TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

OCFL

February, 24, 2023

TLP AMBER

CYBERSECURITY SITUATION APPRAISAL REPORT

About this report

SECURITY INDICATORS

Notable Events Active For The Past 30 Days

Notable Event Type	How Many #
Change in Systems Performance	9
Vulnerability For Open Ports	1
BAS Immediate Threat	7

Number of Attacks Blocked at the Perimeter

MSS-UTM: 0 **MSS-EDR: 0** **MSS-DDOS: 0** **MSS-DLP: 0** **MSS-WAF: 0** **MSS-BOT: 0**

Vulnerabilities

Critical: 4 **High: n/a** **Medium: 45** **Low: 4** **Total: 53**

LATAMHQ
+507 836-5355
USHQ
+1 (321) 430-0500

Hosts

Vulnerable Hosts: 19 **Total Hosts Discovered: 98** **Baselined Hosts: 70**

of Weekly Users to SKYWATCH

0

Systems or Sensors Down

0

Active USB Flash Drives

0

LATAMHQ
+507 836-5355
USHQ
+1 (321) 430-0500

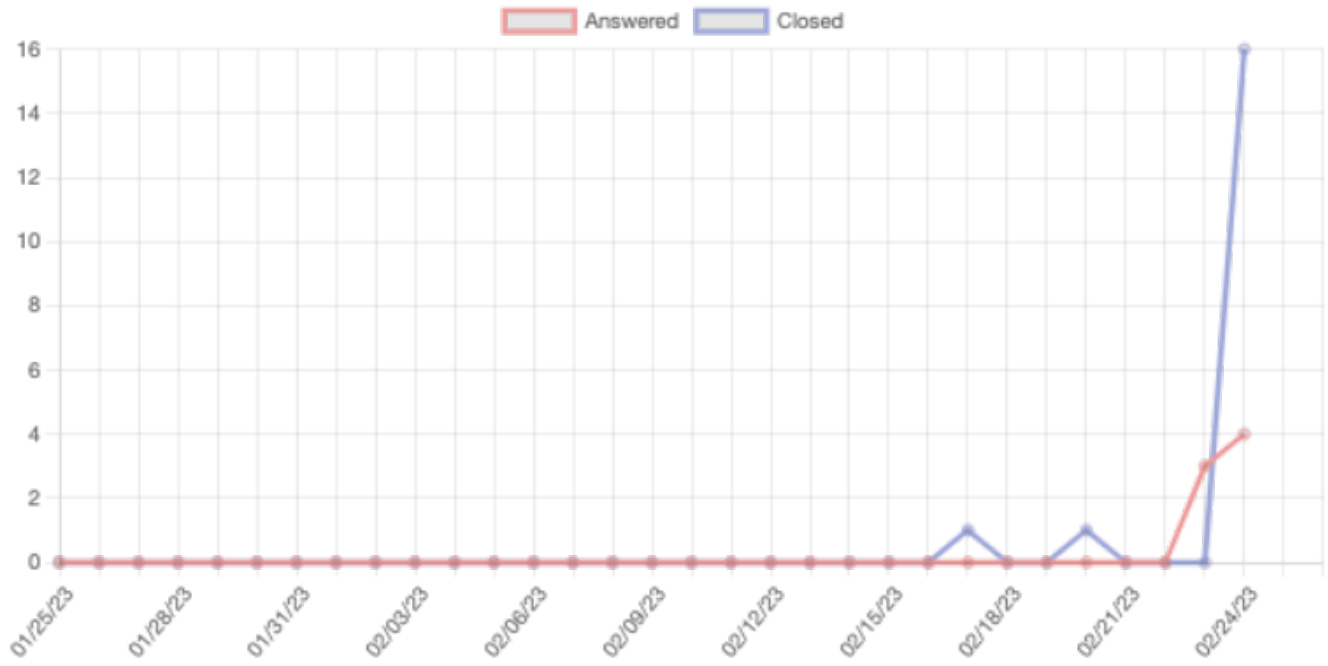
Validation of Countermeasures

Email_Gateway_Score	12
Endpoint_Score	12
Exfiltration_Score	67
Hopper_Score	2
Immediate_Threats_Score	24
Kill_Chain_APT_Campaign_Score	0
Kill_Chain_APT_Scenarios_Score	0
Phishing_Score	0
Recon_Score	0
Web_Application_Firewall_Score	10
Web_Gateway_Score	35

LATAMHQ
+507 836-5355
USHQ
+1 (321) 430-0500

OPERATIONAL METRICS

Cases Activity Histogram



Total Current Cases

Open: 0
Answered: 29

Average Time to Respond and Resolve by Divisions

Divisions	Respond, H	Resolve, H
Compliance	0	0
IT	0	0
Risk	0	0
Security	376.68	655.71

Top 10 Cases:

- 5370 Notable Events: Unauthorized Open Port Detected
- 4955 SQL injection
- 4954 SQL injection
- 4953 SQL injection
- 4951 Cleartext submission of password
- 4952 Cleartext submission of password
- 4956 Silverlight cross-domain policy
- 4957 Flash cross-domain policy
- 5594 MASSIVE ESXIARGS RANSOMWARE ATTACK TARGETS VMWARE ESXI SERVERS WORLDWIDE
- 4408 62694 - Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

LATAMHQ
+507 836-5355
USHQ
+1 (321) 430-0500

Total Remediation Cases By Stage

	Compliance	IT	Risk	Security
Testing & Detection	0	0	0	0
Verification	0	0	0	0
Prioritization and Business Relevance	0	0	0	0
GLESEC Remediation Plan	0	0	0	13
Client Security Team	0	0	0	4
Client Remediation Team	0	0	0	0
Closed	0	0	0	0
Total	0	0	0	17

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.**

LATAMHQ
+507 836-5355
USHQ
+1 (321) 430-0500

GLESEC

COMPLETELY PERCEPTIVE

TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

HOW CAN WE HELP?

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

LATAMHQ
+507 836-5355

USHQ
+1 (321) 430-0500