IBM

Security Summit 2019

Istanbul

A Real Life SOC Journey, Yapi Kredi Bank

Who am I?

~10 Years IT Security Experience

Bahçeşehir University – MIS (Managed Information Systems)

Yıldız Technical University – Computer Engineering

Yapi Kredi Bank – IT Security Incident Management Unit Manager (~2 Years)

Yapi Kredi Bank – IT Security Incident Management Specialist (~2 Years)

Garanti Bank – Network Security Platform Specialist (~3,5 Years)

Doğan Gazetecilik – IT Security Specialist (~2,5 Years)

Agenda

- **Cyber Security Challenges**
- Real Scenarios

Cost of a Data Breach

How long is the lifecycle of a data breach?

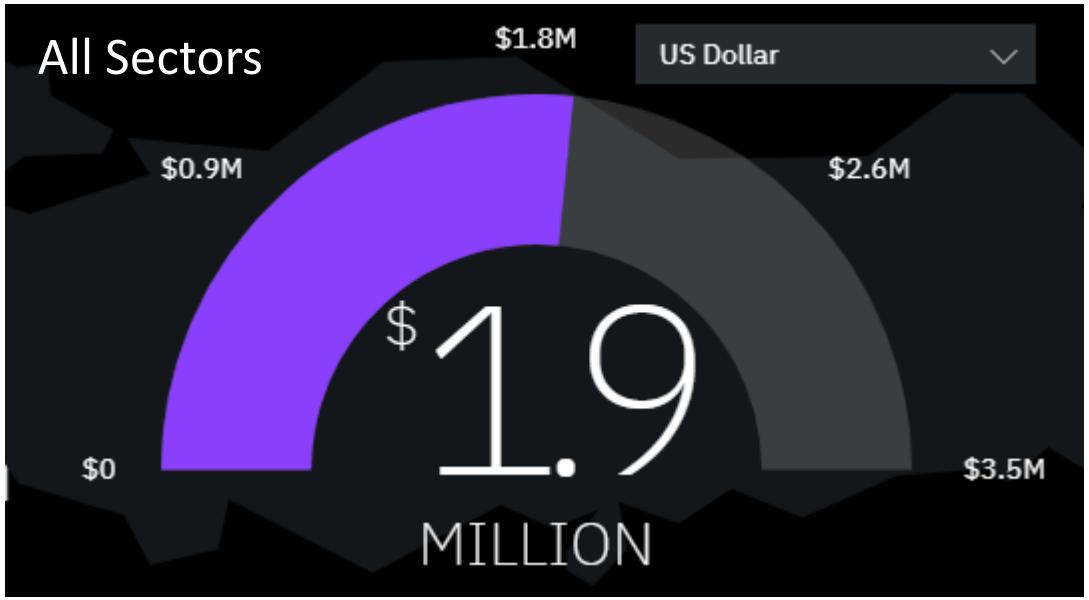
The type of breach, your industry, region, and organizational structure all factor into how long it takes to identify and ultimately contain a data breach.

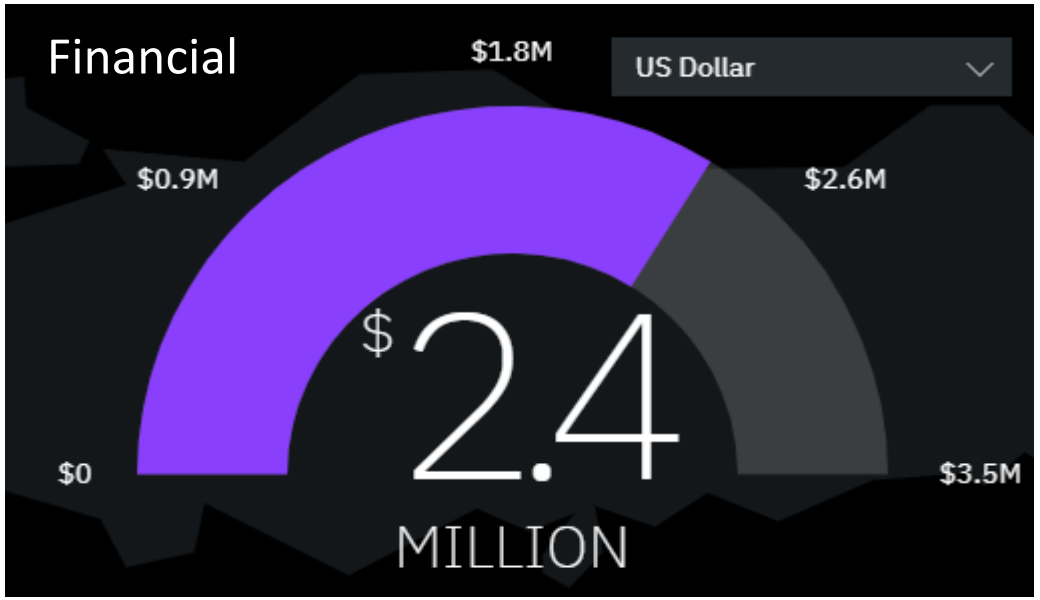
279 Days
Average time to identify and contain a breach

