GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC
May 26, 2024

GLESEC 05/26/2024

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to april 2024 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

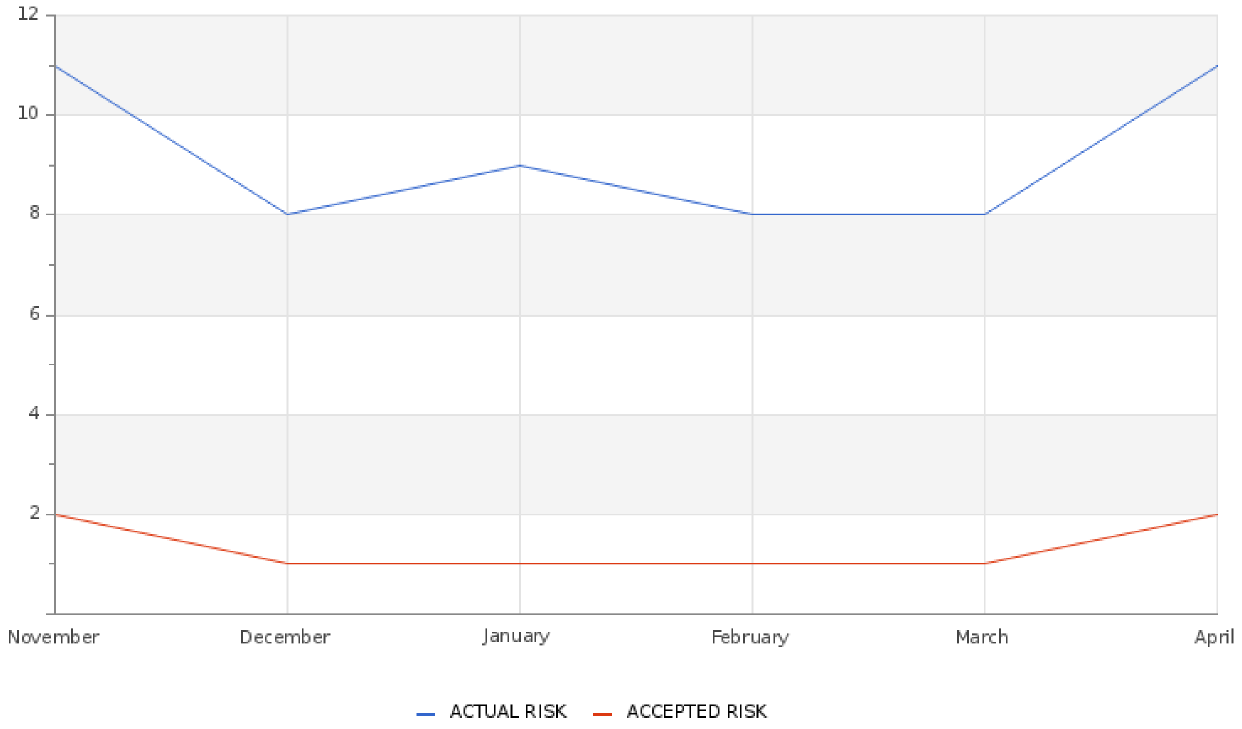
The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

RISK

Actual Risk	Accepted Risk	Confidence
11%	2%	Medium

Accepted & Actual Risk

GLESEC 05/26/2024



Over the course of this month, there has been a noticeable increase in the risk levels. The current risk now sits at 11%, and the accepted risk at 2%. This represents a significant rise from the previous month's figures, where the actual risk was recorded at 7% and the accepted risk at 1%.

