



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

# BOARDROOM EXECUTIVE REPORT

GLESEC  
August 27, 2023



GLESEC 08/27/2023

# TLP AMBER BOARDROOM EXECUTIVE REPORT

This report corresponds to July and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC's Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, Cyber Security Validation and Access

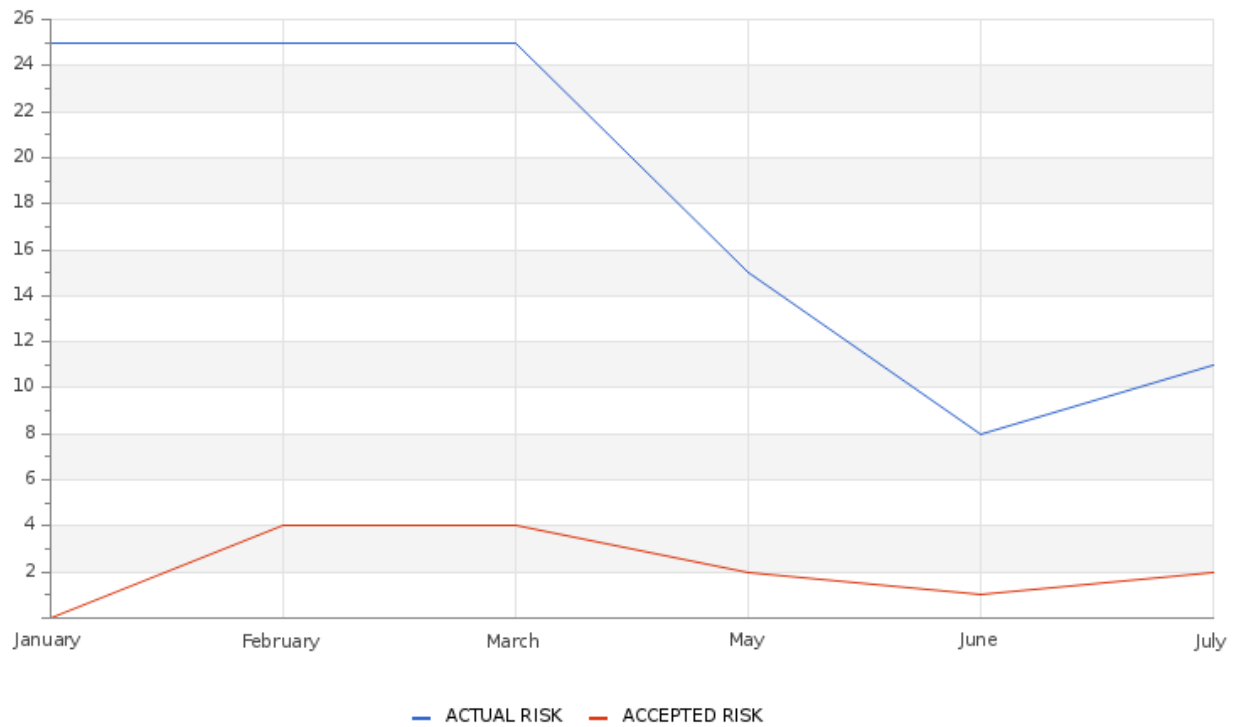
## ABOUT THIS REPORT

The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

**Actual Risk****11%****Accepted Risk****2%****Confidence****High**

GLESEC 08/27/2023

Accepted & Actual Risk

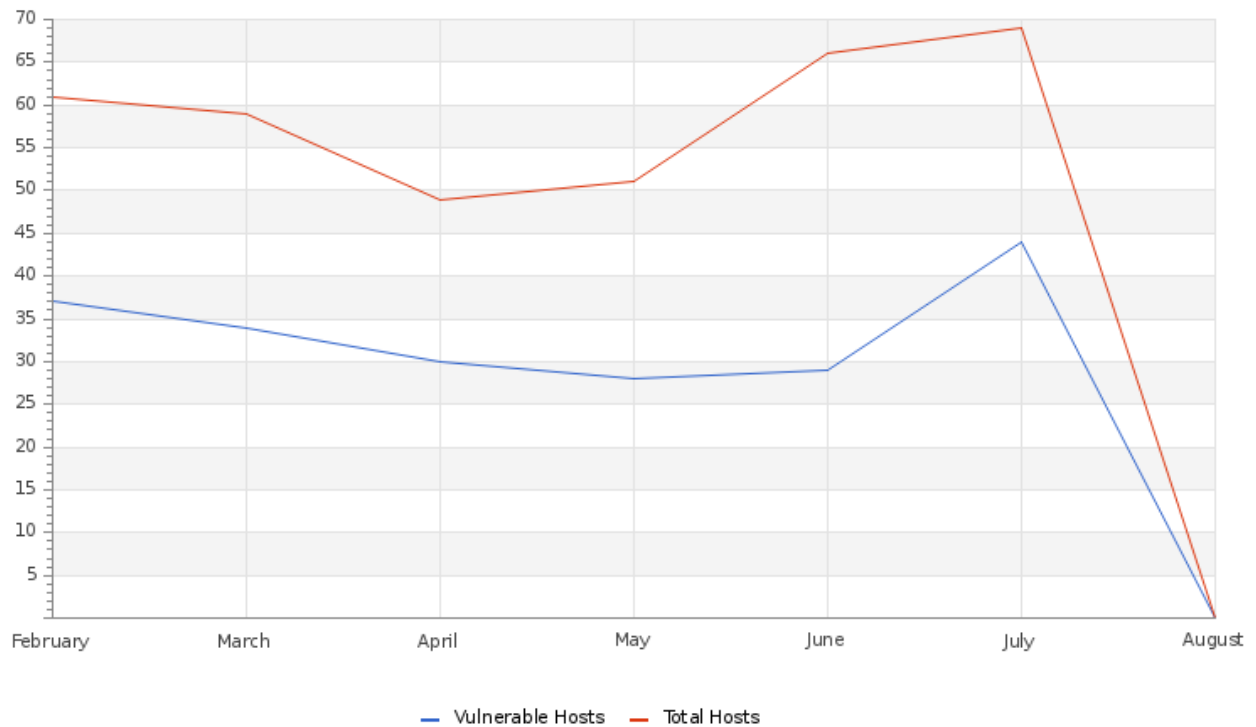


The current risk level has increased in the month of July. During this month, the current risk stands at 11, while the accepted risk remains at 2. Compared to the previous month, where the current risk was 10 and the accepted risk was also 2, it is evident that the risk has increased.



GLESEC 08/27/2023

## Hosts & Vulnerable Hosts In Last 6 Months



The graph shows a marked increase in vulnerabilities and hosts discovered during the month, pointing to security deficiencies. Critical flaws in Google Chrome and Windows permissions issues are fixable with updates, while vulnerabilities in Apache Log4j and Palo Alto GlobalProtect Agent need specific attention. The remaining vulnerabilities are largely associated with outdated software and protocols. It is recommended that these risks be addressed immediately to strengthen organizational security.

## Total Attacks Successfully Blocked

**1522**

Throughout the month, our systems successfully detected and blocked 1522 attacks targeting your devices. With continuous monitoring and agile response, we have put in place specific cases to address persistent attacks. It is relevant to note that many of these attacks emanate from malicious IP addresses and Botnets, sources known for their damaging nature.

