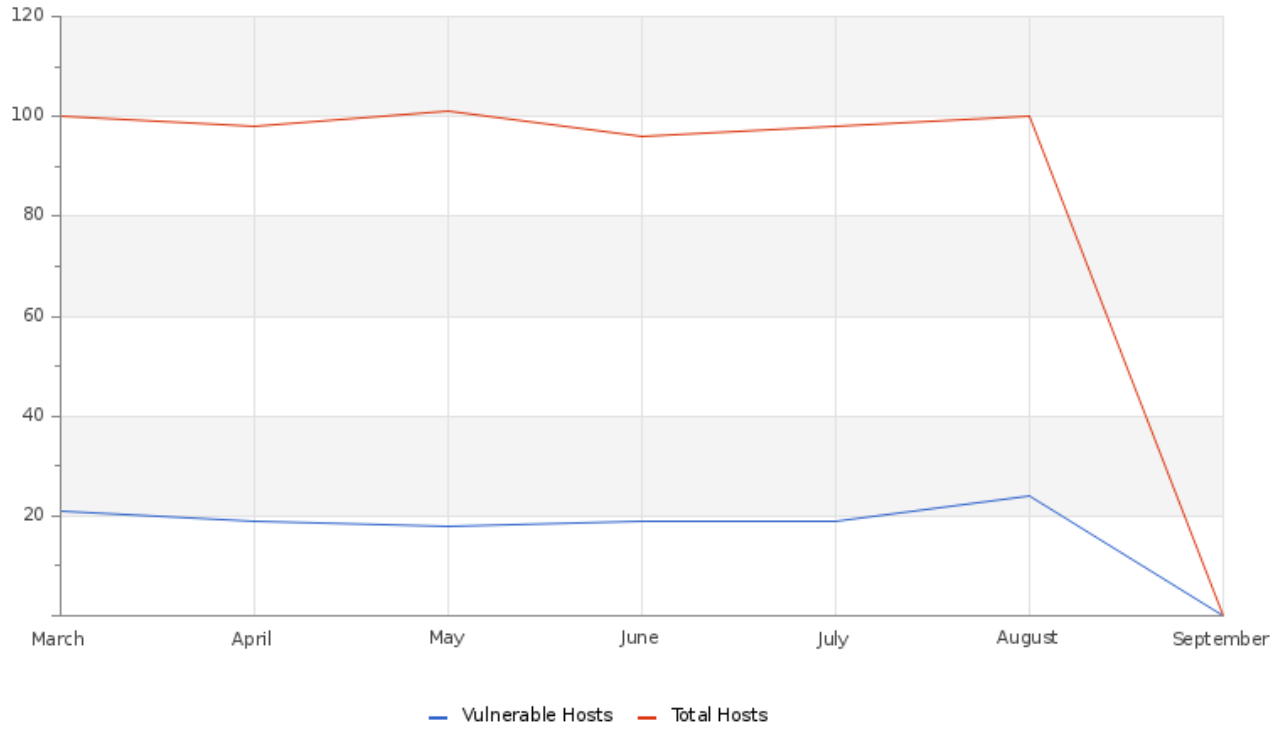
This report corresponds to THIS MONTH and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC`s Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, 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



The graph reflects the persistence of vulnerabilities in the systems over the last months. All vulnerabilities that have been identified by our SOC, have been documented indicating the type of vulnerabilities and remediation, you can view it in our Skywatch platform in the cases section (C&RU).

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

OCFL 09/25/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	74	69
Hosts Discovered	82	81
Vulnerable Hosts	15	17
Critical Vulnerabilities Count	5	4
High Vulnerabilities Count	0	0
Medium Vulnerabilities Count	48	49
Low Vulnerabilities Count	5	4
Phishing Score	0	0
Email Gateway Score	4	5
Web Application Firewall Score	10	10
Web Gateway Score	15	36
Endpoint Score	7	6
Hopper Score	31	2
DLP Score	38	42

The external network range 192.234.90.0/24 was scanned for vulnerabilities, reflecting in its results an increase in vulnerabilities compared to the previous month. Some of the vulnerabilities present in your company belong to the following categories: General, Misc, Portal Scanners, SMTP Problems, among others.

