Reduce Detection and Response Time by Artificial and Threat Intelligence

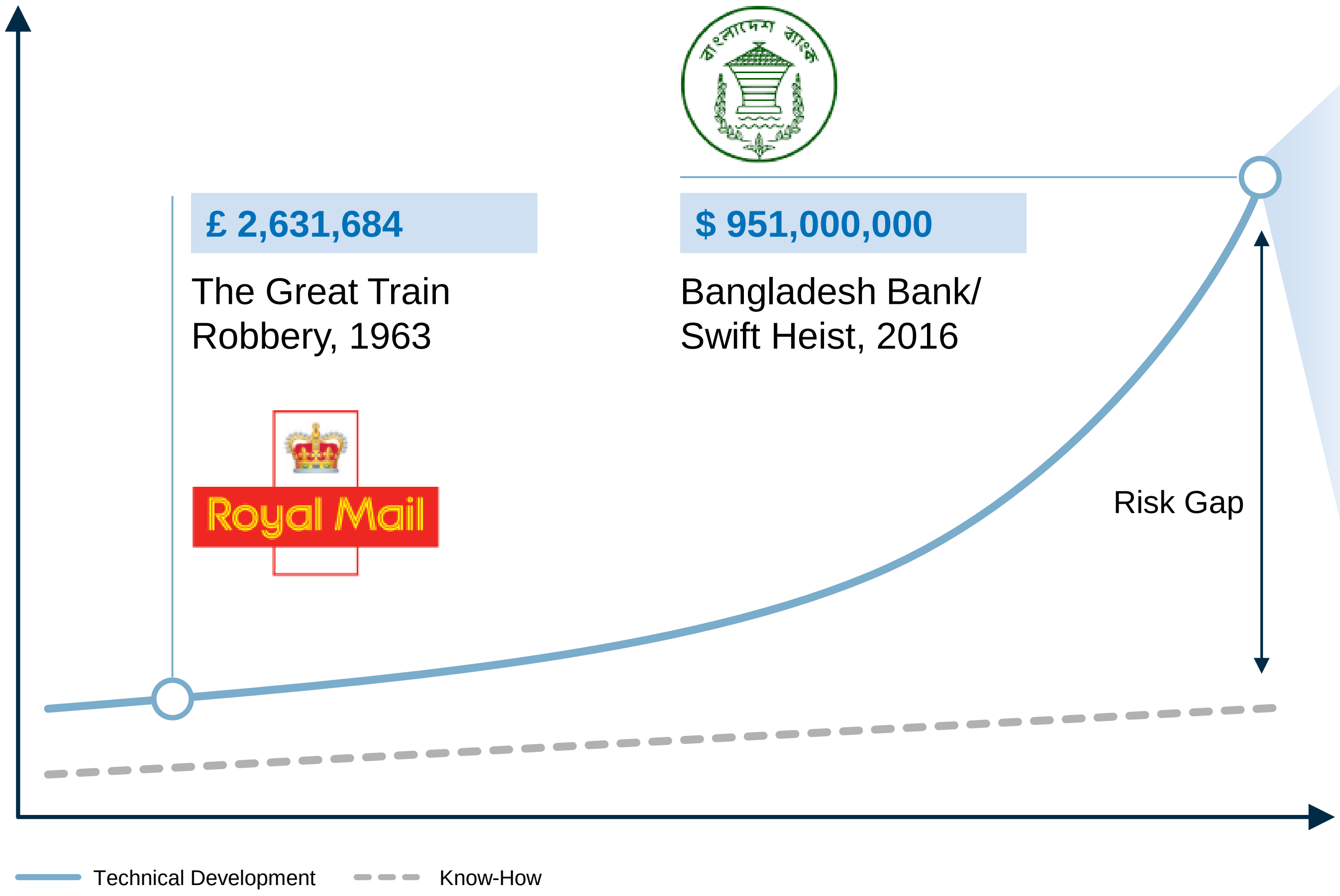
Wolfgang Kiener

Global Head, Advanced Threat Center of Excellence

TÜVRheinland®
Precisely Right.

