



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

# CYBERSECURITY SITUATION APPRAISAL

GOAA

July 05, 2024



## CYBERSECURITY SITUATION APPRAISAL

GOAA 07/05/2024

# 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 #
BAS Immediate Threat	4

### Vulnerabilities

critical: high: medium: 51 low: 8 Total: 59

### Hosts

Vulnerable Hosts: 30 Total Hosts Discovered: 42 Baselined Hosts: 42

### Weekly Users to Skywatch

0



CYBERSECURITY SITUATION APPRAISAL

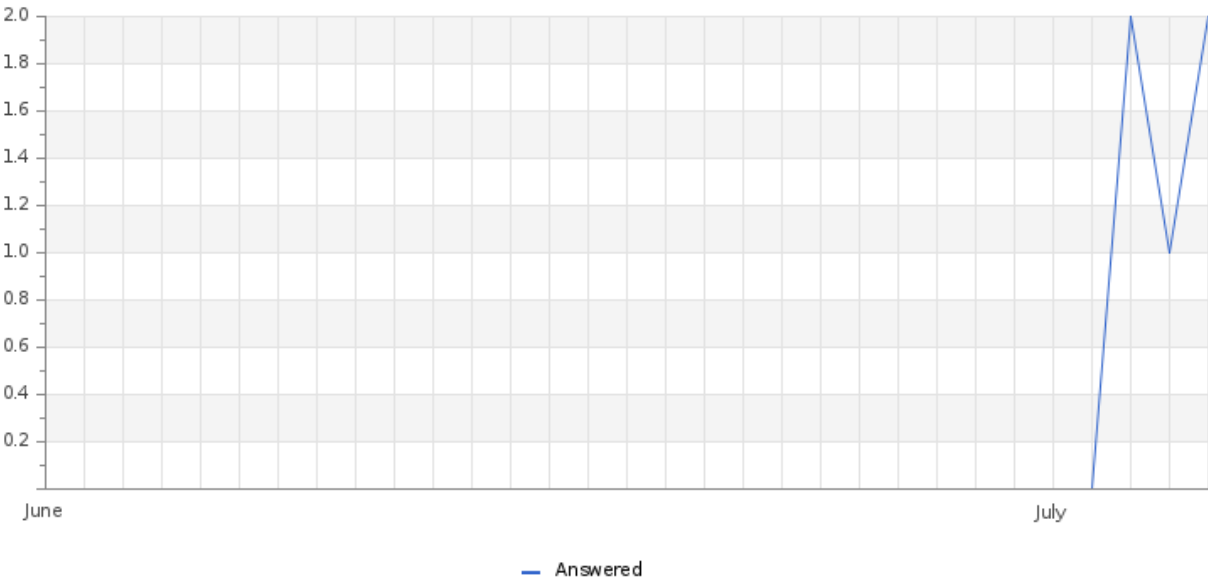
GOAA 07/05/2024

Validation of Countermeasures

Email Gateway Score	0
Endpoint Score	13
Exfiltration Score	0
Hopper Score	0
Immediate Threats Score	38
Kill Chain APT Campaign Score	0
Kill Chain APT Scenarios Score	0
Phishing Score	0
Recon Score	0
Web Application Firewall Score	0
Web Gateway Score	35

OPERATIONAL METRICS

Cases Activity Histogram



Total Current Cases



## CYBERSECURITY SITUATION APPRAISAL

GOAA 07/05/2024

Open: 0

Answered: 3

## Average Time to Address and Respond by Divisions

Divisions	Address, H	Respond, H

## Top 10 Cases:

- 14843 Notable Event Alert: RisePro Information Stealer
- 14839 Notable Event Alert: New Ransomware Operator Volcano Demon Unleashes LukaLocker
- 14816 Notable Event Alert: Supply Chain Compromise and the Spread of Trojanized Installers

## 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 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.**





GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

## CYBERSECURITY SITUATION APPRAISAL

### HOW CAN WE HELP?

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

