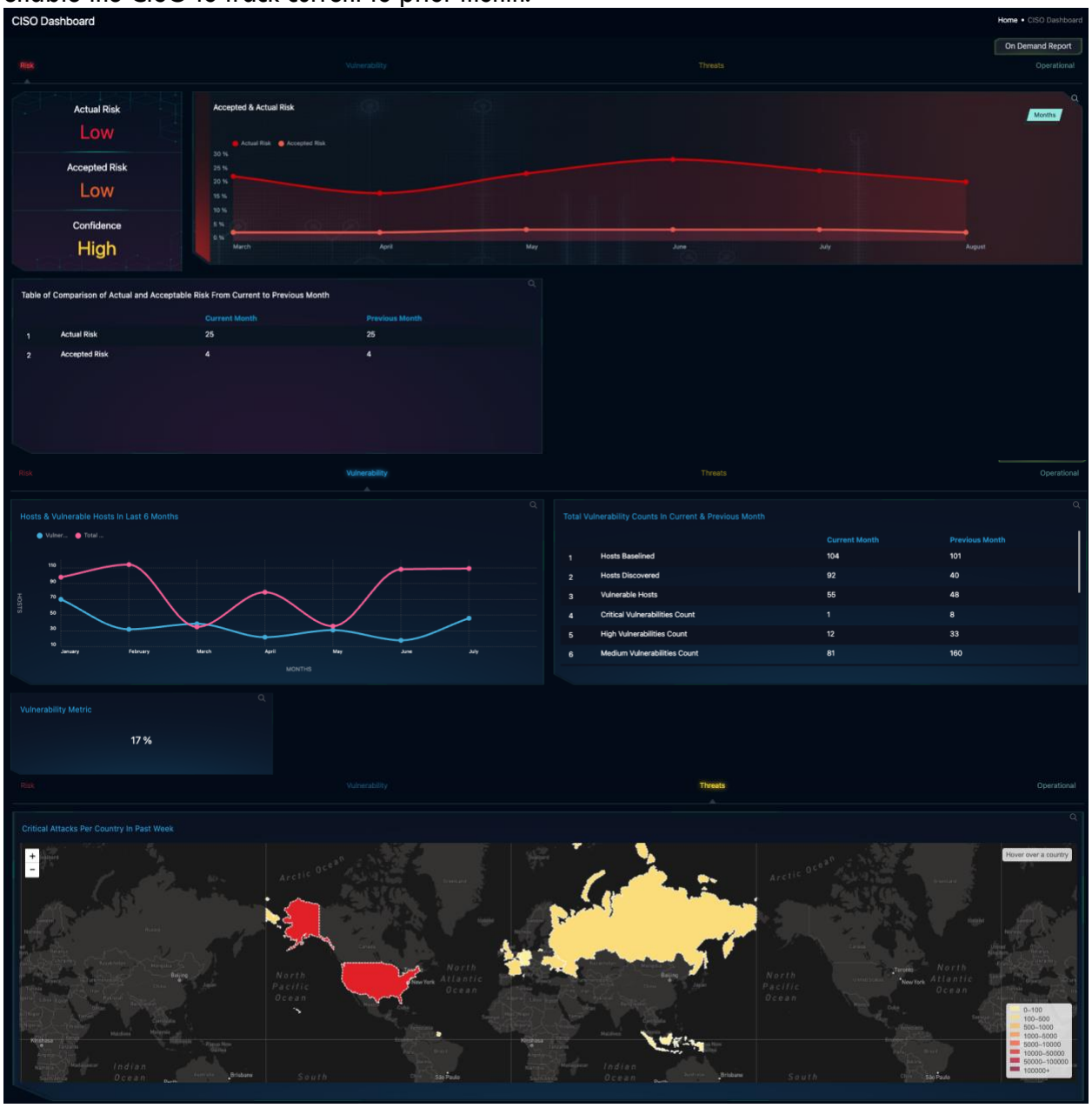
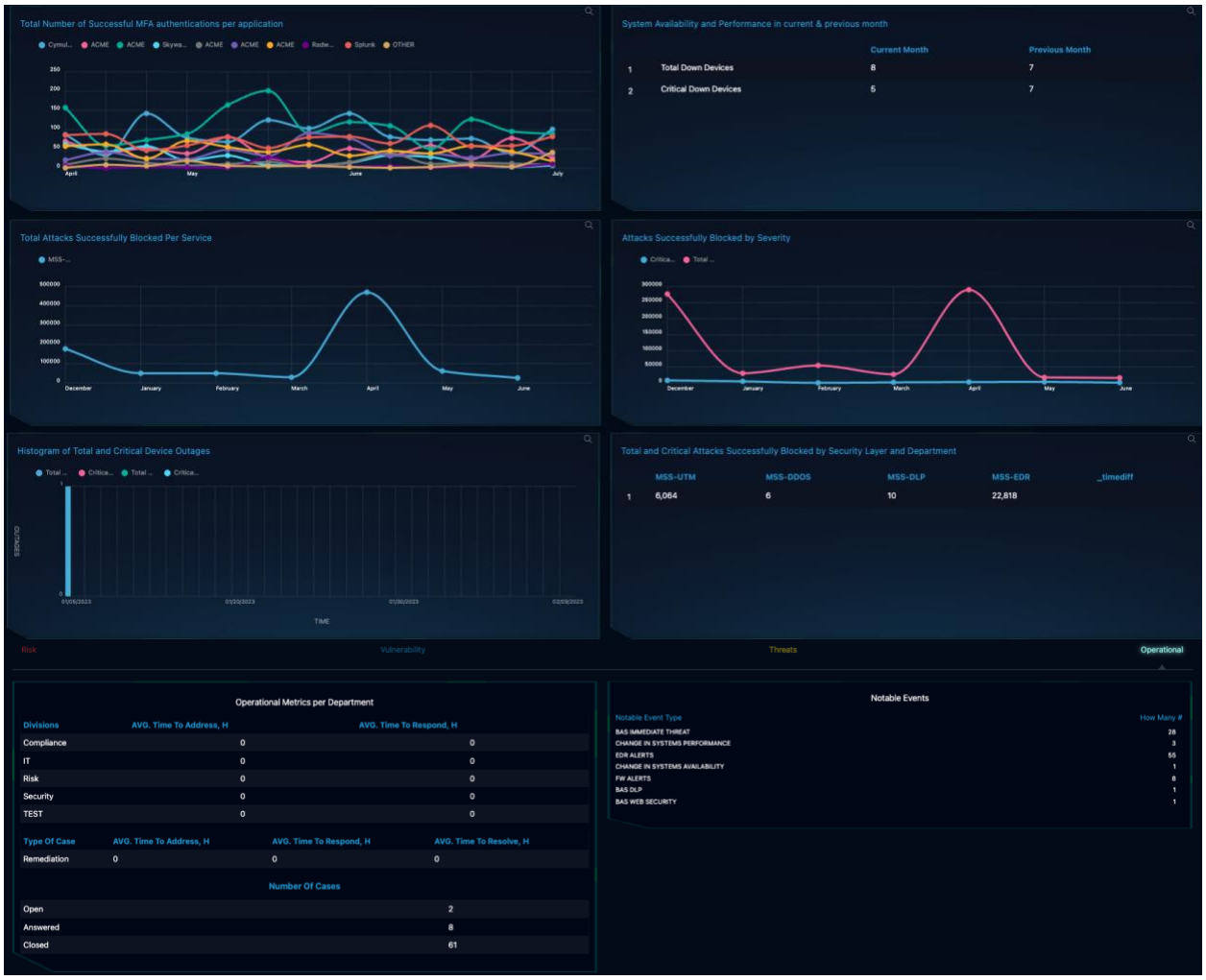
SKYWATCH EXECUTIVE DASHBOARDS: CISO

