Chainsaw Aracı - Eğitim Materyali

# 🧠 Chainsaw Nedir?

Chainsaw, olay günlüklerini (event logs) analiz etmek ve tespit kuralları (detection rules) ile korelasyon sağlamak amacıyla kullanılan hızlı, taşınabilir ve komut satırı tabanlı bir olay avcılığı (threat hunting) aracıdır. Sigma kurallarını destekler ve özellikle Windows olay günlükleri üzerinde etkilidir.

# 🚀 Özellikleri

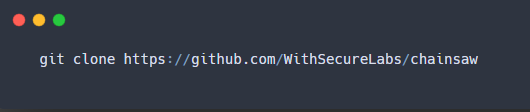
- Windows olay günlüklerinden hızlı analiz (EVTX dosyaları)  
- Sigma kuralları ile tehdit tespiti  
- Komut satırında çalışır, taşınabilir (binary olarak)  
- Özelleştirilebilir detection kuralları  
- Olayları zaman çizelgesine göre sıralama (timeline)

# 🎯 Kullanım Alanları

- Adli analiz (forensic) ve tehdit avcılığı (threat hunting)  
- Sigma kuralına dayalı saldırı izi tespiti  
- Windows sistem günlüklerinin hızlı incelenmesi  
- Olay müdahale süreçlerinde zaman çizelgesi çıkarma

# 🛠️ Kurulum

1. Chainsaw GitHub üzerinden indirilir:

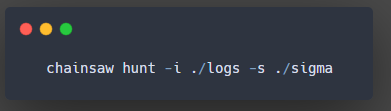
******

2. Derlemeye gerek yoktur, doğrudan binary çalıştırılır.

3. Windows'ta veya Linux’ta kullanılabilir.

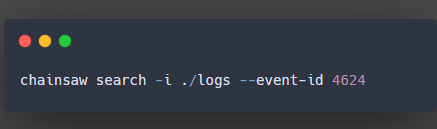
# 🧪 Örnek Komutlar ve Açıklamaları

✅ Sigma Kurallarıyla EVTX Taraması:

******

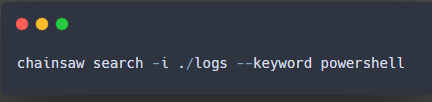
→ logs dizinindeki tüm EVTX dosyaları, sigma kurallarına göre taranır.

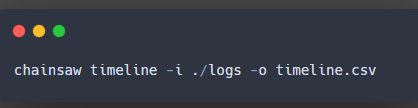
✅ Belirli Event ID ile Arama:

******

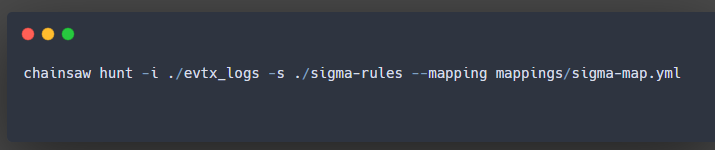
→ Tüm başarılı kullanıcı oturum açma girişimleri (4624) listelenir.

✅ Anahtar Kelime ile Arama:

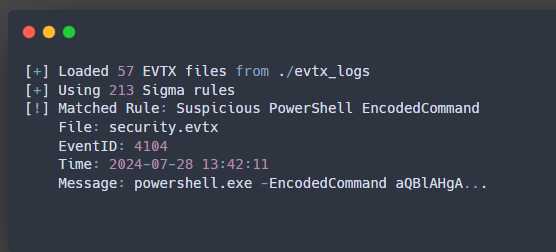
******

✅ Timeline (Zaman Çizelgesi) Oluşturma: **

**✅ 1. Sigma Kuralları ile EVTX Taraması**

**Komut:** ****

Örnek Çıktı:

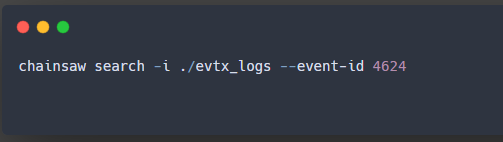


📌 Açıklama:

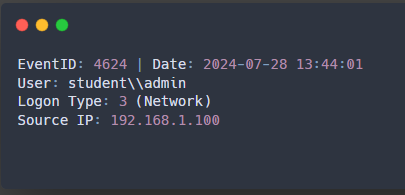
* PowerShell üzerinden şifrelenmiş komut çalıştırıldığı tespit edildi.
* Sigma kuralı bu davranışı zararlı olarak tanımlıyor.

**✅ 2. Belirli Event ID ile Arama (örneğin 4624 - Logon)**

**Komut:**



Örnek Çıktı:

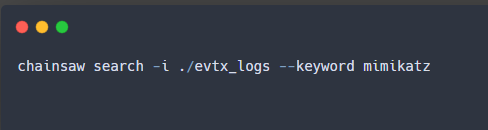


📌 Açıklama:

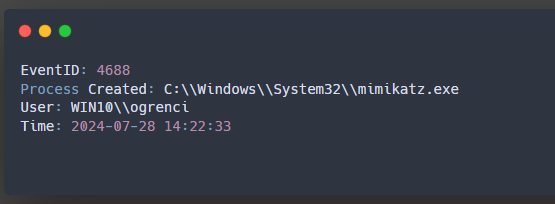
* Başarılı bir ağ oturumu açılmış (Logon Type 3).
* Ağ üzerindeki başka bir cihazdan gelen oturum girişimi izleniyor.

**✅ 3. Anahtar Kelime ile Hızlı Arama**

**Komut:**



Örnek Çıktı:

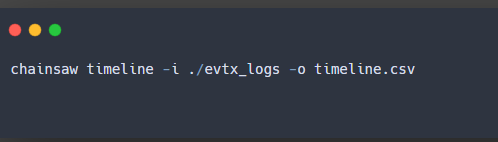


📌 Açıklama:

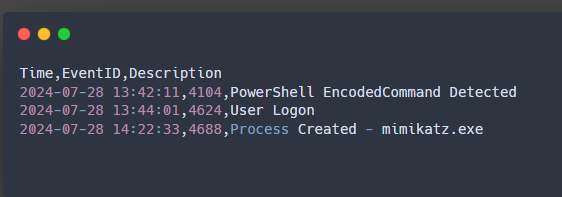
* Kullanıcı ogrenci, “mimikatz.exe” adlı şüpheli aracı başlatmış.
* Bu davranış tipik olarak kimlik bilgisi sızıntısı girişimidir.

**✅ 4. Zaman Çizelgesi Oluşturma (Timeline)**

**Komut:**



Örnek CSV Çıktısı:



📌 Açıklama:

* Olaylar zaman sırasına göre sıralanmıştır.
* Tüm olaylar bir CSV dosyasına aktarılır, Excel veya SIEM sisteminde analiz edilebilir.

# 📎 Notlar

- Chainsaw yalnızca EVTX dosyalarını işler.  
- Sigma kurallarını içeren dizin (.yml dosyaları) ile çalışmalıdır.  
- En çok kullanılan Event ID’ler: 4624 (logon), 4688 (process), 4697 (service)  
- Çıktılar CSV veya JSON formatında alınabilir ve SIEM’e aktarılabilir.