314 Days
Lifecycle of a malicious attack from breach to containment

$1.2 M
A breach lifecycle under 200 days costs $1.2 million less than a lifecycle over 200 days

Cost of a Data Breach in Turkey





*IBM Security and Ponemon Institute release the 2019 edition of the Cost of a Data Breach Study

SOC Defined

- A security operations center provides centralized and consolidated cybersecurity incident prevention, detection and response capabilities.

- SOC involves **PEOPLE** and **PROCESSES**, which are in fact MORE IMPORTANT than **tools**.

Reminder: SOC = People, process and technology (so, no "SOC vendors")

PROCESS

PEOPLE

TECHNOLOGY

Technology – IBM QRadar

To Detect you have to see…

SIEM Infrastructure

- 170K EPS, 2M FPM License
- Daily ~3.3 Billion Log
- Daily ~5TB Data Ingest
- Totally ~800TB Hot Data
- 7.500+ Log Source
- 300+ Use Case
- 10+ Custom Integration

Technology – IBM Resilient

Alert overload dilemma…

SOAR Infrastructure

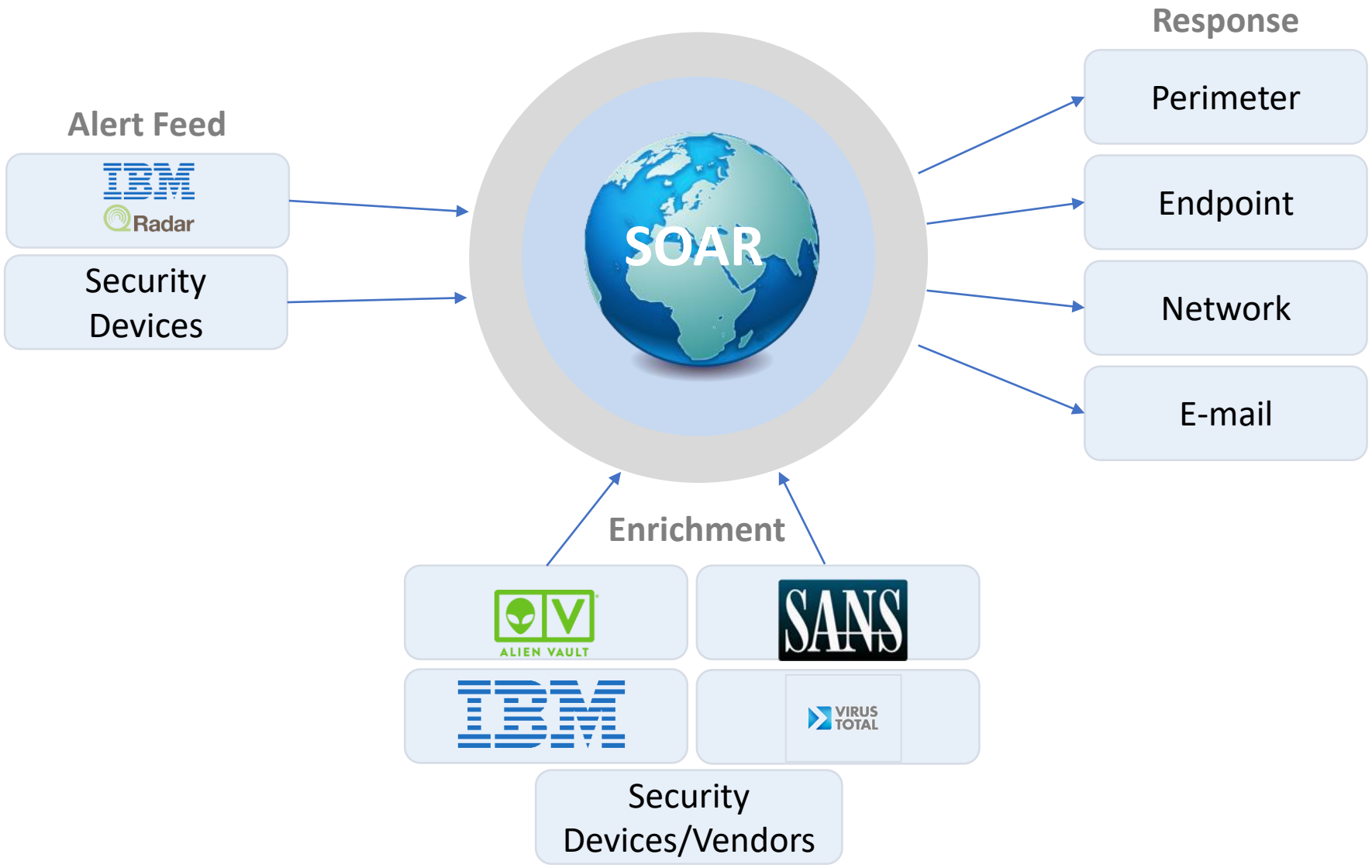
- 40 User license
- All Incidents are centralized
- 40+ Integration, 5+ bidirectional integration
- All incident categories are standardized
- 15+ playbook implemented