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

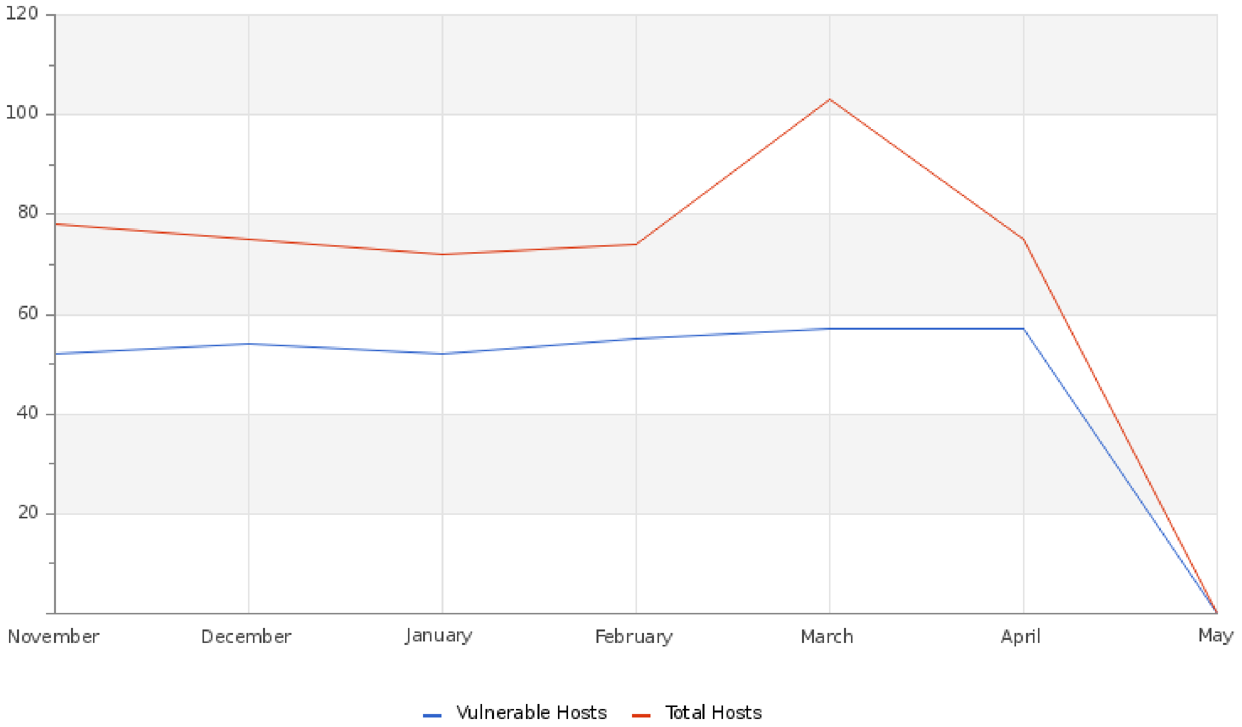
	Current Month	Previous Month
Actual Risk	11	7
Accepted Risk	2	1

Actual risk has increased by 4 points with respect to the previous month;
Accepted Risk has increased by 1 point with respect to the previous month.
These shifts in the realm of cybersecurity highlight how our environment is constantly evolving, underscoring the need for ongoing vigilance and adaptation to the emerging conditions in information security.

VULNERABILITY

GLESEC 05/26/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph illustrates a rise in the number of identified hosts coupled with a decline in vulnerabilities over the month, hinting at possible breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct vulnerabilities.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	72
Hosts Discovered	69	73
Vulnerable Hosts	48	54
Critical Vulnerabilities Count	51	23
High Vulnerabilities Count	47	35
Medium Vulnerabilities Count	336	280
Low Vulnerabilities Count	61	53

