



CORP OVERVIEW

All Requests



TOP SIGNALS

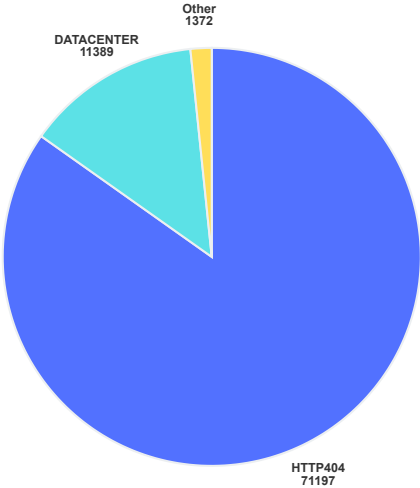
ATTACK SIGNALS

Indicators that suggest attempts or activities of potential attacks in the system

ANOMALY SIGNALS

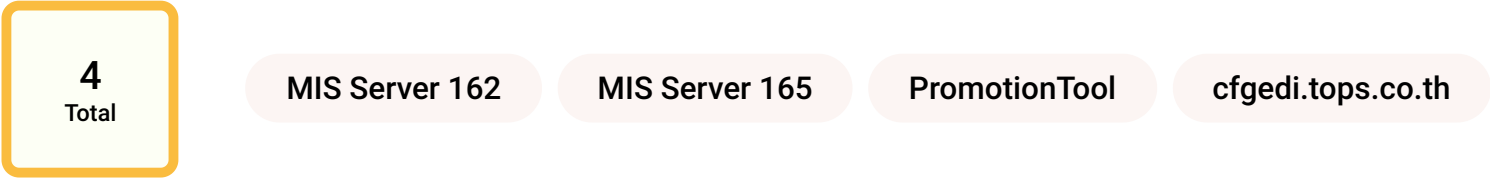
Indicators that suggest there may be irregularities in the system

No data available for Attack Signals



SITE NAME

All site.



SITE URL

URL of all sites.





## REQUESTS BY SITE

Site : **misserver165**  
Attack by country

No Data

Requests with attack signals

All Requests  
786

Attack  
0

Block  
0



No attack data

No attacks detected during this period

Site : **misserver162**  
Attack by country

No Data

Requests with attack signals

All Requests  
1.7k

Attack  
0

Block  
0



No attack data

No attacks detected during this period





## REQUESTS BY SITE

Site : **promotiontool**  
Attack by country

No Data

Requests with attack signals

All Requests  
12

Attack  
0

Block  
0



No attack data

No attacks detected during this period

Site : **cfgedi.tops.co.th**  
Attack by country

No Data

Requests with attack signals

All Requests  
239.4k

Attack  
0

Block  
0



No attack data

No attacks detected during this period

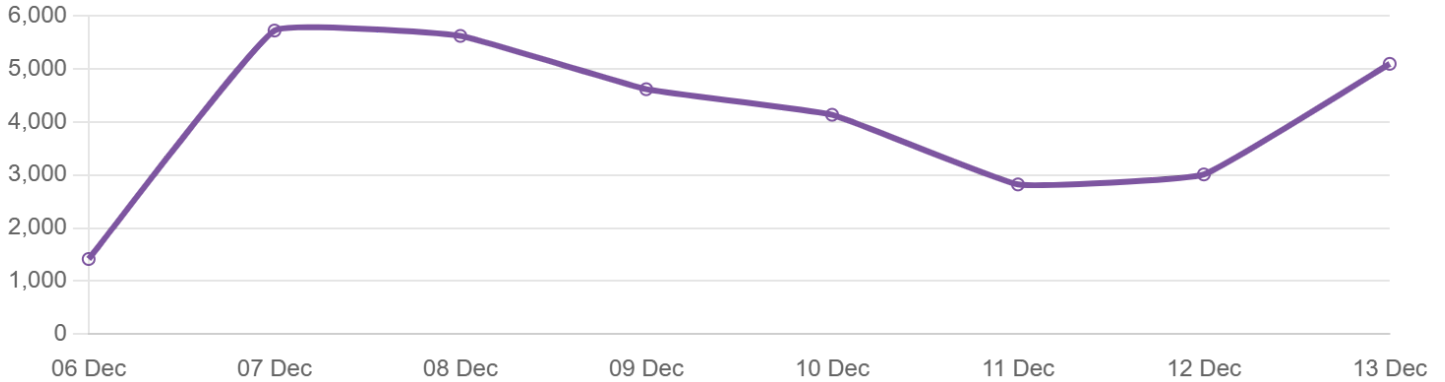




## Request Volume

All requests for this site.