Who benefits from continues technological evolvement?

Risks develop exponential in the digital transformation.



£ 2,631,684

The Great Train Robbery, 1963

$ 951,000,000

Bangladesh Bank/ Swift Heist, 2016

INDUSTRY 4.0

- Automation in detection and response
- Scalability and Interconnectivity
- AI and Machine Learning
- Agility

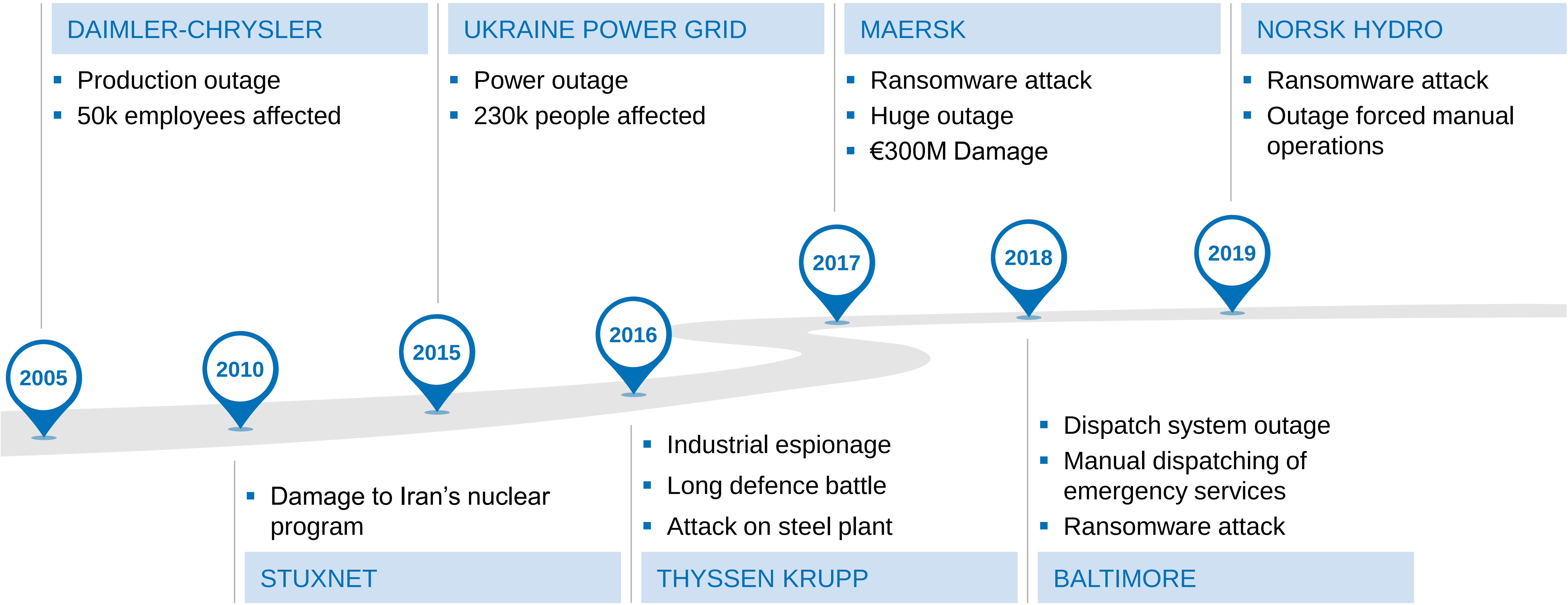
CYBER RISK 4.0

- Attack automation
- AI and Machine Learning
- Attackers are agile
- Complexity increases attack surface
- Vulnerabilities are hardly to avoid

Cyber Risk = Business Risk

Attack frequency and impact is increasing

Attacks impact the business, but more important: attackers target business and safety



