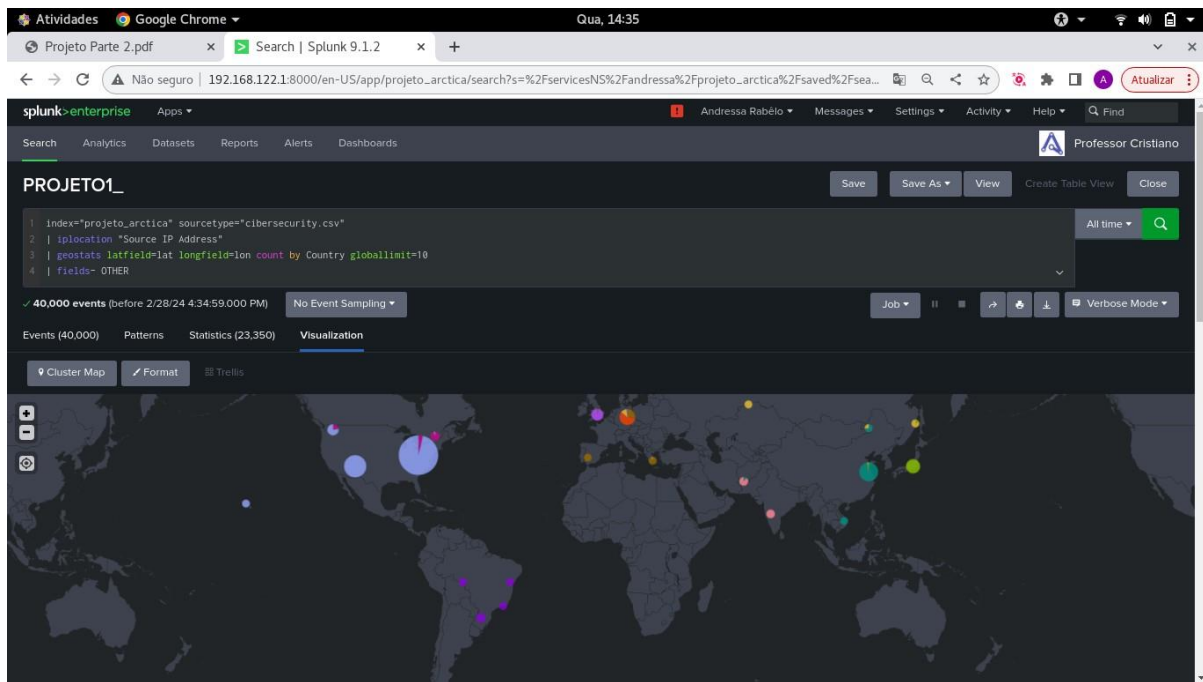




Andressa Emily Rabêlo Pereira
Dayane Francisca de Oliveira Vaz

PROJETO ARCTICA



Atividade 1:

- `| iplocation "Source IP Address"`
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- `| geostats latfield=lat longfield=lon count by "Country" globallimit=10`
 - Comando para gerar estatísticas geográficas (como latitude e longitude por exemplo) e gerar um resumo em mapa.
 - Foi utilizado para gerar um mapa com contagem por País;
 - Para limitar o número total dos resultados;
- `| fields- OTHER`
 - Utilizamos esse comando, junto ao operador aritmético (-) para retirar os falsos positivos da pesquisa;
 - Campo vazio.

