



## Project Subject

SPLUNK İLE GÜVENLİK BİLGİ VE OLAY YÖNETİMİ (SIEM) ÇÖZÜMÜ UYGULAMASI

## Full Name

Haydar Can Kotanoglu

## Project Duration

Bitis Tarihi: 08/06/2025



## Project Aims

### • Log Toplama ve Entegrasyonu:

- Basta STD4 test makinesi (10.10.1.14) ve saldırı simülasyonu Linux sunucusu (10.10.1.52) olmak üzere belirlenen sistemlerden merkezi log toplama işlemini kurmak. Log Kaynakları ve Akis Doğrulaması.
- Windows Güvenlik (Security), Sistem (System), Uygulama (Application) ve Sysmon loglarının Splunk sunucusundaki main indeksine aktarılmasını sağlamak.
- Linux sunucu üzerine Splunk Universal Forwarder kurulumu ve /var/log/syslog izlemesi.
- Fortinet güvenlik duvarı loglarını entegre etmek.

### • Ortam Kurulumu ve Gelistirilmesi:

- STD4 makinesinde detaylı aktivite takibi için Microsoft Sysinternals paketindeki Sysmon aracını, SwiftOnSecurity tarafından geliştirilen gelişmiş bir yapılandırma dosyası (config.xml) ile kurmak.
- Splunk Common Information Model (CIM), InfoSec App & Splunk Security Essentials, Lookup File Editor, Punchcard visualization, Force Directed visualization ve Sankey Diagram gibi temel Splunk uygulamalarını ve eklentilerini kurmak.

### • Güvenlik Kullanım Senaryosu Gelistirme (STD4 (10.10.1.14) makinesi üzerinde test edilecek): En az üç kritik güvenlik kullanım senaryosu geliştirmek:

- Kaba Kuvvet Saldırısı Tespiti: Sistemlere yönelik kaba kuvvet (brute force) saldırılarını tespit etmek.
- Supheli Konumlardan Çalışan Proseslerin Tespiti: Zararlı yazılımların sıkça kullandığı geçici dizinler (%TEMP%, %APPDATA% vb.) gibi supheli konumlardan çalıştırılan prosesleri tespit etmek.
- Dis Kaynaklı Trafik Cografi Analizi: İnternet üzerinden gelen ağ trafiğinin kaynak IP adreslerini coğrafi olarak harita üzerinde gorselleştirerek saldırıların coğrafi kökenlerini analiz etmek.

### • Alarmlama ve Gorselleştirme:

- Her kullanım senaryosu için özel SPL sorguları oluşturmak.
- Tanımlanmış tehditler için alarmlar yapılandırmak.
- Sonuçları panolar üzerinde gorselleştirmek.

## Project Achievements

### Ortam Kurulumu ve Yapilandirma Basarimlari:

Log mimarisinin temeli, test ortamindaki Windows ve Linux sunucularindan logların Splunk sunucusuna aktarilmasiyla basariyla olusturuldu.

- STD4 (10.10.1.14) Windows Sanal Makinesi ve saldiri simulasyonu icin kullanim 10.10.1.52 IP adresli Linux sunucusundan log akisi saglandi. Splunk Universal Forwarder ajani kurularak Windows Guvenlik, Sistem, Uygulama ve Sysmon loglarının Splunk main indeksine aktarilmasi saglandi. Log akisinin saglikli ve anlik oldugu dogrulandi.
- STD4 makinesinde Sysmon, SwiftOnSecurity yapilandirma dosyasi (config.xml) ile kuruldu (sysmon64.exe -c config.xml).
- Linux sunucuya Splunk Universal Forwarder kuruldu ve /var/log/syslog izlemesi icin yapilandirildi.
- Splunk Common Information Model (CIM), InfoSec App & Splunk Security Essentials ve yardimci gorsellestirme uygulamalari (Lookup File Editor, Punchcard visualization vb.) ortama dahil edildi.

---

### Gelistirilen Guvenlik Kullanım Senaryosu 1: Brute Force Saldirilarinin Tespiti

**Amac:** Sistemlere yönelik kaba kuvvet saldırılarını tespit etmek.

**İlgili Veri:** STD4'ten toplanan Windows Guvenlik Logu, EventCode=4625 (Basarisiz Giriş).

#### Tespit Sorgusu (SPL):

```
index=main sourcetype=WinEventLog:Security EventCode=4625
| bin _time span=5m
| stats count by _time, user, src, host
| where count > 3
| sort -_time, -count
```

**Test Yontemi ve Bulgular:** 10.10.1.52 IP adresli Linux makinesinden, hedefteki 10.10.1.14 IP adresli STD4 makinesine karsi bir RDP brute force saldirisi (Hydra araci ve SecLists kullanicı adi/sifre listeleri ile) duzenlenerek basariyla test edildi. Splunk panosunda yapilandirilan "Cok Sayida Basarisiz Oturum Acma Denemesi" alarminin tetiklendiği gözlemlendi.

