



# SecOps-Research-Framework (SRF)

Otonom Savunma ve Sürekli Doğrulama Mimarisi

SAFA HACIBAYRAMOĞLU

2420191014

BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ

# SecOps-Research-Framework

Otonom Savunma ve Sürekli Doğrulama Mimarisi

1

## DevSecOps & Siber Güvenlik

Otonom Test ve Tespit Mühendisliği odaklı kategori

2

## Teknoloji Yığını

Bash Scripting, Wazuh API, JSON-First Architecture

3

## Detection as Code

Kod olarak tespit prensibi ile çalışan temel mimari



 PROBLEM

# Geleneksel SOC Yapılarındaki "Sessiz Hatalar"

## Reaktif Yapı

Mevcut savunma sistemleri pasiftir; sadece saldırı gerçekleştiğinde tepki verir.

## Sessiz Hatalar

Log taşıyıcı servislerin durması veya kuralların bozulması durumunda sistem sessiz kalır.

## Kör Noktalar

Güvenlik ekipleri, sistemin çalışmadığını genellikle bir ihlal yaşıandıktan sonra fark eder.

*"Sistem şu an %100 görünürünlüğe sahip mi?"* sorusuna anlık ve kanıtlanabilir bir yanıt verilememektedir.



# SRF ve Sürekli Doğrulama

01

## Aktif Doğrulama

Saldırganı beklemek yerine periyodik simülasyon

02

## Mühendislik Yaklaşımı

CI/CD süreçlerinin siber güvenliğe uyarlanması

03

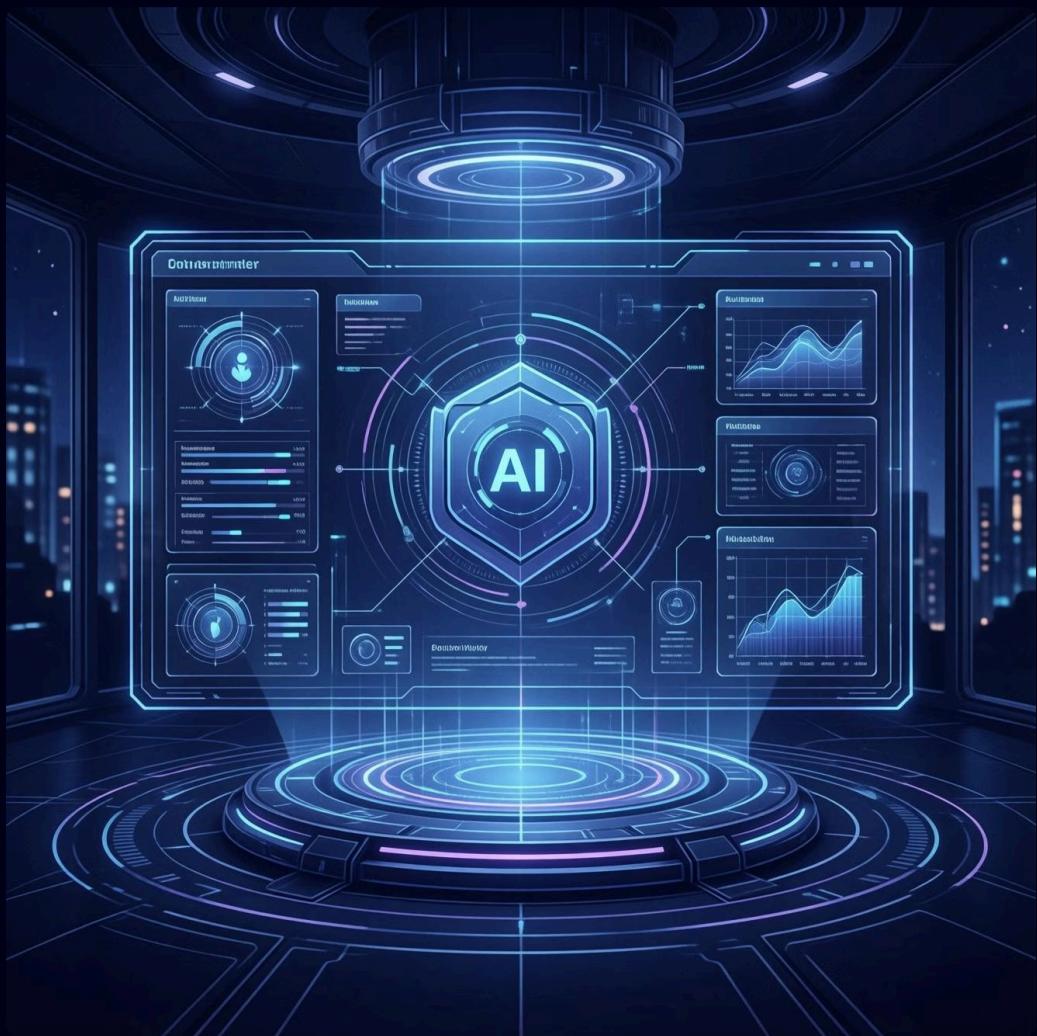
## Otonom Gözgü

İnsan müdahalesi olmadan sistem denetimi

04

## Kanıt Tabanlı Güvenlik

API yanıtlarıyla matematiksel ispat



# Modüler Sistem Mimarisi

Proje, endüstriyel standartlara uygun üç ana katmandan oluşur:



## Yönetim Katmanı (SRF-CLI)

Bash tabanlı merkezi orkestrasyon aracı. Servis sağlığı kontrolleri ve kullanıcı etkileşimi.