Atividades Google Chrome Qua, 14:35

Projeto Parte 2.pdf Search | Splunk 9.1.2

Não seguro | 192.168.122.1:8000/en-US/app/projeto_arctica/search?s=%2FservicesNS%2Fandressa%2Fprojeto_arctica%2Fsaved%2Fsea... Atualizar

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards Professor Cristiano

PROJETO2_ Save Save As View Create Table View Close

```
1 index="projeto_arctica" sourcetype="cibersecurity.csv"
2 | iplocation "Source IP Address"
3 | top limit=10 "Country" showperc=false
4 | fields- OTHER
```

All time

40,000 events (before 2/28/24 4:35:40.000 PM) No Event Sampling Job II View Download Verbose Mode

Events (40,000) Patterns Statistics (10) Visualization

20 Per Page Format Preview

Country	count
United States	16312
China	3768
Japan	2184
Germany	1682
United Kingdom	1446
South Korea	1211
Brazil	979
France	891
Canada	841
Australia	615

Atividade 2:

- | iplocation "Source IP Address"
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- | top limit=10 "Country" showperc=false
 - Foi utilizado o comando | top limit=10 para mostrar (como um ranking, por exemplo) os 10 países que mais lançaram ataques;
 - Para retirar as porcentagem (que aparecem quando utilizamos o comando | top;
- | fields- OTHER
 - Utilizamos esse comando, junto ao operador aritmético (-) para retirar os falsos positivos da pesquisa.
 - Campo vazio;

The screenshot shows the Splunk Enterprise interface. The search bar contains 'token3_PROJETO'. The search results show 10 results (before 2/28/24 4:36:13.000 PM). The search is using the 'inputlookup token3_projeto.csv' command. The search results are displayed in a table view with the following data:

Country	count
United States	16312
China	3768
Japan	2184
Germany	1602
United Kingdom	1446
South Korea	1211
Brazil	979
France	891
Canada	841
Australia	615

Atividade 3:

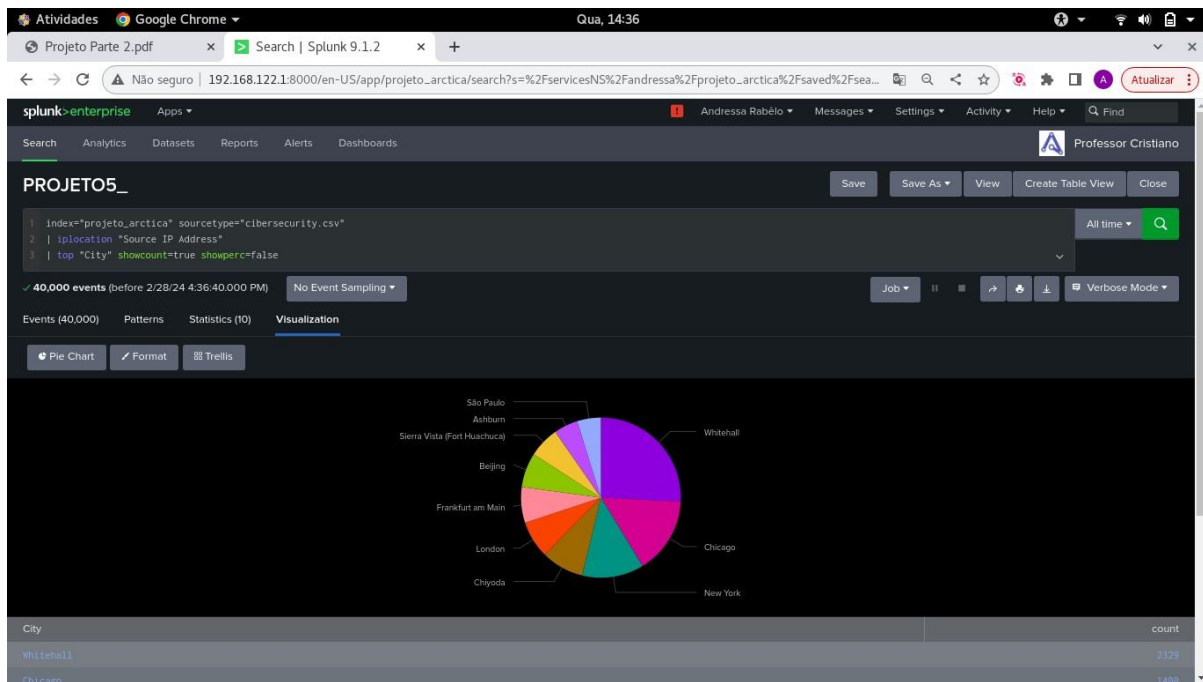
Criação da lookup (outputlookup):

