



Effectiveness of SIEM SOC in protecting critical information Assets'

ISC2+ISACA Conference
11th October 2018

Presenters:

Roshan Sherifudeen MBA, CISA, CISM, CRISC, PCIP, CEH, ISO27K LA

Ernst & Young Management Consulting GmbH

DIGITAL TRANSFORMATION IS CHANGING EVERYTHING



CLOUD COMPUTING

INTERNET OF THINGS

ANALYTICS

ARTIFICIAL INTELLIGENCE

ROBOTICS

BLOCKCHAIN



EMERGING MARKETS



PERSONAL



TRANSPORT



BUILDINGS & CITIES



HOME



GOVERNMENT



MEDICAL



ENVIRONMENTAL



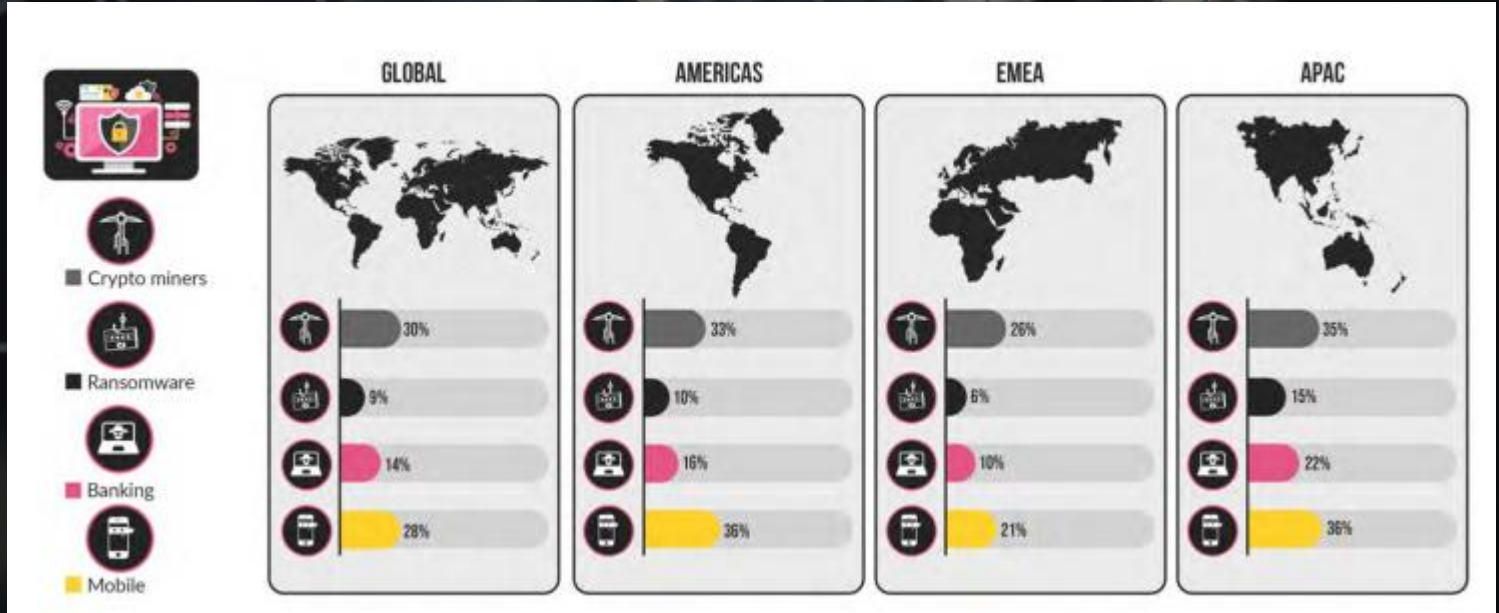
INFRASTRUCTURE