Agenda

- Cyber Security Challenges
- **Real Scenarios**

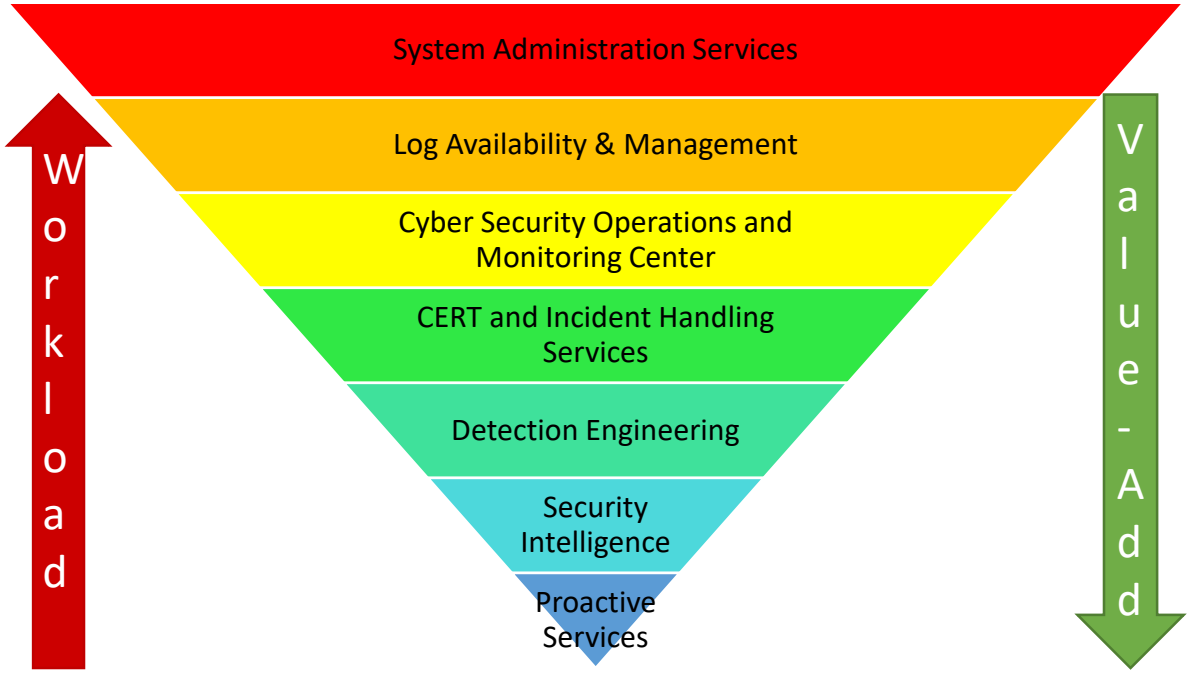
Real Scenario – SOC Triage & Automation

- Automatic Triage based on **custom criterias**
- Effective management of Hybrid Model SOC with **standardized playbooks** and **centralized incident response platform**
- Data Enrichment processes are automated, **%25 of incident investigation** time saved
- Integrated incident response on **4** different **countries infrastructure**

