TLP:AMBER

CISO EXECUTIVE REPORT

OCFL

August 17, 2023

OCFL 08/17/2023

TLP AMBER CISO
EXECUTIVE REPORT

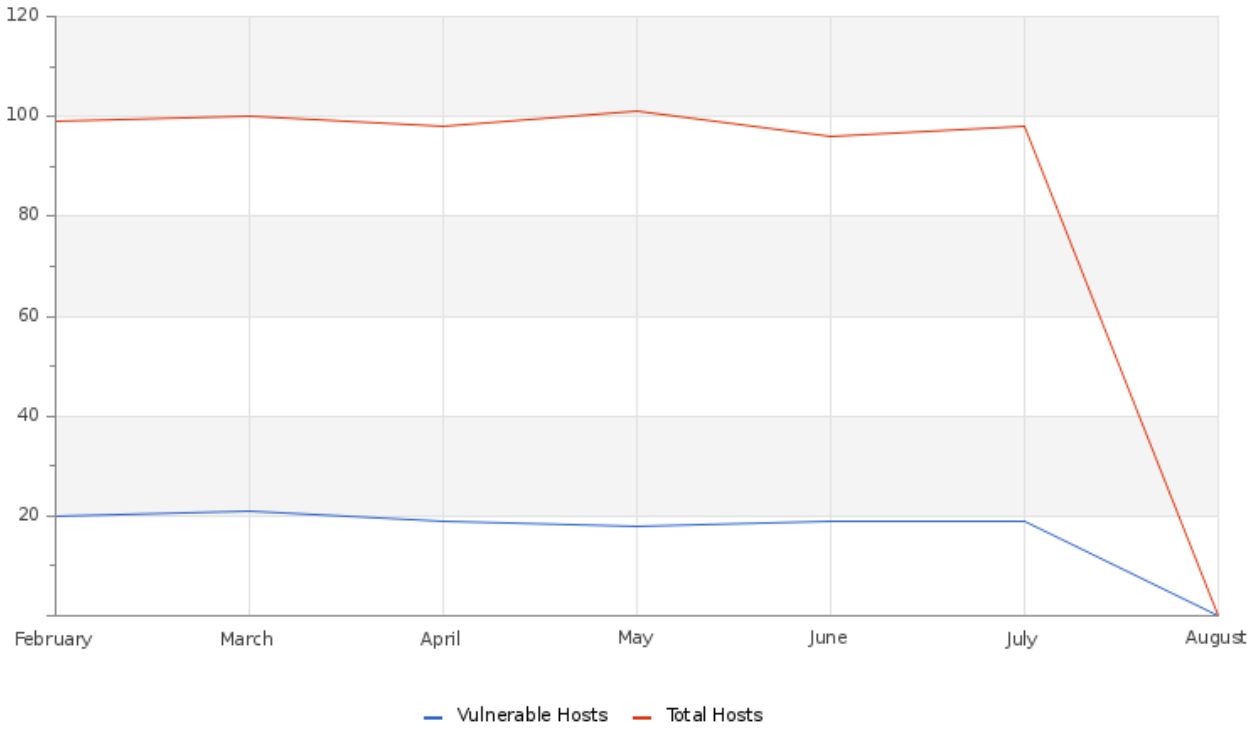
This report corresponds to THIS MONTH and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC`s Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance,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



A slight increase in the number of hosts discovered has been observed. On the other hand, the number of vulnerable hosts has experienced a slight decrease. These data suggest a possible improvement in security and detection measures, although it is essential to continue monitoring and implementing preventive strategies to maintain a secure and efficient technological infrastructure.

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

OCFL 08/17/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	69	68
Hosts Discovered	81	84
Vulnerable Hosts	17	16
Critical Vulnerabilities Count	4	4
High Vulnerabilities Count	0	0
Medium Vulnerabilities Count	49	47
Low Vulnerabilities Count	4	4
Phishing Score	0	0
Email Gateway Score	5	12
Web Application Firewall Score	10	10
Web Gateway Score	36	33
Endpoint Score	6	7
Hopper Score	2	32
DLP Score	42	38

The assessments performed in MSS-BAS indicate ransomware can penetrate by two of the methods tested (Email and Browser navigation) and it can execute in the endpoint (Endpoint testing). Further, there is a very high penetration in the DLP testing, with the exfiltration of pass phrases through common network protocols.
The Immediate Threat vector provided us valuable IOCs and tested the current state of your posture.

