



**CYBER STRUGGLE
TASK- STAY ALERT, STAY ALIVE**

**Hazırlayan:
DCS001 Hakan ŞEN
Ekim 2023
Ankara**

Dear Security Team,

URGENT : Immediate Action Required - Port Scan Alert

Our security systems have detected port scans, indicating potential intrusion attempts on our network. We must act swiftly to assess the situation.

Your task is to use our SIEM solution, Splunk, to identify and document any port scans involving more than 20 ports within a 5-minute timeframe. Time is of the essence, and we need to understand the extent of this threat promptly.

Also explain what log sources can be used to collect port traffic logs for further collection of logs? How can we distinguish normal port traffic from port scan ?

Thank you for your immediate attention and dedication to our security.

Stay vigilant and proactive.

Best regards,

Jennifer Lee

Senior Security Analyst

Bravo Solutions Ltd.

Note: Use the index "network".

Öncelikle port taramasını Vertical ve Horizontal olarak ikiye ayırabiliriz.

Vertical Port Scan = bir ip tek bir sistem üzerinde birçok porta tarama yapabilir.

Horizontal Port Scan = bir ip birden çok sistemi tek bir port için tarayabilir.

Task'tan anlaşıldığı üzere 20 üzerinde port taraması içeriği istendiğinden vertical port scan'e yönelik olarak bir araştırma yapmamız gerektiği değerlendirilmiştir.

```
index="network" source="cisco_firewall.cef" | bin _time span=5m | stats dc(dpt) as dc_dest_port by src, dst
| where dc_dest_port > 20
```

New Search

Save As Create Table View Close

index="network" source="cisco_firewall.cef" | bin _time span=5m | stats dc(dpt) as dc_dest_port by src, dst
| where dc_dest_port > 20

246,788 events (before 10/30/23 9:12:43.000 PM) No Event Sampling

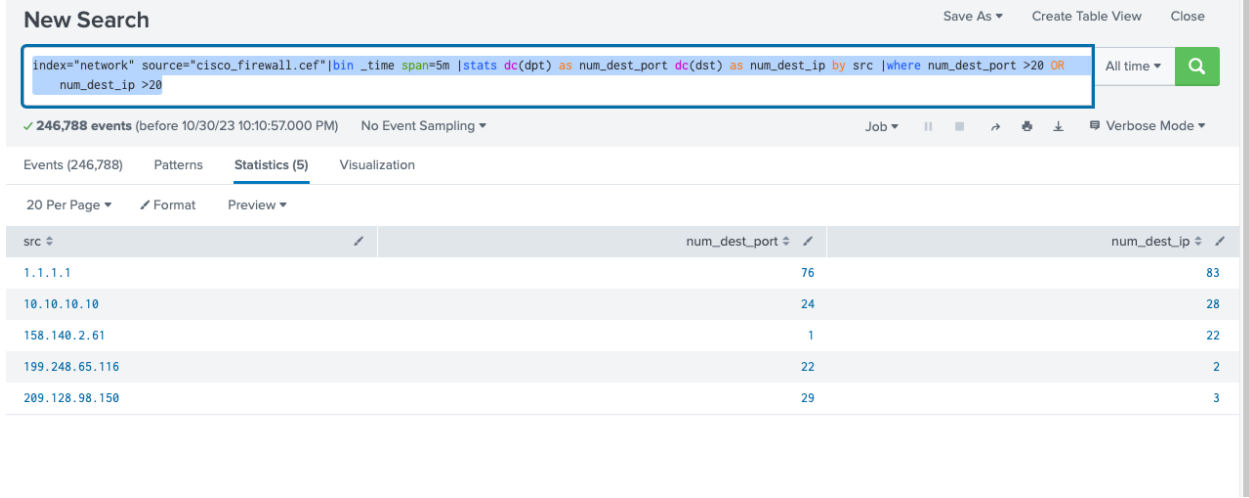
Events (246,788) Patterns Statistics (2) Visualization

20 Per Page Format Preview

| src | dst | dc_dest_port |
|----------------|---------------|--------------|
| 1.1.1.1 | 78.187.171.46 | 61 |
| 199.248.65.116 | 65.85.126.55 | 21 |

Aslında iki yöntemide tek bir yerde toplayarak port veya network taramasını aşağıdaki sorgu ile kontrol edilmesinde fayda olacağını değerlendiriyorum.

```
index="network" source="cisco_firewall.cef"|bin _time span=5m |stats dc(dpt) as num_dest_port dc(dst) as num_dest_ip by src |where num_dest_port >20 OR num_dest_ip >20
```



The screenshot shows a Splunk search interface. At the top, there's a 'New Search' header with options to 'Save As', 'Create Table View', and 'Close'. Below this is a search bar containing the query: `index="network" source="cisco_firewall.cef"|bin _time span=5m |stats dc(dpt) as num_dest_port dc(dst) as num_dest_ip by src |where num_dest_port >20 OR num_dest_ip >20`. To the right of the search bar is a 'All time' filter and a search icon. Below the search bar, it indicates '246,788 events (before 10/30/23 10:10:57.000 PM)' and 'No Event Sampling'. The interface has tabs for 'Events (246,788)', 'Patterns', 'Statistics (5)', and 'Visualization'. The 'Statistics (5)' tab is active, showing a table with 20 rows per page. The table has three columns: 'src', 'num_dest_port', and 'num_dest_ip'. The data is as follows:

| src | num_dest_port | num_dest_ip |
|----------------|---------------|-------------|
| 1.1.1.1 | 76 | 83 |
| 10.10.10.10 | 24 | 28 |
| 158.140.2.61 | 1 | 22 |
| 199.248.65.116 | 22 | 2 |
| 209.128.98.150 | 29 | 3 |

Port taramasına yönelik olarak ip ve port bilgisini tutan firewall, IPS veya IDS, Switch, Router, Proxy Serverları, Uygulama Logları kullanılabilir.

Port taramasını normal trafikten ayırmak için;

Tarifiğin paternlerine bakılabilir, Örnek normal bir trafik düzenli ve beklenen bir iletişim sahipken port taramasında hızlı ve değişik portlara beklenmedik istekler gidecektir.

Başarı sayısına bakılabilir, örnek olarak normal trafik genellikle başarılı bağlantı kurarken port taramasında başarısız bağlantılar dikkat çekecektir.

TCP Flagları dikkat çeker. Normal bağlantı düz bir şekilde 3 way handshake'i tamamlarken port taraması sadece SYN gönderebilir.

Bilinen servislere ulaşım sayısına bakılabilir. Örnek normal bir trafikte bilinen servisler arasında iletişim varken port taramasında bilinen servislerin dışına da bir istek bulunacaktır.