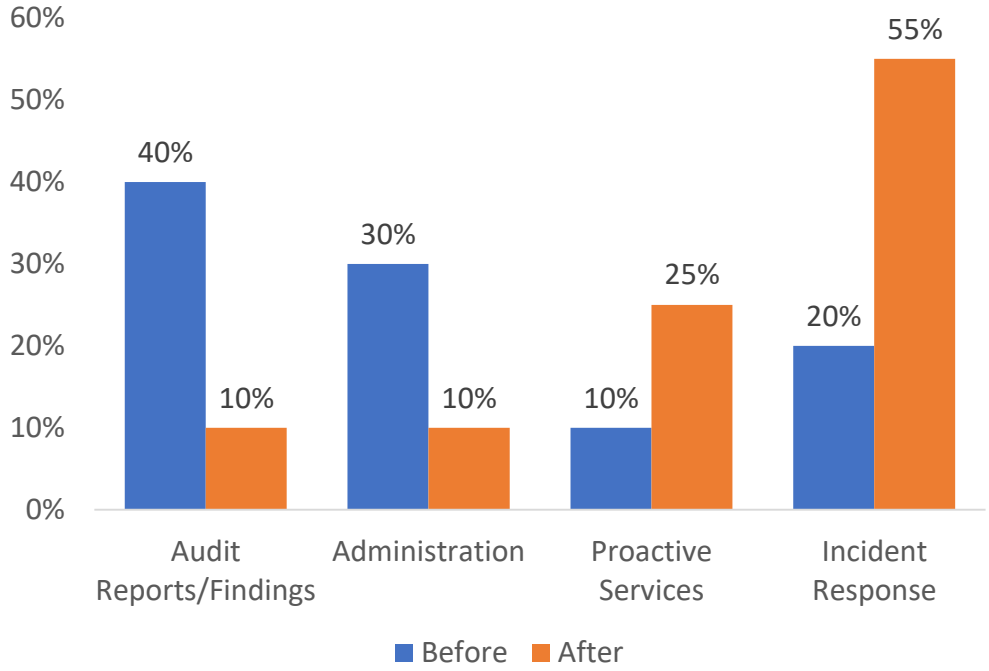


Real Scenario – Effectiveness of SOC

- SOC have to focus on **differentiating services**
- Other SOC functions such as **Threat Intel, Log Management and Threat Hunting** playbooks implemented



- Effective **reporting** and **SLA/KPI** calculation
- %80 of **workload automated**
- **%80** of YapiKredi 7x24 **SOC Operations** automated
- Times saved on **%90 of security actions**



Real Scenario – Maturing Threat Intel Program

- Combine information from external sources, internal events and specific Financial related threats **to increase detection** capabilities and stop attackers earlier in the attack life cycle

- Proactively discover intrusions and intrusion attempts by using Threat Intelligence **to respond effectively** in a **shorter period of time**

- Align with our IBM Resilient platform so **TI alerts** turn into **incidents**

Threat Intelligence Maturity Levels

Real Scenario – Log Source & Asset Management

- Total of 7.500+ log source feeding into SIEM
- Unix/Windows log source management is **automated**
- **Ticket management** for auditing and fast response capability
- Automated QRadar **asset criticality management** with CMDB data through Resilient Platform

What we learned?

- SOC involves **People** and **Processes**, which are in fact **more important** than **tools**.
- The hardest part of SIEM is **Log Source Continuity Management**
- Incident Response Platform gives **a single pane of glass for monitoring all incidents** and provides **task management**
- As the **cybersecurity skills gap** is present, automating as much work as possible allows us to **use limited resources more efficiently**
- Incident Response Platform is **not a plug and play tool,** you have to customize based on your tools and SOC model


Questions?