****

**CYBER STRUGGLE**

**TASK – Playing With Fire**

**Hazırlayan:**

**DCS001 Hakan ŞEN**

**Ekim 2023**

**Ankara**

İÇİNDEKİLER

[STORYLINE 3](#_Toc148656773)

[Task1: The objective is to focus on finding every destination and the request URL belongs to every source. 3](#_Toc148656774)

[Task2: She needs to detect any instances of uncommon ports being accessed externally or internally, which could indicate unauthorized services or applications running on the network. 4](#_Toc148656775)

[Task3: Detecting traffic originating from or going to specific countries that are not relevant to the company’s business operations. This can help prevent connections from potentially malicious locations. 5](#_Toc148656776)

# **STORYLINE**

In the headquarters of a global banking corporation, Jane Mitchell, a seasoned security analyst, has been tasked with the critical responsibility of analyzing firewall events within Splunk, the company's chosen Security Information and Event Management (SIEM) tool, while utilizing Cisco as the firewall product. Splunk’s web service is hosted in default port. Her responsibility is writing Splunk queries to identify some suspicious situations as below.

# **Task1: The objective is to focus on finding every destination and the request URL belongs to every source.**

Öncelikli olarak metin üzerinden Jane Mitchell’ın sadece Cisco firewall loğları üzerinde inceleme yapacağı değerlendirilmiştir. Bu nedenle source type olarak cisco firewall seçilmiştir.

Her source için destination ve istek URL’i içeren query aşağıda verildiği gibidir.

|  |
| --- |
| index="network" source="cisco\_firewall.cef"| stats count by src,dst,request |sort - count |

A screenshot of a computer

Description automatically generated

Şekil 1 Screenshot

Sorgunun içeriği;

* index="network" sadece network indeksindeki verileri içereceğini belirtir.
* Source = “cisco\_firewall.cef” aramanın sadece cisco\_firewall.cef adlı log dosyasından (kaynaktan) gelen verileri göstereceğini belirtir.
* | stats count by src,dst,request source, destination ve request alanlarına göre istatistiksel bilgileri hesaplamak için kullanılır. Yani sadece her bir kaynak, hedef ve istek kombinasyonu için kaç tane log girişi olduğunu sayar.
* ­| sort – count elde edilen istatistikleri count alanuna göre azalan sırayla sıralar, - işareti azalan sıralama anlamına gelir.

Toplamda 45 adet benzersiz src,dst ve request kombinasyonu bulunmuştur.

Çıkan sonuçlarda url encoded olduğu düşünülen “/%69%6E%64%78%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E” değeri decode edildiğinde “/indx.....................................................” değeri elde edilmiştir. İleriki aşamalar için not edilmiştir.

Ayrıca soruda esas olarak her source için tüm destinationlar ve ayrıca url bilgileri isteniyorsa ;

Ek bir query olarak yukarıdaki sorguya request eklenmeden ve ayrıca daha anlamlı olması açısından source port ve destination port eklenerek aşağıda verilen sorgu eklenebilir.

|  |
| --- |
| index="network" source="cisco\_firewall.cef"| stats count by src,dst,spt,dpt |sort - count |

# **Task2: She needs to detect any instances of uncommon ports being accessed externally or internally, which could indicate unauthorized services or applications running on the network.**

0-1024 numaralı portlar well-known portlar olarak bilinmektedir. Bu nedenle bunların dışında kalan portlar uncommon ports olarak değerlendirilmiştir.

Burada erişim için kullanılan destination portlara bakacağız.

|  |
| --- |
| index="network" source="cisco\_firewall.cef" dpt>1024 |stats count by src,dst,dpt |sort - count |

Sorgunun içeriği olarak;

* index="network" source="cisco\_firewall.cef" : Bir önceki sorudaki gibi index ve source aynı seçilmiştir.
* dpt>1024 : destination portu 1024’ten küçük olan portlar arama dışında bırakılmıştır.
* stats count by src,dst,dpt: istatistiksel olarak dizinin sayısını bulmak için,
* |sort – count: count değerinin azalan olarak sıralamak için kullanılmıştır.

A screenshot of a computer

Description automatically generated

Şekil 2 Screenshot

10.0.112.9 ip adresinden 199.248.65.116 ip adresi 3562 portuna 2024 defa istekte bulunduğu şüphe çekmiştir.

# **Task3: Detecting traffic originating from or going to specific countries that are not relevant to the company’s business operations. This can help prevent connections from potentially malicious locations.**

In this situation, Jane is uncertain about the malicious locations. She reaches out to her colleague, that’s you, to help identify them. You inform her about the countries deemed malicious. Later, she discovers that the logs lack country information. As her experienced colleague, you explain that Splunk has the ability to determine locations from IP addresses. While it's not always accurate, she must locate instances where it successfully identified locations.

Destination için query;

|  |
| --- |
| index="network" source="cisco\_firewall.cef" | iplocation dst | stats count by dst,Country | sort - count |

A screenshot of a computer

Description automatically generated

Source için query;

|  |
| --- |
| index="network" source="cisco\_firewall.cef" | iplocation src | stats count by src,Country | sort - count |

A screenshot of a computer

Description automatically generated

Sorguların açıklaması diğer sorgularda açıklandan farklı olarak ;

* İplocations src veya dst : src veya dst field’ının coğrafi konum bilgilerini almak için kullanılır.

Şirketimizin Çin ile herhangi bir iletişimi olmadığını ve zararlı olarak değerlendirelim, bu durumda Çin’e giden ve gelen trafik bilgileri sorguları aşağıdaki şekilde yapılabilir.

|  |
| --- |
| index="network" source="cisco\_firewall.cef" | iplocation dst | stats count by dst,Country | where Country="China" |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| index="network" source="cisco\_firewall.cef" | iplocation src | stats count by src,Country | where Country="China" |

A screenshot of a computer

Description automatically generated