
TLP:AMBER

# CYBERSECURITY SITUATION APPRAISAL

## WINSOUTHCU

June 15, 2026

# 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 # |
|---|---|
| Monitoring for open ports | 1 |

### 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

### Hosts

Vulnerable Hosts: 0 Total Hosts Discovered: 4 Baselined Hosts: 3

### Weekly Users to Skywatch

**0**



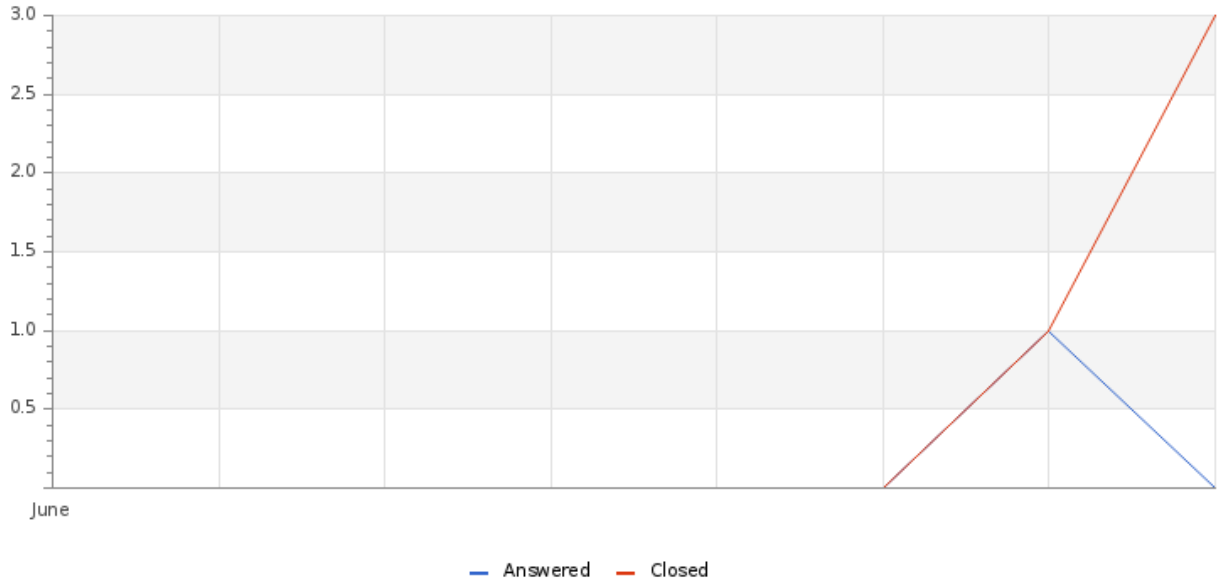
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

### Validation of Countermeasures

| | |
|---|---|
| Customer | WINSOUTHCU |
| Email Gateway | 0 |
| Endpoint | 4 |
| Exfiltration | 0 |
| Hopper | 0 |
| Immediate Threats | 31 |
| Kill Chain APT Campaign | 0 |
| Kill Chain APT Scenarios | 0 |
| Phishing | 0 |
| Recon | 0 |
| Web Application Firewall | 0 |
| Web Gateway | 7 |

# OPERATIONAL METRICS

### Cases Activity Histogram



TLP:AMBER

# CYBERSECURITY SITUATION APPRAISAL

WINSOUTHCU 06/15/2026

## Total Current Cases

Open: 0
Answered: 6

## Average Time to Address and Respond by Divisions

| Divisions | Address, H | Respond, H |
|---|---|---|

## Top 10 Cases:

- 44372 Notable Events Alert: Concern For Open Ports
- 43159 Notable Event Alert: Change in Systems Availability
- 42626 CASE – Linux Privilege Escalation Exposure Review – CVE-2026-46300 / Fragnesia- WINSOUTHCU
- 36318 Notable Events: Unauthorized Open Port Detected
- 29488 Notable Event Alert: Lazarus APT Group Carries Out Attacks Against Defense Sector
- 29485 Notable Event Alert: APT27 Expands Global Cyber Espionage With SysUpdate Malware
- 29163 Notable Event Alert: CVE-2025-31324 Critical SAP Vulnerability How to Protect Your Enterprise
- 29159 Notable Event Alert: Malware Campaign Leverages SVGs Email Attachments and CDNs to Drop XWorm and Remcos via BAT Scripts
- 29152 Notable Event Alert: New BrowserVenom malware being distributed via fake DeepSeek phishing website
- 29095 Notable Event Alert: AMOS Malware Targets macOS Users Via Fake Ledger Apps

## Total Remediation Cases By Stage

| |
|---|
| Testing & Detection |
| Verification |
| Prioritization and Business Relevance |
| GLESEC Remediation Plan |
| Client Security Team |
| Client Remediation Team |
| Closed |
| Total |

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


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

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