TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

GLESEC

February, 20, 2023

TLP AMBER

CYBERSECURITY SITUATION APPRAISAL REPORT

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et
dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip
ex ea commodo consequat.

About this report

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et
dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip
ex ea commodo consequat.

SECURITY INDICATORS

Notable Events Active For The Past 30 Days

Notable Event Type	How Many #
BAS Immediate Threat	10
EDR Alerts	363
Change in Systems Performance	8
Change in Systems Availability	6
Vulnerability For Open Ports	1
High Persistency Detection	86
Change in High or Critical Vulnerabilities	1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

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

Number of Attacks Blocked at the Perimeter

MSS-UTM: 199,243 **MSS-DDOS: 0** **MSS-DLP: 0** **MSS-EDR: 21,768**

MSS-WAF-CLOUD: 141,727

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Vulnerabilities

Critical: 11 **High: 21** **Medium: 166** **Low: 15** **Total: 213**

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Hosts

Vulnerable Hosts: 37 **Total Hosts Discovered: 61** **Baselined Hosts: 59**

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

---

of Weekly Users to SKYWATCH

2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam,

Systems or Sensors Down

0

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis

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

quis nostrud exercitation ullamco laboris nisi ut aliquip
ex ea commodo consequat.

nostrud exercitation ullamco laboris nisi ut aliquip
ex ea commodo consequat.

Active USB Flash Drives

2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Validation of Countermeasures

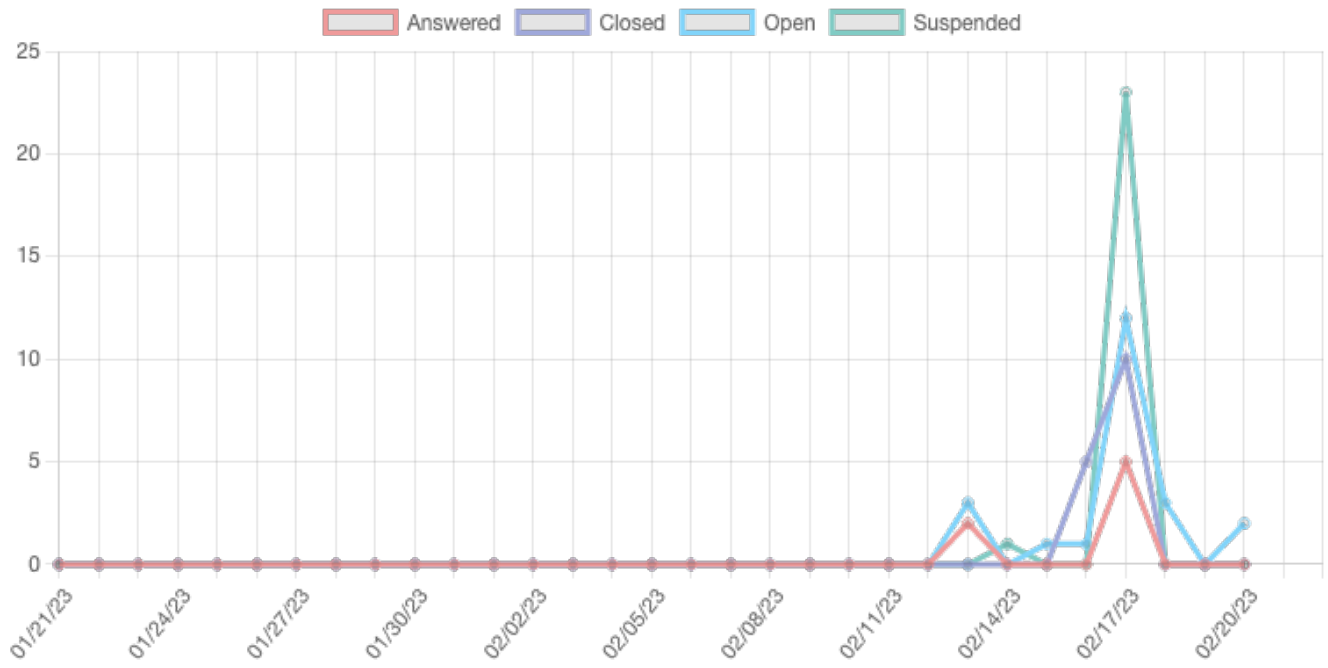
Email_Gateway_Score	12
Endpoint_Score	7
Exfiltration_Score	83
Hopper_Score	1
Immediate_Threats_Score	14
Kill_Chain_APT_Campaign_Score	0
Kill_Chain_APT_Scenarios_Score	0
Phishing_Score	100
Recon_Score	0
Web_Application_Firewall_Score	41
Web_Gateway_Score	52

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

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

OPERATIONAL METRICS

Cases Activity Histogram



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

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

Total Current Cases

Open: 4
Answered: 6

Average Time to Respond and Resolve by Divisions

Divisions	Respond, H	Resolve, H
Compliance	0	0
IT	3.12	407.63
Risk	0	0
Security	320.58	0

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Top 10 Cases:

- 5097 Burp Suite & Nessus Issue
- 3057 GMP: RISK - Analytics Cases
- 5584 Palo Alto GlobalProtect Agent 5.0.x < 5.1.9 or 5.2.x < 5.2.8 Buffer Overflow
- 1306 Intranet Accounting and Billing
- 5008 57608 - SMB signing not required
- 5552 SSH Weak MAC Algorithms Enabled

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

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

Total Remediation Cases By Stage

	Compliance	IT	Risk	Security
Testing & Detection	0	0	0	1
Verification	0	0	0	0
Prioritization and Business Relevance	0	0	0	0
GLESEC Remediation Plan	0	0	0	6
Client Security Team	0	0	0	0
Client Remediation Team	0	2	0	0
Closed	0	0	0	0
Total	0	2	0	7

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

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