SOME Bulmacasından Çıkış Var Mı?

Burak DAYIOĞLU

innovera
We enable.

atarlabs

Siber Güvenliğin Evrimsel Gelişimi

İnceleme ve Yanıt

Çok fazla alarm alıyoruz. Bunları nasıl inceleyip saldırılara yanıt vereceğiz?

Tespit

Belki tüm saldırıları durduramayız ama durduramadıklarımızda alarm alıp incelesek?

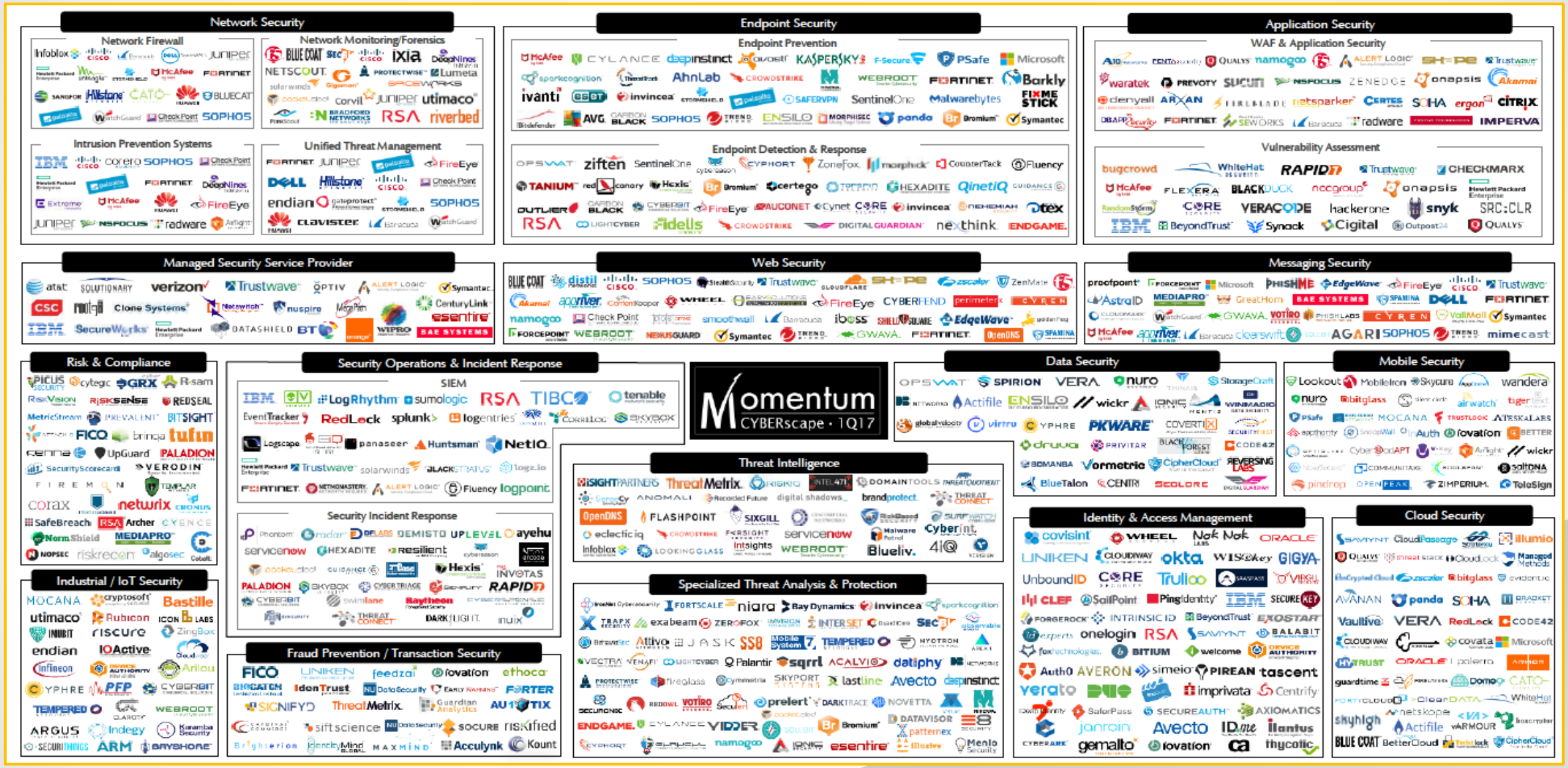
Engelleme

Bu 7-8 katman sayesinde tüm saldırıları durduracağız

innovera
We enable.

