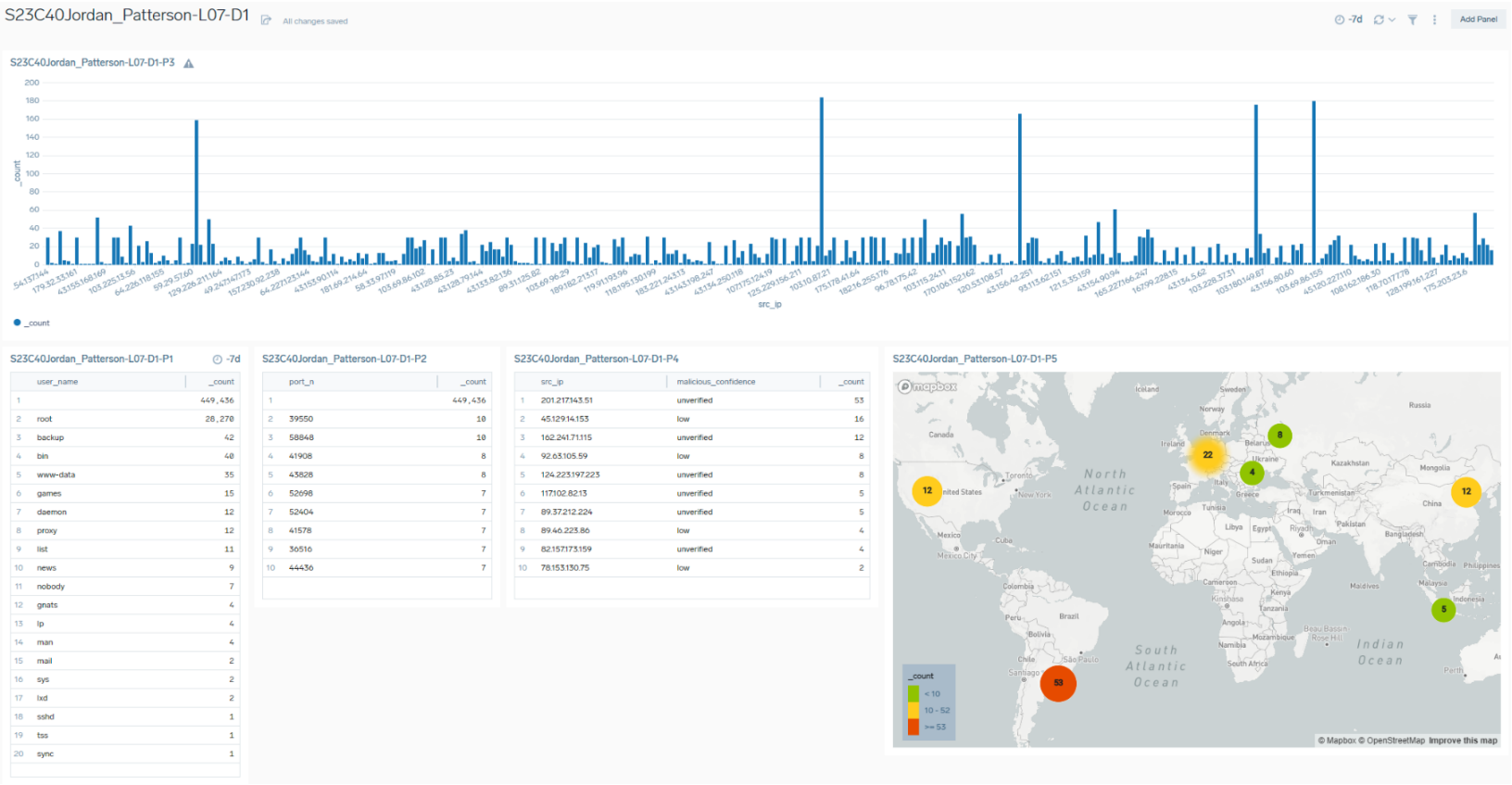
DASHBOARD AND DATA VISUALIZTION IN SUMOLOGIC SIEM

This document demonstrates the queries used to construct a dashboard in Sumologic SIEM to visualize ingested data.