- Foi utilizado a mesma pesquisa da 2 (segue abaixo), mas com a adição do comando `| outputlookup`

```
index="projeto_arctica" sourcetype="cibersecurity.csv"
| iplocation "Source IP Address"
| top limit=10 "Country" showperc=false
| outputlookup token3_projeto.csv
```

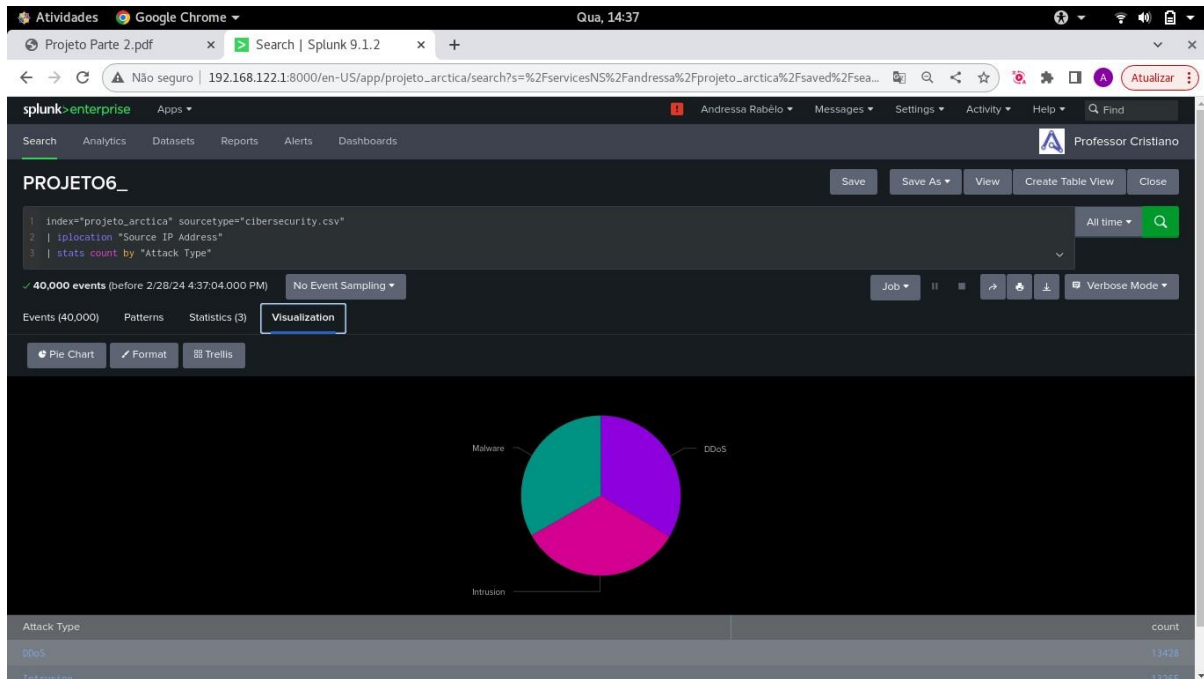
Chamar a lookup (inputlookup):

- `| inputlookup token3_projeto.csv`
 - Tal pesquisa, foi utilizada para difundir o token em todos os gráficos.



