Threat Hunting Project - Eğitim Materyali

# 🔍 Threat Hunting Project Nedir?

ThreatHunting Project, Blue Team (savunma) analistleri için oluşturulmuş açık kaynaklı bir bilgi ve referans deposudur.  
Amacı, sistemlerdeki şüpheli etkinlikleri tespit etmek için kullanılabilecek davranışsal göstergeleri (IOC/TTP) kategorilere ayırmak ve MITRE ATT&CK ile eşleştirmektir.

# 🚀 Özellikleri

- MITRE ATT&CK taksonomisine uygun analiz yapısı  
- Sigma, Sysmon ve ELK gibi araçlarla entegre kural örnekleri  
- IOC (Indicator of Compromise) ve TTP (Tactics, Techniques, Procedures) tanımlamaları  
- Gerçek saldırı davranışlarının avlanabilir örnekleri  
- Güvenlik olaylarını davranışsal olarak tespit etmeyi kolaylaştırır

# 📌 Kullanım Alanları

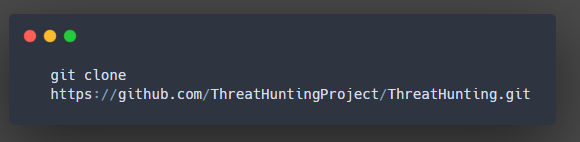
- SOC analisti eğitimi  
- Güvenlik olaylarına karşı proaktif avcılık (threat hunting)  
- MITRE ATT&CK tabanlı tehdit tespiti  
- EDR/SIEM kuralları geliştirme  
- Kurumsal güvenlik farkındalığı

# 🌐 Proje Kaynağı ve Kullanımı

GitHub adresi: https://github.com/ThreatHuntingProject/ThreatHunting

Web dokümantasyon: https://threathunting.net/

1. GitHub’dan repoyu klonla:

******

2. İçeriği keşfet: IOC, TTP, DetectionRule klasörlerini incele

3. MITRE ATT&CK numarası ile arama yaparak ilgili davranışları bul

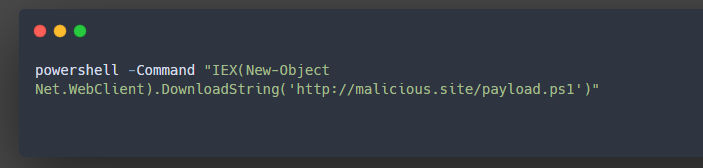
4. Sysmon veya Sigma tabanlı kurallar ile olay tespiti yapılandır

# 🧪 Örnek Kullanım Senaryosu

1. PowerShell ile Dosya İndirme (T1059.001)

### 🎯 Amaç:

Kötü niyetli kullanıcıların PowerShell üzerinden zararlı dosya indirmesini tespit etmek.

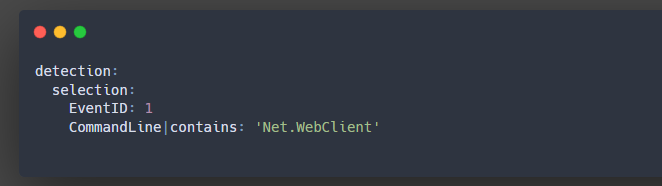


Tespit Yöntemi:

**Sysmon Event ID 1**: Process Create

**IOC:** New-Object Net.WebClient, DownloadString, IEX

**Sigma kuralı örneği:**



**2. Mimikatz ile Kimlik Bilgisi Çalma Girişimi (T1003.001)**

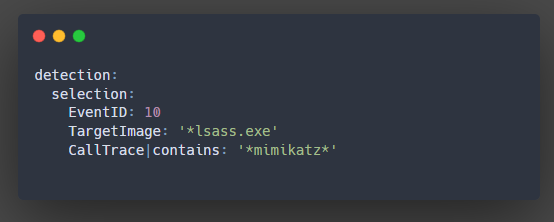
**🎯 Amaç:**

RAM üzerinden kimlik bilgileri çekme denemelerini tespit etmek (örn. sekurlsa::logonpasswords).