2005

DAIMLER-CHRYSLER

- Production outage
- 50k employees affected

2010

STUXNET

- Damage to Iran’s nuclear program

2015

UKRAINE POWER GRID

- Power outage
- 230k people affected

2016

THYSSEN KRUPP

- Industrial espionage
- Long defence battle
- Attack on steel plant

2017

MAERSK

- Ransomware attack
- Huge outage
- €300M Damage

2018

BALTIMORE

- Dispatch system outage
- Manual dispatching of emergency services
- Ransomware attack

2019

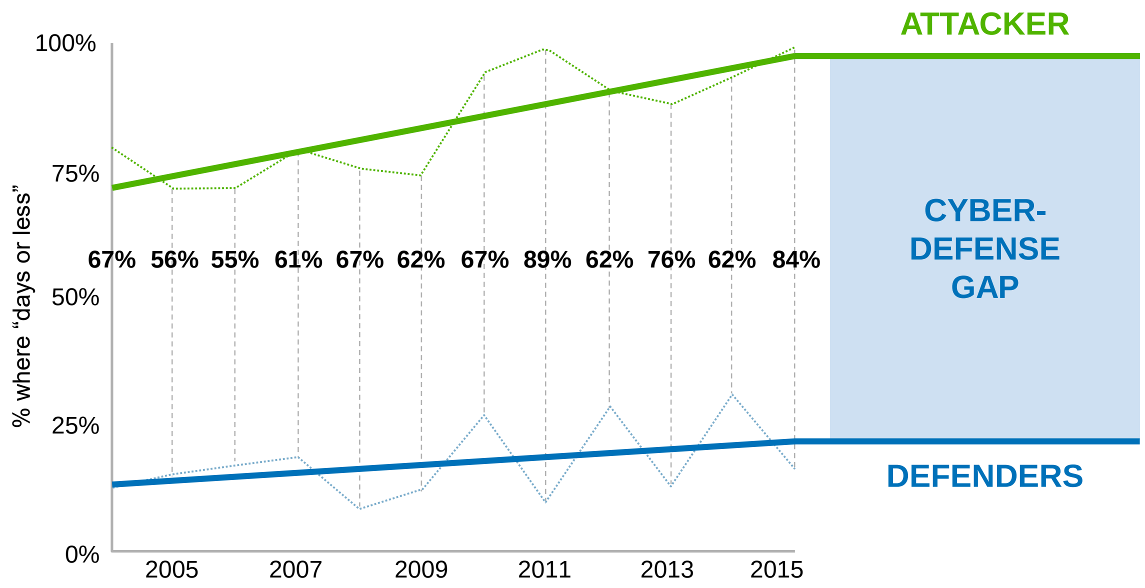
NORSK HYDRO

- Ransomware attack
- Outage forced manual operations

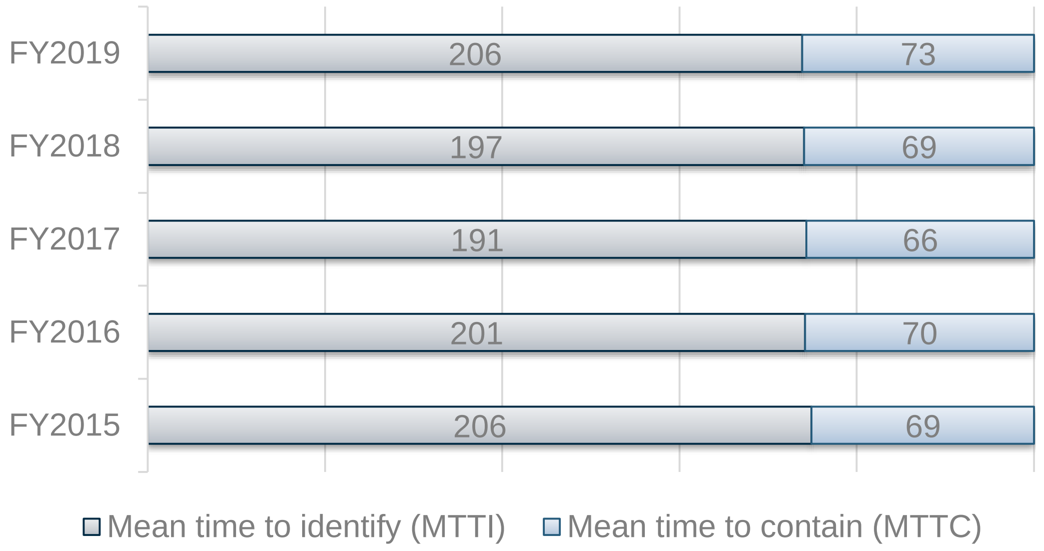
Status Quo: Threat Detection and Response

