

SOME Bulmacasından Çıkış Var Mı?

Burak DAYIOĐLU



Siber Güvenliğin Evrimsel Gelişimi



İnceleme ve Yanıt

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



Tespit

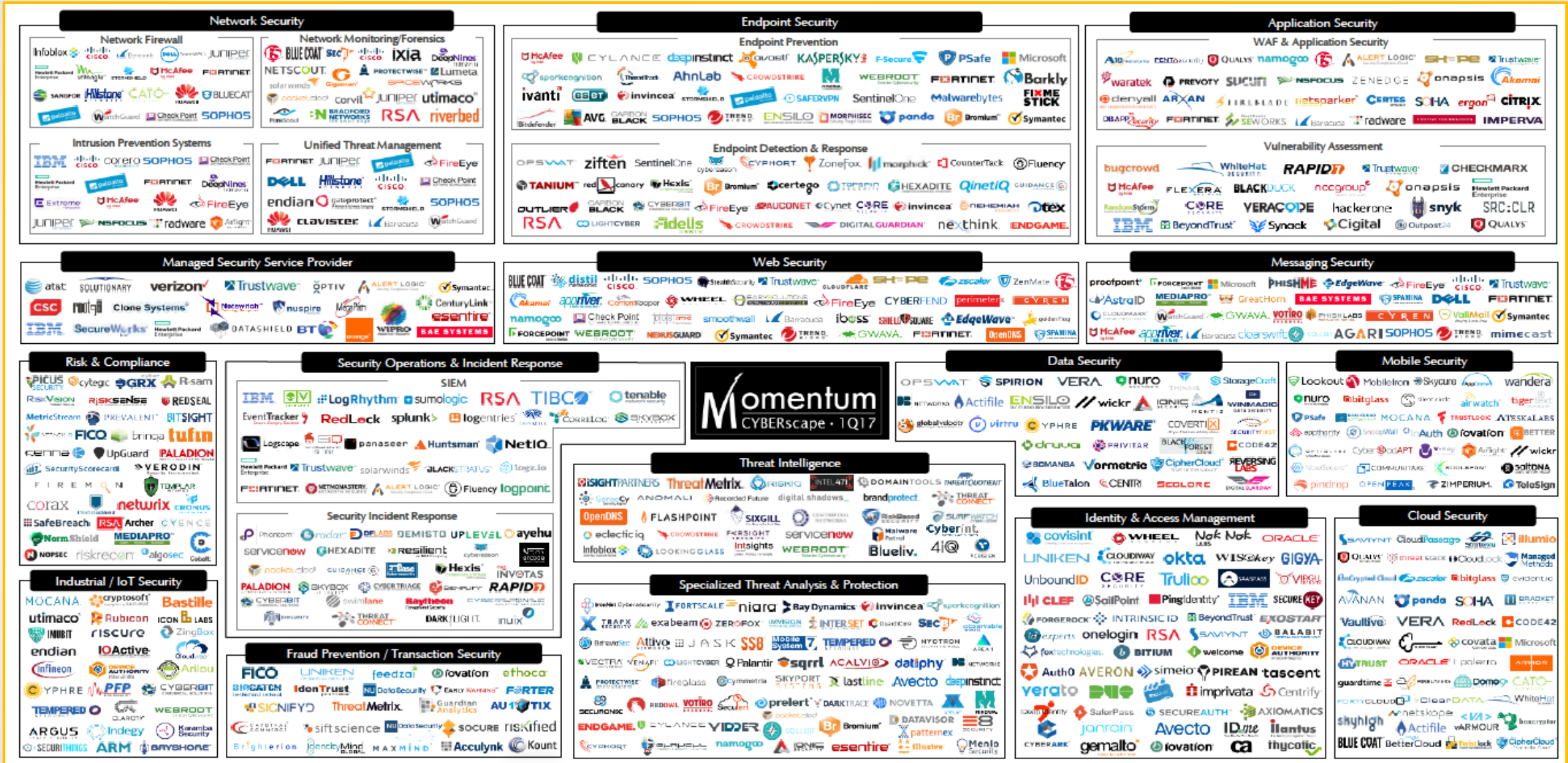
Belki tüm saldırıları durduramayız ama durduramadıklarımızda alarm alıp inceleysek?



