**Sigma Nedir?**

Sigma, siber güvenlik dünyasında kullanılan açık kaynaklı bir kural yazma dilidir. Özellikle log (kayıt) dosyalarını analiz etmek ve şüpheli aktiviteleri tespit etmek için kullanılır.

Basitçe anlatmak gerekirse:

Sigma, sistemlerdeki olayları anlatan log dosyalarını okur ve "şüpheli bir şey olmuş mu?" diye kontrol etmek için kurallar uygular.

Velociraptor, Arkime gibi araçlar log veya trafik toplar. Sigma ise bu log’ların içinden anlamlı ve tehlikeli şeyleri bulmaya yardımcı olur.

**Sigma Ne İşe Yarar?**

Güvenlik olaylarını otomatik tespit etmek

Windows, Linux, firewall, antivirüs gibi sistemlerden gelen logları analiz etmek

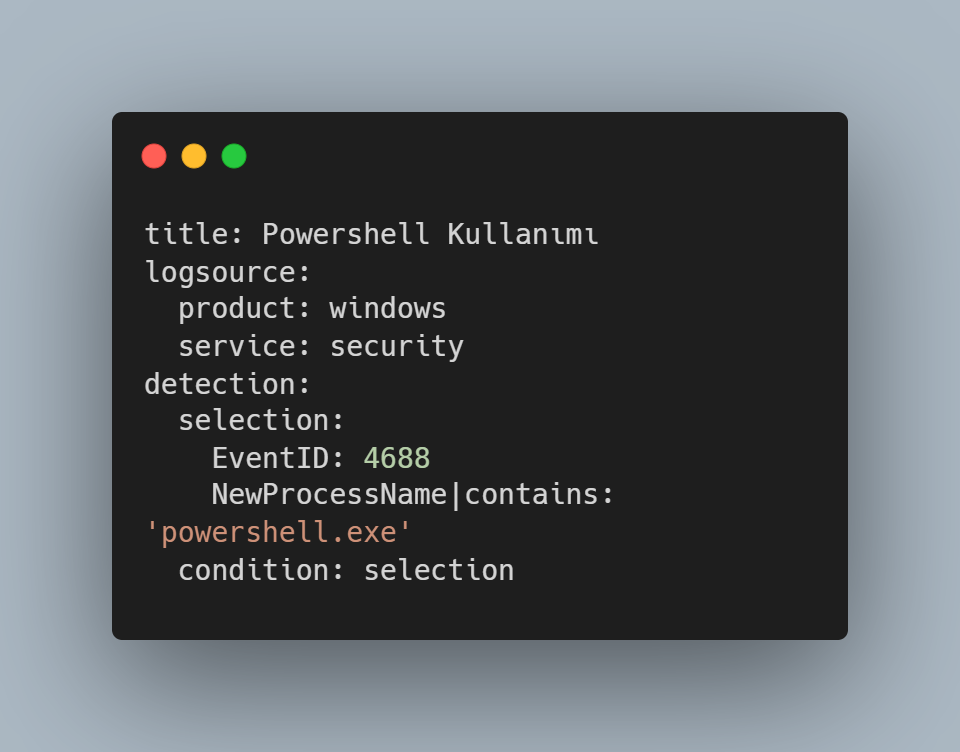
Log içinde şüpheli davranışları belirlemek (örneğin: Powershell ile şifre çalma denemesi)

Güvenlik olaylarını SIEM (Log yönetim sistemleri) ile uyumlu hale getirmek

Hızlı tehdit avı (threat hunting) yapmak

**Sigma Kuralına Örnek**

Aşağıdaki kural, Windows loglarında Powershell kullanımı olup olmadığını kontrol eder:



Bu kural şunu der:

Eğer Windows'ta bir kullanıcı powershell.exe çalıştırdıysa, bu olayı bana bildir.

**Sigma Kurulumu ve Kullanımı (Komut Satırı ile)**

Sigma'nın kendisi aslında bir Python projesidir. Kurulumu ve kullanımı oldukça basittir.

***git clone https://github.com/SigmaHQ/sigma.git***

***cd sigma***

Gerekli Paketleri Yükleme: ***pip install -r requirements.txt***

**Kuralları Birleştirme veya Dönüştürme**

Sigma kuralları, farklı güvenlik araçlarına çevrilebilir (Splunk, Elastic, Qradar vs.)

**Sigma kuralını Elastic araması haline getirme:**

***python3 tools/sigmac -t es-qs rules/windows/powershell/powershell\_start.yml***

Çıktı: ***event.code:4688 AND process.name:\*powershell.exe\****

Yani Elastic gibi sistemlere doğrudan aktarılabilir hale gelir.

**Sigma’nın Avantajları**

* Açık kaynak ve tamamen ücretsiz
* Evrensel kural formatı
* Her sistem için yeniden kural yazmak gerekmez
* Diğer güvenlik araçlarıyla uyumludur (Elastic, Splunk, Sentinel)

**Dikkat Edilmesi Gerekenler:**

* Tek başına çalışmaz, log’lara ihtiyaç duyar
* Kural yazımı için biraz YAML bilgisi gerekir
* Türkçe destek veya arayüz yok