atarlabs

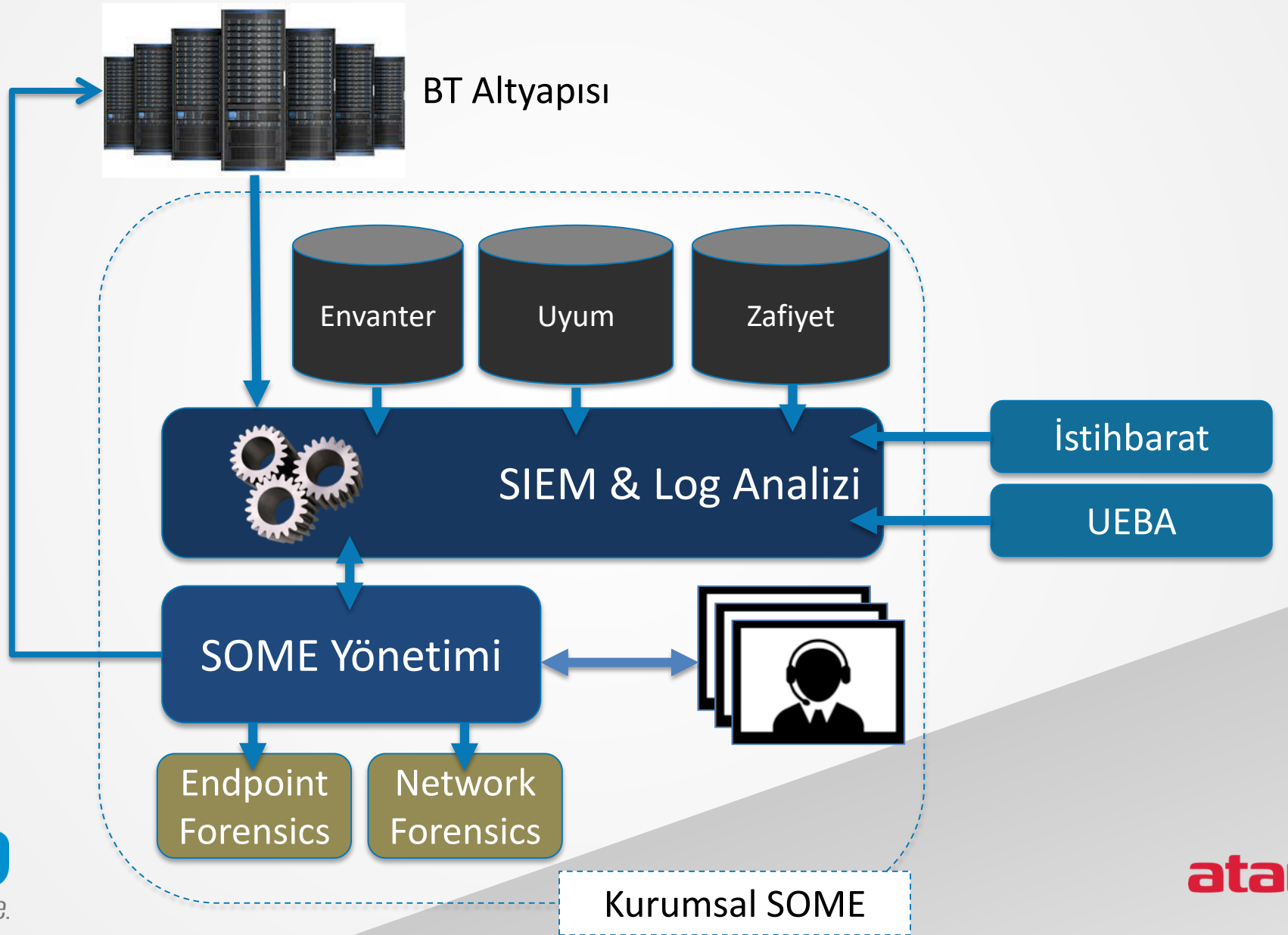
Siber Güvenlik Üretici Haritası



innovera
We enable.

atarlabs

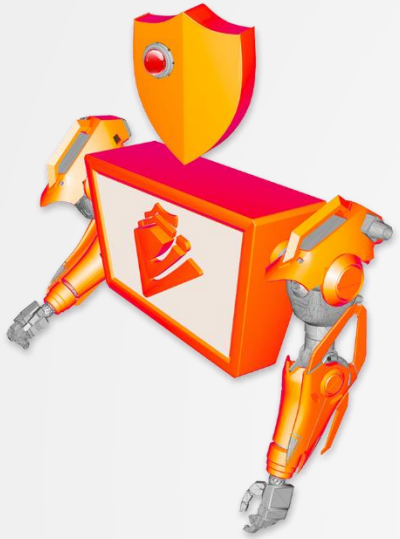
SOME Teknoloji Referans Modeli



innovera
We enable.