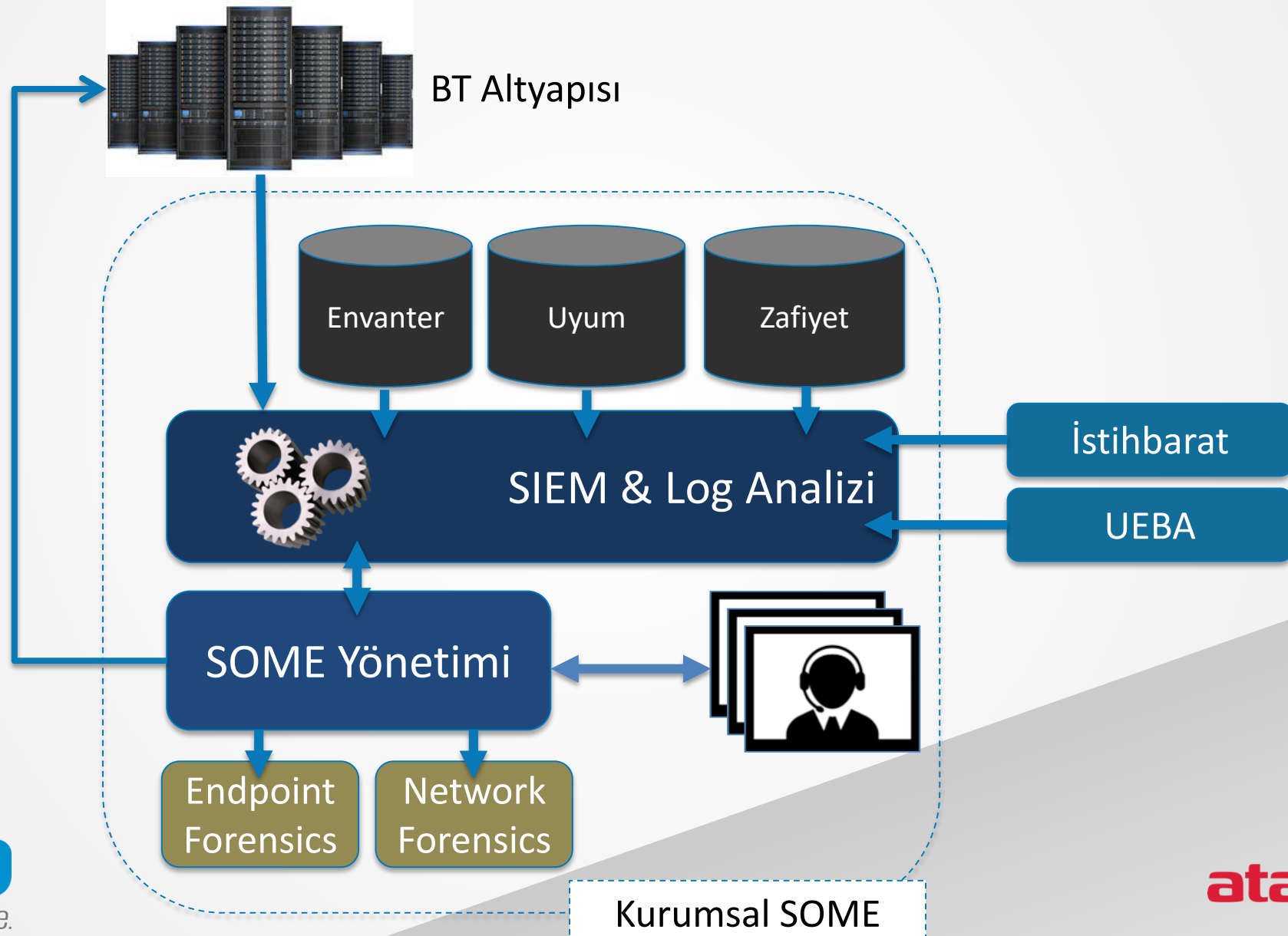
Engelleme

Bu 7-8 katman sayesinde tüm saldırıları durduracağız

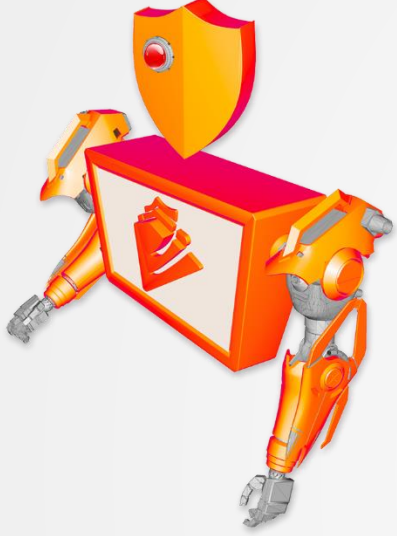
Siber Güvenlik Üretici Haritası



SOME Teknoloji Referans Modeli

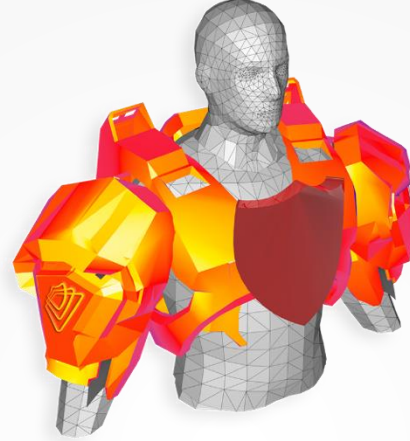


Güvenlik Operasyonu için ATAR



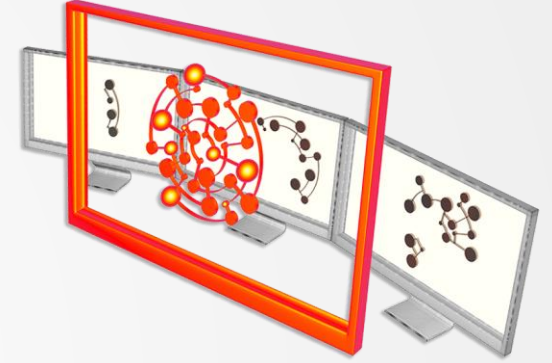
TEKRAR EDENLERİ OTOMATİKLEŞTİR

- 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

ATAR Entegrasyonları

