GLE SEC

COMPLETELY PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC
September 24, 2023

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to August 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

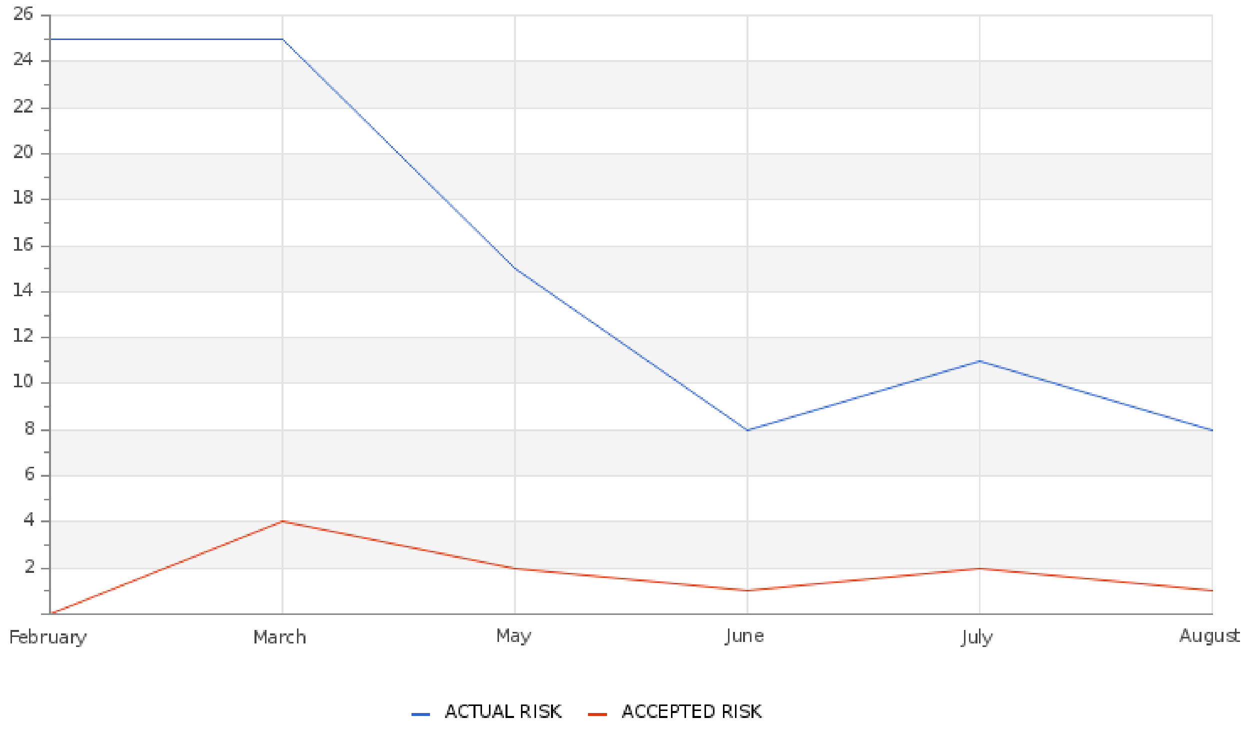
The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

RISK

Actual Risk	Accepted Risk	Confidence
8%	1%	High

Accepted & Actual Risk

GLESEC 09/24/2023



The current risk level has decreased. During this month, the current risk stands at 8, while the accepted risk remains at 1. Compared to the previous month, when the current risk was 10 and the accepted risk was 2, it is evident that the risk has decreased.