## Otomasyon Katmanı

secops-watchdog.sh modülü. Simülasyonu tetikleyen ve API doğrulamasını yapan motor.



## Mantık Katmanı

local\_rules.xml (Detection as Code). Tehdit tespit kurallarının kod tabanlı yönetimi.



# Otonom Test Mekanizması

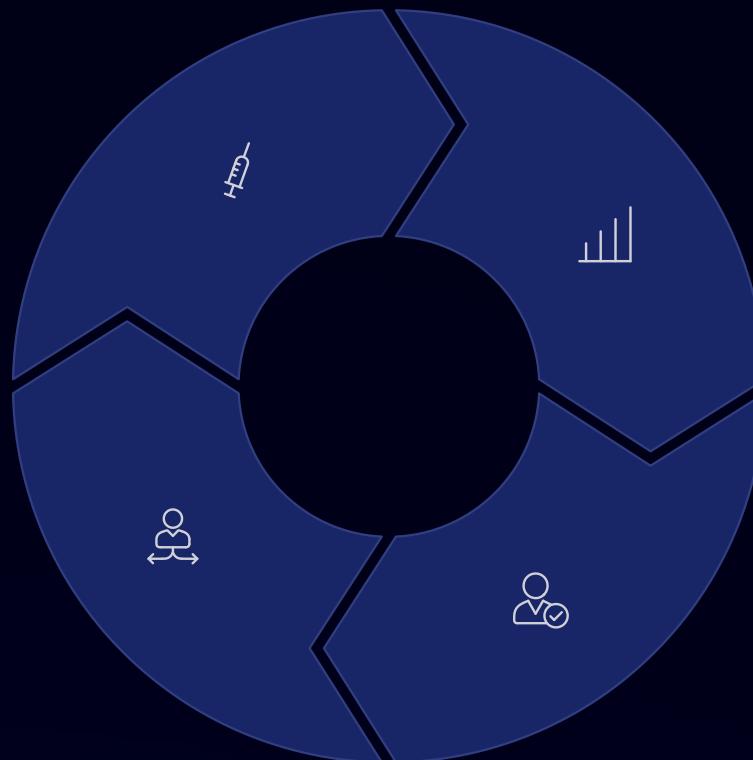
Sistem döngüsü 4 aşamada gerçekleşir:

## Enjeksiyon

Zararsız, özel etiketli (secops-autotest)  
sahte tehdit logu gönderilir

## Karar

PASS: Alarm bulundu, sistem sağlıklı.  
FAIL: Alarm yok, kör nokta var



## Telemetri

Logun işlenmesi, indekslenmesi ve  
korelasyonu için bekleme süresi  
(Latency Buffer)

## Doğrulama

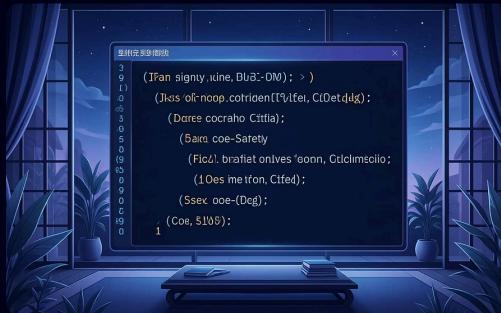
SIEM API'sine bağlanarak logun "Alarm"  
üretip üretmediği sorgulanır



SONUÇLAR

# Canlı Sistem Test Sonuçları

Geliştirilen prototip üzerinde yapılan testlerde:



## JSON-First Entegrasyonu

Veri iletişiminde %100 tip güvenliği sağlanmıştır



## Anlık Raporlama

Sistem durumu saniyeler içinde "Sağlıklı" veya "Kritik" olarak raporlanır



## Denetim İzleri

Her otomatik test, tarih ve sonuç bilgisiyle /var/log altında kayıt altına alınır



## API Güvenliği

Tüm doğrulamalar yetkilendirilmiş (Bearer Token) şifreli kanallar üzerinden yapılır

# Siber Güvenlikte Yeni Bir Standart



## Dönüşüm

Güvenlik operasyonları  
"Operatör" seviyesinden  
"Mühendislik" seviyesine  
taşınmıştır



## Güvence

"Umut tabanlı" güvenlikten, "Veri  
tabanlı" güvenliğe geçiş  
sağlanmıştır



## Sürdürülebilirlik

Sistem, insan hatasından bağımsız olarak kendi kendini izleme ve  
doğrulama yeteneğine kavuşmuştur

**SecOps-Research-Framework:** Otonom, kanıt tabanlı ve sürdürülebilir  
siber güvenlik mimarisi

