TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

ACME FINANCIAL SERVICES

May 02, 2023

TLP AMBER

CYBERSECURITY SITUATION APPRAISAL REPORT

About this report

This on-demand report provides a consolidated view of cybersecurity indicators and operational indicators for the organization during a period of time.

SECURITY INDICATORS

Notable Events Active For The Past 30 Days

Notable Event Type	How Many #
	N/A

Number of Attacks Blocked at the Perimeter

MSS-UTM: 4,797 MSS-EDR: 22,189 MSS-DDOS: 2 MSS-DLP: 0 MSS-WAF: MSS-BOT: 94,105

Vulnerabilities

critical: 3 high: 4 medium: 101 low: 9 Total: 117

Hosts

Vulnerable Hosts: 30 Total Hosts Discovered: 50 Baselined Hosts: 49

Weekly Users to Skywatch	Systems or Sensors Down	Active USB Flash Drives
6	0	0

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

Validation of Countermeasures

Email Gateway Score	11
Endpoint Score	24
Exfiltration Score	79
Hopper Score	0
Immediate Threats Score	36
Kill Chain APT Campaign Score	0
Kill Chain APT Scenarios Score	0
Phishing Score	0
Recon Score	0
Web Application Firewall Score	29
Web Gateway Score	55

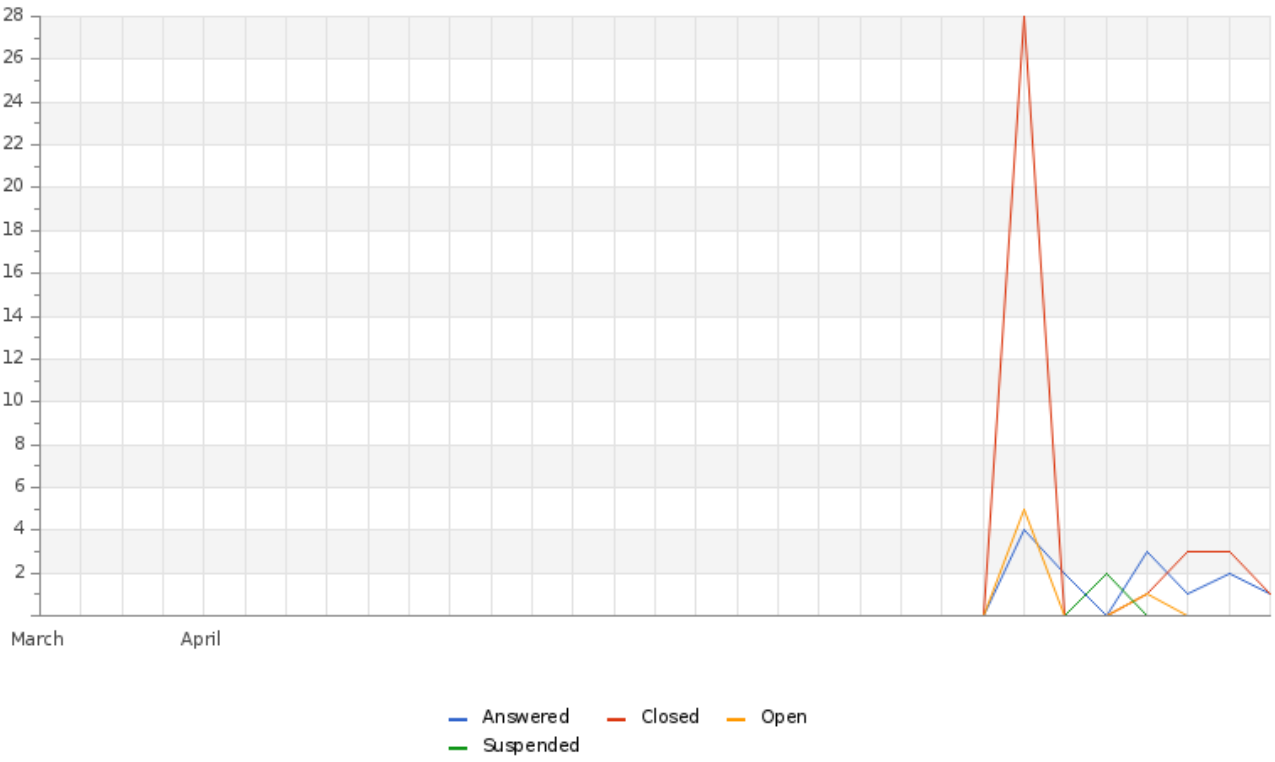
OPERATIONAL METRICS

Cases Activity Histogram

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

CYBERSECURITY SITUATION APPRAISAL

ACME FINANCIAL SERVICES 05/02/2023



Total Current Cases

Open: 2
Answered: 6

Average Time to Address and Respond by Divisions

Divisions	Address, H	Respond, H
Compliance	0	0
IT	0	0
Risk	0	0
Security	0	0

Top 10 Cases:

- 6503 SQL Injection
- 6373 MTA (Agente de transferencia de correo) Open Mail Relaying

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

- 288 Test
- 5607 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) - DEMO CASE
- 5608 INS-01-003 - Multiple Vulnerable Javascript Dependencies - DEMO CASE
- 5609 157288 - TLS Version 1.1 Protocol Deprecated - DEMO CASE
- 289 Test
- 1320 Notable Event - Persitent attacks detected

Total Remediation Cases By Stage

	Compliance	IT	Risk	Security
Testing & Detection	0	0	0	2
Verification	0	0	0	0
Prioritization and Business Relevance	0	0	0	0
GLESEC Remediation Plan	0	0	0	0
Client Security Team	0	0	0	5
Client Remediation Team	0	0	0	1
Closed	0	0	0	0
Total	0	0	0	8

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

GLESEC

COMPLETELY PERCEPTIVE

TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

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