acunetix



ARBOR
NETWORKS



BLUE COAT



FORTINET



JUNIPER
NETWORKS



KASPERSKY



ORACLE



Robtex



SORBS



vmware

VOLATILITY
FOUNDATION



Örnek Otomasyon Senaryosu



SOME İzleme Duvarı

Dashboard

+ Create New Profile

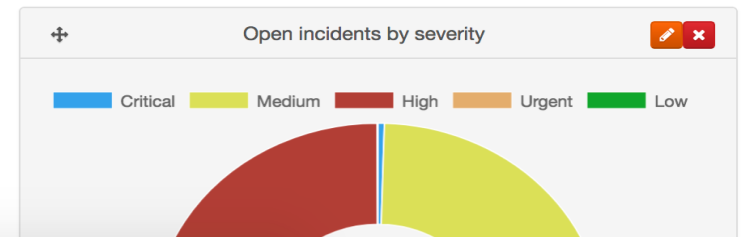
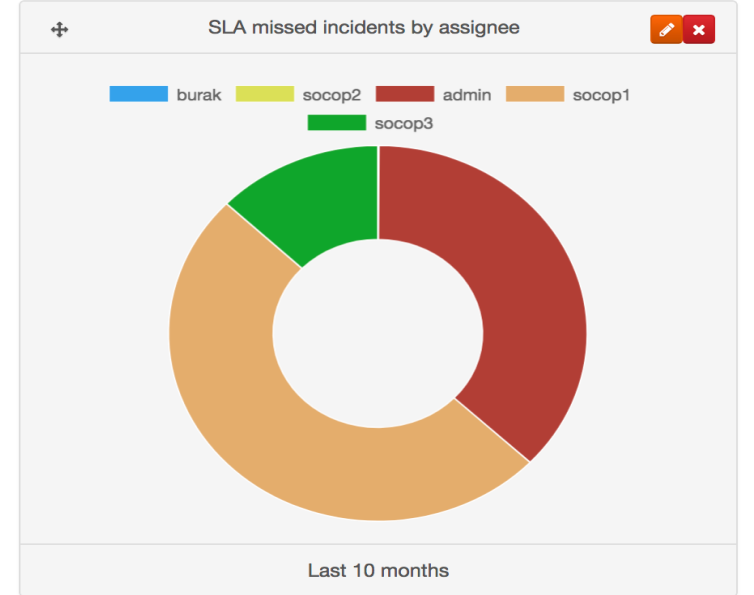
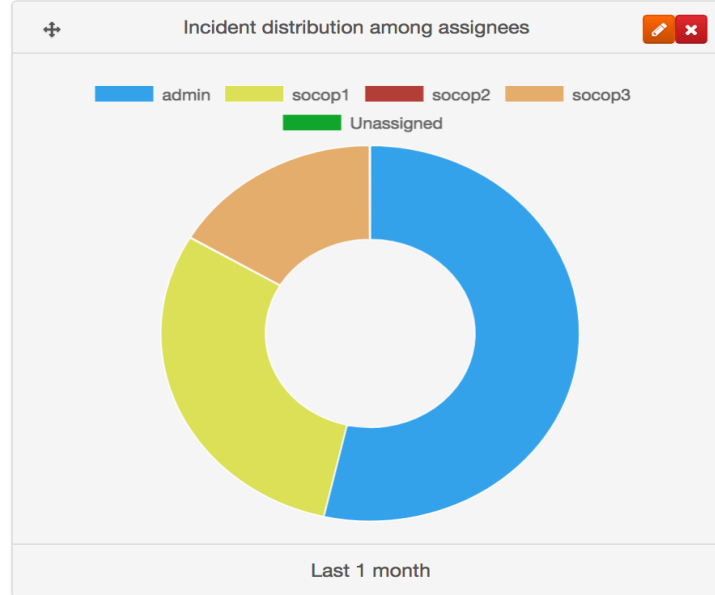
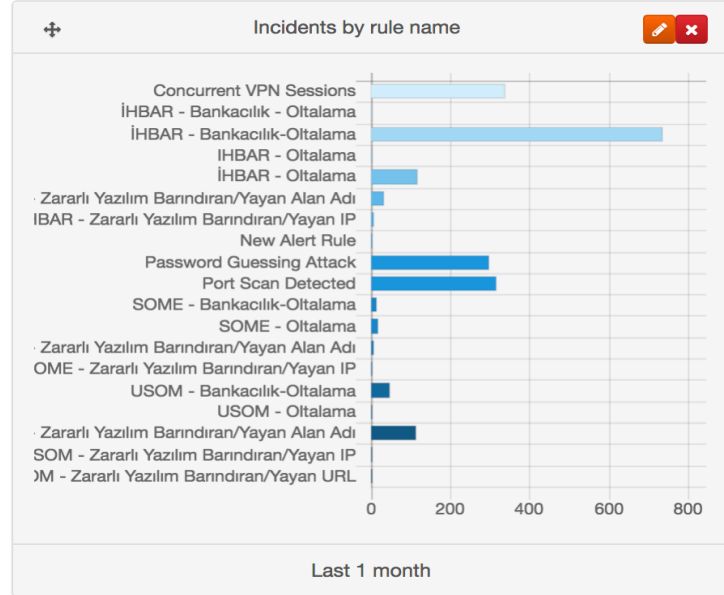
+ New Data Source

Edit

Delete



SOC Manager



Olay Soruşturma Arayüzü

Open Critical Concurrent VPN Sessions (31) ☆

Open Critical 31 38m

Open Medium 33 7m

Open High 32 22m

Open High 27

Open High 24

Open Medium 35

Open Medium 34

Open Medium 30

Search

Description Automatically created alert incident

Rule name Concurrent vpn sessions

Details device event class rule:104


Approval Requests

Checkpoint FW	Gabriela.Weiss@atar.local	✕	✓
---------------	---------------------------	---	---

