TLP:AMBER

CYBERSECURITY SITUATION APPRAISAL

GLESEC
April 27, 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	4
Change in High or Critical Vulnerabilities	5
Monitoring Event for SPLUNK CLOUD	9
BAS DLP	4
BAS Web Security	14
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

Number of Attacks Blocked at the Perimeter

MSS-UTM: 2,468	MSS-EDR: 23,112	MSS-DDOS: 0	MSS-DLP: 0	MSS-WAF:	MSS-BOT: 93,361

Vulnerabilities

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

Hosts

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

# of Weekly Users to SKYWATCH

6

# Systems or Sensors Down

0

# Active USB Flash Drives

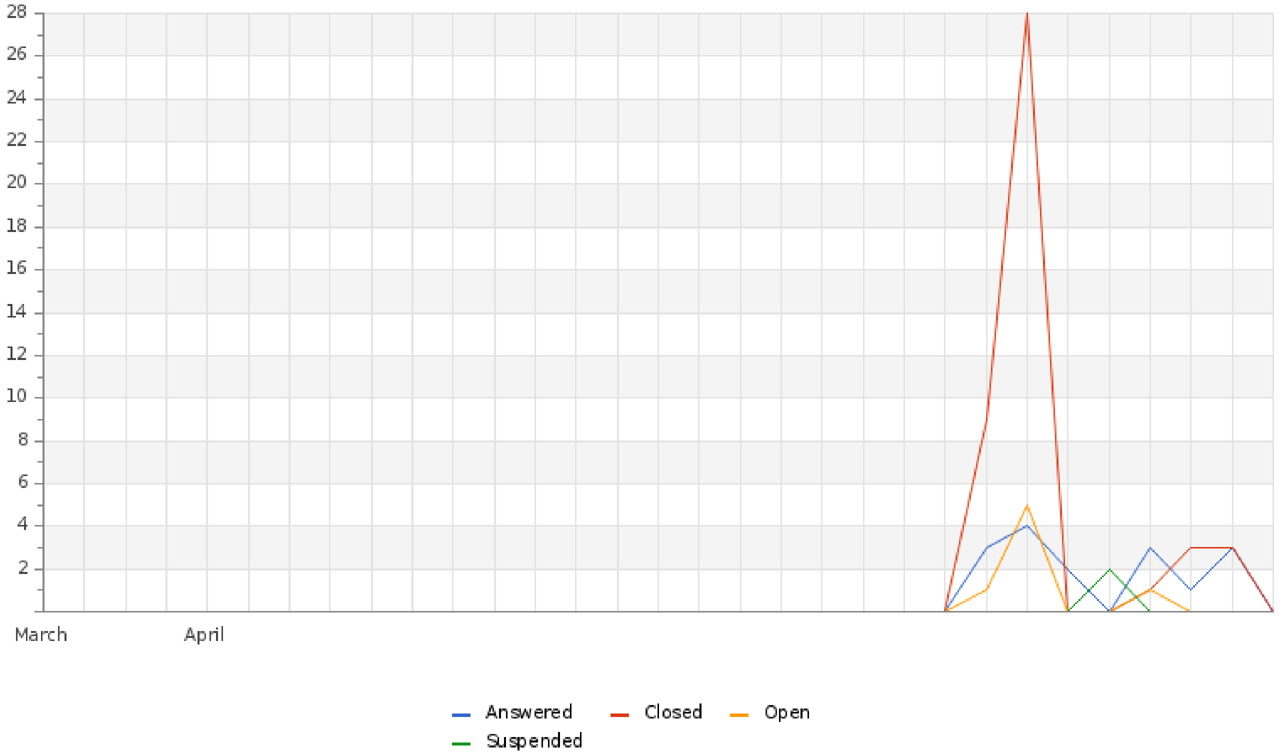
0

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



Total Current Cases

Open: 1
Answered: 22

Average Time to Address and Respond by Divisions

Divisions	Address, H	Respond, H
ADMINISTRATION		
CDS - SALES DEPARTMENT		
Compliance		
GOC		
IT		95084.375
Risk		
S&E		

Divisions	Address, H	Respond, H
Security		431.5

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

ON	CDS - SALES DEPARTMENT		Compliance	GOC	IT	Risk	S&E	Security
	1	Testing&Detection	0	1	0	0	1	1
	0	Verification	0	0	0	0	0	0

ON	CDS - SALES DEPARTMENT		Compliance	GOC	IT	Risk	S&E	Security
	0	Prioritization and Business Relevance	0	0	0	0	0	0
	1	GLESEC Remediation Plan	0	1	0	0	1	1
	1	Client Security Team	0	1	0	0	1	1

ON	CDS - SALES DEPARTMENT	Compliance	GOC	IT	Risk	S&E	Security
	3 ClientRemediationTeam	0	3	2	0	3	3
	1 Closed	0	1	24	0	1	1
	7 Total	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.