Jordan Patterson

2024

Jordan Patterson 2024
Sumologic Dashboard and Query examples



	user_name	_count
1		449,436
2	root	28,270
3	backup	42
4	bin	40
5	www-data	35
6	games	15
7	daemon	12
8	proxy	12
9	list	11
10	news	9
11	nobody	7
12	gnats	4
13	lp	4
14	man	4
15	mail	2
16	sys	2
17	lxd	2
18	sshd	1
19	tss	1
20	sync	1

	port_n	_count
1		449,436
2	39550	10
3	58848	10
4	41908	8
5	43828	8
6	52698	7
7	52404	7
8	41578	7
9	36516	7
10	44436	7

	src_ip	malicious_confidence	_count
1	201.217.143.51	unverified	53
2	45.129.14.153	low	16
3	162.241.71.115	unverified	12
4	92.63.105.59	low	8
5	124.223.197.223	unverified	8
6	117.102.82.13	unverified	5
7	89.37.212.224	unverified	5
8	89.46.223.86	low	4
9	82.157.173.159	unverified	4
10	78.153.130.75	low	2

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P1: Create a table showing the most common tried usernames (top 20) as Panel-1

((_sourceCategory="Linux/system" and ("invalid user" or "disconnected"))) | parse "* * * * *[*]: Disconnected from authenticating user * * port * [preauth]" as month,date,time,host_name,service,pid,user_name,src_ip,port_n nodrop | count by user_name | top 20 user_name by _count

S23C40Jordan_Patterson-L07-D1-P1 -7d

	user_name	_count
1		449,475
2	root	28,354
3	backup	42
4	bin	40
5	www-data	35
6	games	15
7	daemon	12
8	list	11
9	proxy	11
10	news	9
11	nobody	7
12	gnats	4
13	lp	4
14	man	4
15	mail	2
16	sys	2
17	lxd	2
18	sshd	1
19	tss	1
20	sync	1

P1 Analysis: After analysing the data, it seems that most attempts are made using no username at all. The number 2 most tried username is Root.

P2: Create a table of the most common tried port numbers (top 10) as Panel-2

((_sourceCategory="Linux/system" and ("invalid user" or "disconnected"))) | parse "* * * * *[*]: Disconnected from authenticating user * * port * [preauth]" as month,date,time,host_name,service,pid,user_name,src_ip,port_n nodrop | count by port_n | top 10 port_n by _count

S23C40Jordan_Patterson-L07-D1-P2

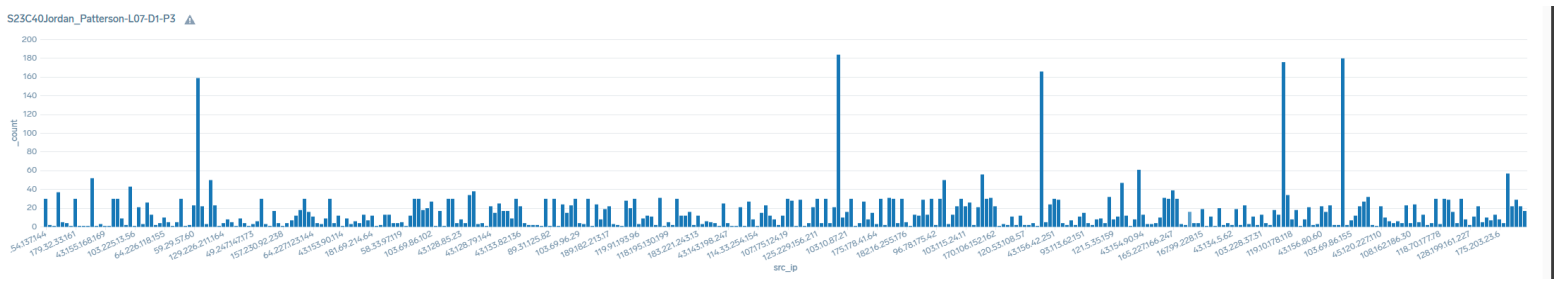
	port_n	_count
1		449,501
2	39550	10
3	58848	10
4	41908	8
5	43828	8
6	52698	7
7	52404	7
8	41578	7
9	36516	7
10	44436	7