37954.38 average RPS



Total Requests

303,635 Requests

## OWASP INJECTION ATTACK

The most common attacks from OWASP Top 10



- SQLI**  
Exploits vulnerabilities in SQL queries to access, modify, or delete database information.
- XSS**  
Inserts malicious scripts into a website, enabling attackers to steal or manipulate user data.
- CMDEXE**  
Executes unauthorized system commands through an application, potentially giving attackers control over the server.
- TRAVERSAL**  
Accesses restricted files by navigating to unauthorized directories, exposing sensitive data.

## SCANNERS

Scanners refer to tools used to check the security of a system.



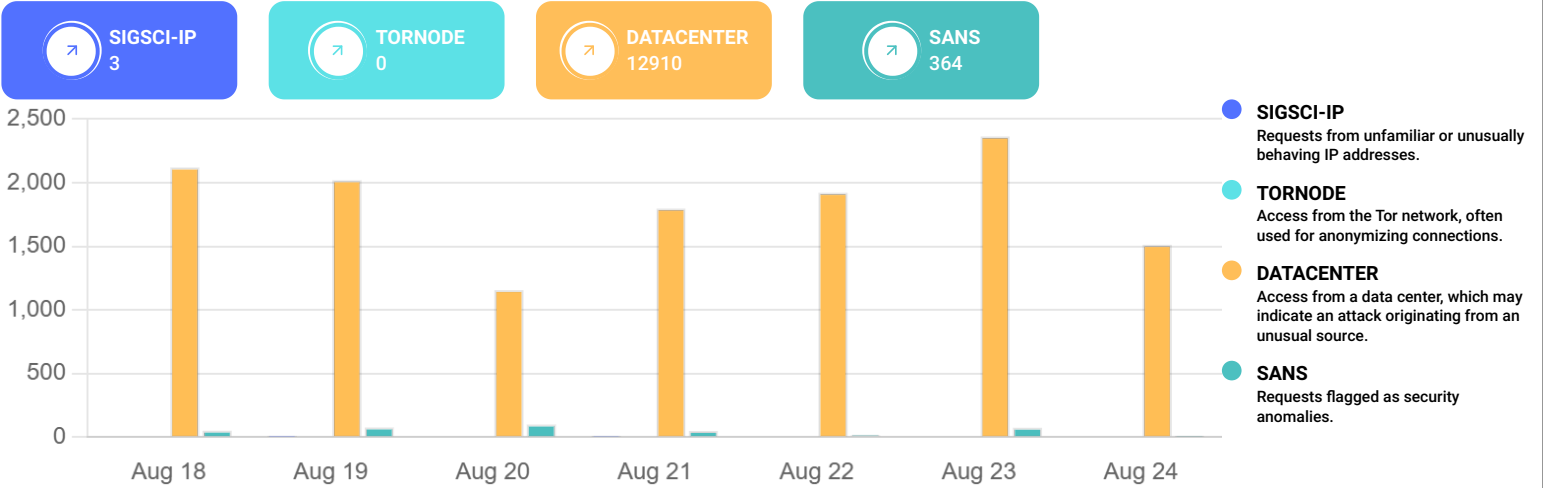
- USERAGENT**  
Scans user agents to detect anomalies.
- BACKDOOR**  
Detects potential backdoor access to systems.
- FORCEFULBROWSING**  
Monitors for unauthorized browsing attempts.
- PRIVATEFILE**  
Identifies private files exposed unintentionally.
- PRI**  
Scans for other potential threats.





