



Protection

# Çözülmesi Planlanan Sorun

- ▶ Ağ cihazlarının, sunucuların, web siteleri ve uygulamaların ortak problemlerinden biri de saldırı tehditleridir. Bu tehditlerin gerçek zamanlı tespiti ve müdahalesi gereklidir.
- ▶ Veri güvenliği, Veri kaybı, Sistem sürdürülebilirliği ve Sistem hakkında anlık bilgi havuzu oluşturma gibi alanlarda hizmet verecek.

# Amaç

- ▶ Sistem Mühendisi, Yazılım Mühendisi, Ağ Mühendisi ve Yetkili kişilerin anlık takibini yapabilecekleri bir sistem oluşturmak.
- ▶ Böylece sistem ve veri güvenliğinin seviyesini arttırmış, hızlı müdahale oranını da doğru orantıda yükseltmiş olmak.

# Çözüm

- Sürekli bir veri akışı ile anlık analizlerin gerçekleşmesi, gerçek zamanlı veri görselleştirilmesi ve müdahale edilmesi gereken durumlar için bildirim mekanizmasının oluşturulması.
- Verilerde beklenmedik değişimlerin analizleri.
- Web siteleri veya uygulamalarda görüntü işleme algoritmaları ile değişimlerin kaydedilmesi ve raporlanması.

# Kullanılacak Teknolojiler ve Programlama Dilleri

- Amazon serverless yapısı
- Python
- ELKStack
- RPA

# Rakiplerinden Farkları

- Serverless yapısı ile daha düşük maliyet ve güncel teknoloji
- Oluşturulan bildirim yapılarının maliyetinin düşük olması
- Görüntü işleme algoritmaları ile desteklenmesi
- Kullanımın daha basitleştirilmiş bir arayüze sahip olması

# Neden Tercih Edilmeliyiz?

- Kaynakların verimli kullanımı
- Maliyetin düşük olması
- Analiz için güncel teknolojilerin kullanımı
- Hızlı ve güvenilir bir mimariye sahip olunması

# Nasıl Çalışır?

- Veriler web servis aracılığıyla okunur ve ELK yapısına gönderilir. ELK 1 lider node ve 2 ara node olmak üzere toplam 3 node olarak oluşturulur. Gelen isteklerin okuma veya yazma ise ara nodelara yönlendirilecek. Durumu kontrol eden lider node olacak.
- Web servis ve Elastic veri tabanımız sunucusuz bir mimaride bulut sistemde çalışacak.
- NoSQL yapısı ile depolanan verilerin analizi öğrenme algoritmaları ile desteklenerek görselleştirme işlemleri yapılacaktır.
- Öğrenilen verilerin önemine göre uyarı sistemi RPA ile denetlenip anlık olarak Slack, Telegram, Mail veya Sms yöntemleri kullanılarak bildirim gönderilecek.
- Tüm işlemler serverless yapısı üzerinde ve NoSQL yapısında olacağından hızlı ve düşük maliyetle sistem çalışacak.



# Ürün Yol Haritası

