



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

September 05, 2023



Organo Judicial 09/05/2023

TLP AMBER CISO

EXECUTIVE REPORT

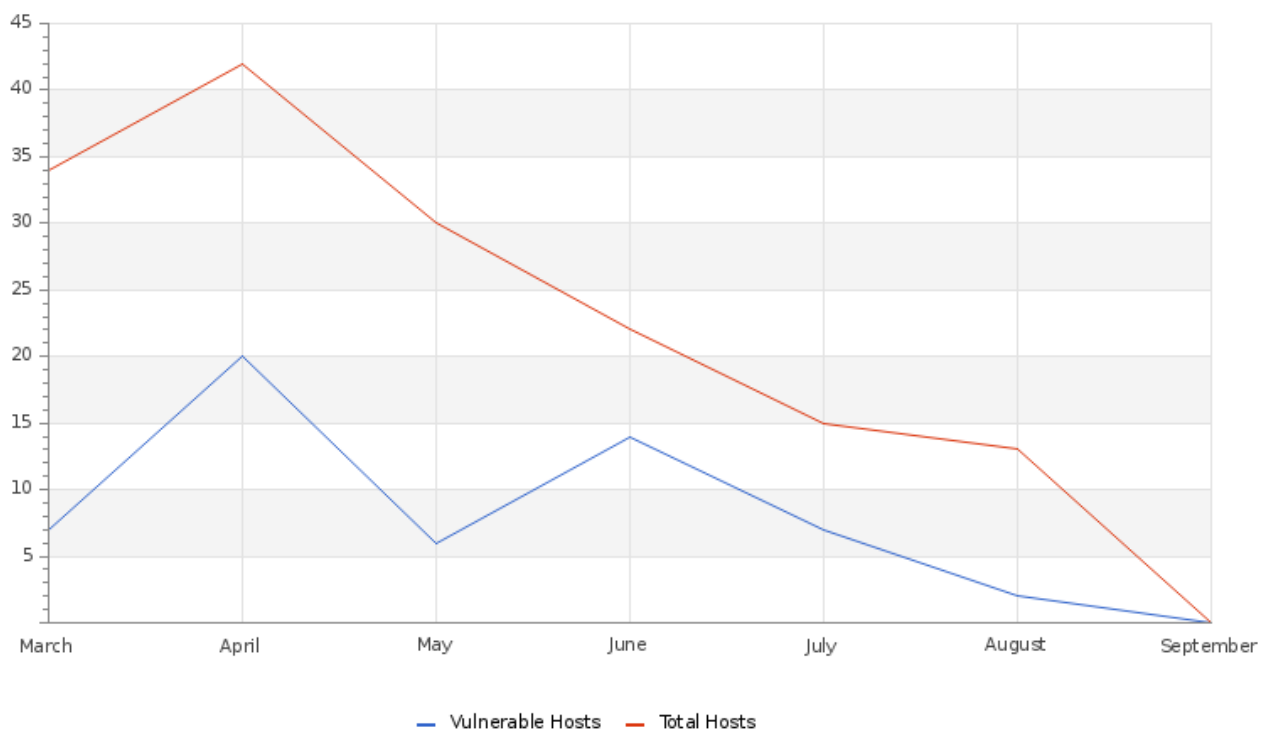
This report corresponds to THIS MONTH and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC's Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance,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

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



En la gráfica se muestra una reducción en las vulnerabilidades que se han descubierto durante el mes. Las vulnerabilidades descubiertas están relacionadas con el uso de protocolos que actualmente son considerados obsoletos. Recomendamos la hacer uso de versiones recientes de estos protocolos, para mejora de la seguridad de su empresa u organización.