Time to detect and respond to threads is increasing

DEFENDERS LOSING THE INNOVATION BATTLE[1]



TIME TO IDENTIFY AND CONTAIN A BREACH[2]



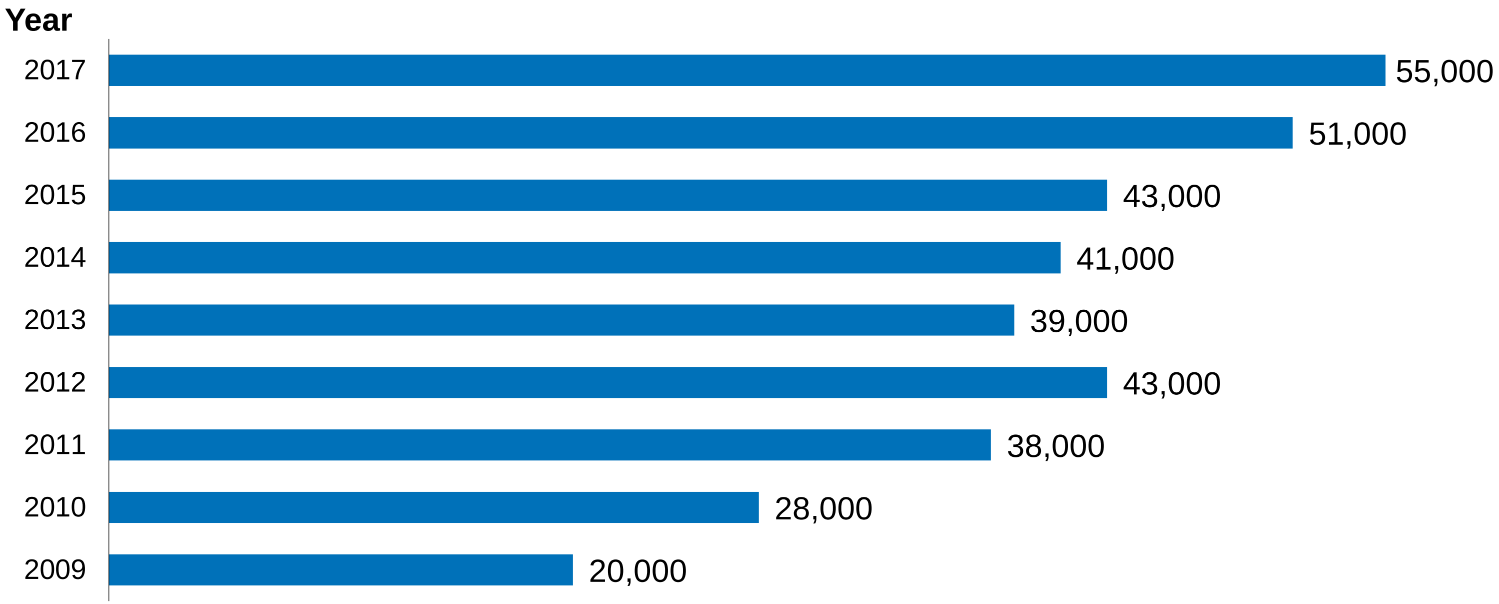
Average total cost of a data breach	Cost per lost record	Time to identify and contain a breach
$3,92M	**$150**	**279 days**

[1] Verizon DBIR 2016 | [2] Ponemon Institute 2019

The biggest Challenge in Cybersecurity

The resource gap in cybersecurity is increasing

OPEN IT POSITIONS IN GERMANY



Source: Bitkom Research 2017

Cybersecurity specialists demand reached 20% of all open IT positions in Germany.