Team

40m ago - User jennifer executed User information enrichment on Microsoft Active Directory

Parameters Details View

	<table><tr><td>CN</td><td>Gabriela Weiss</td></tr><tr><td>Distinguished Name</td><td>CN=Gabriela Weiss,CN=Users,DC=ATAR,DC=LOCAL</td></tr><tr><td>Email</td><td>Gabriela.Weiss@atar.local</td></tr><tr><td>Phone</td><td></td></tr><tr><td>Last Log On Time</td><td></td></tr><tr><td>Last Password Set Time</td><td>Sat Sep 09 01:04:48 UTC 2017</td></tr><tr><td>Created</td><td>20170909010448.OZ</td></tr><tr><td>Changed</td><td>20170929083724.OZ</td></tr><tr><td>Manager</td><td></td></tr></table>	CN	Gabriela Weiss	Distinguished Name	CN=Gabriela Weiss,CN=Users,DC=ATAR,DC=LOCAL	Email	Gabriela.Weiss@atar.local	Phone		Last Log On Time		Last Password Set Time	Sat Sep 09 01:04:48 UTC 2017	Created	20170909010448.OZ	Changed	20170929083724.OZ	Manager	
CN	Gabriela Weiss																		
Distinguished Name	CN=Gabriela Weiss,CN=Users,DC=ATAR,DC=LOCAL																		
Email	Gabriela.Weiss@atar.local																		
Phone																			
Last Log On Time																			
Last Password Set Time	Sat Sep 09 01:04:48 UTC 2017																		
Created	20170909010448.OZ																		
Changed	20170929083724.OZ																		
Manager																			

Tek Tuşla Delil Toplama

Open Critical Concurrent VPN Sessions (31) ☆

Edit Close Enrich Action

Launch Enrichment Plugin

Group name	Enrichment plugin	Capability
Additional Events	Passive Total	Domain query
Endpoint Analysis	RobTex lookup	IP query
External Data	SORBS Query	URL query
Network Tools	Symantec Bluecoat Malware Analysis Appli	File query
Threat Intelligence	VirusTotal Query	Rescan files
Utilities	VxStream Sandbox	

Proxy Device: SQUID HTTP Proxy

Ignore SSL certificate errors:

IP address to query: 37.1.202.26

Close Enrich

Open Critical 31 38m

Concurrent VPN Sessions

Open Medium 33 7m

Port Scan Detected

Open High 32 22m

Password Guessing Attack

Open High 27 1h

Concurrent VPN Sessions

Open High 24 2h

Concurrent VPN Sessions

Open Medium 35 4m

Port Scan Detected

Open Medium 34 4m

Port Scan Detected

Open Medium 30 43m

Port Scan Detected

Search

40m ago

28m ago

✓

Tek Tuşla Aksiyon Alabilme

The screenshot displays a security dashboard interface. On the left, a list of incidents is shown with columns for status (Open), severity (Critical, Medium, High), count, and time. The main area shows a selected incident: 'Concurrent VPN Sessions (31)' with a 'Critical' severity. Below this, a table lists the incident's description and rule name. On the right, there are buttons for 'Edit', 'Close', 'Enrich', and 'Action', along with an 'Approval Requests' section showing a request from 'Gabriela.Weiss@atar.local'. A modal window titled 'Launch Action Plugin' is open, showing a list of devices and capabilities. The 'Alert Offender' field is set to '37.1.202.26'. At the bottom of the modal are 'Close' and 'Create Action' buttons.

Open Critical Concurrent VPN Sessions (31) ☆ [Edit] [Close] [Enrich] [Action]

Description	Automatically created alert incident
Rule name	Concurrent vpn sessions

Approval Requests

Checkpoint FW	Gabriela.Weiss@atar.local	[X] [✓]
---------------	---------------------------	---------

