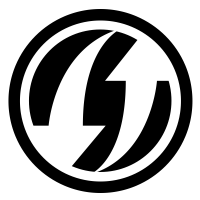
**SYSFLOW**

**1. Nedir?**  
SysFlow, bilgisayar sistemlerinde gerçekleşen olayları takip eden ve bu olayları küçük veri paketleri (flow) halinde kaydeden bir güvenlik izleme sistemidir.  
Kısaca: Sistem içindeki **"ne oldu, nasıl oldu"** sorularına net cevaplar verir.

* Dosya açma
* Ağ bağlantısı kurma
* İşlem başlatma gibi olayları izler.

Bu olayları sadeleştirip, anlaşılır bir şekilde kayıt altına alır. Böylece sistemdeki tüm aktiviteleri **zaman akışıyla** birlikte görebilirsin.



**2. Ne İşe Yarar?**

* Bilgisayarda veya bir sunucuda neler olup bittiğini takip etmeye yarar.
* Özellikle siber güvenlik uzmanları için saldırı analizi yaparken çok kullanışlıdır.
* “Kim ne yaptı?”, “Hangi işlem hangi bağlantıyı kurdu?”, “Ne zaman oldu?” gibi sorulara cevap verir.

➡️ SysFlow, bu olayları birleştirerek bir "akış" (flow) dosyası oluşturur. Böylece karmaşık logları okumaya gerek kalmaz, sadeleştirilmiş bir izleme sistemi sağlar.

**3. Neden Önemlidir?**

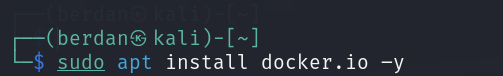
* Klasik log sistemleri çok fazla veri içerir ve anlaması zordur.
* SysFlow bu verileri anlamlı hale getirir.
* **Red Team** (sızma testleri yapan ekipler) saldırıların izini gizlemek istese de, SysFlow bu hareketleri takip edebilir.
* **Blue Team** (savunma ekibi) için kritik bir araçtır çünkü saldırının adımlarını net şekilde ortaya koyar.

Özellikle tehdit avcılığı (threat hunting) ve olay müdahale (incident response) işlemlerinde kullanılır.

**4. Nasıl Kurulur? (Linux Örneği)**  
SysFlow, Docker ile kolayca kurulabilir. Aşağıdaki komutlarla kurulumu yapabilirsin:

**# 1. Docker kurulu değilse yükle**

**sudo apt install docker.io –y**

****

**# 2. SysFlow Collector konteynerini başlat**

**docker run -d --rm --name sf-collector \**

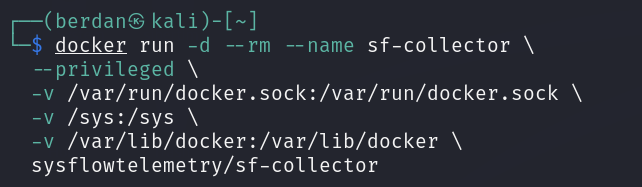
**--privileged \**

**-v /var/run/docker.sock:/var/run/docker.sock \**

**-v /sys:/sys \**

**-v /var/lib/docker:/var/lib/docker \**

**sysflowtelemetry/sf-collector**

****

Not: Çalışan işlemleri ve konteynerleri izlemek için gerekli izinleri otomatik olarak verir. Toplanan veriler .**sf** uzantılı dosyalara yazılır.

**5. Örnek Bir Anlatım:**  
Diyelim ki bir sistemde aşağıdaki olaylar gerçekleşiyor:

1. Kullanıcı firefox tarayıcısını başlattı.
2. /home/user/Downloads/malware.sh adlı dosya açıldı.
3. 198.51.100.5 adresine bağlantı kuruldu.

Bu olaylar normalde farklı log dosyalarında saklanır.  
Ama **SysFlow** bu olayları tek bir zincir gibi birbirine bağlayarak şöyle gösterir:

**firefox →malware.sh** dosyasını çalıştırdı → **198.51.100.5** adresine bağlantı kurdu.

Böylece saldırının adımları açıkça ortaya çıkar. Güvenlik uzmanı saldırının nereden başladığını, nereye gittiğini kolayca görebilir.

⚠️ **Uyarı:**  
SysFlow, saldırıların tespiti ve analizinde çok güçlüdür. Ancak doğru şekilde yapılandırılmazsa bazı olaylar gözden kaçabilir. Bu yüzden her sistemde ayrı ayrı test edilmesi önerilir.