Sysmon Modular Configs - Eğitim Materyali

# 🛡️ Sysmon Modular Configs Nedir?

Sysmon (System Monitor), Microsoft tarafından sunulan bir sistem izleme aracıdır. Özellikle olay günlüğü analizi ve kötü amaçlı etkinliklerin izlenmesinde kullanılır.  
SwiftOnSecurity ve Olaf Hartong tarafından geliştirilen Sysmon yapılandırmaları, tehdit algılamayı kolaylaştırmak için özel olarak optimize edilmiştir.

# 🔧 SwiftOnSecurity & Olaf Hartong Yapılandırmaları

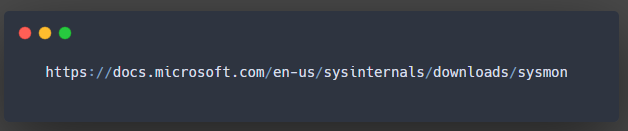
- SwiftOnSecurity: Geniş kapsamlı, kolay uygulanabilir ve düşük gürültülü (low-noise) bir config sağlar.  
- Olaf Hartong: MITRE ATT&CK uyumlu, gelişmiş tehdit tespiti odaklı modüler yapıdadır.  
- Her ikisi de XML formatında Sysmon için özelleştirilmiş kurallar içerir.

# 📌 Kullanım Alanları

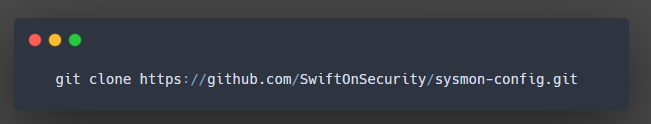
- Zararlı yazılım analizi  
- İç tehdit tespiti  
- Sistem olaylarının detaylı kaydı  
- MITRE ATT&CK tabanlı olay izleme  
- Güvenlik farkındalığı eğitim ortamları

# 🛠️ Kurulum ve Yapılandırma Adımları

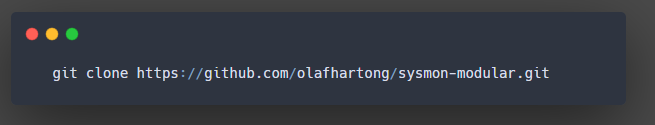
1. Sysmon’u Microsoft Sysinternals sitesinden indirin ve çıkartın:

******

2. SwiftOnSecurity config’ini indir:

******

3. Olaf Hartong modular config’ini indir:

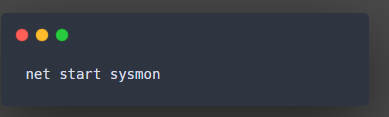
******

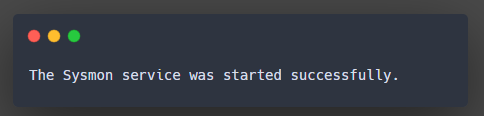
4. Sysmon'u yapılandırma ile birlikte kur (örnek SwiftOnSecurity):

# 

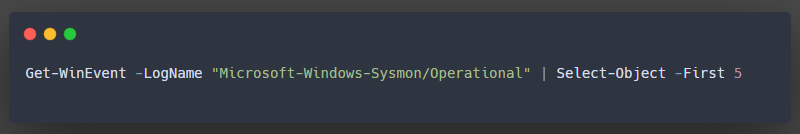
# 🧪 Örnek Sysmon Komutları ve Olası Çıktılar

## ✅ Sysmon Servisinin Başlatılması

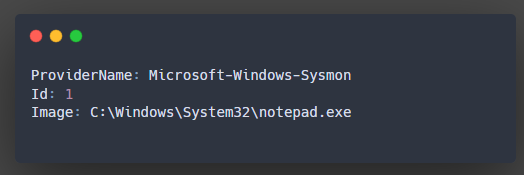
Komut:  


Çıktı:  