Atividade 5:

- | iplocation "Source IP Address"
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- | top limit=10 "City" showcount= false showperc=false
 - Foi utilizado o comando | top limit=10 para mostrar (como um ranking, por exemplo) as 10 cidades que mais lançaram ataques;
 - Para retirar a contagem (que aparece quando utilizamos o comando | top;
 - Para retirar as porcentagem (que aparecem quando utilizamos o comando | top;



Atividade 6:

- | iplocation "Source IP Address"
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- | stats count by "Attack Type"
 - Comando para mostrar a estatística de contagem por Tipo de ataque;

The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `1 index="projeto_arctica" sourcetype="cibersecurity.csv"`
`2 | iplocation "Source IP Address"`
`3 | stats count by "Attack Type"`
The results show 40,000 events. The table below displays the attack types and their counts:

Attack Type	count
DDoS	13428
Intrusion	12265
Malware	13307

Token “Tipos de ataques” (ATIVIDADE 7):

- `| iplocation "Source IP Address"`
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- `| stats count by "Attack Type"`
 - Comando para mostrar a estatística de contagem por Tipo de ataque;

The screenshot shows the Splunk Search interface. The search bar contains the query: `1 | index="projeto_arctica" sourcetype="cibersecurity.csv"`
`2 | iplocation "Source IP Address"`
`3 | dedup "City"`
`4 | stats count by "City"`

The results show 6,906 events. The table view displays the following data:

City	count
Taguig	1
's-her:gentoscor	1
6th of October City	1
A Coruña	1
Aachen (Mite)	1
Aslborg	1
Aslsmet	1
Aarpi	1
Aarhus (Aarhus C)	1
Abakan	1
Abbotsford	1
Abcova	1

Token “Cidades” (ATIVIDADE 7):

- | iplocation “Source IP Address”
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- | dedup "City"
- Comando usado para retirar os valores duplicados, nesse caso, o nome das Cidades;
- | stats count by "City"
 - Comando para mostrar a estatística de contagem por Cidades;

The screenshot shows the Splunk Enterprise interface. The search bar contains the following query:

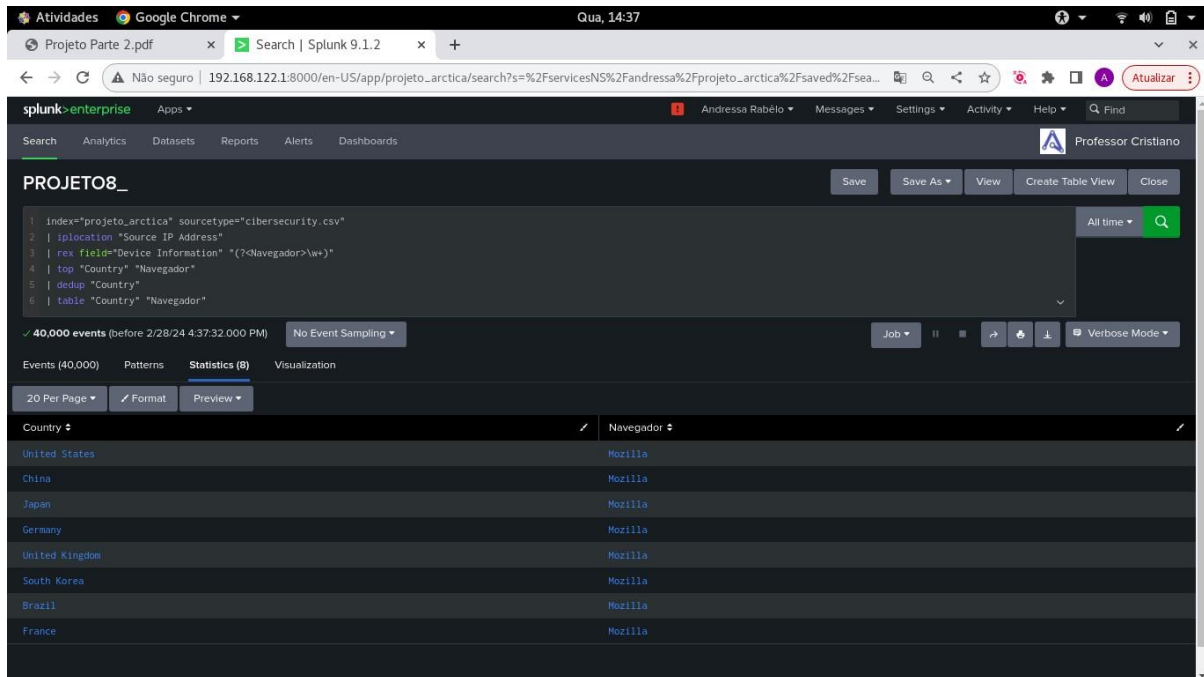
```
1 index="projeto_arctica" sourcetype="cibersecurity.csv"
2 | iplocation "Source IP Address"
3 | dedup "User Information"
4 | stats count by "User Information"
```