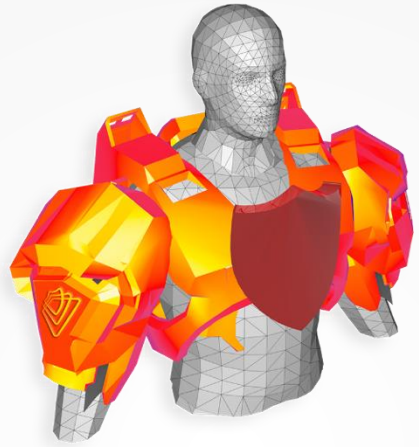
atarlabs

Güvenlik Operasyonu için ATAR



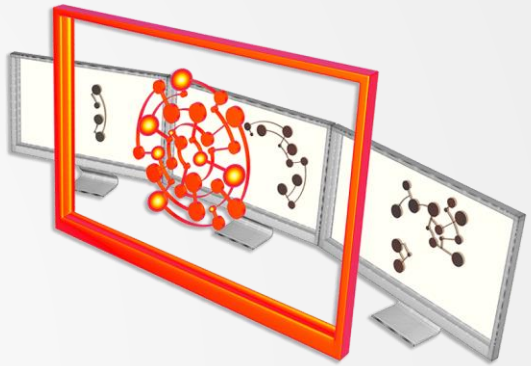
TEKRAR EDENLERİ OTOMATİKLEŞTİR

- Senaryo tabanlı otomasyon
- Karmaşık süreçlere destek
- 80+ platform için destek
- Tam ve yarı otomasyon imkanı



SOME UZMANININ VERİMLİLİĞİNİ ARTTIR

- Teknolojiden bağımsız SOME arayüzü
- Birlikte çalışabilme
- Tek tuşla delil toplama ve aksiyon
- Delil kasası sağlama



SOME ANALİZLERİ SAĞLA

- SOME süreçlerinden ölçüm alabilme
- SLA izleme
- Personel izleme
- Raporlar ve dashboard'lar
- Otomasyon tasarrufları

innovera
We enable.

