GLESEC

COMPLETELY PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

OCFL

July 19, 2023

OCFL 07/19/2023

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to June 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.

RISK

Actual Risk

n/a

The services necessary to present the information on risk values are currently not contracted.

Accepted Risk

n/a

The services necessary to present the information on risk values are currently not contracted.

Confidence

Low

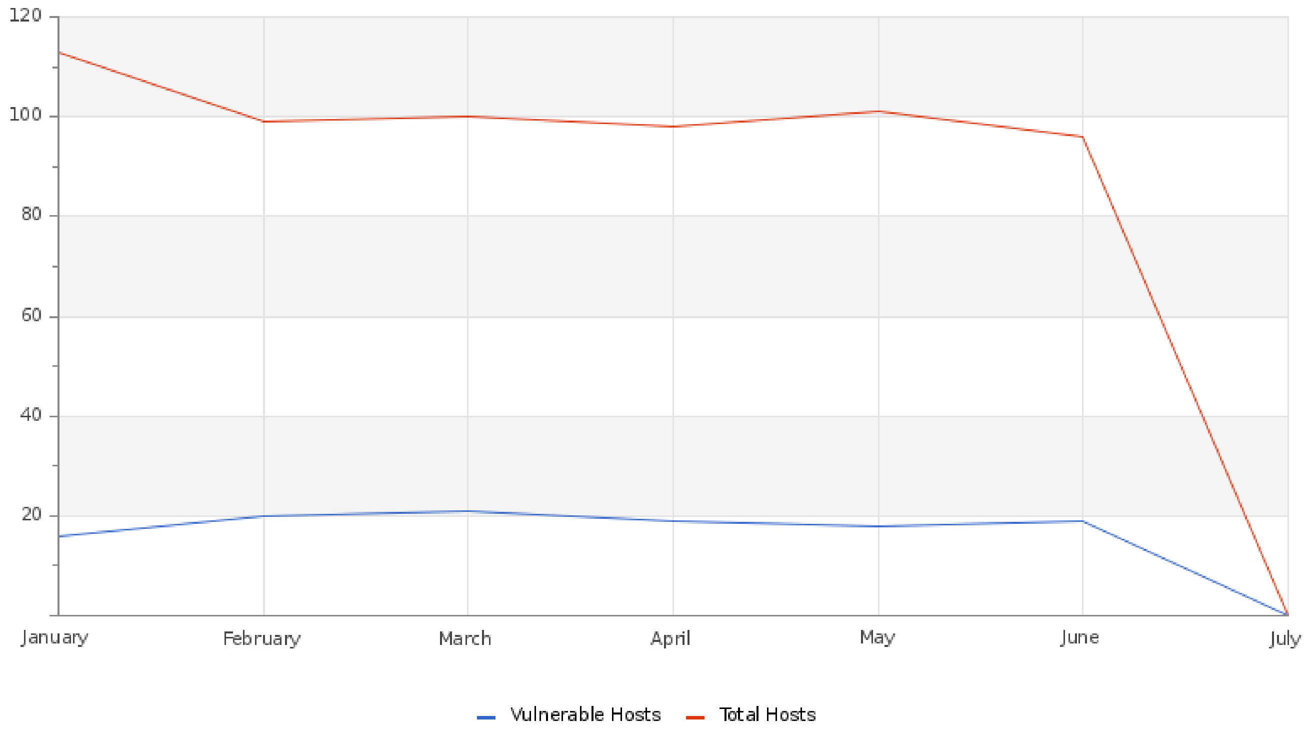
Accepted & Actual Risk

The services necessary to present the information on risk values are currently not contracted.

VULNERABILITY

OCFL 07/19/2023

Hosts & Vulnerable Hosts In Last 6 Months



Overall, most of the network vulnerabilities for this period have been of medium severity, but there are 4 critical and 4 low. For your web application vulnerabilities, there are 90 critical and 1 medium. 17 hosts were found with vulnerabilities. Mitigating these vulnerabilities will reduce the risk score of your organization.

OCFL 07/19/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	68	68
Hosts Discovered	83	83
Vulnerable Hosts	18	17
Critical Vulnerabilities Count	4	4
High Vulnerabilities Count	0	0
Medium Vulnerabilities Count	47	49
Low Vulnerabilities Count	4	4
Phishing Score	0	0
Email Gateway Score	12	12
Web Application Firewall Score	10	10
Web Gateway Score	33	18
Endpoint Score	7	7
Hopper Score	32	31
DLP Score	38	42

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

Our service discovered critical severity vulnerabilities related to MTA Open Mail Relaying Allowed and SSL Version 2 and 3 Protocol Detection, although this vulnerability is whitelisted, we recommend applying the remediation for an efficient optimal security posture.

THREATS

OCFL 07/19/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	31
BAS Web Security	12
Change in Systems Performance	1
Change in Systems Availability	1
Non Baselined Discovered System	6

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.**

GLE SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on our services and security solutions.