GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

GLESEC
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 #
BAS Immediate Threat	5
BAS DLP	5
BAS Web Security	16
Monitoring Event for SPLUNK CLOUD	7
Change in High or Critical Vulnerabilities	3
Change in Systems Performance	3
High Number of Failed Authentications	1
Non Baselined Discovered System	1
Vulnerability For Open Ports	1
High Persistency Detection	2
FW Alerts	2

Number of Attacks Blocked at the Perimeter

MSS-UTM: 4,074 MSS-EDR: 24,270 MSS-DDOS: 0 MSS-DLP: 0 MSS-WAF: MSS-BOT: 116,066

Vulnerabilities

n/a

Hosts

Vulnerable Hosts: 30   Total Hosts Discovered: 49   Baselined Hosts: 48

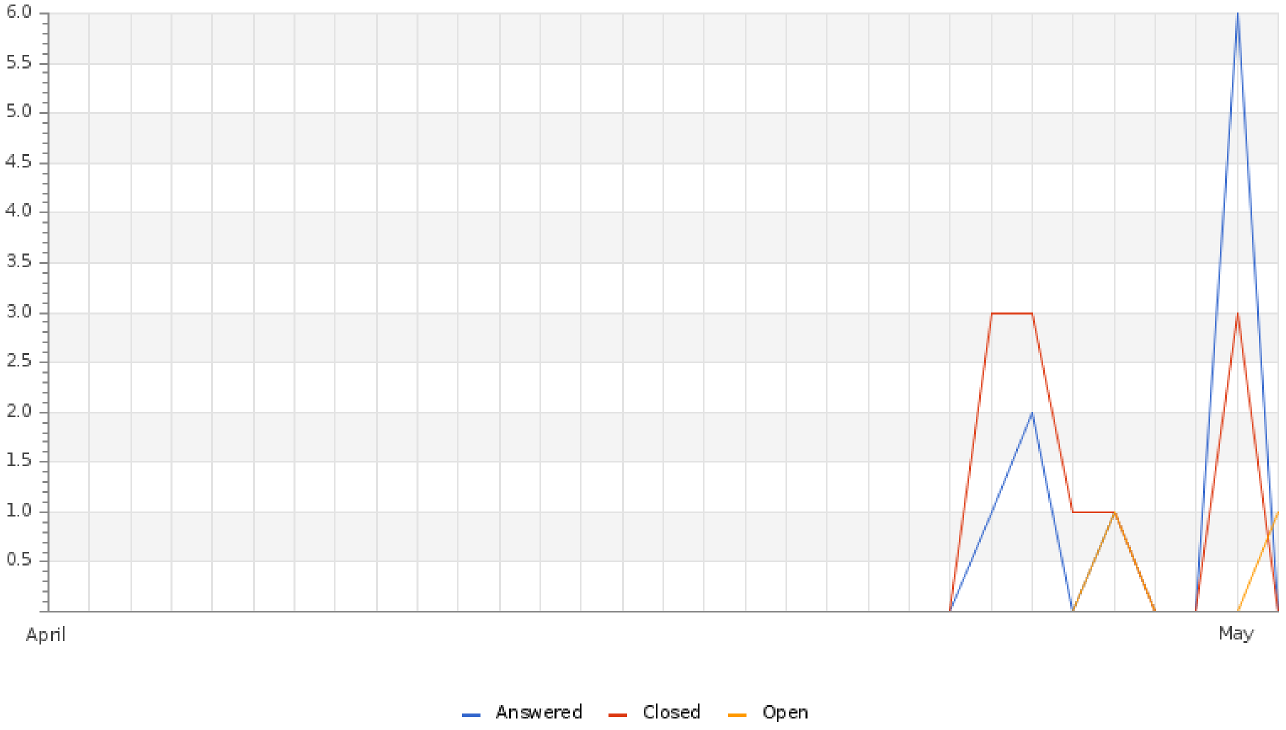
# of Weekly Users to SKYWATCH	# Systems or Sensors Down	# Active USB Flash Drives
6	0	0

Validation of Countermeasures

Email Gateway Score	11
Endpoint Score	25
Exfiltration Score	79
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	28
Web Gateway Score	55

OPERATIONAL METRICS

Cases Activity Histogram



Total Current Cases

Open: 1
Answered: 22

Average Time to Address and Respond by Divisions

Divisions	Address, H	Respond, H
ADMINISTRATION	0	0
CDS - SALES DEPARTMENT	0	0
Compliance	0	0
GOC	0	0
IT	0	26.41
Risk	0	0
S&E	0	0

Divisions	Address, H	Respond, H
Security	0	0.12

Top 10 Cases:

- 5372 Notable Events: Unauthorized Open Port Detected
- 6068 Cross-Origin Resource Sharing: Arbitrary Origin Trusted
- 6069 XSS (DOM-Based)
- 1306 Intranet Accounting and Billing
- 6441 Critical Asset Database-Update

Total Remediation Cases By Stage

	ADMINISTRATION	CDS - SALES DEPARTMENT	Compliance	GOC	IT	Risk	S&E	Security
Testing & Detection	1	1	0	1	0	0	1	1
Verification	0	0	0	0	0	0	0	0
Prioritization and Business Relevance	0	0	0	0	0	0	0	0
GLESEC Remediation Plan	1	1	0	1	0	0	1	1
Client Security Team	1	1	0	1	0	0	1	1
Client Remediation Team	3	3	0	3	2	0	3	3
Closed	1	1	0	1	24	0	1	1
Total	7	7	0	7	26	0	7	7

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.