



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC
December, 29, 2022



GLESEC 12/29/2022

TLP AMBER CISO EXECUTIVE REPORT

ABOUT THIS REPORT

RISK

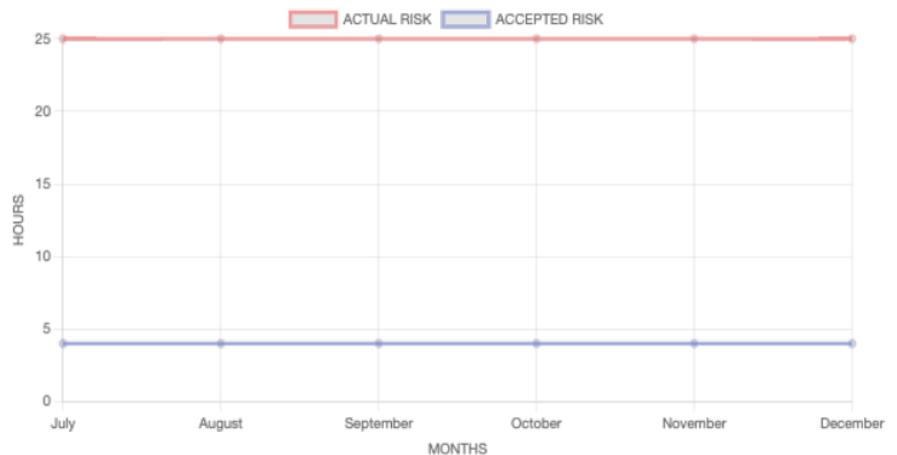
ACTUAL RISK

25%

ACCEPTED RISK

4%

ACCEPTED & ACTUAL RISK HISTOGRAM



GLESEC 12/29/2022

VULNERABILITY

VULNERABILITY METRIC VULNERABILITIES HISTOGRAM - FOR 6 MONTHS

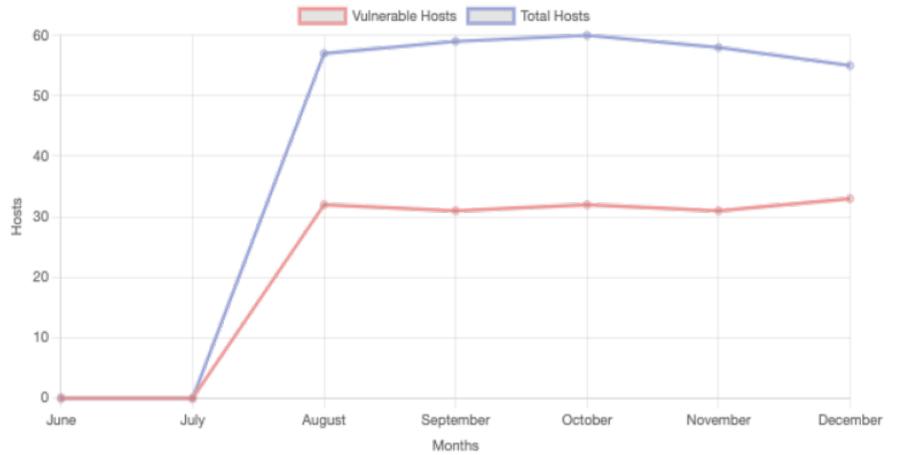


TABLE OF COMPARISON OF TOTAL VULNERABILITY COUNTS FROM CURRENT TO PRIOR MONTH

| | Current Month | Previous Month |
|--------------------------------|---------------|----------------|
| Hosts Baselined | 56 | 56 |
| Hosts Discovered | 56 | 0 |
| Critical Vulnerabilities Count | 41 | 0 |
| High Vulnerabilities Count | 205 | 0 |
| Medium Vulnerabilities Count | 540 | 0 |
| Low Vulnerabilities Count | 38 | 0 |
| Phishing Score | 100 | 100 |
| Email Gateway Score | 14 | 23 |
| Web Application Firewall Score | 67 | 78 |
| Web Gateway Score | 59 | 71 |
| Endpoint Score | 44 | 1 |
| Hopper Score | 1 | 1 |
| DLP Score | 83 | 80 |

