



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

## CISO EXECUTIVE REPORT

BLADEX

July 26, 2023



# TLP AMBER CISO EXECUTIVE REPORT

The report includes: RISK, Cybersecurity and Operational information.

### Sobre este reporte

This on-demand report provides executive level information as of the state of Cybersecurity for your organization including top security indicators and performance.

## RISK

Actual Risk

**n/a**

Accepted Risk

**n/a**

Confidence

**<span title="Low Confidence level 0% to 60%. However, if no Threat or Vulnerability or Assets information is available, then the Confidence will be 0% since it will not be possible to determine risk.">Low</span>**



# CISO EXECUTIVE REPORT

BLADEx 07/26/2023

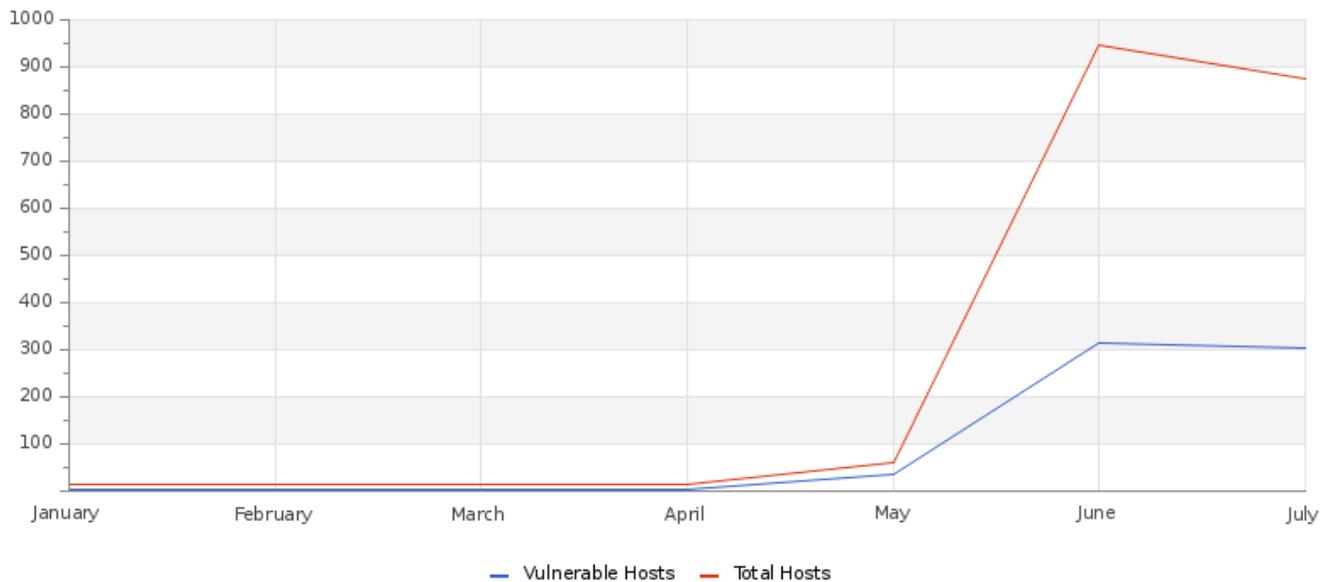
## Accepted & Actual Risk

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

	Current Month	Previous Month
Actual Risk		
Accepted Risk	0	0

## VULNERABILITY

### Hosts & Vulnerable Hosts In Last 6 Months



# CISO EXECUTIVE REPORT

BLADEx 07/26/2023

## Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	898	898
Hosts Discovered	708	896
Vulnerable Hosts	127	313
Critical Vulnerabilities Count	76	134
High Vulnerabilities Count	153	418
Medium Vulnerabilities Count	453	1423
Low Vulnerabilities Count	129	275
Phishing Score	0	0
Email Gateway Score	6	6
Web Application Firewall Score	0	0
Web Gateway Score	19	16
Endpoint Score	30	33
Hopper Score	17	17
DLP Score	100	100

## Vulnerability Metric

**9%**

## THREATS

### Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	44	0

**CISO EXECUTIVE REPORT**BLADEX 07/26/2023

---

**OPERATIONAL****Notable Events Active For The Past 30 Days**

<b>Notable Event Type</b>	<b>How Many #</b>
BAS Immediate Threat	15
Abnormal activity in the file system(s)	70
Change in Baseline Systems Discovered	1
BAS Web Security	6
Change in High or Critical Vulnerabilities	10

---

**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.