The results show 32,389 events. The 'Statistics (32,389)' tab is selected, displaying a table with the following data:

User Information	count
Asina Ahluwalia	1
Asina Arya	1
Asina Babu	1
Asina Bahl	1
Asina Bahri	1
Asina Bakshi	1
Asina Bai	1
Asina Bala	1
Asina Balan	1
Asina Balasubramanian	1
Asina Banal	1

Token “Usuários” (ATIVIDADE 7):

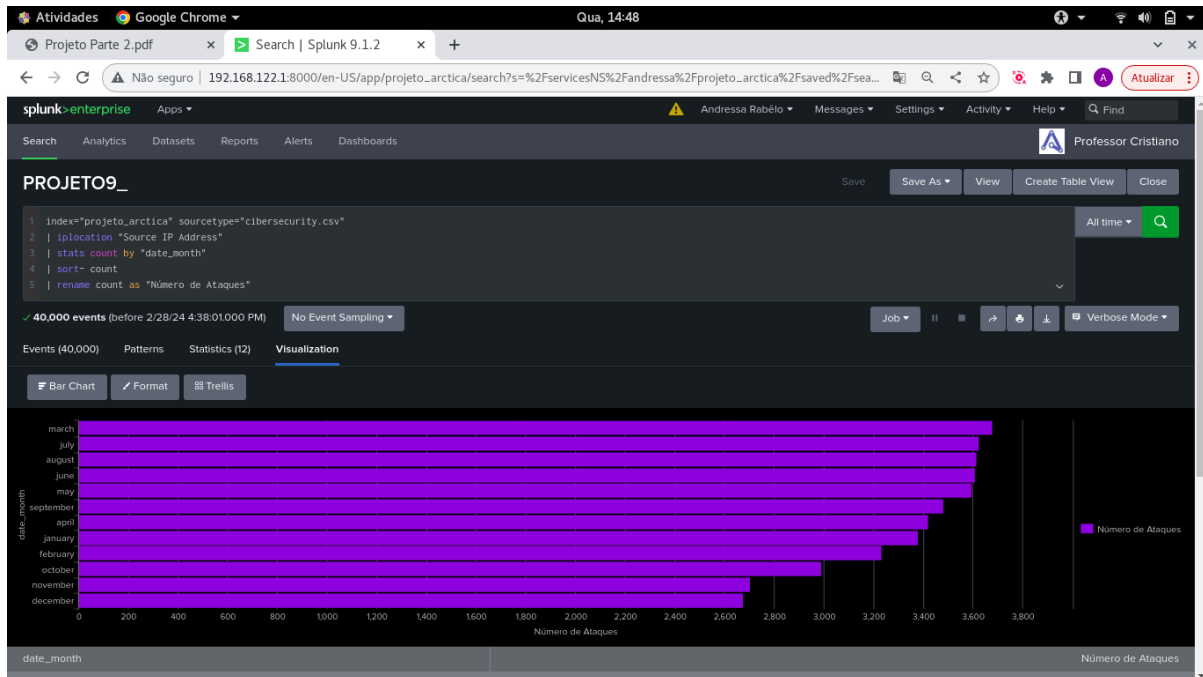
- | iplocation “Source IP Address”
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- | dedup "User Information"
- Comando usado para retirar os valores duplicados, nesse caso, o nome dos usuários;
- | stats count by "User Information"
 - Comando para mostrar a estatística de contagem por Usuário;