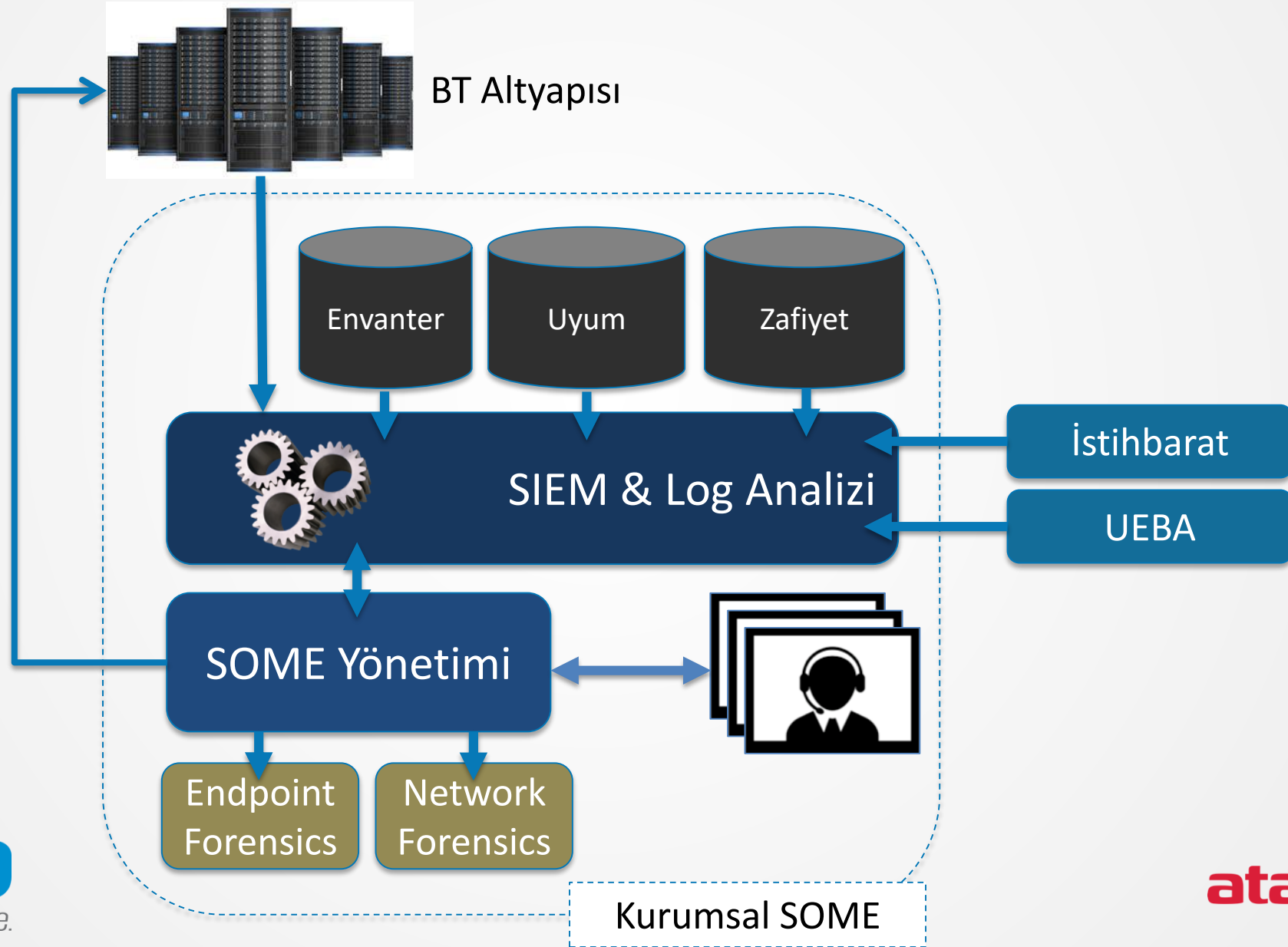
Launch Action Plugin

Device	Capability
ATAR.LOCAL-DC1	Block
ATAR.LOCAL-Exchange1	Custom Script
Checkpoint FW	Disconnect
DEMO-McAfee ePO	
Symantec Messaging Gateway	

Alert Offender: 37.1.202.26

[Close] [Create Action]

SOME Teknoloji Referans Modeli



Gelin SOME'nizi Aktif Hale Getirelim!



Gelin SOME'nizi Aktif Hale Getirelim!