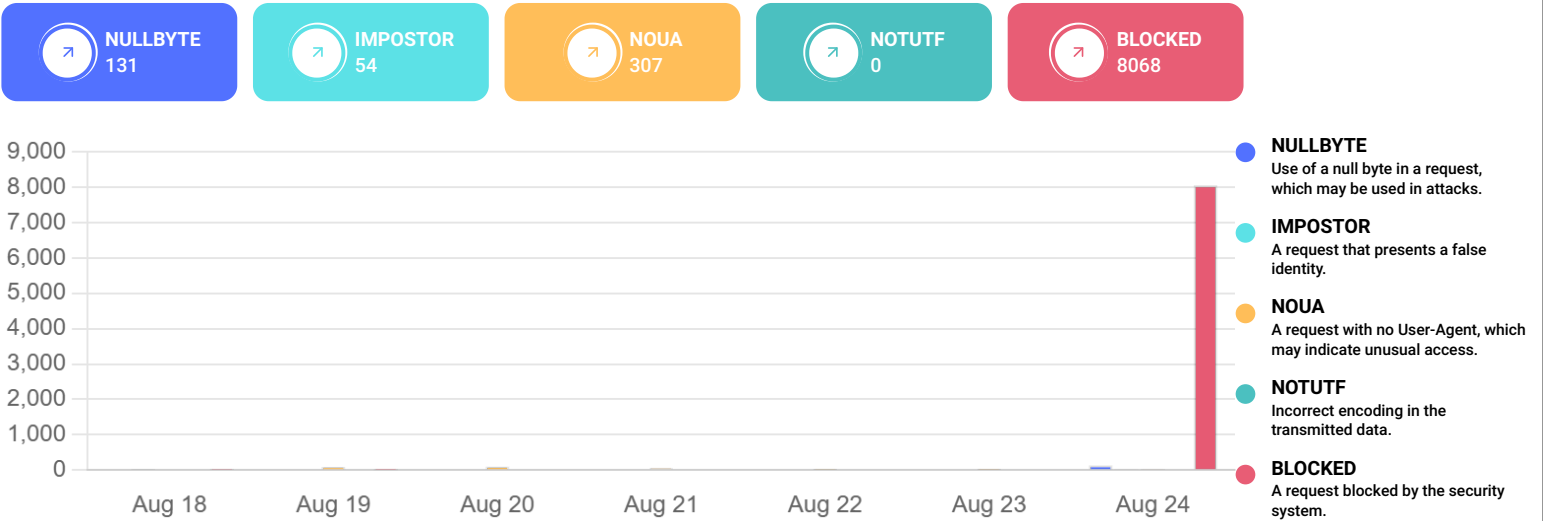
## TRAFFIC SOURCE ANOMALIES

Refer to requests from unusual or questionable sources.