## Critical Attacks Successfully Blocked

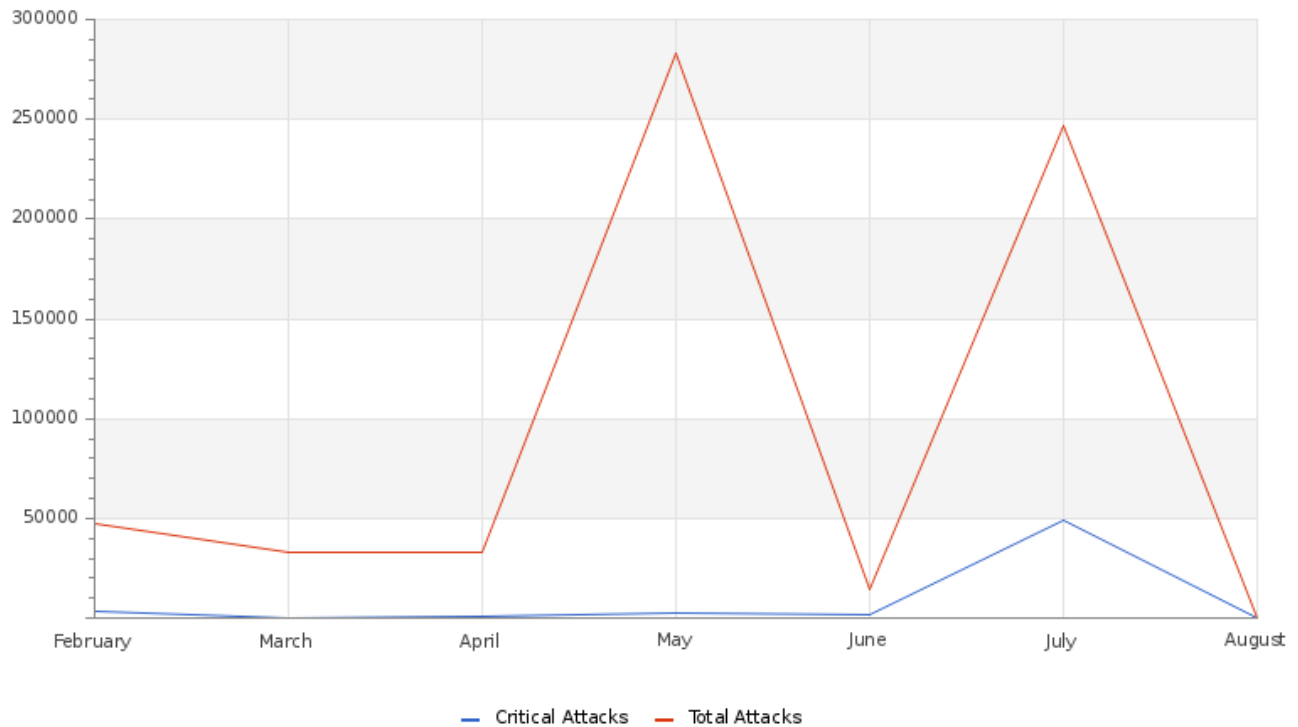
**309**

During the month, we blocked 309 critical attacks. This approach is based on unique real-time intelligence, offering protection against emerging threats, specifically DDoS attacks, evolving IoT and new DNS attack vectors.



GLESEC 08/27/2023

## Attacks Successfully Blocked



The implementation of firewalls in the month of June has had a positive impact on security, as evidenced by the graph showing a significant increase in the number of attacks successfully blocked in July.