Organo Judicial 09/05/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	38	38
Hosts Discovered	12	13
Vulnerable Hosts	2	5
Critical Vulnerabilities Count	0	2
High Vulnerabilities Count	0	2
Medium Vulnerabilities Count	4	9
Low Vulnerabilities Count	0	1
Phishing Score	0	0
Email Gateway Score	1	1
Web Application Firewall Score	0	0
Web Gateway Score	54	54
Endpoint Score	5	5
Hopper Score	0	0
DLP Score	0	0

En la tabla se puede observar los resultados que se han obtenido durante en el mes actual comparado con el mes anterior. Entre los resultados obtenidos destaca el puntaje del servicio Bas Web Gateway, recomendamos realizar una revisión de aquellas extensiones que no están siendo utilizadas y bloquearlas. Todos los resultados obtenidos de las simulaciones realizadas por el servicio MSS-BAS se encuentran documentados en la plataforma SKYWATCH.

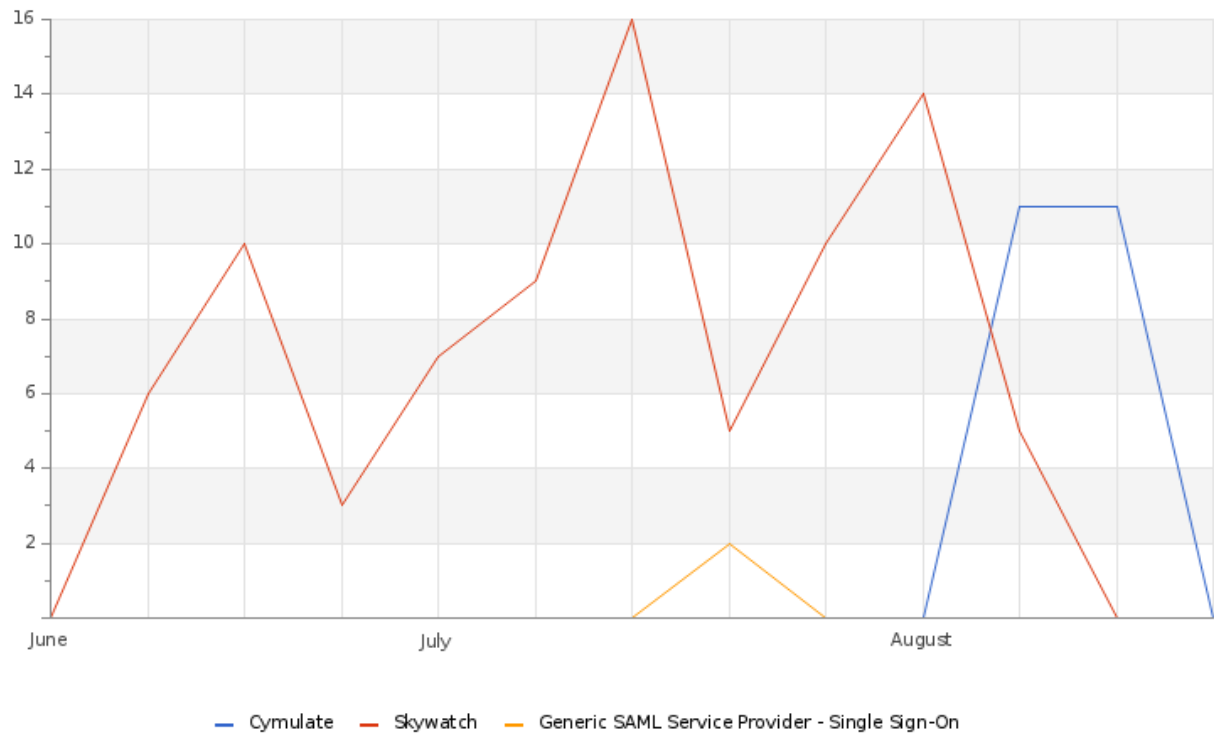
Vulnerability Metric**0**

Se han identificado y recomendando acciones para abordar y mitigar las vulnerabilidades presentes a nivel externo. Estas vulnerabilidades han sido documentadas y pueden ser visualizadas en el apartado C&RU de SKYWATCH