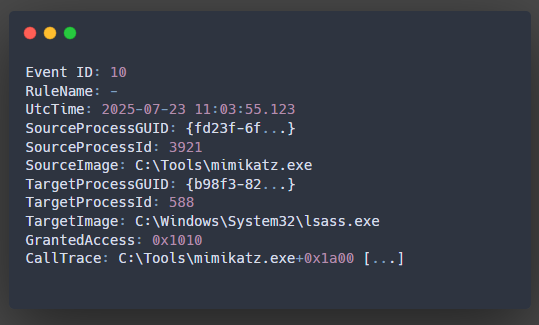
**Gözlemlenebilecek Belirtiler:**

* lsass.exe erişimi
* Sysmon Event ID 10: Process Access
* CommandLine içinde “mimikatz”, “sekurlsa” gibi kelimeler

Sigma Kural Örneği:



Olası Sysmon Logu (Event Viewer çıktısı gibi)



3. Remote Desktop Brute Force (T1110.001)

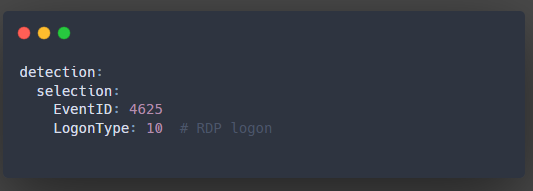
**🎯 Amaç:**

Sisteme RDP üzerinden çok sayıda başarısız oturum açma girişimi (brute force) var mı?

**Belirtiler:**

* Sysmon veya Windows Security loglarında çok sayıda Event ID 4625 (failed login)
* Aynı kullanıcı adı ile farklı IP’lerden deneme

İzleme:

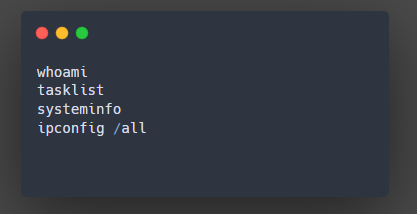


**4. Komut İstemcisi ile Sistem Keşfi (T1082, T1057)**

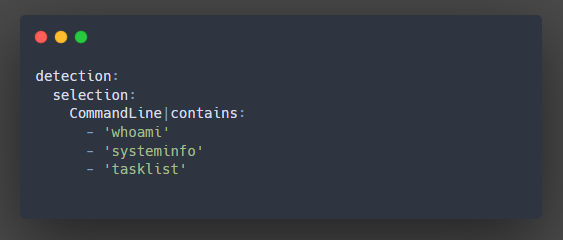
**🎯 Amaç:**

Saldırganın sistem üzerinde keşif amaçlı komutlar çalıştırmasını yakalamak

Komut Örnekleri:



Sigma:



5. DLL Sideloading veya Tuhaf DLL Çağrısı (T1574.002)

**Amaç:**

Zararlı yazılımın meşru bir uygulama üzerinden zararlı DLL dosyasını çağırıp çalıştırması.

**Belirtiler:**

* Sysmon Event ID 7: ImageLoad
* Meşru bir EXE (örneğin OneDrive.exe) zararlı DLL’i yüklüyor

| **Senaryo** | **MITRE ATT&CK ID** |
| --- | --- |
| PowerShell download | T1059.001 |
| Credential dumping (lsass) | T1003.001 |
| RDP brute force | T1110.001 |
| Keşif komutları | T1082, T1057 |
| DLL injection/sideloading | T1574.002 |

# 📎 Notlar

- Bu proje aktif saldırı tespiti değil, davranışsal analiz ile olası ihlalleri bulma amacı güder.  
- Her tespit kuralı manuel test ve doğrulama gerektirir.  
- SIEM/EDR ortamlarında kural entegrasyonu sonrası alarm eşiği test edilmelidir.