INDUSTRIAL

Cyber Security challenges

Understanding the ever changing threat landscape

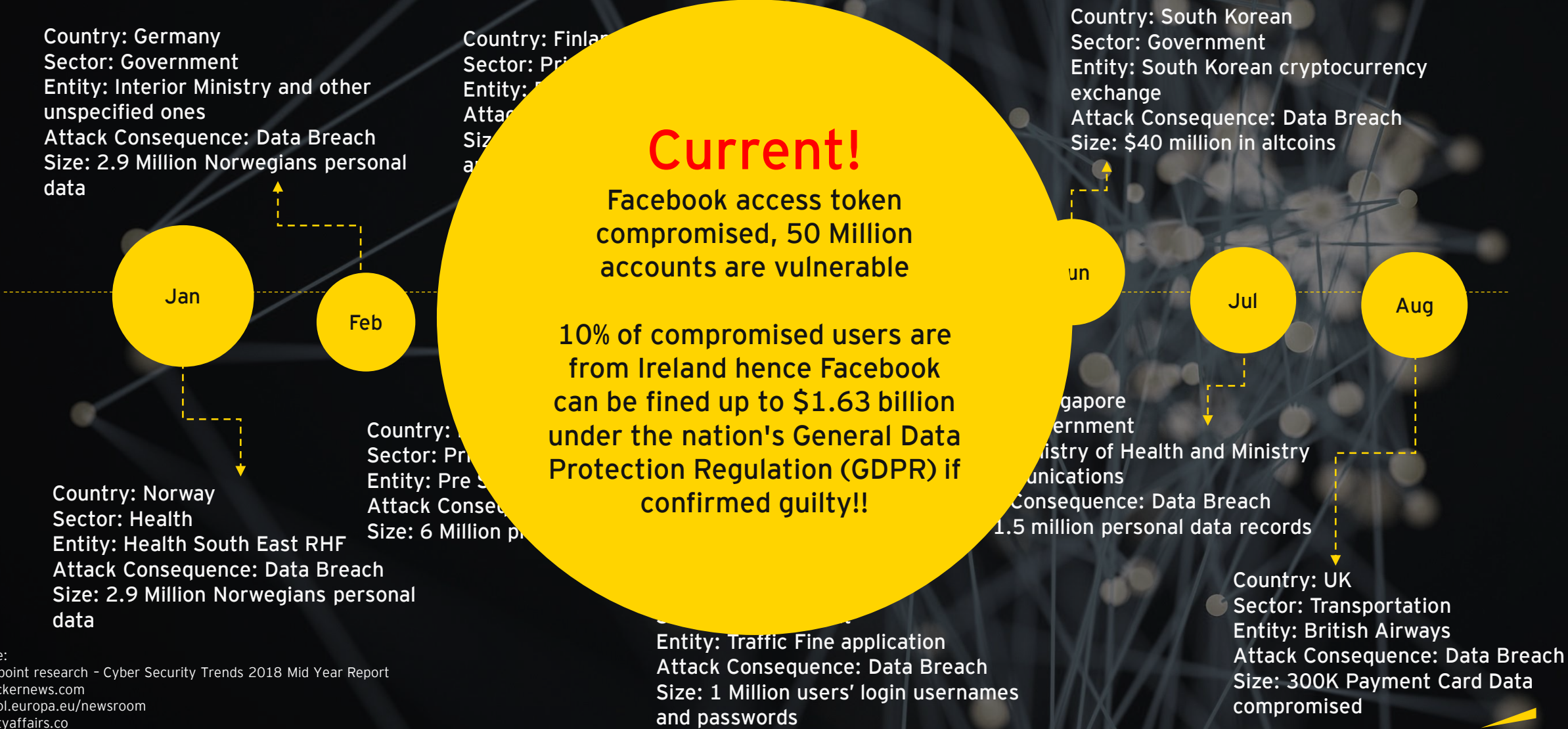


Source: Checkpoint research - Cyber Security Trends 2018 Mid Year Report

Check Point Research indicates **CRYPTO MININERs** are on the rise



EMEA 2018 Attack Timeline

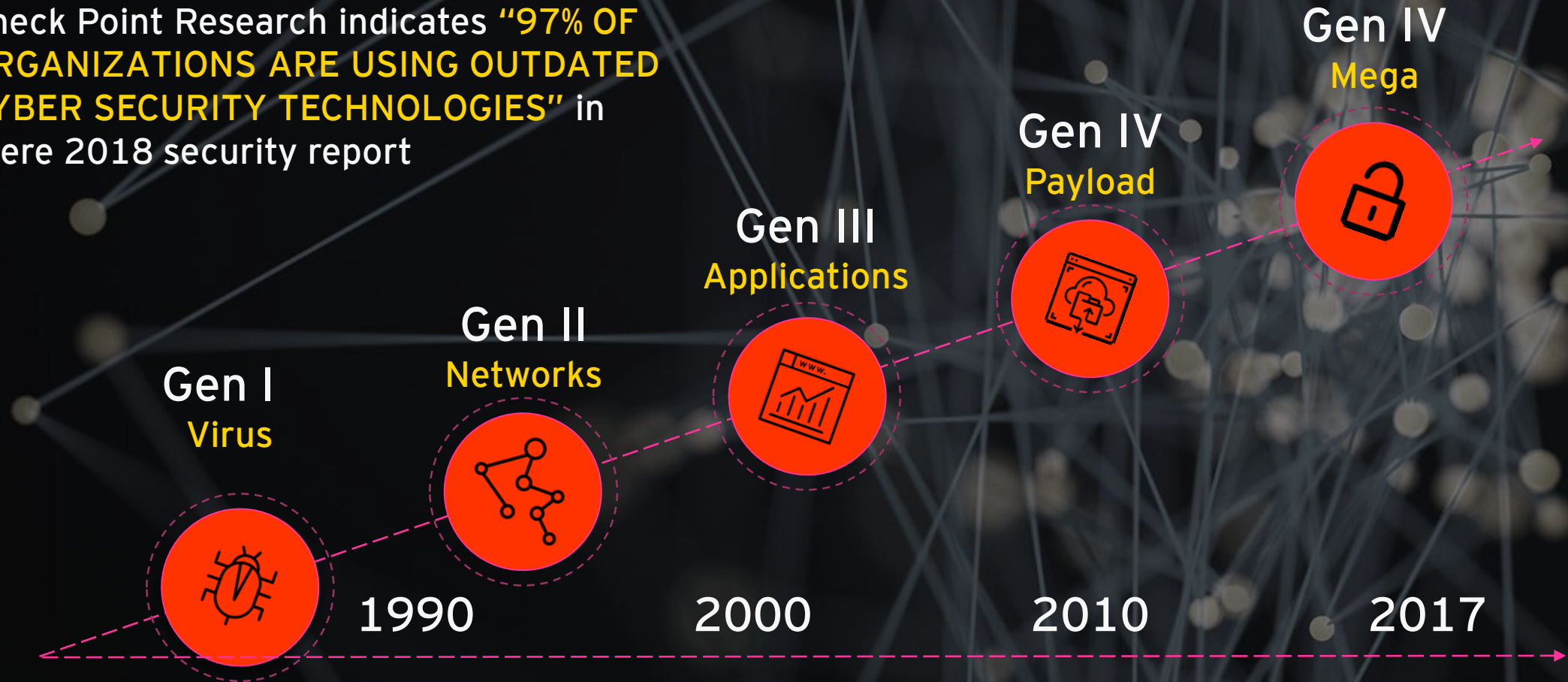


Source:
 Checkpoint research - Cyber Security Trends 2018 Mid Year Report
thehackernews.com
europol.europa.eu/newsroom
securityaffairs.co
theguardian.com
ncsc.gov.uk



Attack Evolution

Check Point Research indicates **"97% OF ORGANIZATIONS ARE USING OUTDATED CYBER SECURITY TECHNOLOGIES"** in there 2018 security report



Source: Checkpoint research - 2018 Security Report

Security Information & Event Management and Security Operations

Assets

Technology



Information Assets



SIEM

Technology



Security Log collect and store



Correlate and alert



SOC

People, Process



response and remediate



Analyse and report

Stakeholder Expectations

The various stakeholders have differing expectations as to what the SIEM SOC should give rise to!