GLESEC 05/26/2024

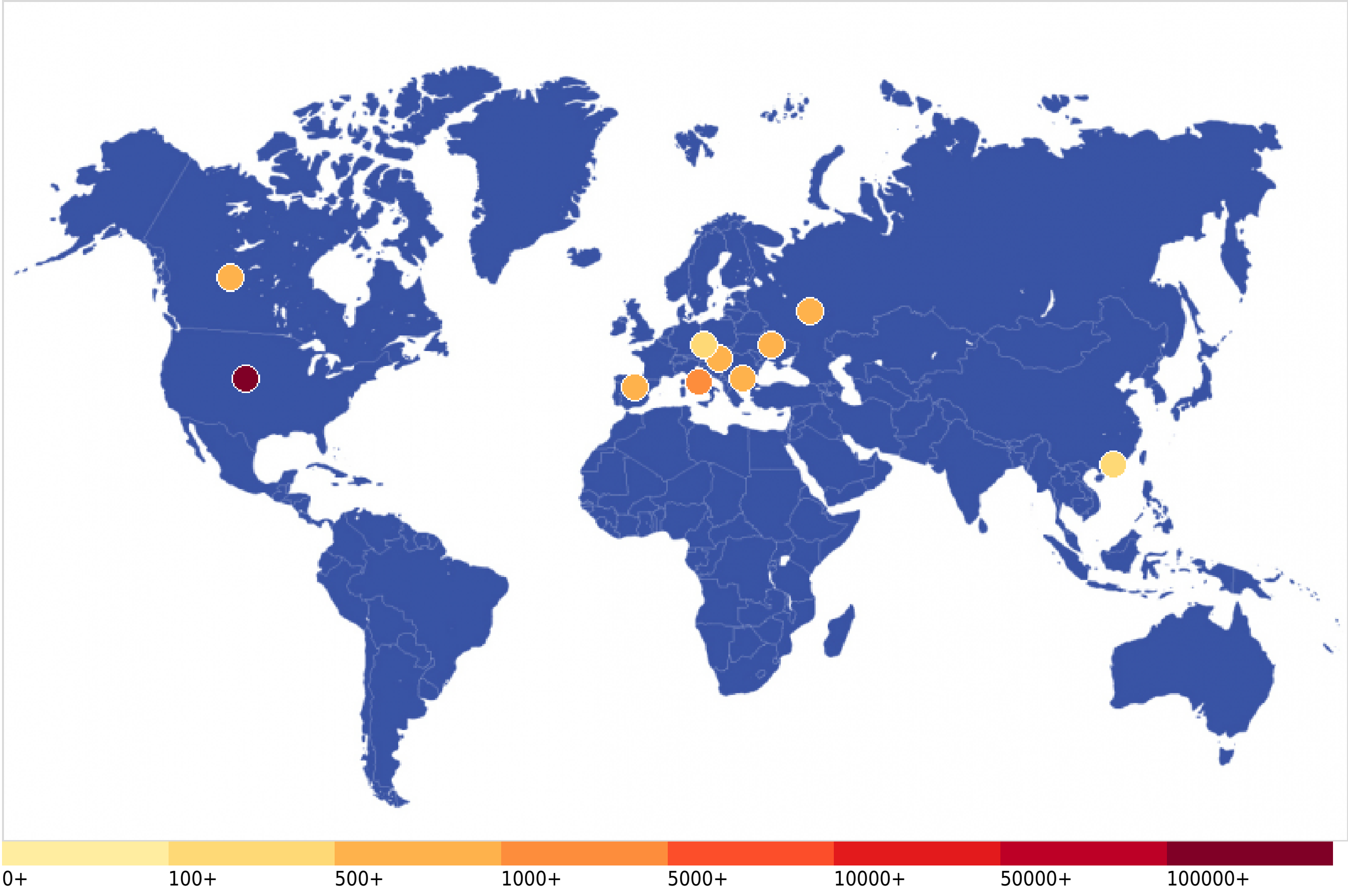
Vulnerability Metric

68

An analysis was conducted on 72 hosts based on their address range, revealing that 0 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 51 vulnerabilities of critical nature, 47 high-risk, 336 medium-risk, and 61 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 68%.

