**Sigma2Splunk**

**1. Nedir?**  
Sigma2Splunk, **Sigma kurallarını Splunk arama sorgularına (SPL)** çeviren bir araçtır.  
Sigma: farklı sistemlerde kullanılabilen **genel saldırı tespit kuralları dilidir**.  
Splunk: log verilerini analiz etmeye yarayan popüler bir güvenlik ve SIEM platformudur.

Kısaca:  
- “Sigma kuralım var”  
- “Splunk'ta nasıl kullanırım?”  
- Cevap: Sigma2Splunk ile çevirerek.



**2. Ne İşe Yarar?**

* Sigma kuralları, saldırıları tanımlamak için evrensel yazılmış kurallardır.
* Ancak her güvenlik aracı bu kuralları doğrudan anlayamaz.
* **Splunk**, kendi dilini (SPL) kullanır.
* Sigma2Splunk, bu kuralları **Splunk için anlaşılır hale getirir**.

➡️ Sonuç: Sigma kuralını alırsın, birkaç saniyede Splunk’a özel hale getirirsin.

**3. Neden Önemlidir?**

* Güvenlik analistleri genellikle topluluklardan hazır Sigma kuralları alır.
* Eğer sistemde Splunk kullanılıyorsa, bu kurallar çalışmaz.
* Sigma2Splunk sayesinde manuel çeviri yapmana gerek kalmaz.
* **Hızlı ve doğru tehdit tespiti** için çok faydalıdır.

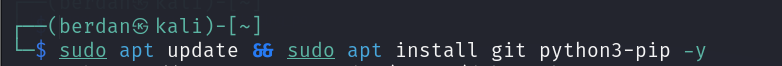
Red Team saldırılarını tanımlamak, Blue Team için savunma kuralları oluşturmak kolaylaşır.

**4. Nasıl Kurulur? (Linux Örneği)**

Sigma2Splunk, Python ile çalışır. Kurulumu oldukça basittir:

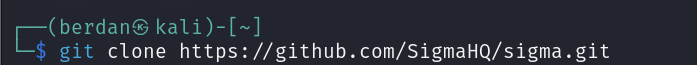
**# 1. Python ve Git kurulu olmalı**

**sudo apt update && sudo apt install git python3-pip –y**

****

**# 2. Sigma kütüphanesini klonla**

**git clone** [**https://github.com/SigmaHQ/sigma.git**](https://github.com/SigmaHQ/sigma.git)

****

**cd sigma/tools**

****

**# 3. Gerekli Python paketlerini yükle**

**pip3 install -r requirements.txt**

****

**# 4. Sigma2Splunk çevirisi için komut**

**python3 sigmac -t splunk <kural\_dosyası.yml>**

****

Not: **<kural\_dosyası.yml>** yerine çevirmek istediğin Sigma kural dosyasını yazarsın. Örnek: **windows\_failed\_login.yml**

**5. Örnek Bir Anlatım:**  
Elinde şöyle bir Sigma kuralı var:

**title: Failed Logon Attempts**

**logsource:**

**product: windows**

**detection:**

**selection:**

**EventID: 4625**

**condition: selection**

Bu, “Windows’ta başarısız oturum açma girişimi” kuralıdır. Şimdi bunu Splunk’a çevirmek istiyorsun:

**python3 sigmac -t splunk windows\_failed\_login.yml**

Çıktı olarak şu SPL sorgusunu alırsın:

**(index=windows) EventCode=4625**

Artık bu sorguyu doğrudan Splunk’a yapıştırıp tehditleri izleyebilirsin!

**Uyarı:**  
Sigma2Splunk bir çeviri aracıdır. Kuralların içeriği ne kadar doğru yazılırsa, çıkan SPL sorgusu da o kadar anlamlı olur. Otomatik çeviriden sonra sorguyu gözden geçirmek her zaman iyi bir fikirdir.