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

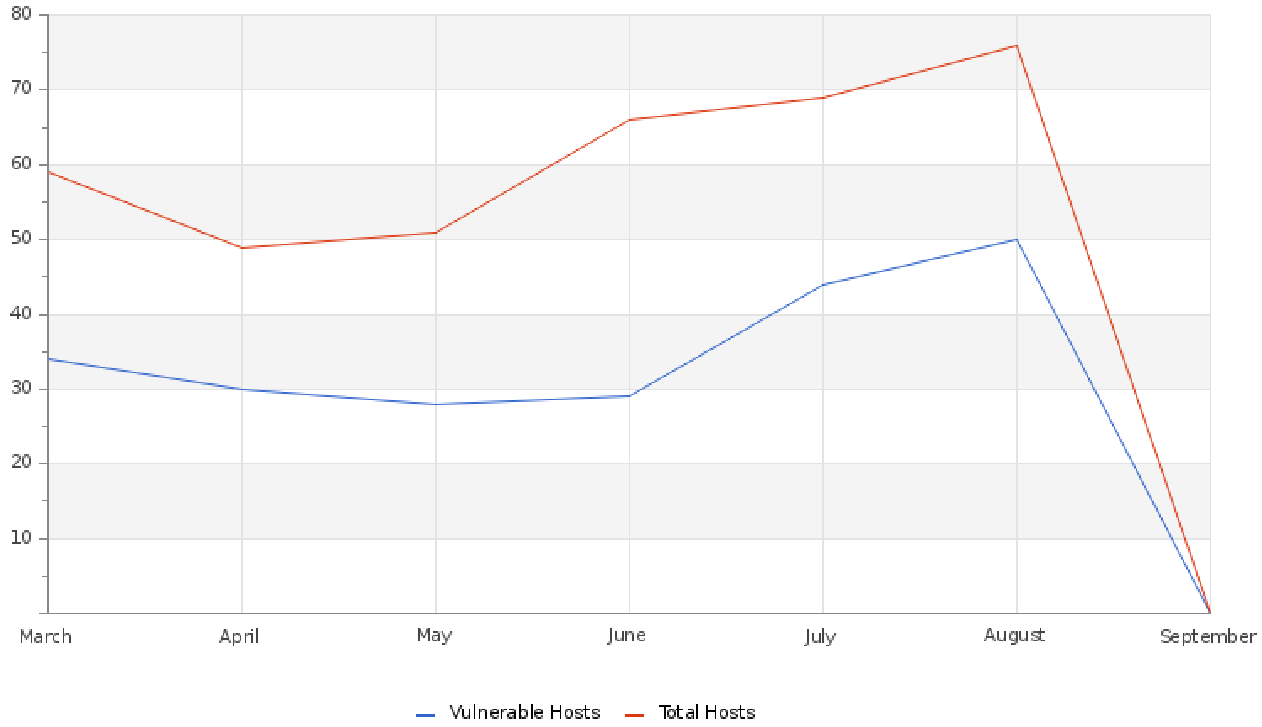
	Current Month	Previous Month
Actual Risk	8	10
Accepted Risk	1	2

Actual Risk has decreased by 2 points compared to the previous month;
Accepted Risk has decreased by 1 point compared to the previous month.
These fluctuations reflect the changing dynamics in our environment, underscoring the importance of monitoring and adapting to current conditions.

VULNERABILITY

GLESEC 09/24/2023

Hosts & Vulnerable Hosts In Last 6 Months



The graphic shows an increase in the number of hosts discovered and a decrease in vulnerabilities during the month. From this, we observe breaches in its security perimeter. Among the high-risk vulnerabilities, vulnerabilities in Apache POI, insecure Windows permissions, Cross-site scripting (DOM-based) and pending updates to Microsoft ASP.NET Core were identified. It is critical to also consider updating Palo Alto's GlobalProtect. To ensure a more secure environment, it is essential to address these areas promptly.

GLESEC 09/24/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	56
Hosts Discovered	67	64
Vulnerable Hosts	34	41
Critical Vulnerabilities Count	0	1
High Vulnerabilities Count	8	4
Medium Vulnerabilities Count	103	121
Low Vulnerabilities Count	22	25
Phishing Score	0	0
Email Gateway Score	9	10
Web Application Firewall Score	23	24
Web Gateway Score	54	51
Endpoint Score	43	14
Hopper Score	0	0
DLP Score	76	79

Simulations were carried out on our systems to evaluate different security aspects. The results obtained were as follows: a Phishing Score of 0, an Email Gateway Score of 9, a Web Application Firewall Score of 23, a Web Gateway Score of 54, an Endpoint Score of 43, a Hopper Score of 0, and a DLP Score of 76. These scores show the areas of strength and those that require greater attention in our security infrastructure.