Atividade 8:

- `| iplocation "Source IP Address"`
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- `| rex field="Device Information" "(?<Navegador>\w+)"`
 - O comando `| rex field=` é usado para extrair campos, nesse caso retirar apenas o nome do navegador;
 - Nome do campo de onde a informação será extraída;
 - Expressão para extrair apenas a primeira parte dos dados, parte essa onde está o navegador. Nesse processo foi criado o campo "Navegador", onde ficam armazenados os navegadores.
- `| top "Country" "Navegador"`
 - Foi utilizado o comando `| top` para mostrar (como um ranking, por exemplo) os países que mais lançaram ataques e seus navegadores;

- | dedup "Country"
 - Comando usado para retirar os valores duplicados, nesse caso, o nome dos países;
- | table "Country" "Navegador"
 - O comando | table foi usado apenas para criar uma tabela com os campos acima descritos;
 - Nome dos campos utilizados para a criação da tabela;



Atividade 9:

- `| iplocation "Source IP Address"`
 - Utilizamos esse comando para extrair informações de localização através do IP
 - Nome do campo onde os IPs de lançamento estavam armazenados;
- `| stats count by "date_month"`
 - Comando para mostrar a estatística de contagem por Mês;
- `| sort- count`
 - O comando `| sort` é usado para ordenar, seguido do operador aritmético (-) ele ordena os países de acordo com a ordem decrescente das suas contagens;
 - Campo que será ordenado;
- `| rename count as "Número de Ataques"`
 - Esse comando foi usado para renomear um campo, no caso o "count".
 - Campo renomeado;
 - Novo nome;

Atividades Google Chrome Qua, 20:33

Dashboards | Splunk 9.1.2 x PROJETO_FINAL_2 | Splunk x Meet: urg-omrd-bjm x +

Não seguro | 192.168.122.1:8000/en-US/app/projeto_arctica/projeto-final3/edit

splunk enterprise Apps Andressa Rabêlo Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Gridlines 76% Dark View Save

PROJETO_FINAL_2

Enter dashboard description.

Global Time Range All time TOP 10 Pais All Pais: Default Text

Cibersecurity

Country	Navegador
United States	Mozilla
China	Mozilla
Japan	Mozilla
Germany	Mozilla
United Kingdom	Mozilla
South Korea	Mozilla
Brazil	Mozilla
France	Mozilla

World map visualization showing data points across various countries.

Horizontal bar chart showing data for various countries.