P2 Analysis: It seems that the most used port number has no value. The second most used port number is 39550 which is TCP/UDP.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P3: Create a graph to show the number of failed tries per source IP (brute force) as Panel-3

((_sourceCategory="Linux/system" and ("invalid user" or "disconnected"))) | parse "* * * * *[*]: Disconnected from authenticating user * * port * [preauth]" as month,date,time,host_name,service,pid,user_name,src_ip,port_n nodrop | count by src_ip



P3 Analysis: The source IP with the highest number of failed tries is 180.101.88.198 which has 184 failed tries.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P4: Check malicious_confidence of src_ip using "| threatip src_ip" function and "| where !(isNull(malicious_confidence))" condition. Create a table of src_ip and there malicious_confidence level as Panel-4

((_sourceCategory="Linux/system" and ("invalid user" or "disconnected"))) | parse "* * * * *[*]: Disconnected from authenticating user * * port * [preauth]" as month,date,time,host_name,service,pid,user_name,src_ip,port_n nodrop | threatip src_ip | where !(isNull(malicious_confidence)) | count by src_ip,malicious_confidence | sort by _count DESC

S23C40Jordan_Patterson-L07-D1-P4

	src_ip	malicious_confidence	_count
1	201.217.143.51	unverified	53
2	45.129.14.153	low	16
3	162.241.71.115	unverified	12
4	92.63.105.59	low	8
5	124.223.197.223	unverified	8
6	117.102.82.13	unverified	5
7	89.37.212.224	unverified	5
8	89.46.223.86	low	4
9	82.157.173.159	unverified	4
10	78.153.130.75	low	2

P4 Analysis: The malicious confidence of most IP's is still unverified. The verified IP's have a low malicious confidence.

P5: Visualize the location of src_ips by malicious_confidence low or above. Panel-5

((_sourceCategory="Linux/system" and ("invalid user" or "disconnected"))) | parse "* * * * *[*]: Disconnected from authenticating user * * port * [preauth]" as month,date,time,host_name,service,pid,user_name,src_ip,port_n nodrop | threatip src_ip | where !(isNull(malicious_confidence)) | lookup latitude,longitude, country_code, country_name, region, city, postal_code from geo://location on ip=src_ip | count by longitude,latitude,malicious_confidence | sort by _count DESC

S23C40Jordan_Patterson-L07-D1-P5

P5 Analysis: The location with the highest level of malicious attempts is Uruguay with 53 attempts.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

S23C40Jordan_Patterson-L07-D2 All changes saved -7d

Create a template variable +

S23C40Jordan_Patterson-L07-D2-P5

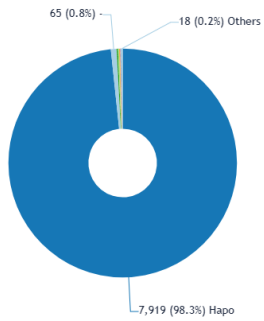
S23C40Jordan_Patterson-L07-D2-P6

	user_agent	_count
1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Bolu	367
2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	162
3	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0	53
4	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 SOC	35
5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0	13
6	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Mobile Safari/537.36	5
7	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	4
8	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	4
9	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)	4
10	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0	3

S23C40Jordan_Patterson-L07-D2-P1

	user_agent	_count
1	Hapo	7,919
2	-	65
3	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0	15
4	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	14
5	raw	6
6	Zach	3
7	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	3
8	Dalvik/2.1.0 (Linux; U; Android 13; SM-F936B Build/TP1A.220624.014)	3
9	Niha	2
10	Baharan	2