THREATS

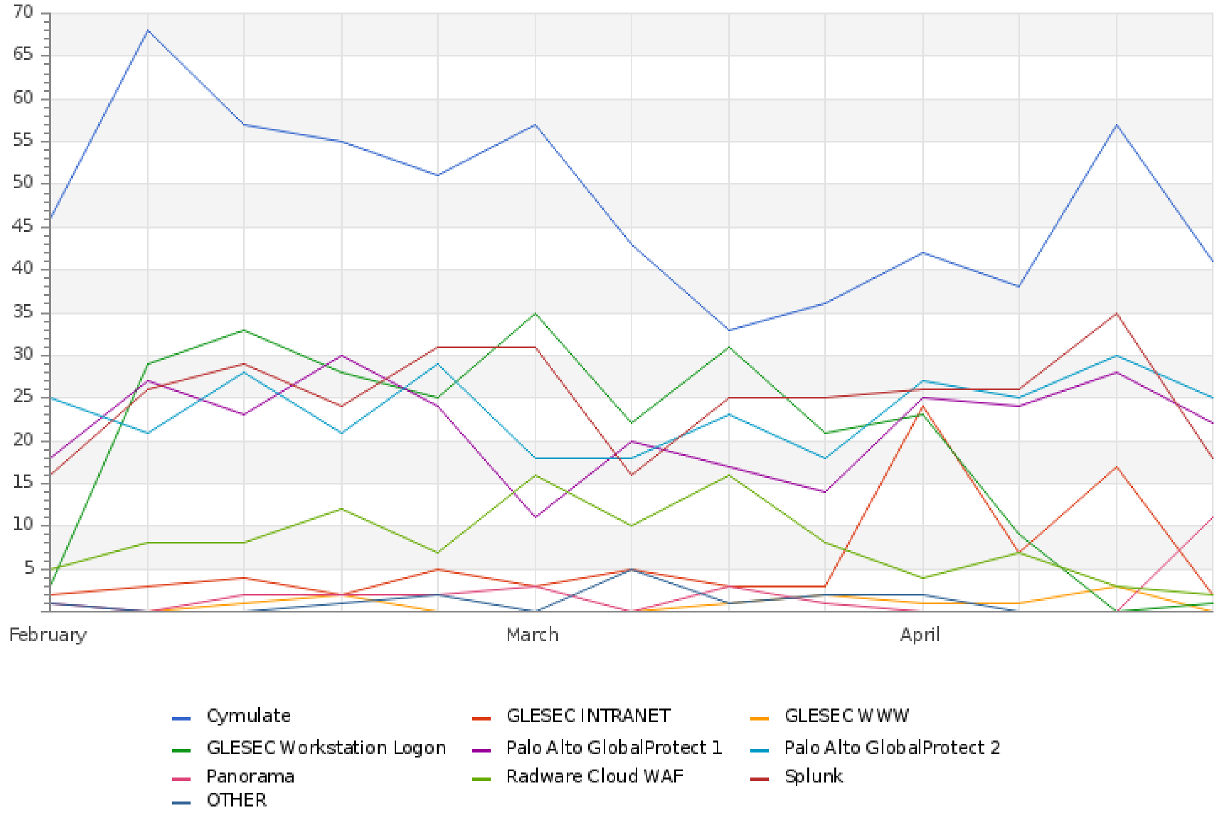
Critical Attacks Per Country In Past Week



United States - 121259
Italy - 1227
Hungary - 984
Ukraine - 972
Russia - 848
Canada - 770
Spain - 675
Bulgaria - 598
Czechia - 479
Hong Kong - 316

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 121,259 attacks. It is followed by the Italy with 1227 and Hungary with 984. Other countries like Ukraine, Russia, the Netherlands, Mexico, and India report lower figures. The map underscores the need to focus cybersecurity efforts mainly on threats originating from the U.S., while maintaining global vigilance.

