TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

ACME FINANCIAL SERVICES

August 11, 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 #
EDR Alerts	188
BAS Immediate Threat	33
Change in Systems Availability	2
FW Alerts	9
Change in Systems Performance	9
BAS DLP	2
BAS Web Security	1
Change in High or Critical Vulnerabilities	4

Number of Attacks Blocked at the Perimeter

MSS-UTM: 7,490 MSS-EDR: 26,430 MSS-DDOS: 7 MSS-DLP: 7 MSS-WAF: 198,872 MSS-BOT: 414,857

Vulnerabilities

critical: 4 high: 11 medium: 239 low: 19 Total: 299

Hosts

Vulnerable Hosts: 50 Total Hosts Discovered: 105 Baselined Hosts: 75

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

CYBERSECURITY SITUATION APPRAISAL

ACME FINANCIAL SERVICES 08/11/2023

Weekly Users to Skywatch	Systems or Sensors Down	Active USB Flash Drives
7	2	1

Validation of Countermeasures

Email Gateway Score	20
Endpoint Score	26
Exfiltration Score	119
Hopper Score	5
Immediate Threats Score	30
Kill Chain APT Campaign Score	7
Kill Chain APT Scenarios Score	9
Phishing Score	2
Recon Score	2
Web Application Firewall Score	47
Web Gateway Score	30

OPERATIONAL METRICS

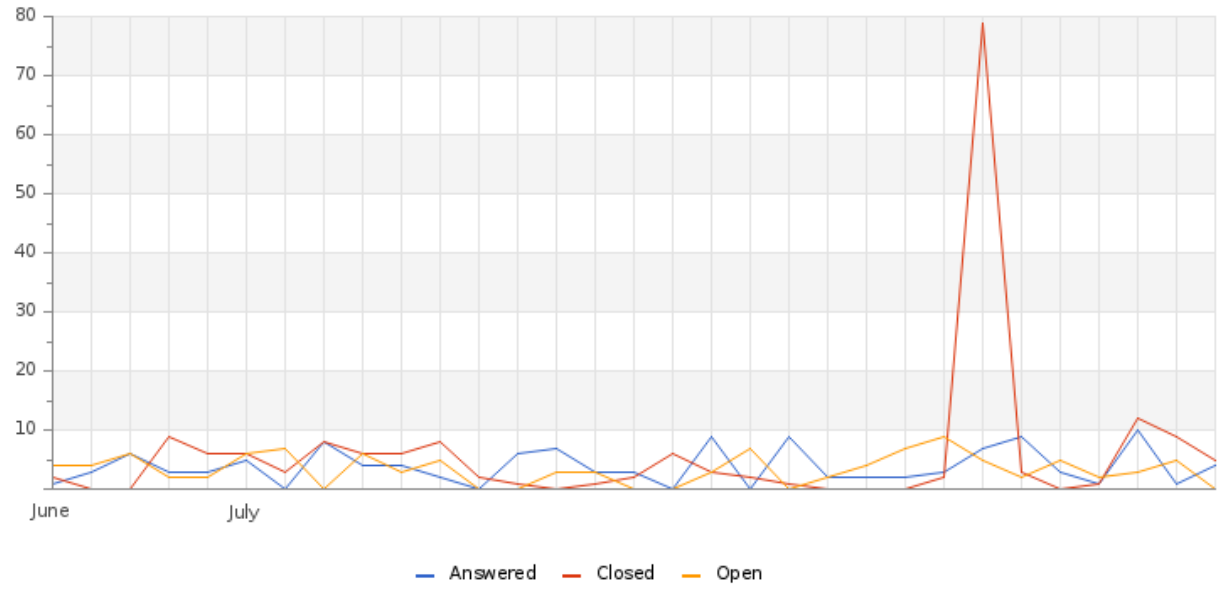
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

CYBERSECURITY SITUATION APPRAISAL

ACME FINANCIAL SERVICES 08/11/2023

Cases Activity Histogram



Total Current Cases

Open: 2
Answered: 146

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
TEST	0	0

Top 10 Cases:

- 8392 Notable Event Alert: EDR Alert
- 8143 Notable Event Alert: Change in Systems Availability
- 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
- 8193 Notable Event Alert: Change in High or Critical Vulnerabilities
- 8195 Notable Event Alert: Change in High or Critical Vulnerabilities
- 8197 Notable Event Alert: Change in High or Critical Vulnerabilities
- 8199 Notable Event Alert: Change in High or Critical Vulnerabilities
- 5608 INS-01-003 - Multiple Vulnerable Javascript Dependencies - DEMO CASE

Total Remediation Cases By Stage

	Compliance	IT	Risk	Security	TEST
Testing & Detection	0	0	0	2	0
Verification	0	0	0	0	0
Prioritization and Business Relevance	0	0	0	0	0
GLESEC Remediation Plan	0	0	0	0	0
Client Security Team	0	0	0	4	0
Client Remediation Team	0	1	0	1	0
Closed	0	0	0	0	0
Total	0	1	0	7	0

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