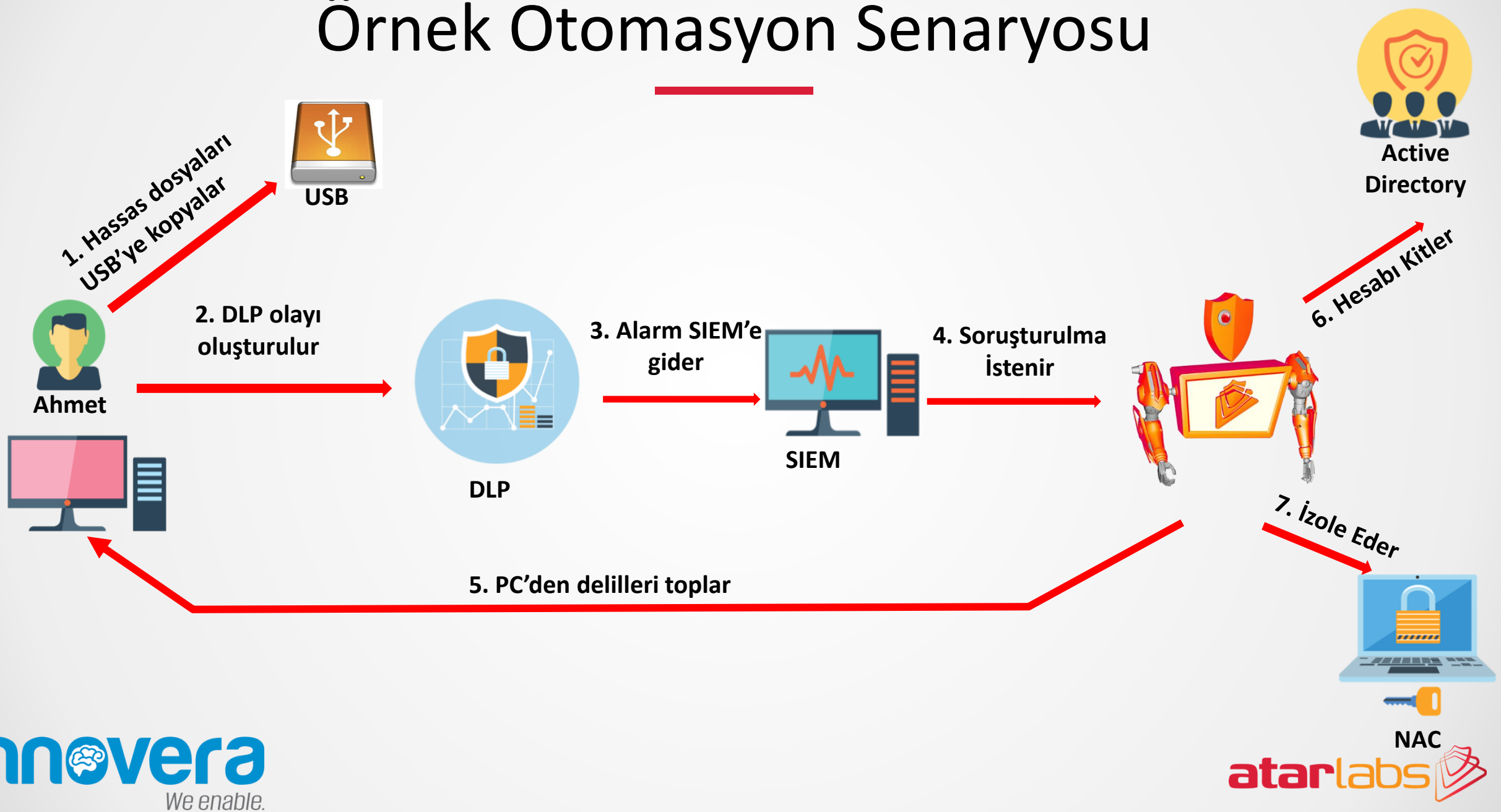
atarlabs

ATAR Entegrasyonları

innovera
We enable.

