

{{ logo }}

{{ month }} {{ year }}

|  |
| --- |
| SOC REPORT  2023 |
|  |
| 17 Şubat  CYBER GLADIATORS |

# ABOUT YOUR COMPANY

EXAMPLE

CyberGladiators has been working in the field of Cyber ​​Security since 2015. It always maintains customer satisfaction with its team and state-of-the-art products, including many attack vectors that are frequently encountered today.

CyberGladiator Certifacates

* ISO27001, BS 10012 .etc

# CONTENTS

[ABOUT YOUR COMPANY 2](#_Toc127521426)

[EXECUTIVE SUMMARY 4](#_Toc127521427)

[CYBER SECURITY DEVELOPMENTS IN {{ month }} 5](#_Toc127521428)

[STATISTICS DATA 10](#_Toc127521430)

[ACTIVITIES OF THE {{ month }} 12](#_Toc127521444)

# EXECUTIVE SUMMARY

EXAMPLE

This report was created as a result of the analysis of defense and tracking systems established by CyberGladiators analysts. It is aimed to report the systems monitored 24/7 on a monthly basis. It is important to consider the systems in terms of more stable and safe operation.

{%if total\_ticket\_number>0:%}{{ total\_ticket\_number}} tickets were opened by the CyberGladiators team in {{ month }}. Of these {%if system\_performance\_ticket\_number>0:%} {{system\_performance\_ticket\_number}} are system-related,{%endif%} {%if windows\_events\_ticket\_number > 0:%}{{ windows\_events\_ticket\_number}} Windows Security Events {%endif%}{%if incident\_info\_ticket\_number > 0:%}{{ incident\_info\_ticket\_number }} contain attack variations{%endif%}. {%else%}no activity was found.{%endif%}

{{ month }} specific to the month..

# CYBER SECURITY DEVELOPMENTS IN {{ month }}

NOT FOR YOU !

# TheHackerNews, BleepingComputer, Dark Reading etc. You can write the news and developments covering Cyber ​​Security from the addresses.

# STATISTICS DATA

# In this part of the monthly SOC report prepared by CyberGladiators experts, firm-oriented attack and system performance statistics are given. In {{ year }} in the month {{ month }}…

# A.OFFENSIVE STATISTICS

# ATTACK VECTORS

{% if incident\_info\_ticket\_number > 0: %}

The graph of attack vectors arriving on {{ user\_project }} systems in {{ year }} in {{ month }} is as follows.

{{ attack\_vectors\_graph }}

{% else %}

There are no attack variations on {{ user\_project }} systems within {{ year }} month {{ month }}.

{% endif %}

# WINDOWS SECURITY EVENTS

{% if windows\_events\_ticket\_number > 0: %}

The Windows Security Event graph that came to {{ user\_project }} systems in {{ year }} in {{ month }} is as follows.

{{ windows\_security\_events\_graph }}

|  |  |  |  |
| --- | --- | --- | --- |
| Windows Security Events |  |  | Number of Problems Experienced |
| {{%tr for w\_items in windows\_events %}} | | | |
| {{ w\_items[0] }} |  |  | {{ w\_items[1] }} |
| {{%tr endfor %}} | | | |

{% else %}

No Windows Security Events events were observed on {{ user\_project }} systems during {{ year }} month {{ month }}.

{% endif %}

# SOURCE IP’s

{% if source\_ips\_control\_number != 0 %}

The source IP addresses graph of the attacks carried out on {{ user\_project }} systems in {{ year }} in {{ month }} is as follows.

|  |  |
| --- | --- |
| IP Addresses | Number of Problems Experienced |
| {{%tr for s\_items, s\_value in source\_ips %}} | |
| {{%tr for s\_key in s\_items %}} | |
| {{ s\_key }} | {{ s\_value }} |
| {{%tr endfor %}} | |
| {{%tr endfor %}} | |

{% else %}

No source ip information was found for {{ user\_project }} systems in {{ year }} month {{ month }}.