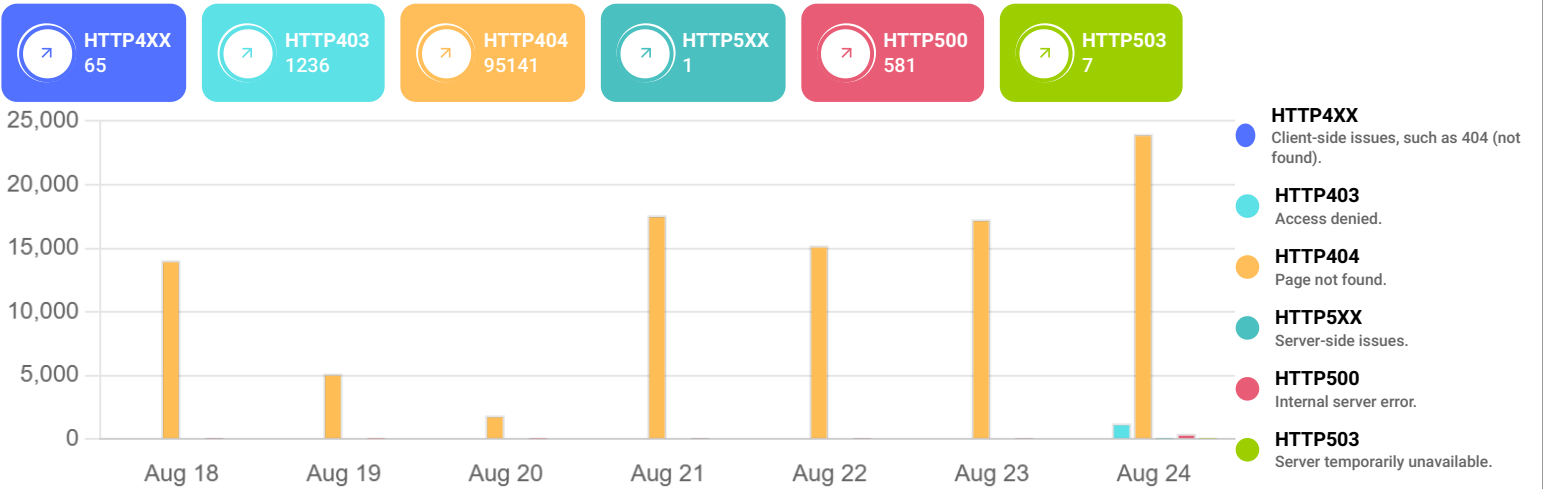
## REQUEST ANOMALIES

Anomalous behaviors within request headers.



## RESPONSE ANOMALIES

Client and server error codes.





## Even

IPs flagged for exceeding thresholds

<div><div></div><div>5.253.41.69 (JP)</div></div> <div><div>SQLI</div><div>BLOCKED</div></div> <div>2024-12-12T06:19:01Z</div>	<div><div></div><div>5.253.41.69 (JP)</div></div> <div><div>SQLI</div><div>BLOCKED</div></div> <div>2024-12-12T06:18:28Z</div>	<div><div></div><div>5.253.41.69 (JP)</div></div> <div><div>SQLI</div><div>BLOCKED</div></div> <div>2024-12-12T06:18:25Z</div>
--	--	--

## TOP ATTACKS

Top URLs containing attack signals

<div><div></div><div>cfgedi.tops.co.th/wpt_prod/</div></div>	4000 requests
<div><div></div><div>cfgedi.tops.co.th/wpt_prod/default.aspx</div></div>	379 requests
<div><div></div><div>cfgedi.tops.co.th/wpt_prod/WS_Login/</div></div>	162 requests

## EVENT ATTACK REQUEST

SOURCE	SIGNALS/PAYLOADS	RESPONSE
<div><div></div><div>(Japan)</div><div>5.253.41.69</div><div>cfgedi.tops.co.th/wpt_prod/</div></div>	<div><div>SQLI</div><div>BLOCKED</div></div>	<div>Status: Blocked</div> <div>Agent: 406</div> <div>Server: 406</div> <div>Response size: 0B</div>
<div><div></div><div>(Japan)</div><div>5.253.41.69</div><div>cfgedi.tops.co.th/wpt_prod/WS_Login/fonts/font-awesome-4.7.0/fonts/</div></div>	<div><div>SQLI</div><div>BLOCKED</div></div>	<div>Status: Blocked</div> <div>Agent: 406</div> <div>Server: 406</div> <div>Response size: 0B</div>
<div><div></div><div>(Japan)</div><div>5.253.41.69</div><div>cfgedi.tops.co.th/wpt_prod/WS_Login/fonts/ubuntu/</div></div>	<div><div>SQLI</div><div>BLOCKED</div></div>	<div>Status: Blocked</div> <div>Agent: 406</div> <div>Server: 406</div> <div>Response size: 0B</div>
<div><div></div><div>(Japan)</div><div>5.253.41.69</div><div>cfgedi.tops.co.th/wpt_prod/WS_Login/images/icons/</div></div>	<div><div>SQLI</div><div>BLOCKED</div></div>	<div>Status: Blocked</div> <div>Agent: 406</div> <div>Server: 406</div> <div>Response size: 0B</div>
<div><div></div><div>(Japan)</div><div>5.253.41.69</div><div>cfgedi.tops.co.th/wpt_prod/WS_Login/</div></div>	<div><div>SQLI</div><div>BLOCKED</div></div>	<div>Status: Blocked</div> <div>Agent: 406</div> <div>Server: 406</div> <div>Response size: 0B</div>
<div><div></div><div>(Japan)</div><div>5.253.41.69</div><div>cfgedi.tops.co.th/wpt_prod/default.aspx</div></div>	<div><div>SQLI</div><div>BLOCKED</div></div>	<div>Status: Blocked</div> <div>Agent: 406</div> <div>Server: 406</div> <div>Response size: 0B</div>