Vulnerability Metric

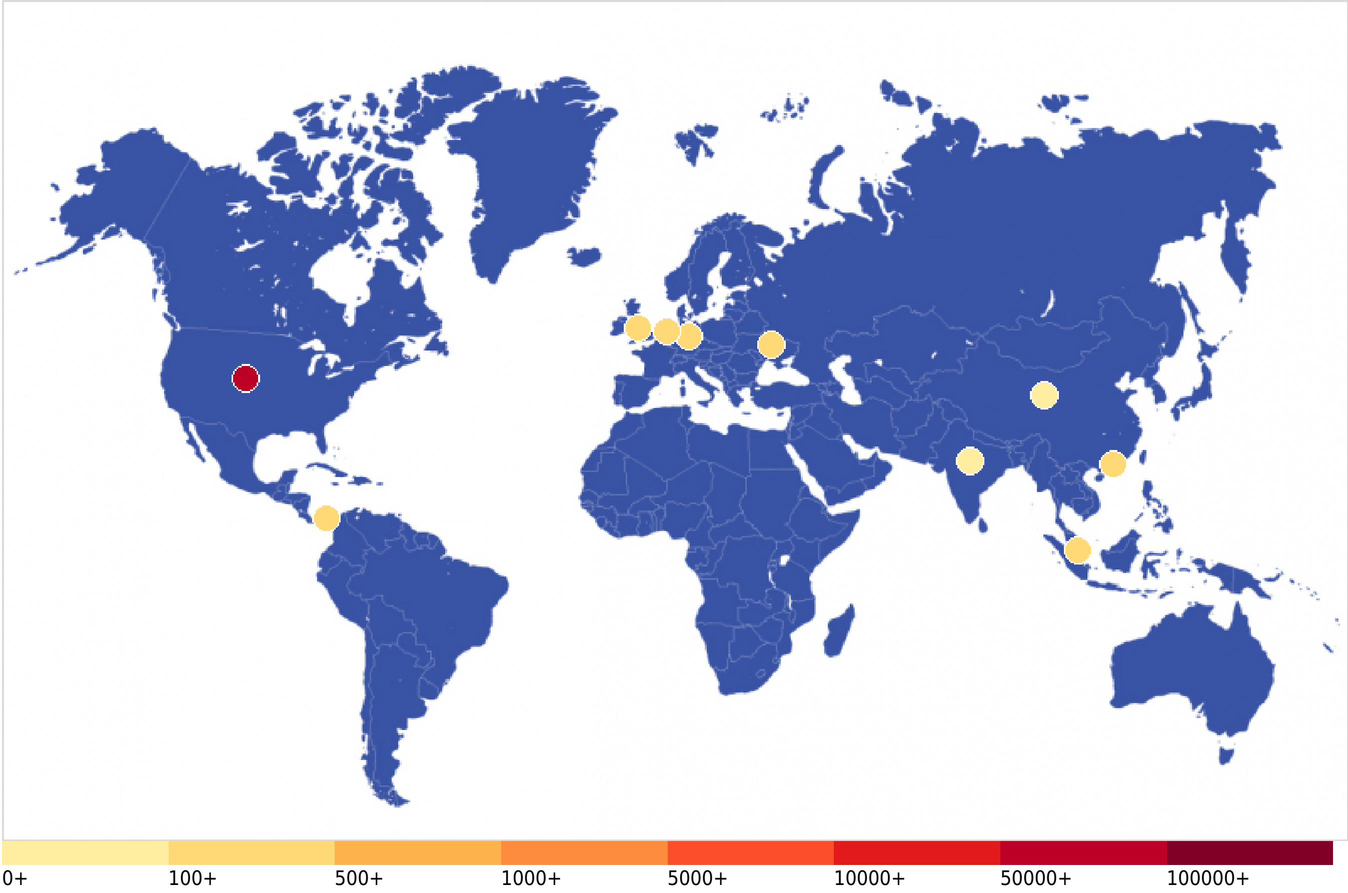
29

According to the range of addresses, a total of 67 hosts were analyzed, of which 34 were found to be vulnerable. Vulnerabilities are categorized according to their severity, as detailed in the table below. During this period, no critical vulnerabilities were recorded, but 8 high-risk vulnerabilities, 103 medium-risk vulnerabilities and 22 low-ranking vulnerabilities were recorded. Based on this data, the vulnerability index of your organization stands at 29%.