{% endif %}

# TARGET IP’s

{% if target\_ips\_control\_number != 0 %}

The target IP addresses graph of the attacks carried out on {{ user\_project }} systems in {{ year }} in {{ month }} is as follows.

|  |  |
| --- | --- |
| IP Addresses | Number of Problems Experienced |
| {{%tr for d\_items, d\_value in target\_ips %}} | |
| {{%tr for d\_key in d\_items %}} | |
| {{ d\_key }} | {{ d\_value }} |
| {{%tr endfor %}} | |
| {{%tr endfor %}} | |

{% else %}

No target ip information was found for {{ user\_project }} systems within {{ year }} month {{ month }}.

{% endif %}

# LOCATIONS

{% if location\_control\_number != 0 %}

The location information of the attacks on {{ user\_project }} systems in {{ year }} in {{ month }} is as follows.

|  |  |
| --- | --- |
| Country | Number of Attack |
| {{%tr for c\_items, c\_value in countries %}} | |
| {%tr for c\_key in c\_items %} | |
| {{ c\_key }} | {{ c\_value }} |
| {{%tr endfor %}} | |
| {{%tr endfor %}} | |

{% else %}

There is no location information for {{ user\_project }} systems within {{ year }} month {{ month }}.

{% endif %}

# TARGET PORT INFORMATION

{% if target\_ports\_control\_number != 0 %}

The target port information of the attacks that came to {{ user\_project }} systems in {{ year }} in {{ month }} is as follows.

|  |  |
| --- | --- |
| Target Port | Number of Targeted Attacks |
| {{%tr for dp\_items, dp\_value in destination\_ports %}} | |
| {%tr for dp\_key in dp\_items %} | |
| {{ dp\_key }} | {{ dp\_value }} |
| {{%tr endfor %}} | |
| {{%tr endfor %}} | |

{% else %}

There is no target port information for {{ user\_project }} systems within {{ year }} month {{ month }}.

{% endif %}

# RATE OF KNOWN TO HARMFUL IP

{% if dangerous\_state\_control\_number > 0: %}

It was formed as a result of comparing the IP addresses that attacked {{ user\_project }} systems in {{ year }} with cyber intelligence sites. IPs that have one or more activities in the cyber intelligence sources used are considered harmful by us, even though they are not reported by cyber intelligence sites.

{{ dangerous\_state\_graph }}

{% else %}

No attacking IP addresses were observed on {{ user\_project }} systems in {{ year }}.

{% endif %}

# B.SYSTEM STATISTICS

# SYSTEM PERFORMANCE STATISTICS

{% if system\_performance\_control\_number != 0 %}

System problems in {{ user\_project }} systems during {{ year }} month {{ month }} are as follows.

|  |  |
| --- | --- |
| Category | Number of Opened Tickets |
| {{%tr for sp\_items, sp\_value in system\_performance %}} | |
| {%tr for sp\_key in sp\_items %} | |
| {{ sp\_key }} | {{ sp\_value }} |
| {{%tr endfor %}} | |
| {{%tr endfor %}} | |

{% else %}

No system problems were found on {{ user\_project }} systems during {{ year }} {{ month }}.

{% endif %}

# SYSTEM PERFORMANCE SOURCE IP’s

{% if system\_performance\_source\_ip\_control\_number != 0 %}

|  |  |
| --- | --- |
| IP Addresses | Number of Problems Experienced |
| {{%tr for spsi\_items, spsi\_value in system\_performance\_source\_ip %}} | |
| {%tr for spsi\_key in spsi\_items %} | |
| {{ spsi\_key }} | {{ spsi\_value }} |
| {{%tr endfor %}} | |
| {{%tr endfor %}} | |

{% else %}

No servers with system performance problems were found on {{ user\_project }} systems.

{% endif %}

# INVENTORY LIST

|  |  |  |
| --- | --- | --- |
| Server Name | IP Address | Server Availability |
| {{%tr for host\_info in hosts\_info %}} | | |
| {{ host\_info.host }} | {{ host\_info.ip }} | {% if host\_info.available == “1” %} PAINT ME GREEN ☺  {% elif host\_info.available == “2” %} PAINT ME RED ☹ {% elif host\_info.available == “0” %} PAINT ME GRAY 😐 {% endif %} |
| {{%tr endfor %}} | | |

# ACTIVITIES OF THE {{ month }}

# General checks were made.

# The programs have been updated.

# Servers checked.

# DNS vulnerabilities, Logs etc. Write down all the transactions made during that month.