Vulnerability Metric

3

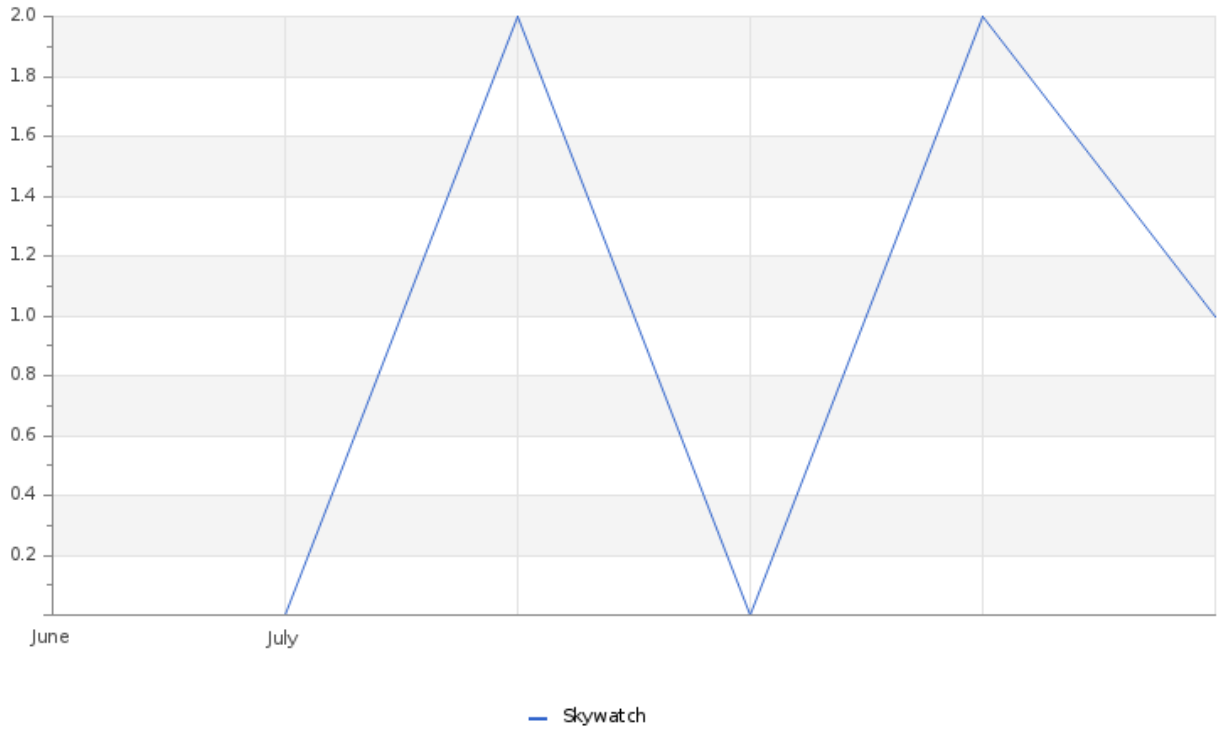
According to the range of addresses provided, the total number of hosts analyzed is 81, of which 17 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. For this period, there are 4 critical vulnerabilities and 49 medium vulnerabilities. Thus, the vulnerability metric for your organization is 3%.

THREATS

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

OCFL 08/17/2023

Total Number of Successful MFA authentications per application



The above shows the number of SKYWATCH authentications during the month of July.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	1	12
Critical Down Devices	0	0

We detected one warning over the last month from all sensors/monitors.

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

OCFL 08/17/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Web Security	10
BAS Immediate Threat	40
Non Baselined Discovered System	10

We have created cases about the most relevant vulnerabilities that contain the definition, recommended solution and affected hosts so that it is available for you on our SKYWATCH, the idea is that you can check this information and proceed to remediate them in a consistent and organized way. If there are any questions about this new feature do not hesitate to contact the GLESEC GOC or Professional Services.

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