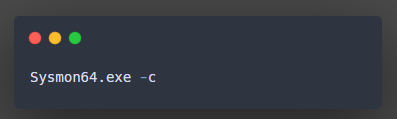
## ✅ Event Viewer'dan Günlükleri Görmek

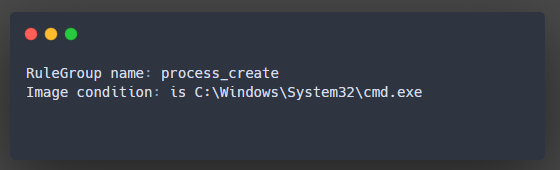
Komut:  


Çıktı (örnek):

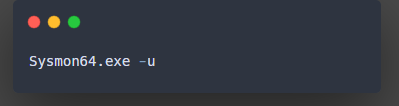


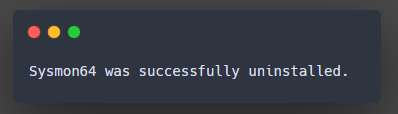
## ✅ Aktif Kuralları Görüntüleme

Komut:  


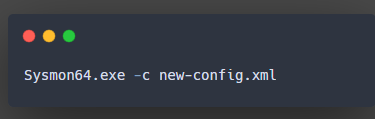
Çıktı:  


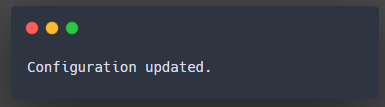
## ✅ Sysmon'u Kaldırma

Komut:  


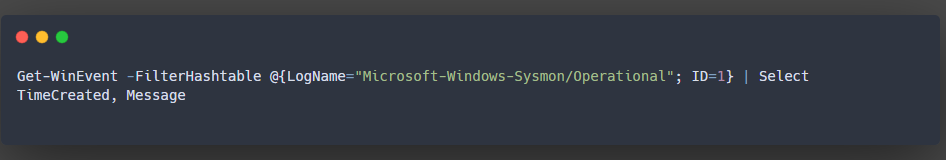
Çıktı:  


## ✅ Yeni Konfigürasyon Yükleme

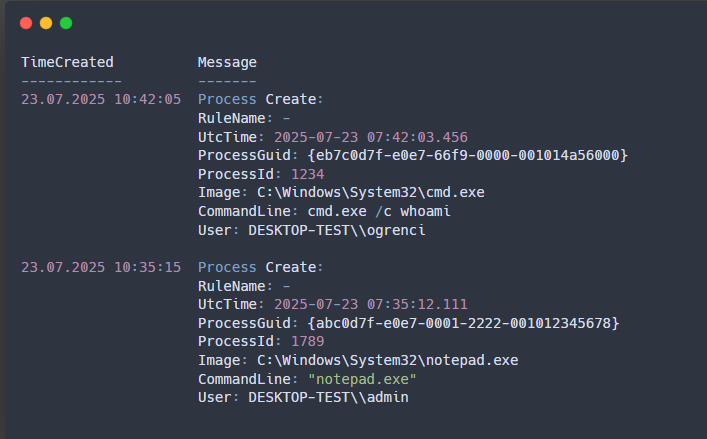
Komut:  


Çıktı:  


## ✅ Belirli Event ID ile Günlük Filtreleme

Komut:  


***Çıktı:***

******

## 📝 Yaygın Sysmon Event ID'leri

|  |  |
| --- | --- |
| Event ID | Açıklama |
| 1 | Process Create |
| 3 | Network Connect |
| 10 | Process Access |
| 11 | File Create |
| 22 | DNS Query |

# 📎 Notlar

- Yapılandırmalar XML formatındadır, güncellenmeden önce dikkatlice incelenmelidir.  
- Günlükler Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon altında bulunur.  
- SwiftOnSecurity config daha az alarm üretirken, Olaf Hartong konfigürasyonu MITRE ATT&CK uyumlu detaylı analizler sunar.