atarlabs

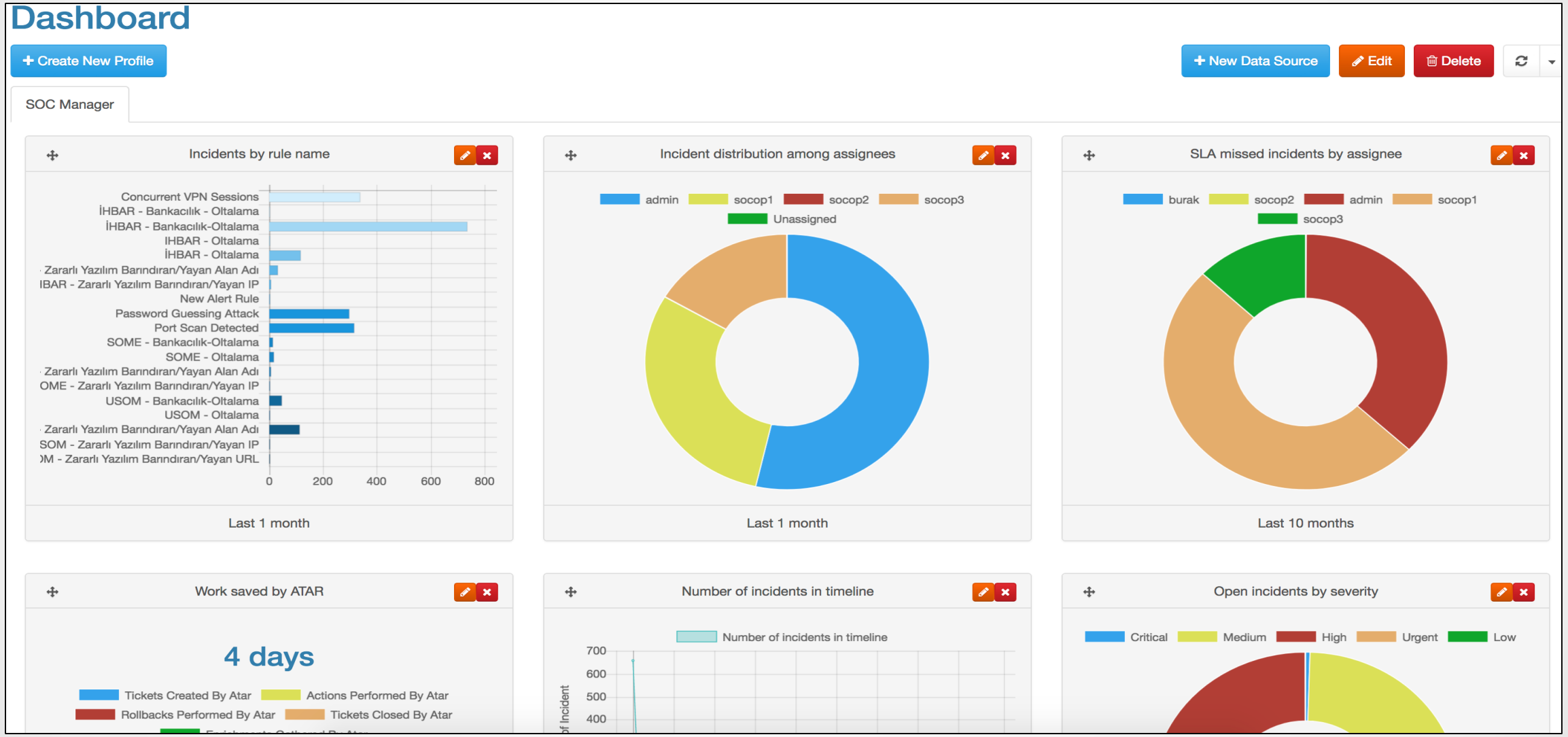
Örnek Otomasyon Senaryosu