The information curated in this dashboard presents – in real time - the state of Cybersecurity of the organization and enables the CISO to easily propagate to the rest of the organization. Aligned with the GLESEC Seven Elements Model and the National Institute of Standard (NIST) framework.

The dashboard contains divisional (or per department) information, GLESEC Notable Events (GNE), Operational Metrics and several RISK, VULNERABILITY, and THREAT indicators and histograms to enable the CISO to track current to prior month.



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



Indicators and graphic representation

RISK

- Actual Risk Value (organization-wide)
- Acceptable Risk Value (organization-wide)
- Risk Histogram (showing actual and acceptable risk)
- Table of comparison of actual and acceptable risk from current to prior month

VULNERABILITY

- Vulnerability Metric (organization-wide)
- Vulnerability Histogram
- Table of comparison of total vulnerability counts from current to prior month
    - # of assets discovered compared with # of assets baselined
    - # of vulnerabilities (total critical | high | medium | low)
    - Validation of controls penetration (email | web | endpoint | waf | dlp | lm | immediate threat)
    - # of patches missing

  - Gap to validation of endpoints
- Graph of number of cases per vulnerability handling stage with link to the list of cases and link to the individual cases

THREATS

- Total and critical attacks successfully blocked by security layer (DDOS | Firewalls | WAF | DLP | EDR) and Department
- Histogram of Total and critical attacks successfully blocked by security layer and Department
- Top 10 Persistent Attacks Blocked
  - Source (DNS translated)
  - Destination (DNS translated)
  - # of events in 30 days
  - Attack Vector (MSS-UTM or MSS-DDOS or MSS-WAF)
- Histogram of total number of successful multi-factor authentications per application
- Global map of critical attacks per country for past week
- Total and critical system availability and performance by Department of current compared to prior month
- Histogram of Total and critical system availability and performance by Department

OPERATIONAL

- Notable Events Active for the past 30 days
- Collaboration
  - Number of users per Department that accessed SKYWATCH in the month
- Operational Metrics per Department and per REMEDIATION, INCIDENTS, ANOTHER category
  - Average Time to Respond and Average Time to Resolve
  - # of cases open | answered | closed

Reports

The dashboard supports on-demand report generation for the current value of the indicators. The report follows TLP (Transport Layer Protocol) standard from Homeland Security and will be filed under SKYWATCH / Reports / On-demand section.

On the monthly basis, the same type of report is created by GLESEC Operations with information from the prior month and filed in the SKYWATCH / Reports / Boardroom Report.

Service
MSS-CSO
MSS-TAS
Vulnerability Handling (MSS-VME; MSS-VME-ADV; MSS-VM; MSS-EPM; MSS-BAS)
Any threat related service at the perimeter (MSS-DDOS or MSS-WAF or MSS-WAF-CLOUD or MSS-UTM)
Internal threats (MSS-EDR and MSS-DLP)

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

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