THREATS

Organo Judicial 09/05/2023

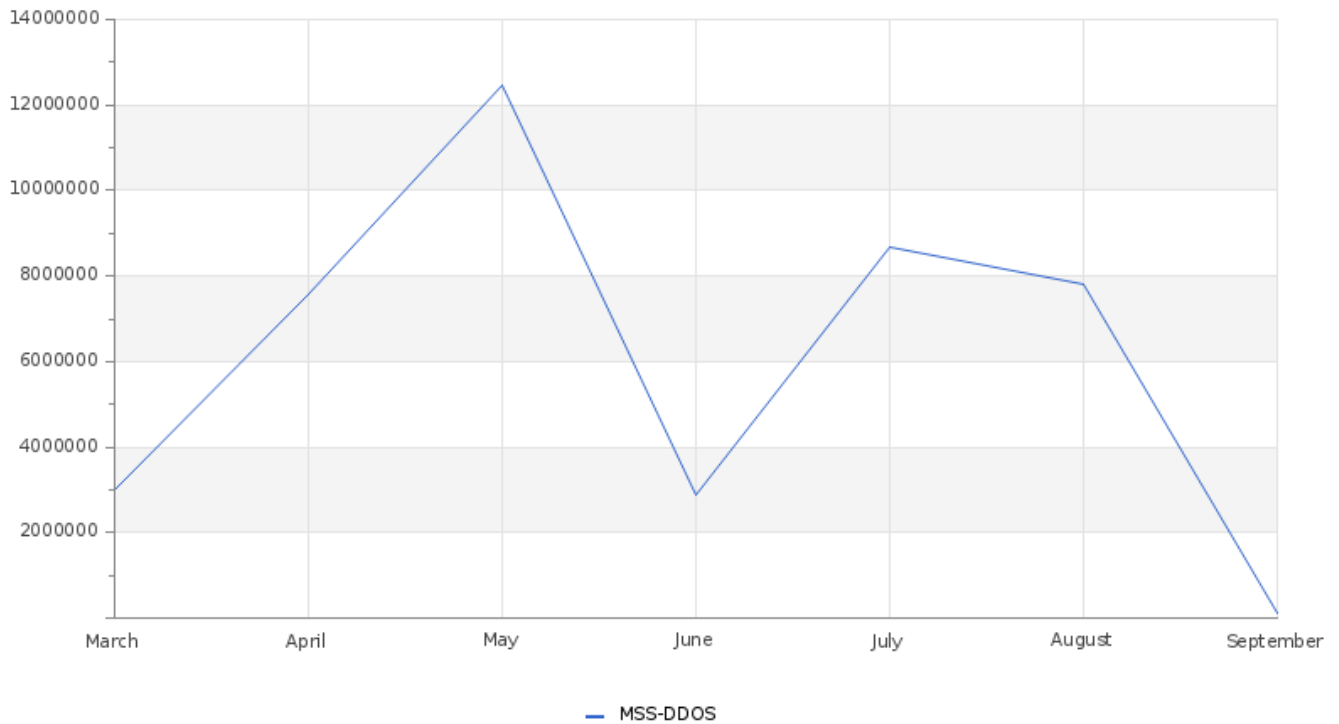
Total Number of Successful MFA authentications per application



La gráfica muestra la actividad constante y la cantidad de ingresos de los usuarios a las plataformas de Skywatch y Cymulate durante el mes.