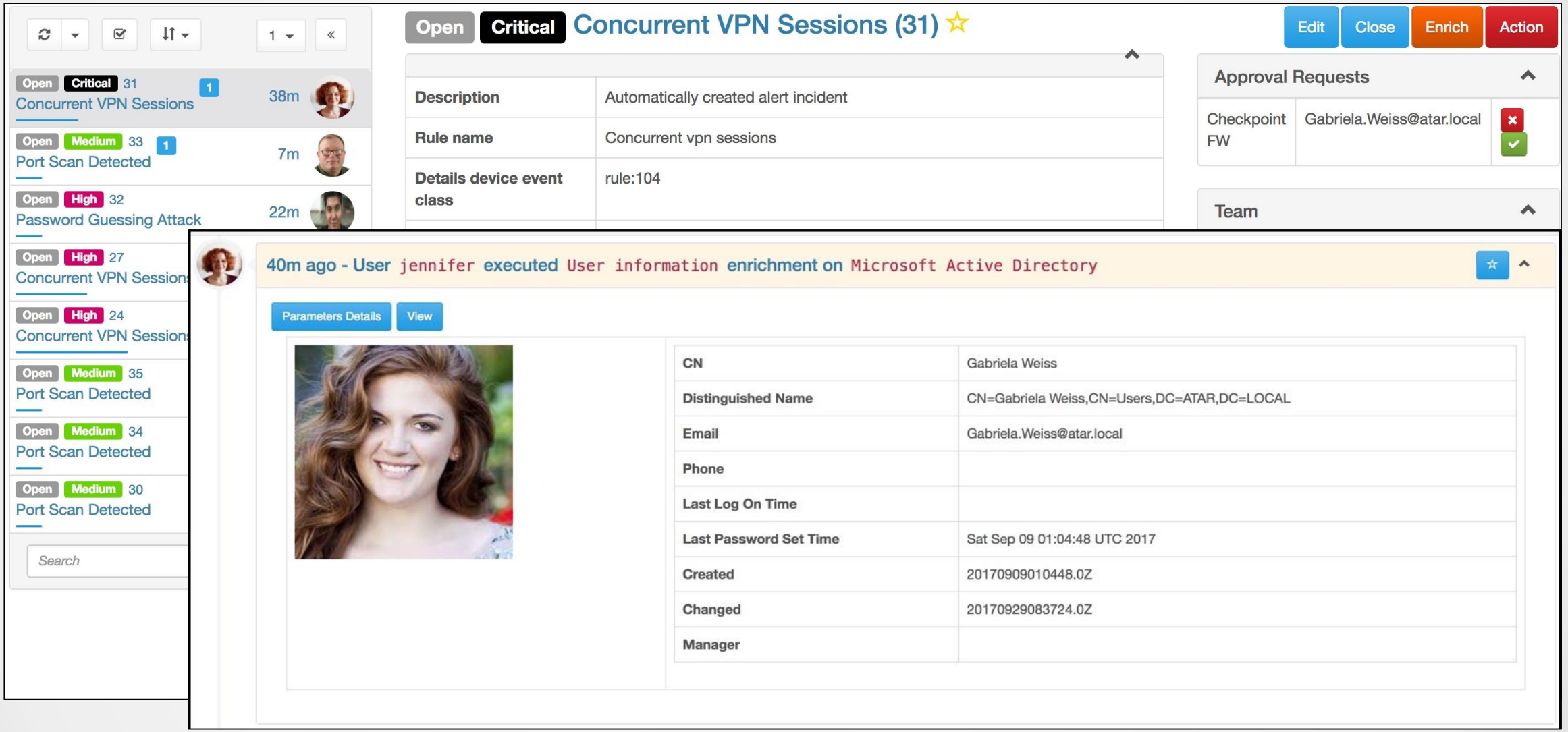
innovera
We enable.