THREATS

Critical Attacks Per Country In Past Week

GLESEC 09/24/2023

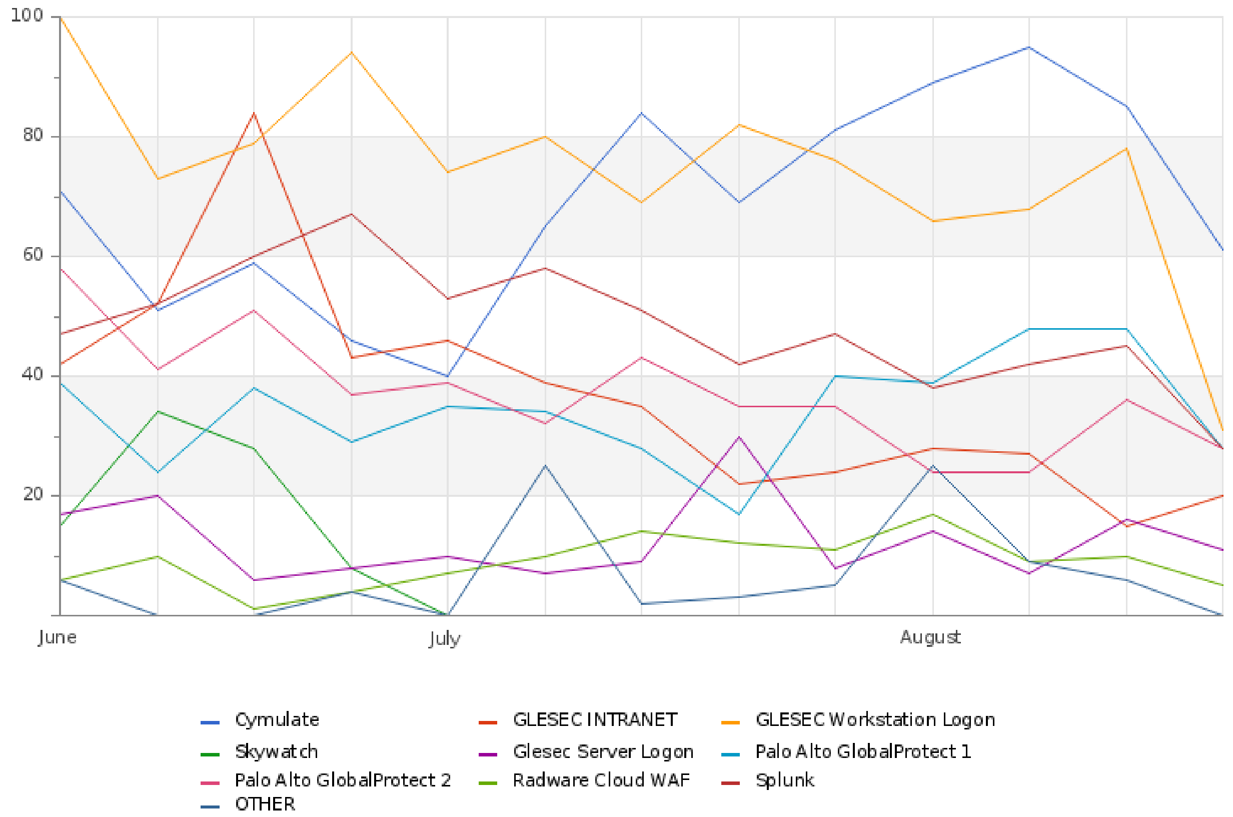


United States - 52880	Germany - 190	Panama - 183	United Kingdom - 160
Ukraine - 152	Singapore - 146	Netherlands - 107	Hong Kong - 100
China - 97	India - 59		

The graph shows that the vast majority of attacks, with a total of 52,880, originate in the United States. In contrast, Germany, the UK and Ukraine show considerably lower numbers, with fewer than 200 attacks per country. Given such an imbalance, cybersecurity strategies should focus primarily on threats originating in the United States.