BUSINESS

Cyber attacks that target our core business are responded to in a timely manner in order to reduce the impact



BOARD

What is our return on investments in people, process and technology to protect information assets



SECURITY

Identifying internal and external threats to safeguard the organization's interest



IT

Identify threats related to my technology platform so that I can serve my business



CUSTOMERS

The information that I have shared with the organization is adequately protected from internal and external attacks - Digital trust

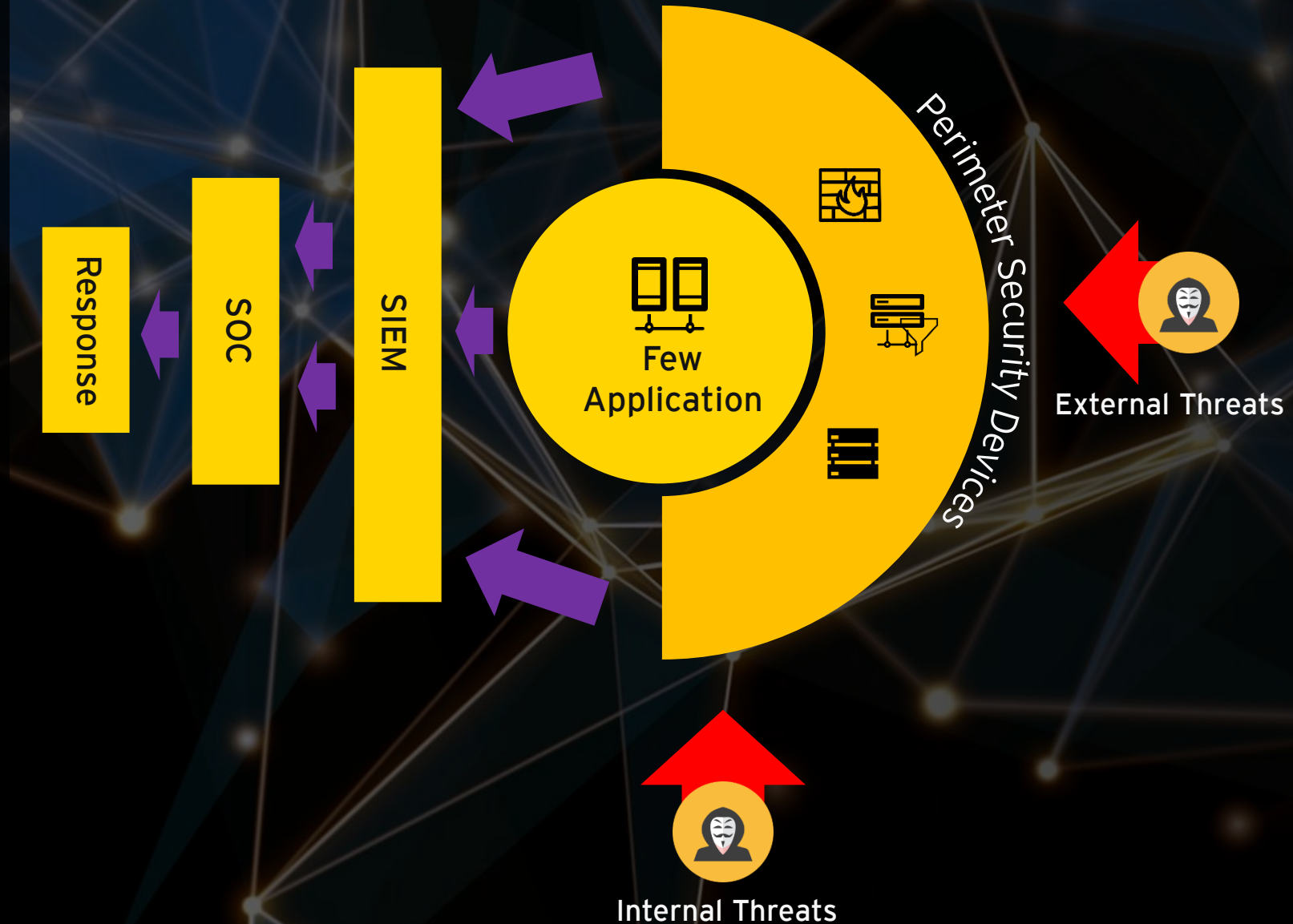


REGULATORS

What measures companies have taken to protect customer information and ensure compliance with applicable laws

Traditional SIEM Security Operation

- Monitor few assets without **business or threat** view
- Implementing **default use-case**
- Partial monitoring
- **Reactive response** model
- Monitoring using dual role resources
- Resources with **limited skills**
- Less or no **innovation** and adoption to new monitoring technologies



The traditional strategy involves securing the perimeter, integrating a few important applications and building default use cases. However, receiving the best benefits from your SIEM SOC requires considering a multi-dimensional approach.