Configuration

On click Link to dashboard

Select an App Professor Cristiano

Select a Dashboard PROJETO_FINAL_1

Owner: andressa Global

View Dashboard

☒ Open in new tab

Set Tokens

Token Name Token Value

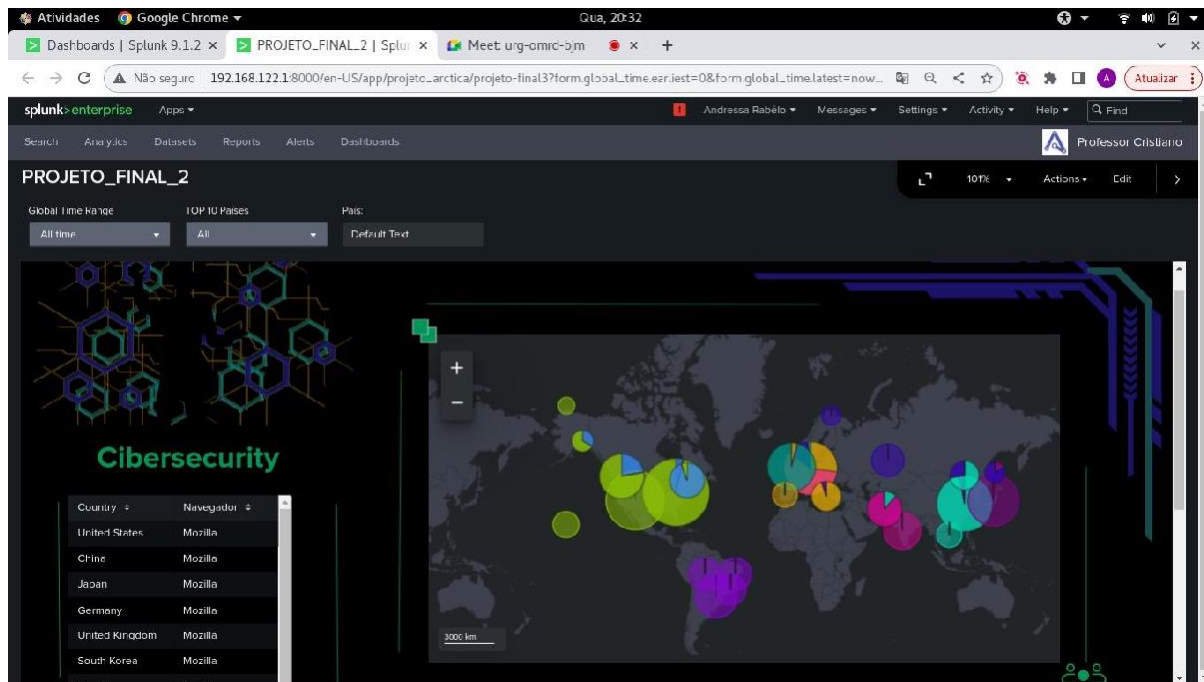
Enter a name = Enter a value

+ Add token

Use tokens to set values in the target dashboard. For example: host = row.hostvalue Learn more

Cancel Apply

- Drilldown para ligar os dois dashboards;



- No segundo dashboard temos os gráficos das atividades: 1, 2, e 8;
- 1 filtro em dropdown, filtrando todos os gráficos (TOP 10 Países);
- 1 filtro de texto para todos os gráficos (Países);
- 1 link via drilldown, conectando os 2 dashboards.

TOP 10 País...

P...

City

Ataqu...

Usuár...

Global Time Ran...

All

Default Text

All

All

All

All time

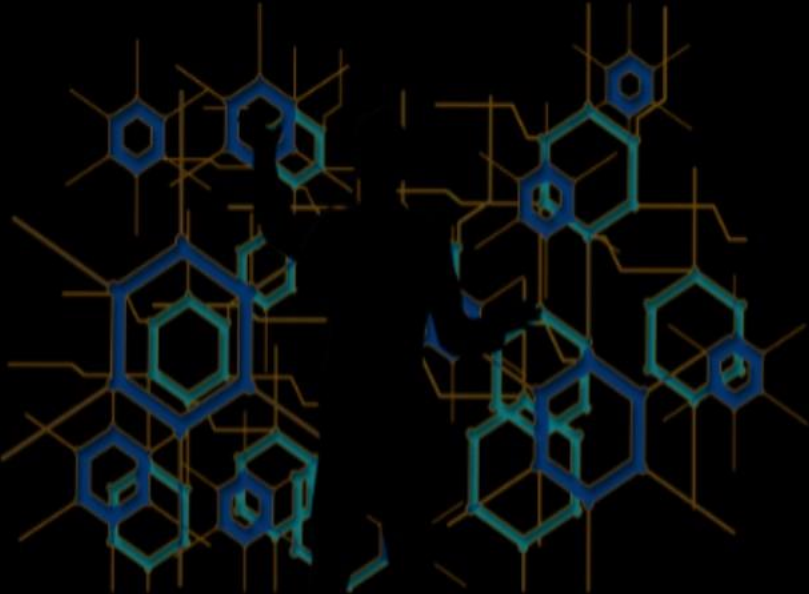
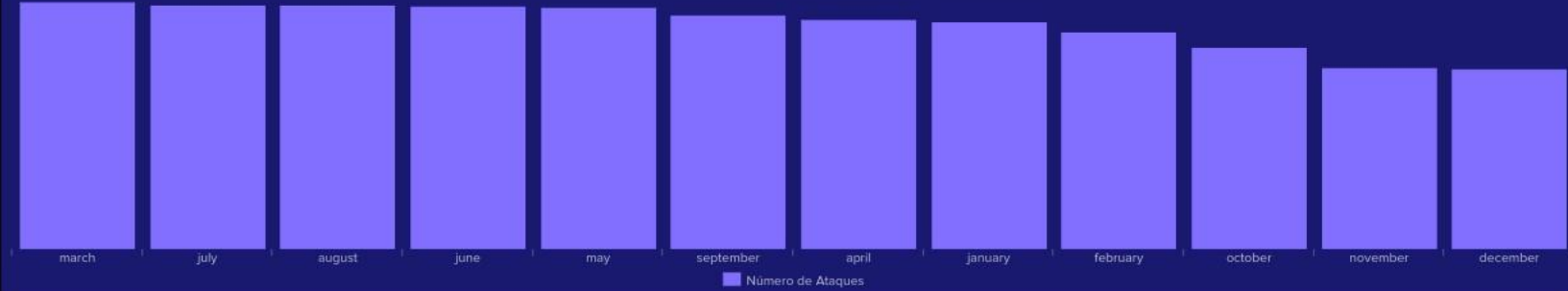
Cidades que mals lançaram ataques:



Attack	Device	Log	User	Protoc...	Severity	Traffic	Action	Ci...	Count...
Malware	Opera/9.79.(Windows NT 5.1; el-CY) Presto/2.9.166 Version/11.00	Firewall	Anaya Sangha	TCP	Medium	HTTP	Blocked	Glasgow	United Kingdom
Intrusion	Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/535.0 (KHTML, like Gecko) CriOS/15.0.821.0 Mobile/30N406 Safari/535.0	Server	Kiaan Samra	ICMP	Medium	DNS	Ignored	Chicago	United States
Malware	Mozilla/5.0 (iPod; U; CPU iPhone OS 4_2 like	Server	Nitara Mammen	TCP	High	FTP	Blocked	Tyler	United States

<Prev12345...Next>

CIBERSECURITY



Global Time Ran...

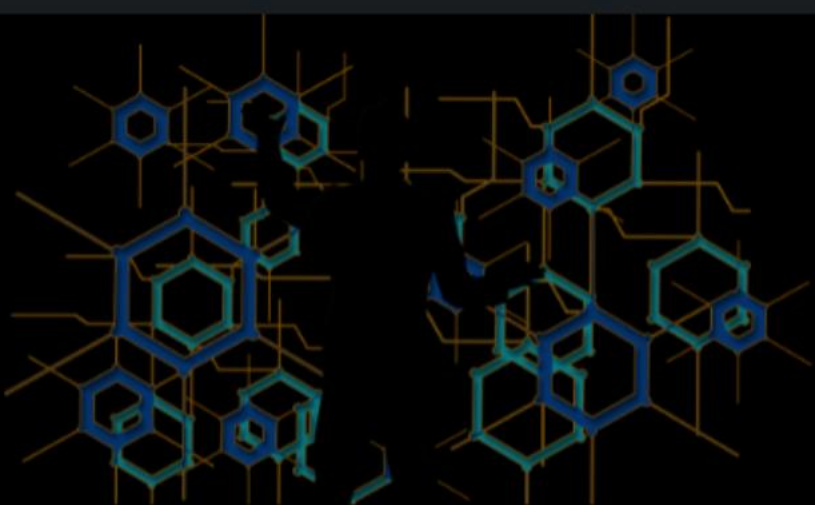
TOP 10 País...

Pa...

All time

All

Default Text



Cibersecurity

Count...	Navegad...
United States	Mozilla
China	Mozilla
Japan	Mozilla
Germany	Mozilla
United Kingdom	Mozilla
South Korea	Mozilla
Brazil	Mozilla
France	Mozilla