S23C40Jordan_Patterson-L07-D2-P2



S23C40Jordan_Patterson-L07-D2-P4

	status_code	user_agent	_count
1	200	Lakshay	656
2	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Bolu	367
3	200	WesleyNS	336
4	200	WesleyNero	275
5	200	jeff	217
6	200	Mia	169
7	200	Hapo	168
8	200	Wesley	165
9	200	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	161
10	200	Yu_Jingyu	124

S23C40Jordan_Patterson-L07-D2-P3

	user_agent	_count
1	-	1
2	yigittttt	3
3	Hapo	6
4	yigit	3

Jordan Patterson 2024
Sumologic Dashboard and Query examples

Browse http://cslab.softether.net:8989/ from your host machine then try to connect to this URL with both default and customized User Agent "your nickname" (user agent spoofing). You can use different browser features to do this or use an assessment tool like Nikto: nikto -h http://cslab.softether.net:8989/ -user-agent "your nickname" then Use this (_source="klj23-03-apache-access") source and write queries to:

P1: Extract different information and create a table view to show different user agents and count each user agent [12h] Panel-1

(_source="klj23-03-apache-access") | parse "* - - [*:*] \"* * *\" * * \"-\" \"*\"" as src_ip,date,time,http_method,http_request,http_version,http_code,length,user_agent | count by user_agent | sort by _count DESC

S23C40Jordan_Patterson-L07-D2-P1 -12h

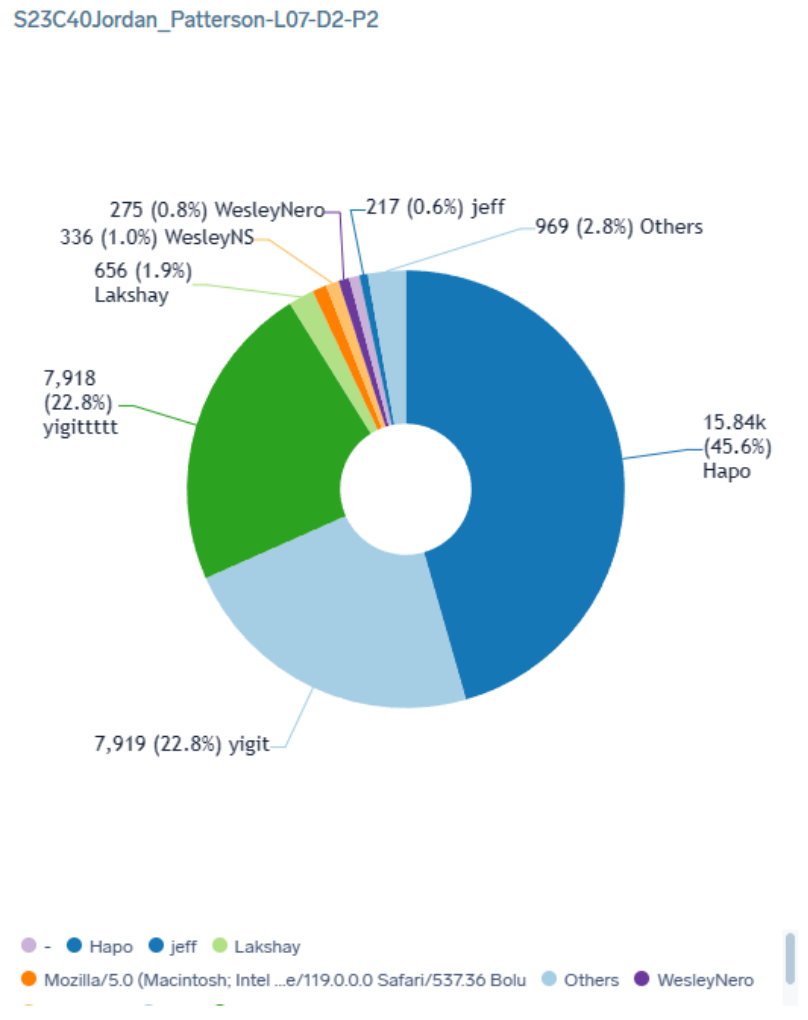
	user_agent	_count
1	Hapo	7,919
2	-	65
3	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0	15
4	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	14
5	raw	6
6	Zach	3
7	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	3
8	Dalvik/2.1.0 (Linux; U; Android 13; SM-F936B Build/TP1A.220624.014)	3
9	Niha	2
10	Baharan	2
11	ummu	2
12	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	2
13	parmi	2
14	Parminder	2
15	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0	2
16	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0	1
17	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Mobile Safari/537.36	1
18	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0	1
19	Mozilla/5.0 (iPhone; CPU iPhone OS 17_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.1.1 Mobile/15E148 Safari/604.1	1
20	Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0	1
21	Hadi	1