What is a **multi-dimensional** SIEM SOC strategy?

BUSINESS CONTEXT

A clear understanding of threats that affect the business operation

SECURITY CONTEXT

What information is needed to identify the threats that are affecting the business

TECHNOLOGY CONTEXT

Selection of the right technology that fits the purpose

PROCESS CONTEXT

Defining, streamlining and testing processes to support operations and incident response

PEOPLE CONTEXT

Training and awareness of cyber security and incident handling

GOVERNANCE CONTEXT

A strong governance with direct leadership supervision

EXTERNAL CONTEXT

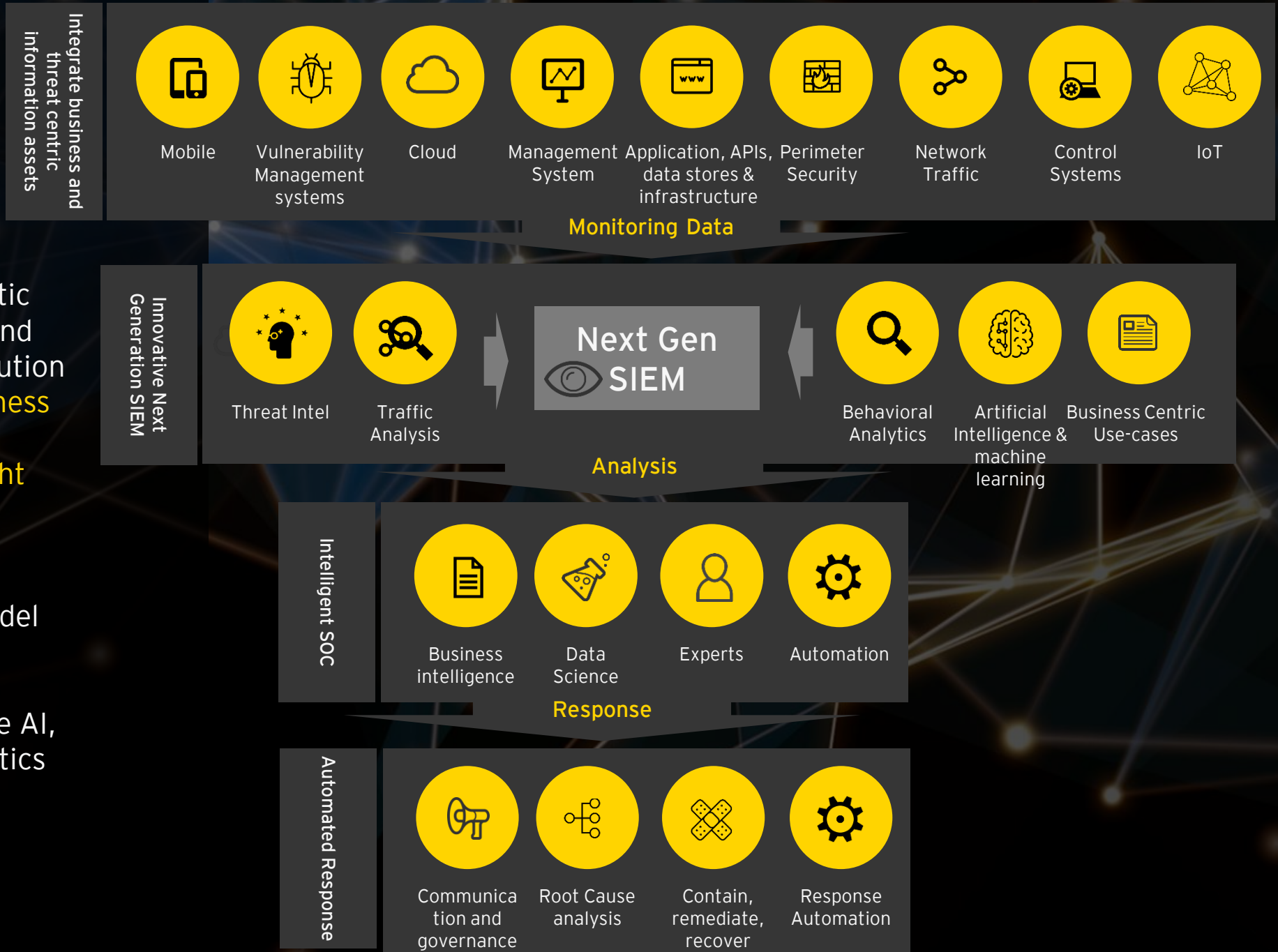
Consider the legal, regulatory and compliance aspects as non-functional requirements