Vulnerability Metric

3

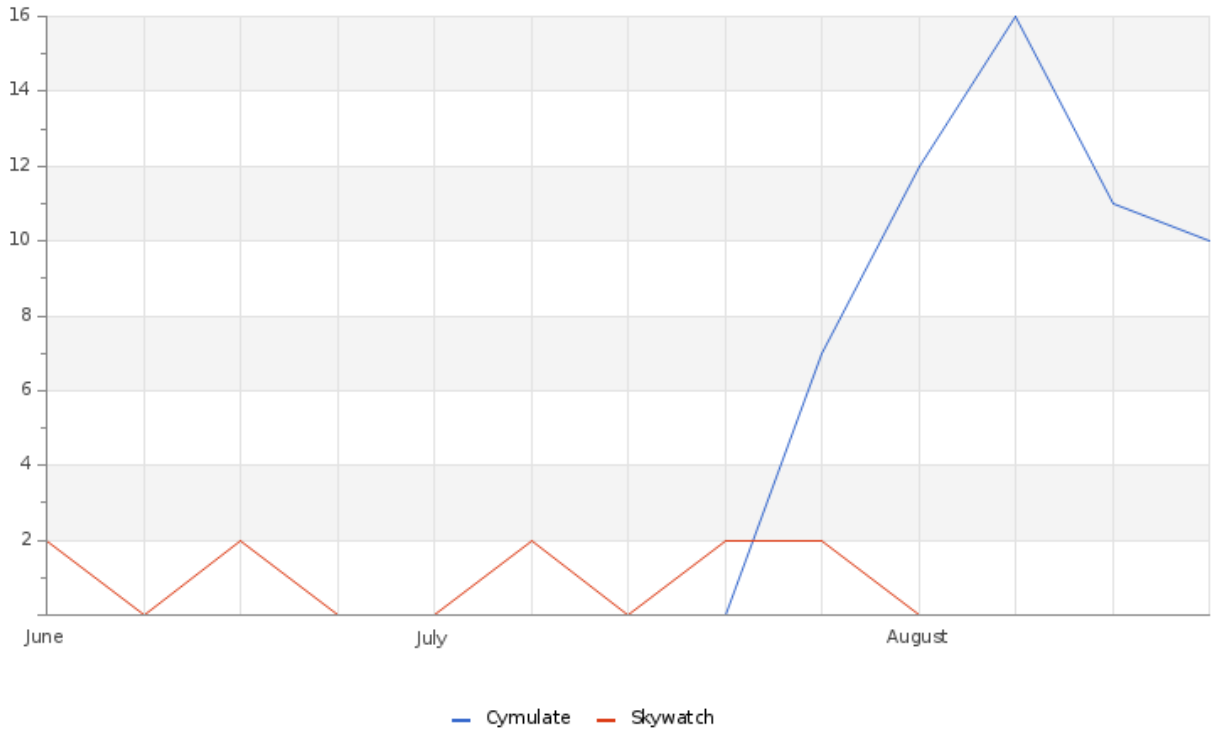
Recommendations have been made to address and mitigate the various vulnerabilities identified in its external systems. The documentation of the vulnerabilities can be found in the Skywatch platform in the cases section.

THREATS

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

OCFL 09/25/2023

Total Number of Successful MFA authentications per application



In the graph we can observe the activity presented by the users in the different platforms. The new bar reflected in the graph is due to the implementation of user access to Cymulate and the activity they have registered on the platform. In Skywatch you can find detailed documentation on cases, incidents, reports, etc., which provide useful information that allows you to strengthen the security of your company.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	2	1
Critical Down Devices	0	0

The service remains under constant monitoring by our SOC; during the month, various alerts were generated that were remedied to maintain correct operation.

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

OCFL 09/25/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	42
Non Baselined Discovered System	130
BAS Web Security	12
Change in Systems Availability	1
Change in Systems Performance	2
BAS Endpoint Security	3

For the MSS-BAS service, detailed documentation was created that allows you to know the security status of your company; related to the MSS-BAS-IMTHREAT services, incident reports were created detailing the correlation between various cases generated by this service. Detailed information can be found in SkywatchReport-Incident Report; The MSS-VME service has its corresponding documentation where we provide you with a description of the vulnerabilities present and the remediations that can be implemented. It is recommended to review these cases and apply the corresponding mitigations. For more information you can access our customer platform https://skywatch.glesec.com in the C&RU section

---

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

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