GLESEC 09/24/2023

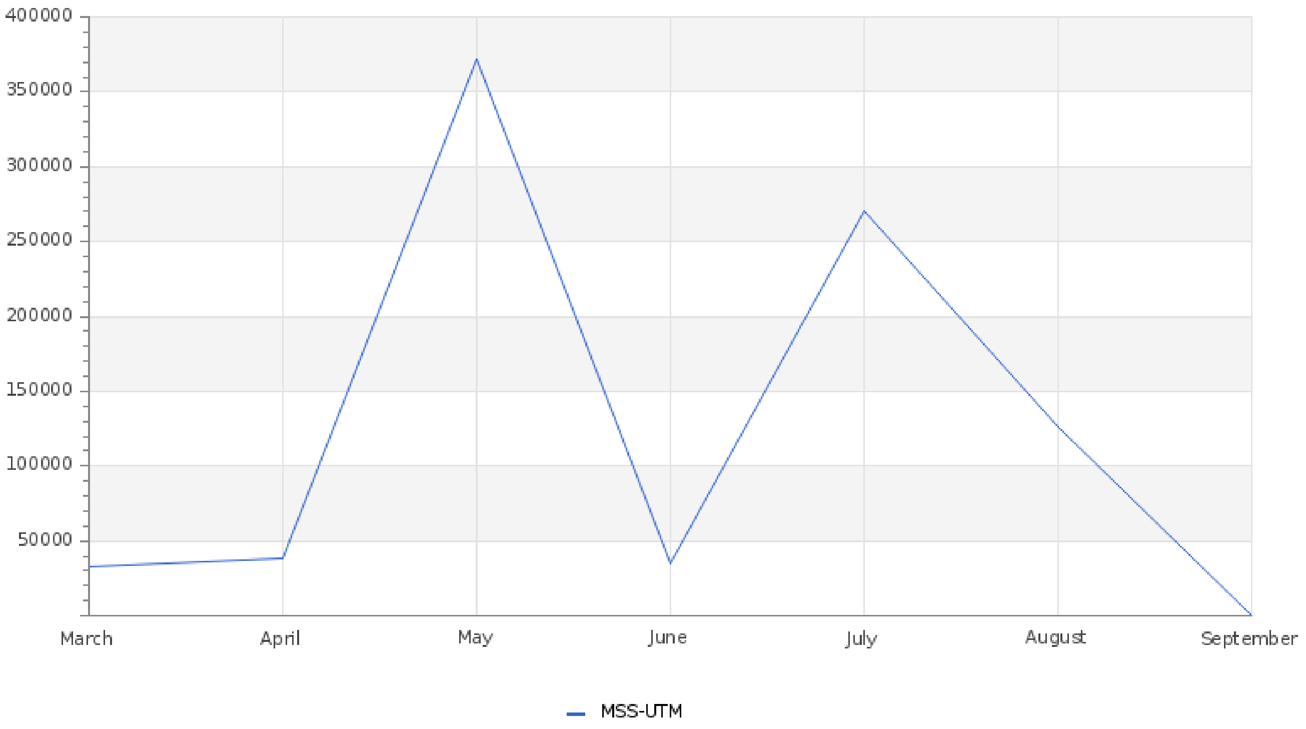
Total Number of Successful MFA authentications per application



The graph shows a clear trend in terms of authentications: it can be seen that the applications where logins predominate are, in particular, workstations and Cymulate. This information highlights the relevance of these two points in daily activity and could indicate areas of special interaction or importance within the organization's environment.