INTERNAL CONTEXT

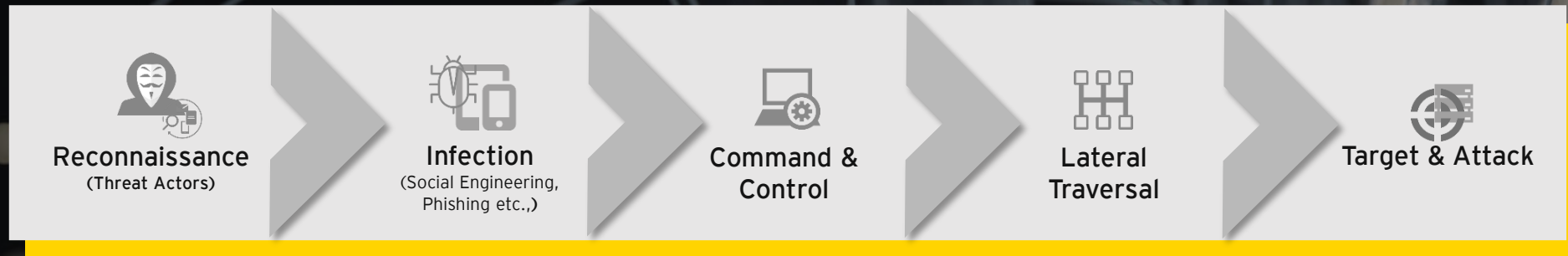
Consider adherence to internal policies, staff council agenda, contracts, etc.

Next Gen SIEM View

- SIEM SOC is part of holistic cyber security strategy and not to see as isolated solution
- Monitor assets with **business and threat** view
- Implementing well **thought through threat centric correlated use-case**
- 24/7 Monitoring
- **Proactive monitoring** model
- Using **automation** for response
- Adopt new **innovation** like AI, Robotics, Behavior analytics etc.
- Holistic cyber view



Modern Threat execution process



“Mean time to **detect** is long”