atarlabs

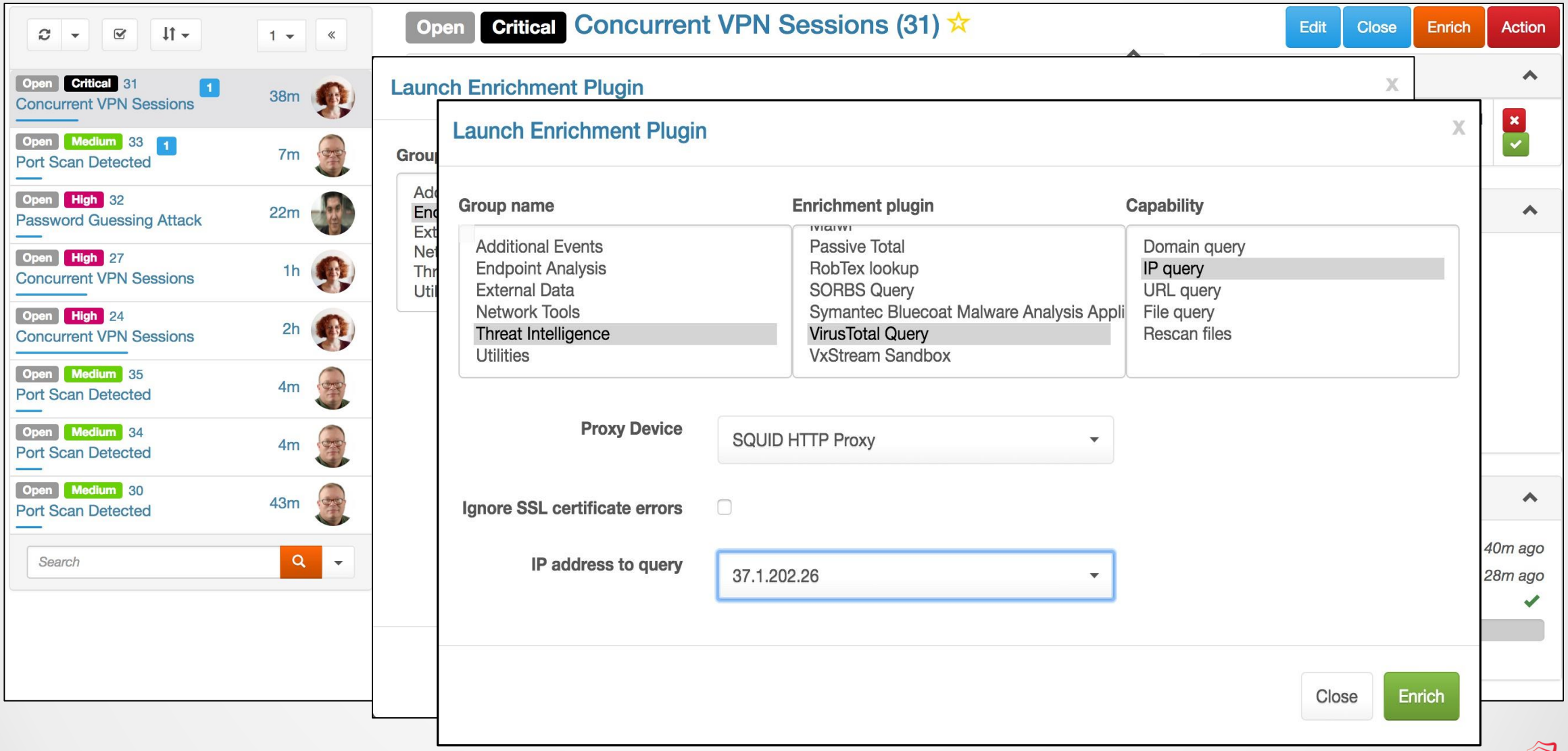
SOME İzleme Duvarı



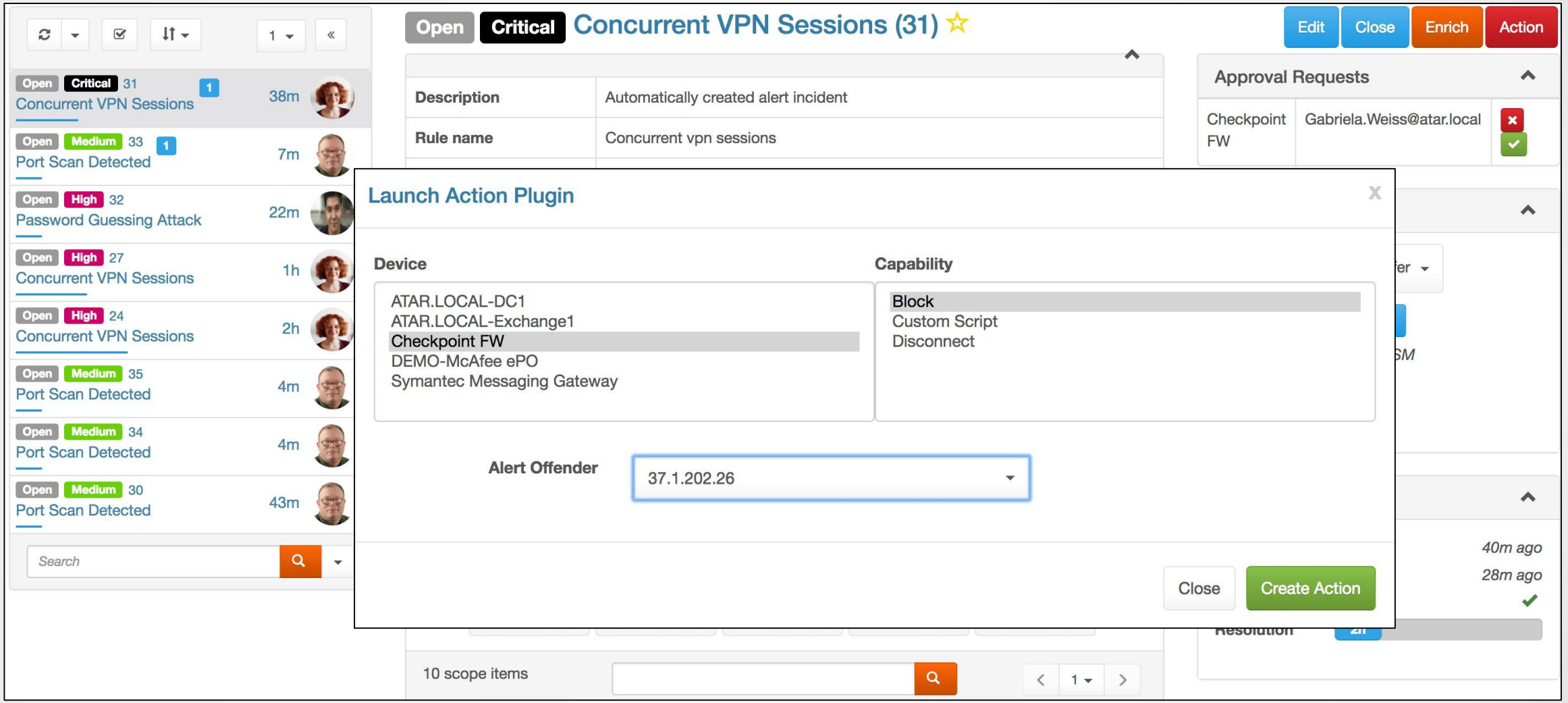
Olay Soruşturma Arayüzü



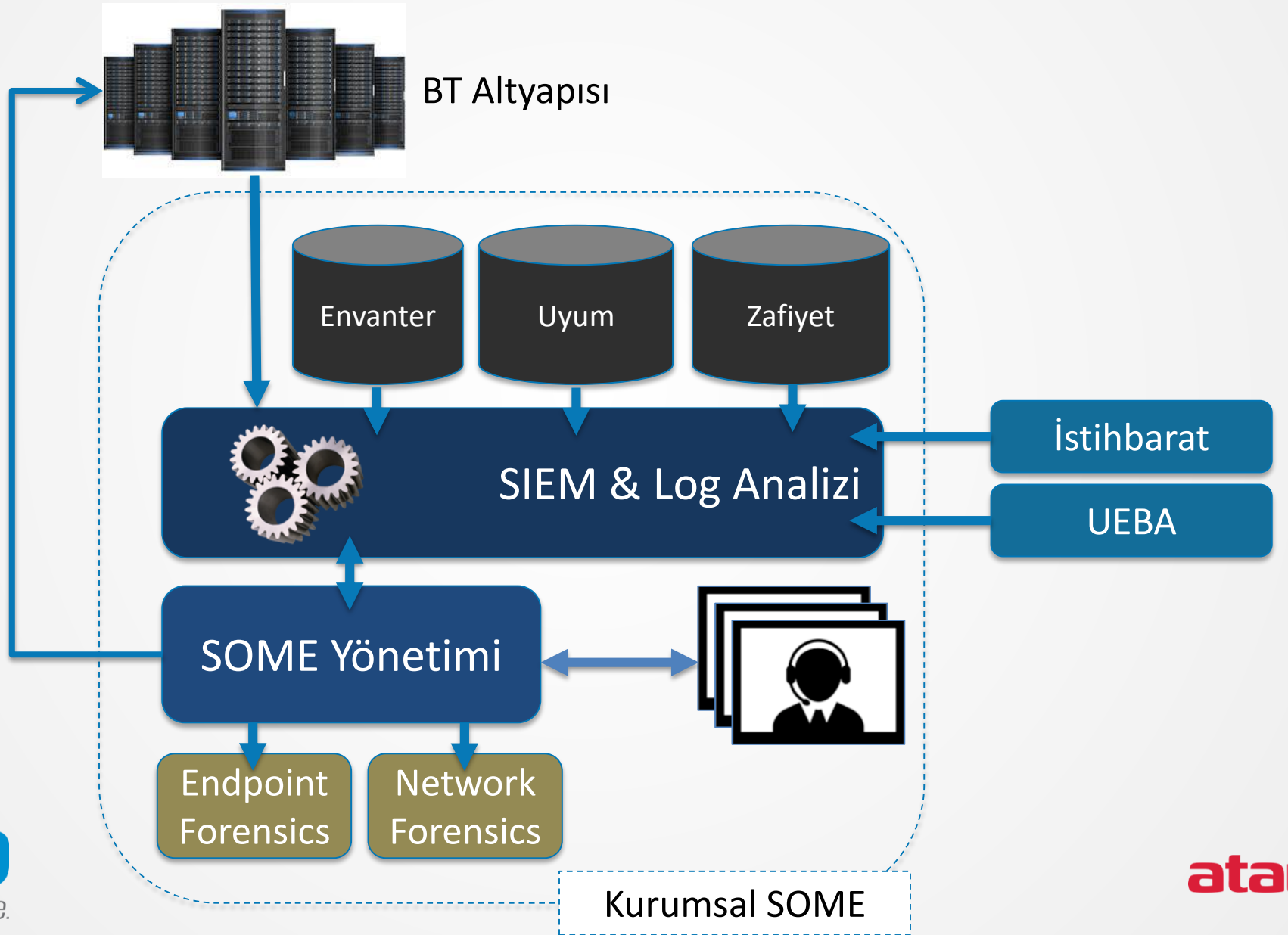
Tek Tuşla Delil Toplama



Tek Tuşla Aksiyon Alabilme



SOME Teknoloji Referans Modeli



innovera
We enable.

atarlabs

Gelin SOME’nizi Aktif Hale Getirelim!

Gelin SOME’nizi Aktif Hale Getirelim!