Organo Judicial 09/05/2023

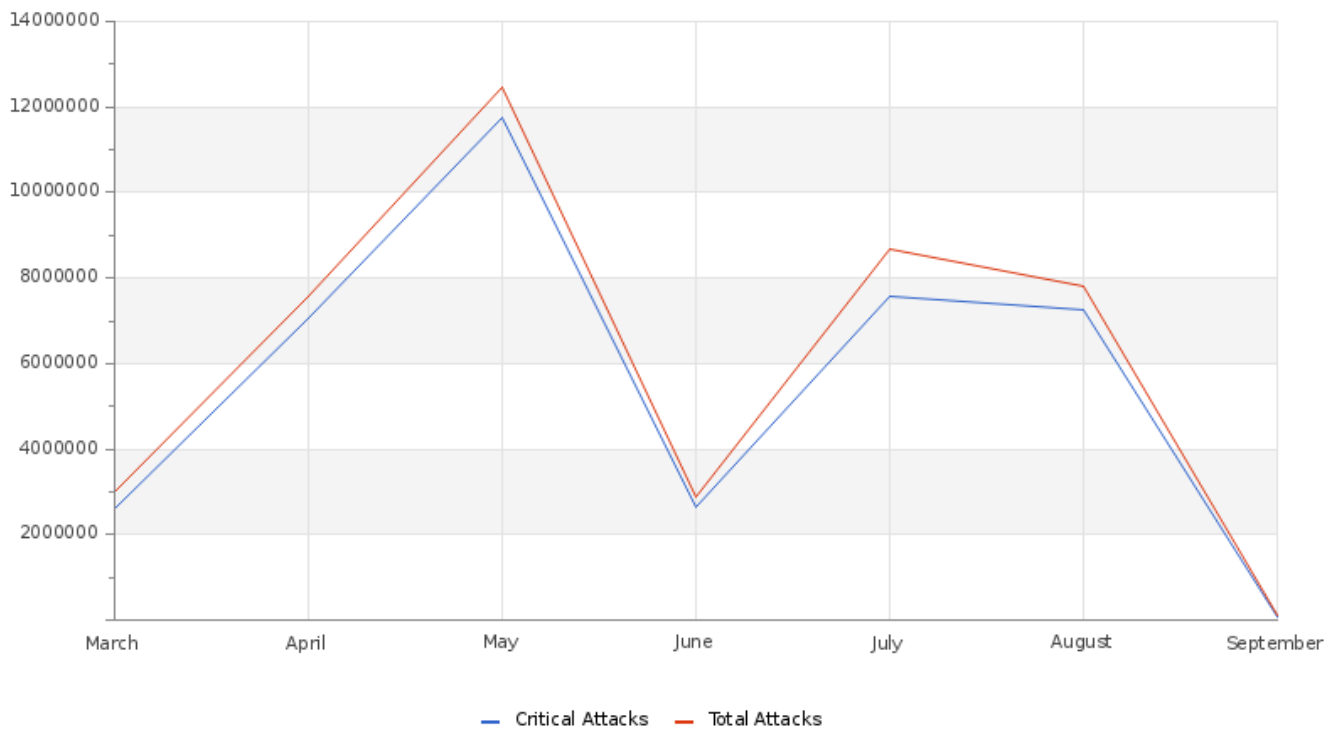
Total Attacks Successfully Blocked Per Service



Durante el mes se registraron un total de 7,823,972 ataques, hemos estado monitoreando estas actividades de manera constante . La mayor parte de estos ataques suelen provenir de IP's maliciosas y Botnets.

Organo Judicial 09/05/2023

Attacks Successfully Blocked by Severity



La cantidad de ataques críticos recibidos durante el mes fue de 7,267,159, la mayoría de estos clasificados como ataques ErtFeed. ErtFeed se centra en una inteligencia única en tiempo real que puede proporcionar protección preventiva contra amenazas emergentes específicas de DDoS, incluido IoT en evolución botnets y nuevos vectores de ataque DNS.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	2	0
Critical Down Devices	0	0

Debido a las restricciones de conexiones provenientes del exterior, se generaron estas alertas que indican que el dispositivo de encuentra Down.

Histogram of Total and Critical Device Outages



Organo Judicial 09/05/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	37
Change in Systems Performance	1
Immediate Threat System Vulnerable and Remediation by Patch Management	8
Change in Critical Perimeter Attacks	1
BAS Web Security	2

Durante el mes se han actualizado el estado de aquellas vulnerabilidades que todavía persisten en sus sistemas, han sido documentados los resultados de las pruebas realizadas por el servicio MSS-BAS. Recomendamos revisar detenidamente y aplicar las soluciones correspondientes, específicamente aquellas relacionadas con con amenazas inmediatas, que buscan probar la resiliencia de su entorno a las amenazas recientes. Para más información puede acceder a nuestra plataforma para clientes <https://skywatch.glesec.com> en la sección CR&U.

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.