Signes ignored

Data Lost among
other information

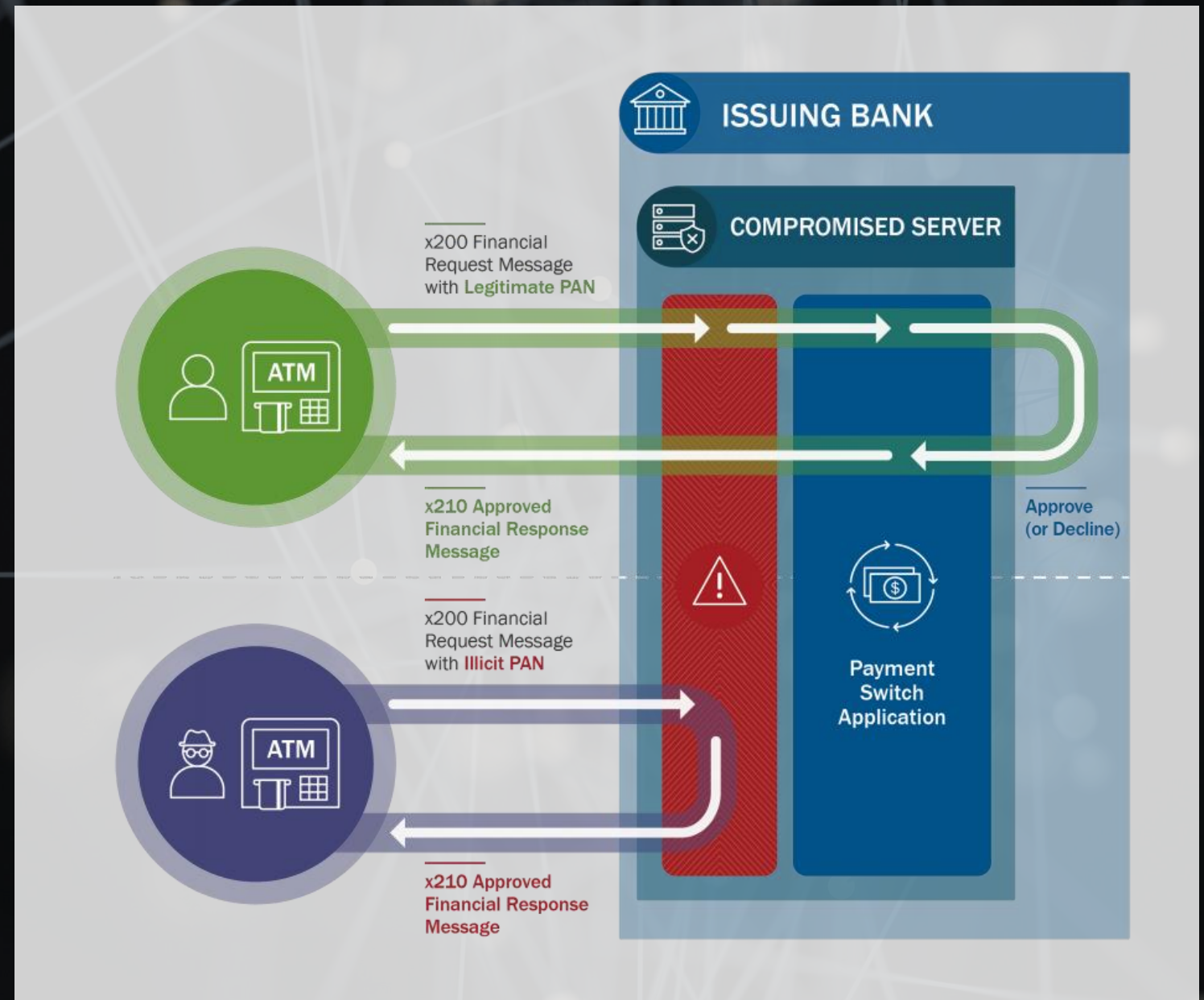
Does not fall under
regular detection
use cases

Right level of log
data are not
collected

Example: “HIDDEN COBRA – FASTCash Campaign”

The US-CERT has released a joint technical alert from the DHS, the FBI, and Treasury warning about a new ATM scheme being used by the prolific North Korean APT hacking group known as Hidden Cobra

Bank Servers Hacked to Trick ATMs into Spitting Out Millions in Cash



“FASTCash Campaign” postmortem

Method:

Spear-phishing emails, containing malicious Windows executable, against employees in different banks

Target:

Banks in Africa and Asia

Vulnerability:

Access and Network exploitation and AIX executables

Threat Actor:


North Korean APT hacking group known as Hidden Cobra.

1. Spear-phishing emails
2. Infect user device and lateral movement of the executable
3. Payment Switch Application is infected with the exploit
4. Inspecting and inbound financial request messages at the transport layer for a particular account numbers using a function
5. The function then check:
If (the incoming PAN is not part of the illicit PAN list)
Then (send the request to issuing bank for processing)
Else (a. drop the message from sending to processing bank
b. malicious code creates a valid response for processing
c. block any declined messages if necessary)


Reconnaissance
(Threat Actors)


Infection
(Social Engineering,
Phishing etc.,)


Command &
Control


Lateral
Traversal


Target & Attack

Key to the fort „Business relevant threat based Use case Modeling“

Threat: Cyber Fraud

Identify threat

- Cyber Fraud that includes phishing, spear phishing, vishing, Walling

Identify logs sources

- Netflow, payment system logs, request and response logs, transaction system logs, change logs

Define the use cases

- Deference between Cash balance in ATM vs total amount of processed transaction by payment banks
- Unauthorized changes to the switch application server
- Transaction pattern anomalies in the payment switch

Define alert rules

- Alert when there is a variation between served amount vs processed amount
- Alert Unauthorized Changes
- Keep the anomalies in the watch list and further carryout investigations

Analyze and Respond

- Analyze and categories the incident
- When a level 1 incident is triggered, suspend the ATMs from operations
- Further Investigate and mitigate
- Communicate to stakeholders

Summary

