### **Hayabusa**

**Hayabusa**, Windows Event Log (EVTX) dosyalarını hızlı ve kapsamlı şekilde analiz etmek için kullanılan açık kaynaklı bir **olay günlüğü analiz aracıdır**. Forensik analiz, olay müdahalesi ve tehdit avcılığı (threat hunting) gibi süreçlerde Windows sistem günlüklerinden şüpheli aktiviteleri ortaya çıkarmak için tasarlanmıştır.

Hayabusa, Windows sistemlerdeki olay günlüklerini (örneğin Security.evtx, System.evtx, Application.evtx) analiz eder ve:

* şüpheli oturumlar,
* yetki yükseltmeleri,
* dosya erişimleri,
* komut çalıştırmaları  
  gibi davranışları otomatik olarak tespit etmeye çalışır.

Kullanıcıya geniş filtreleme, renklendirme, CSV/JSON çıktısı alma ve hızlı tarama gibi yetenekler sunar.

### **Hayabusa ne işe yarar?**

Windows ortamlarında gerçekleşen siber olaylar genellikle Event Log’lara iz bırakır. Ancak bu günlükler karmaşık, büyük ve elle analiz edilmesi zordur. Hayabusa bu dosyaları:

* hızlı bir şekilde işler (özellikle paralel işlem desteğiyle),
* belirli kurallara göre şüpheli aktiviteleri ön plana çıkarır,
* dijital delil niteliğinde olan olayları kategorize eder.

Özellikle sızma testi sonrası olay izlerini analiz etmek, APT davranışlarını takip etmek ya da fidye yazılımı saldırısı sonrası sistem incelemek için idealdir.

### **Kurulum**

Hayabusa, Go ile yazıldığı için çalıştırılabilir binary olarak indirilebilir veya kaynak koddan derlenebilir.

* git clone https://github.com/Yamato-Security/hayabusa
* cd hayabusa
* go build

### **Örnek Komut**

aşağıdaki komut, bir klasördeki Security.evtx dosyasını analiz eder ve sonuçları CSV olarak kaydeder:

* hayabusa -f ./evtx/Security.evtx -o output.csv

Örneğin birden fazla log dosyasını birden taramak için:

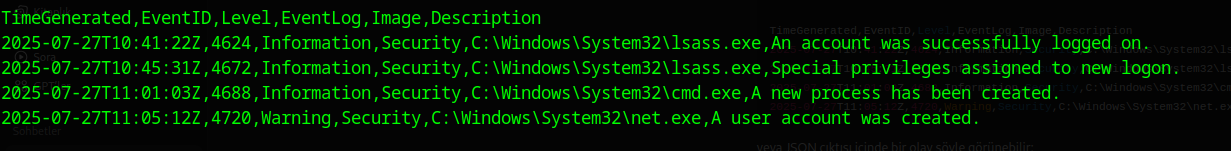
* hayabusa -f ./evtx/ -r -o report.json

bu komut:

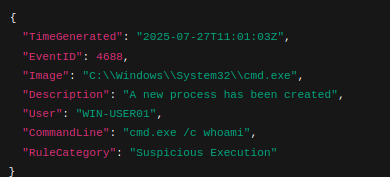
* ./evtx/ klasöründeki tüm EVTX dosyalarını (recursive) tarar,
* şüpheli olayları report.json dosyasına JSON formatında ya

### **Örnek Çıktı**

CSV çıktısının ilk birkaç satırı şu şekilde olabilir:



veya JSON çıktısı içinde bir olay şöyle görünebilir:



bu örnek, cmd.exe üzerinden komut çalıştırıldığını ve olayın şüpheli olarak etiketlendiğini gösterir.

### **Sık Kullanılan Parametreler**

* -f <dosya veya klasör>  
  Tek bir EVTX dosyası ya da klasördeki tüm EVTX dosyalarını analiz eder.  
  Örnek: -f /mnt/logs/Security.evtx
* -r  
  Recursive mod: klasör içinde alt dizinleri de tarar.
* -o <dosya>  
  Çıktıyı dosyaya kaydeder. Formatı uzantıdan otomatik belirler (.csv, .json, .html, vb.)
* --rule-category <kategori>  
  Belirli türde kurallar çalıştırılır (örneğin: lateral\_movement, privilege\_escalation, execution).
* --timezone <zaman\_dilimi>  
  Zaman damgalarını belirli bir dilime göre gösterir.  
  Örnek: --timezone "UTC+3"
* --color  
  Terminalde çıktı renklendirmesi yapar (varsayılan: açık).
* --quiet  
  Bilgilendirme mesajlarını kapatır.

**Hayabusa**, olay müdahalesi (IR) ve dijital adli analiz (DFIR) süreçlerinde, Windows log dosyalarından şüpheli aktiviteleri çıkarmak için kullanabileceğiniz güçlü ve hızlı bir araçtır. Hacimli EVTX dosyalarıyla başa çıkabilir, otomatik kurallarla dikkat çekici olayları öne çıkarır. Özellikle fidye yazılımı bulaşmaları, lateral movement analizleri ve oturum takibi gibi konularda oldukça etkilidir.