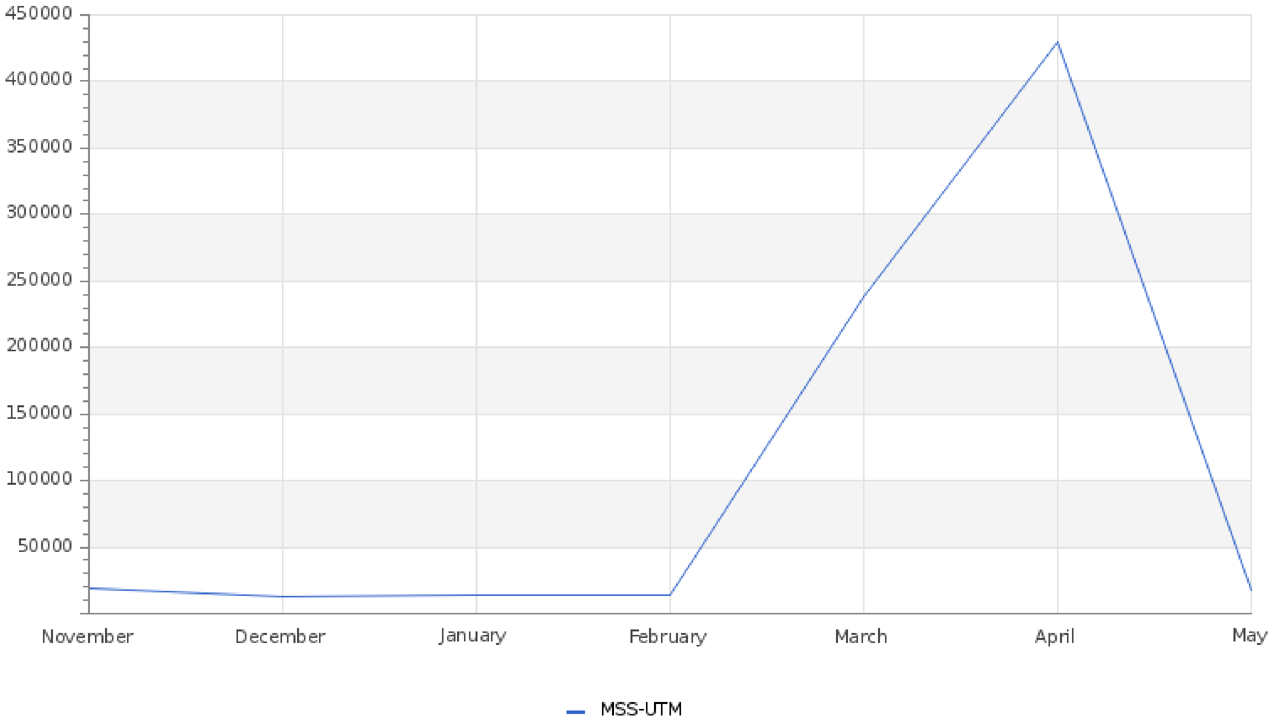
Total Number of Successful MFA authentications per application



The graph reveals a distinct trend in authentication patterns, with workstations and Cymulate emerging as the predominant applications for logins. This trend underscores the significant role these two areas play in daily activities, possibly indicating key interaction points or areas of importance within the organizational environment.