## Gelistirilen Guvenlik Kullanım Senaryosu 2: Supheli Konumlardan Calisan Proseslerin Tespiti

**Amac:** STD4 makinesinde supheli konumlardan (örn. %TEMP%, %APPDATA%) calistirilan prosesleri tespit etmek.

**Ilgili Veri:** STD4'ten toplanan Sysmon Logu, EventCode=1 (Process Create).

### Tespit Sorgusu (SPL):

```
index=main (EventCode=1 OR EventID=1)
| search (process_path="*\\Users\\*\\AppData\\*.exe" OR
process_path="*\\Temp\\*.exe")
| stats count by process_name
| sort -count
| head 10
```

**Gorsellestirme:** Supheli konumlardan calisan en yaygin 10 prosesin dagilimi, proje panosunda bir Pasta Grafik (Pie Chart) ile gorsellestirildi.

---

## Gelistirilen Guvenlik Kullanım Senaryosu 3: Dis Kaynakli Trafigin Cografi Analizi

**Amac:** Internet uzzerinden gelen ag trafiginin kaynak IP adreslerini cografi olarak analiz etmek.

**Ilgili Veri:** Fortinet Guvenlik Duvari Loglari.

### Tespit Sorgusu (SPL):

```
index=fortinet*
| search srcip!="192.168.*" AND srcip!="10.0.0.0/8" AND
srcip!="172.16.0.0/12"
| iplocation srcip
| where isnotnull(Country)
| geostats count by Country
```

**Gorsellestirme:** Dis kaynakli IP'lerin ulke bazinda dagilimi bir Choropleth Haritasi uzzerinde gosterildi. Incelenen veri seti dahilinde en yogun trafigin Ukrayna'dan kaynaklandigi gozlemlendi.

- 
- **Sonuc (Genel Basarim):** Proje, gorev taniminda belirtilen tum hedeflere basariyla ulasmistir. Splunk platformu uzzerinde, farkli kaynaklardan gelen loglari isleyebilen, en az uc adet kritik siber guvenlik tehdidini proaktif olarak tespit edebilen ve sonuclari anlamlı panolarda sunabilen islevsel bir SIEM ortamı prototipi olusturulmustur.
  - **Karşılaşılan Zorluklar ve Çözümler**

Proje sürecinde karşılaşılan temel zorluklar arasında; Splunk arayüzünde görülen olay zamanları ile yerel saat arasındaki uyumsuzluklar, Splunk veri akışında yaşanan anlık duraklamalar ve coğrafi görselleştirme için gerekli olan GeoIP yapılandırmasının önemi yer almaktadır. Bu sorunlar, saat dilimi ayarlarının kontrolü, STD4 gibi kaynak makinelerde NTP senkronizasyonunun gerekliliği ve Splunk komutlarının doğru kullanımı gibi konuların incelenmesiyle aşılmıştır.

## Unrealized Targets

**Gelişmiş Tehdit Azaltma:** Davranış tabanlı izleme ve sanal alan (sandboxing) tekniklerinin uygulanması.

- **SIEM Entegrasyonu:** Güvenlik duvarı ve güvenlik loglarının merkezi izleme için bir SIEM sistemi ile entegrasyonu (Bu zaten projenin ana konusu olduğu için bu maddeyi "Daha Kapsamlı SIEM Entegrasyonları" veya "Diğer Güvenlik Araçlarıyla Entegrasyon" olarak gösterebilirsiniz).
- **Olay Müdahale Testi:** Gerçek zamanlı tehditlere karşı kurumun hazırlığını test etmek için olay müdahale tatbikatları yapmak.
- **Yüksek Erisilebilirlik ve Yedeklilik:** Kesintisiz ağ güvenliği sağlamak için güvenlik duvarı cihazları için yedeklilik ve yüksek erişilebilirlik yapılandırmaları oluşturmak (Bu madde Splunk SIEM için de düşünülebilir).

## Disclosures

**Kaynaklar ve Lisanslama:** Bu projede kullanılan tüm yazılım araçları ve platformlar (Splunk, kullanılan işletim sistemleri vb.) lisanslama ve kullanım koşullarına uygundur.

- **Veri Gizliliği:** Test verileri kullanılmış olup, proje boyunca hassas verilerin korunması ve gizliliğin sağlanması için en iyi güvenlik uygulamaları izlenmiştir.
- **Risk Yönetimi:** Riskleri azaltmak için her türlü çaba gösterilmiş olsa da, bazı beklenmedik sorunlar ortaya çıkabilir ve bir olay müdahale planı hazırlanmıştır (Bu madde projede gerçek bir riskten ziyade genel bir ifadedir).



# Graduation Project Report

**Oak** Academy

*Participant*

*Haydar Can Kotanoglu*

*Training Institution*

*Oak Academy*



info@oakacademy.de



www.oakacademy.de



+49 201 764 08 726



Bischoffstraße 134, 45329 Essen/Germany

**Oak** Academy