GLESEC 09/24/2023

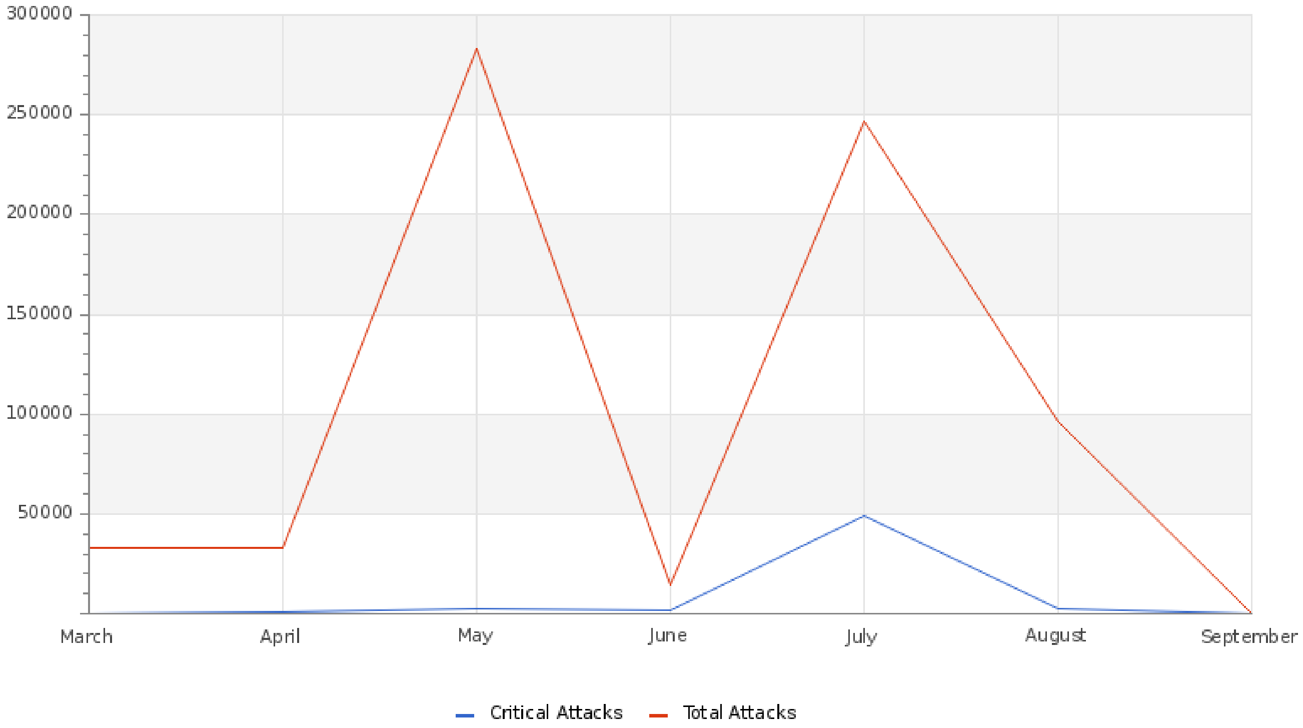
Total Attacks Successfully Blocked Per Service



The graph clearly shows how the adoption of measures has had a positive impact on security. In contrast to the previous month, we have experienced a decrease in the number of attacks, with an increase in the number of attacks that have been successfully blocked.

GLESEC 09/24/2023

Attacks Successfully Blocked by Severity



The graph shows favorable results in terms of security, highlighting the increase in the number of successfully neutralized attacks. Proactively, it has protected against emerging risks, such as DDoS attacks, IoT botnets, advanced phishing techniques, malware intrusions, zero-day threats and sophisticated DNS spoofing attack strategies.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	7	12
Critical Down Devices	0	0

Devices that experienced outages were restored within seconds. These incidents are the result of false positives caused by brief disconnections.

Histogram of Total and Critical Device Outages

Devices that experienced downtime were restored in just seconds, ensuring rapid recovery. These incidents, although momentary, are the result of false positives caused by brief disconnections. It is essential to monitor and understand these occurrences to ensure smooth operation and minimize future outages.

GLESEC 09/24/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
1,295	0	0	23,205

The MSS-EDR statistics are inflated, largely due to the BAS evaluations conducted through our specialized MSS-BAS service. It's essential to account for this skew when analyzing the data to gain a more accurate and contextual understanding of the security situation.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
EDR Alerts	424
BAS Immediate Threat	43
Monitoring Event for SPLUNK CLOUD	9
Change in Systems Performance	5
Change in Systems Availability	2
FW Alerts	1
BAS DLP	5
Change in High or Critical Vulnerabilities	29
Non Baselined Discovered System	1
Change in Baseline Systems Discovered	1
High Number of Failed Authentications	1
Breach and Attack Simulation Succesful Execution	1
BAS Endpoint Security	8
BAS Web Security	16

For details on specific cases, I invite you to explore the Skywatch platform. Once there, simply use the C&RU filter to choose the type that piques your curiosity - discover what Skywatch has in store for you!

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.