GLESEC 05/26/2024

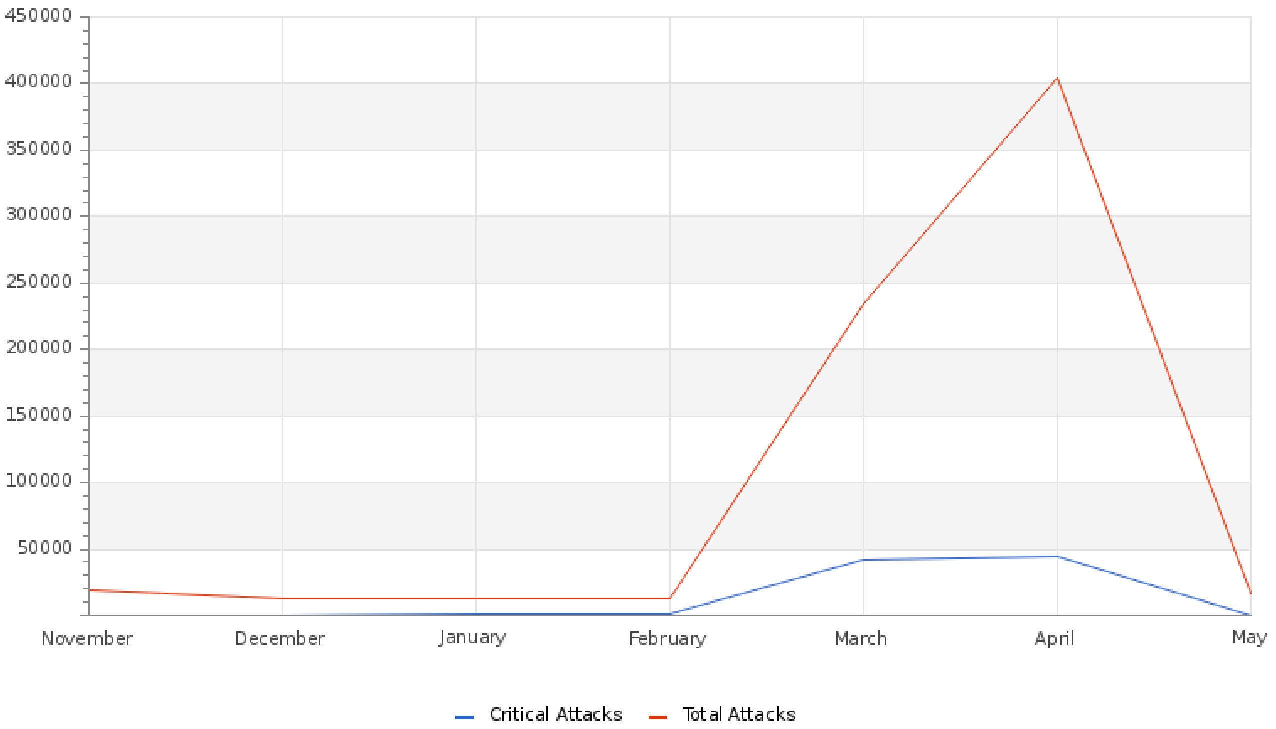
Total Attacks Successfully Blocked Per Service



The chart distinctly illustrates the positive effect of implemented security measures. Compared to the previous month, there has been a reduction in the total number of attacks, accompanied by an increase in the number of successfully thwarted attacks

GLESEC 05/26/2024

Attacks Successfully Blocked by Severity



The chart presents encouraging security outcomes, emphasizing the rise in successfully countered attacks. It proactively safeguards against emerging threats, including DDoS attacks, IoT botnets, advanced phishing methods, malware infiltrations, zero-day vulnerabilities, and complex DNS spoofing tactics.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	8	3
Critical Device Outages	0	0

Devices impacted by outages experienced swift recovery, with functionality being restored within seconds. These incidents primarily originated from false positives, attributed to transient disconnections.

Histogram of Total and Critical Device Outages

Devices experiencing downtime were swiftly brought back online within seconds, ensuring rapid recovery and minimal disruption. These incidents involved sensors that were reported and momentarily disconnected, highlighting the need for continuous monitoring and immediate response mechanisms to maintain operational efficiency and security.

GLESEC 05/26/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
22,370	0	0	0

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	83
Change in Systems Performance	4
FW Alerts	9
BAS DLP	7
BAS Web Security	12
BAS WAF	6
Immediate Threat System Vulnerable and Remediation by Patch Management	2
Change in High or Critical Vulnerabilities	20
High Number of Failed Authentications	1
Monitoring Event for SPLUNK CLOUD	2

For a closer look at specific instances, I recommend visiting the Skywatch platform. By applying the C&RU (Create & Review Update) filter there, you can choose the category that interests you the most. This approach will allow you to uncover the insights that Skywatch provides!

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.