GLESEC 12/29/2022

THREATS

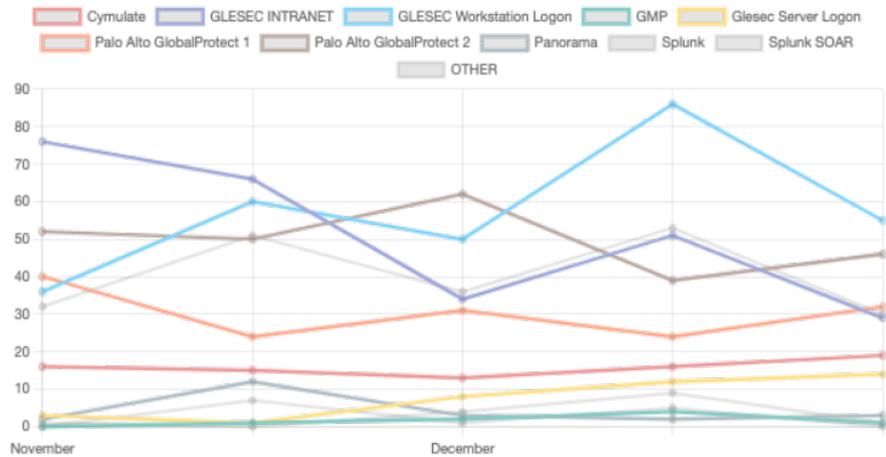
GLOBAL MAP OF CRITICAL ATTACKS PER COUNTRY FOR PAST WEEK

n/a

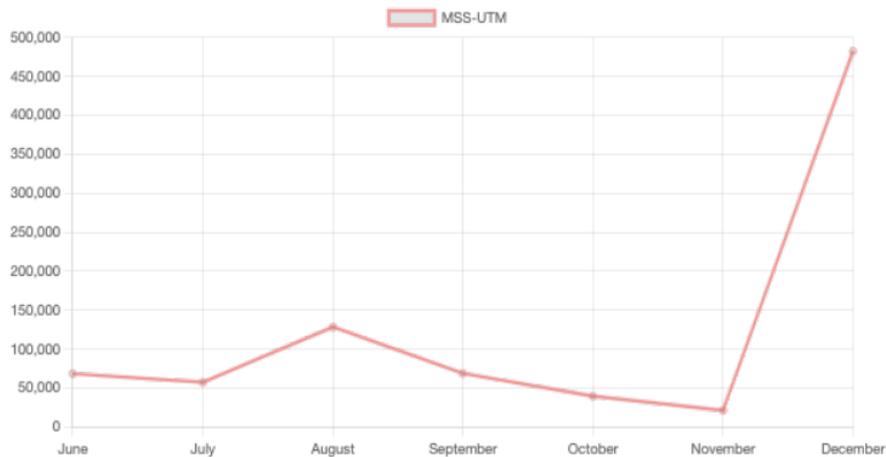


GLESEC 12/29/2022

HISTOGRAM OF TOTAL NUMBER OF SUCCESSFUL MULTI-FACTOR AUTHENTICATIONS PER APPLICATION

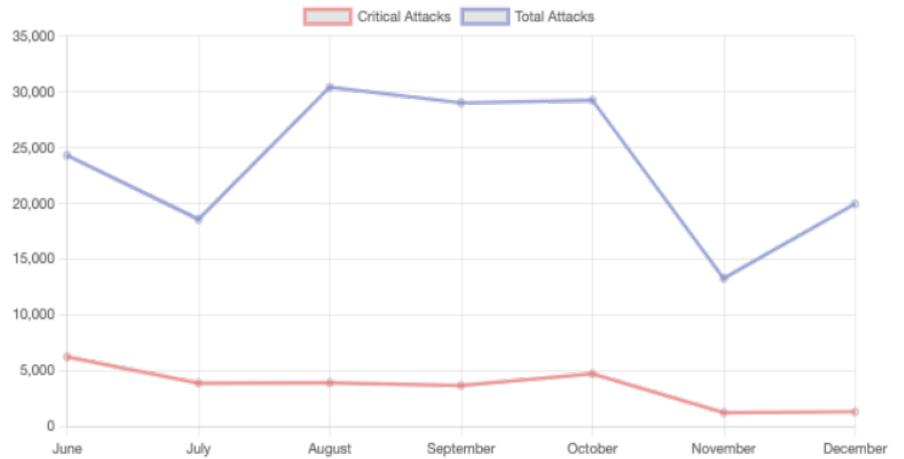


ATTACKS BY SERVICE - TOTAL AND CRITICAL ATTACKS SUCCESSFULLY BLOCKED BY SECURITY LAYER AND DEPARTMENT



ATTACKS BY SEVERITY - TOTAL AND CRITICAL ATTACKS SUCCESSFULLY BLOCKED BY SECURITY LAYER AND DEPARTMENT

GLESEC 12/29/2022



TOTAL AND CRITICAL SYSTEM AVAILABILITY AND PERFORMANCE BY DEPARTMENT OF CURRENT COMPARED TO PREVIOUS MONTH

| | Current Month | Previous Month |
|-----------------------|---------------|----------------|
| Total Down Devices | 10 | 8 |
| Critical Down Devices | 0 | 0 |

GLESEC 12/29/2022

OPERATIONAL

NOTABLE EVENTS ACTIVE FOR THE PAST 30 DAYS

| Notable Event Type | How Many # |
|--|------------|
| Abnormal activity in the file system(s) | 26 |
| High Persistency Detection | 50 |
| Change in High or Critical Vulnerabilities | 17 |
| EDR Alerts | 8 |
| Monitoring Event for SPLUNK CLOUD | 14 |
| Change in Systems Performance | 3 |

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

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

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