P1 Analysis: The user_agent with the highest count is Hapo with 7,919.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P2: Create a graph to visualize this information. Panel-2

Query: (_source="klj23-03-apache-access") | parse "* - - [*:*] \"* * *\" * * \"-\" \"*\"" as src_ip,date,time,http_method,http_request,http_version,http_code,length,user_agent | count by user_agent | sort by _count DESC



P2 Analysis: Hapo Accounts for 45.6% of all attempts.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P3: Use a query to search your custom user agent. Panel-3

(_source="klj23-03-apache-access") | parse "* - - [*:*] \"* * *\" * * \"-\" \"*\"" as src_ip,date,time,http_method,http_request,http_version,status_code,length,user_agent | where user_agent matches "*" | where length <= 400 | count by user_agent

S23C40Jordan_Patterson-L07-D2-P3

	user_agent	_count
1	-	1
2	yigittttt	3
3	Hapo	6
4	yigit	3

P3 Analysis: I could not find my user_agent so I replaced the value with a wildcard.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P4: Write a query to visualize the number of successful accesses per user agent. Panel-4

(_source="klj23-03-apache-access") | parse "* - - [*:*] \"* * *\" * * \"-\" \"*\"" as src_ip,date,time,http_method,http_request,http_version,status_code,length,user_agent | where status_code = "200" | count by status_code,user_agent | sort by _count

S23C40Jordan_Patterson-L07-D2-P4

	status_code	user_agent	_count
1	200	Lakshay	656
2	200	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Bolu	367
3	200	WesleyNS	336
4	200	WesleyNero	275
5	200	jeff	217
6	200	Mia	169
7	200	Hapo	168
8	200	Wesley	165
9	200	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	161
10	200	Yu,Jingyu	124

P4 Analysis: The user_agent with the most successful accesses is Lakshay with 656.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P5: Show source IP locations on a map. Panel-5

(_source="klj23-03-apache-access") | parse "* - - [*:*] \"* * *\" * * \"-\" \"*\"" as src_ip,date,time,http_method,http_request,http_version,status_code,length,user_agent | lookup latitude,longitude, country_code, country_name, region, city, postal_code from geo://location on ip=src_ip | count by longitude,latitude

S23C40Jordan_Patterson-L07-D2-P5

P5 Analysis: 35 thousand attempts are coming from Canadian IP addresses.

Jordan Patterson 2024
Sumologic Dashboard and Query examples

P6: Find your default User Agent and compare it with your browser. Panel-6

(_source="klj23-03-apache-access") | parse "* - - [*:*] \"* * *\" * * \"-\" \"*\"" as src_ip,date,time,http_method,http_request,http_version,status_code,length,user_agent | where user_agent matches "Mozilla*" | count by user_agent | sort by _count

S23C40Jordan_Patterson-L07-D2-P6

	user_agent	_count
1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Bolu	367
2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	162
3	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0	53
4	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 SOC	35
5	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Edg/119.0.0.0	13
6	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Mobile Safari/537.36	5
7	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36	4
8	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	4
9	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)	4
10	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0	3

P6 Analysis: Most attempts come from Firefox, Safari, or Chrome browsers. The most common OS used is Windows followed by MacOS and then Linux.