## Vulnerability Metric

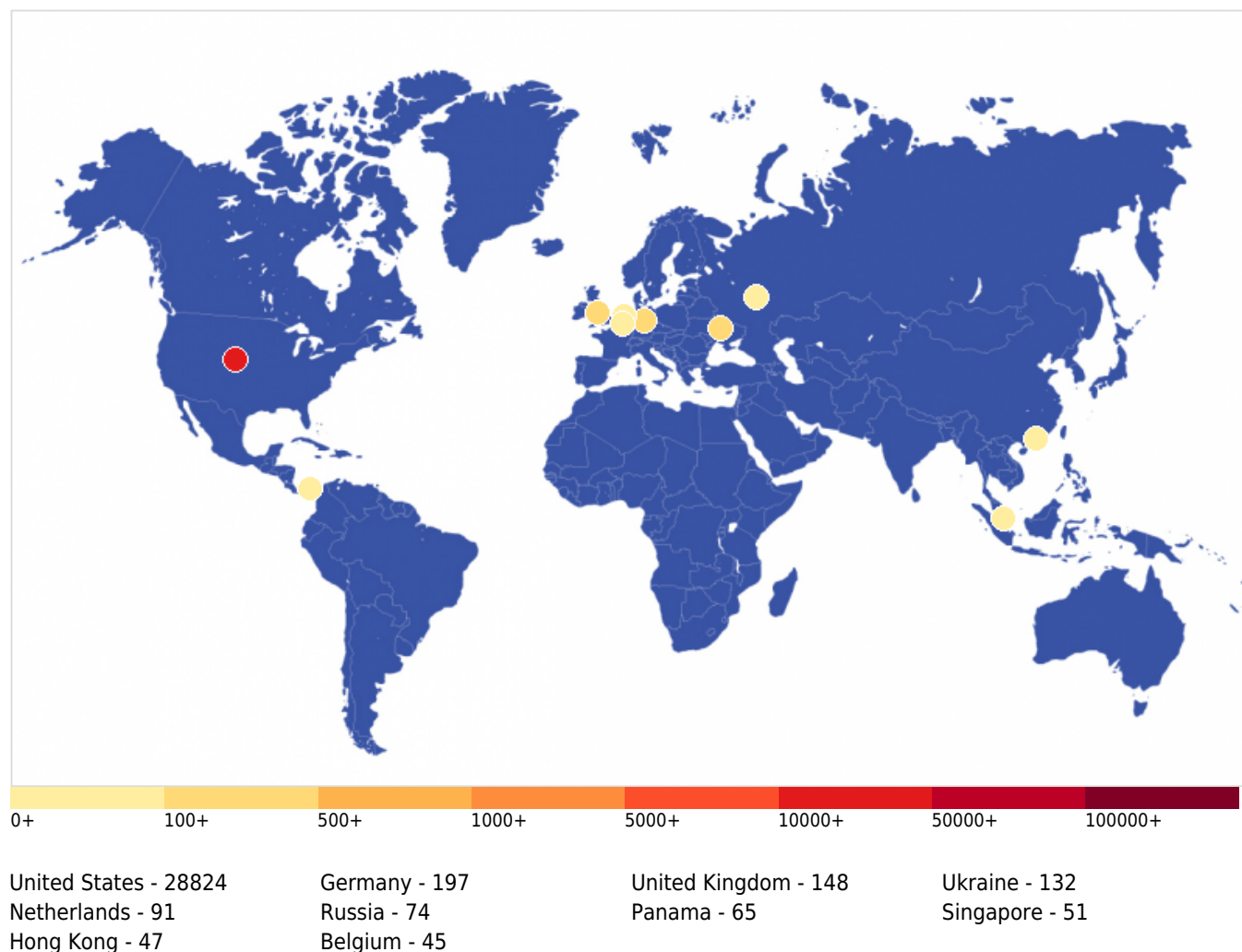
# 26

According to the range of addresses provided, the total number of hosts analyzed is 64, of which 40 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. For this period, there are 0 critical vulnerabilities, 2 high vulnerabilities, and 115 medium vulnerabilities. Thus, the vulnerability metric for your organization is 26%.

## Critical Attacks Per Country In Past Week



GLESEC 08/27/2023



The graph indicates that the vast majority of attacks, 28,824 in total, come from the United States. By comparison, Germany, the UK and the Ukraine all record much lower numbers, with fewer than 200 attacks each. Given this disparity, cybersecurity measures should especially focus on threats originating in the United States.

**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**

## BOARDROOM EXECUTIVE REPORT

### HOW CAN WE HELP?

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