Source: Bitkom Research 2017

One million cybersecurity job openings in 2016 … projected shortfall of two million by 2019.

Source: Cisco and ISACA

Average cybersecurity salary for experts is at €76k and increasing (Germany).

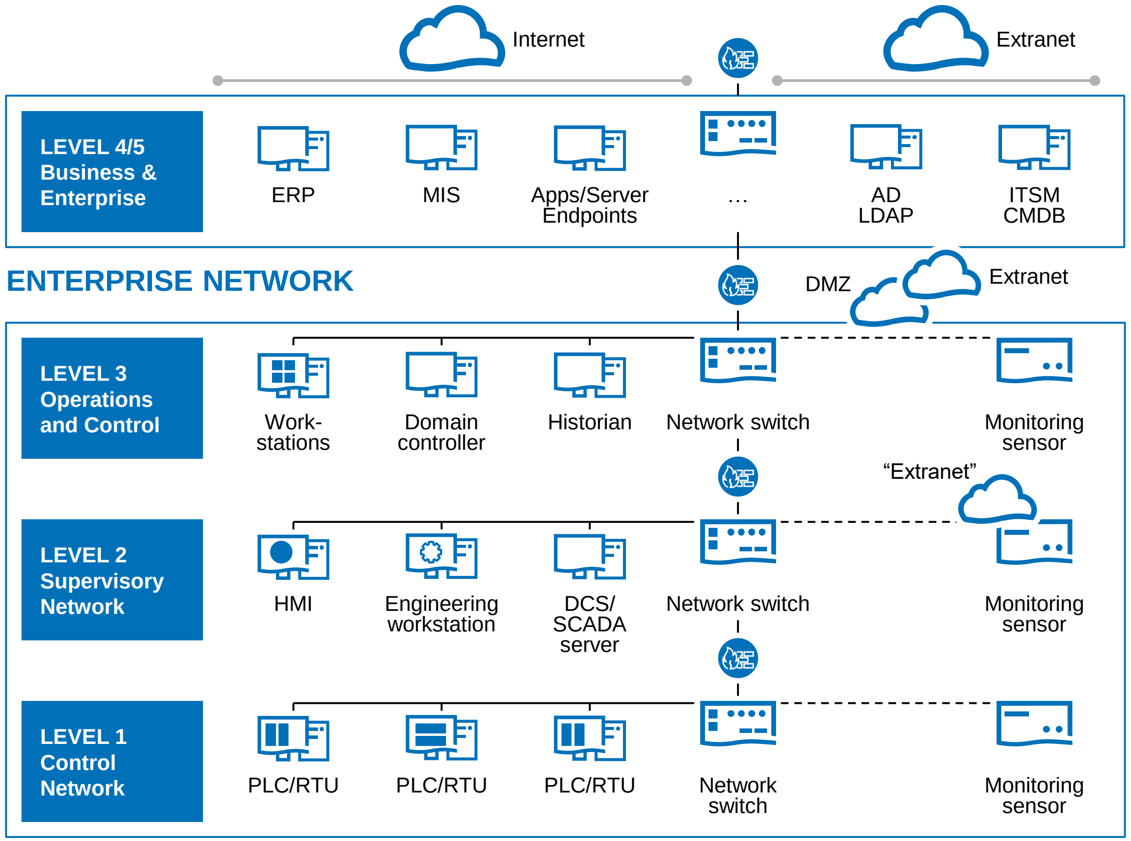
Source: Heise Medien

! The Resource Gap is the biggest challenge in Cybersecurity right now and in future.

TÜVRheinland®
Precisely Right.

How to deal with the huge amount of data in detection and response?

Achieving a complete picture across the entire enterprise



Manufacturing Environment

DETECTION AND RESPONSE

Data from
- Security Infrastructure
- Endpoints, Servers, ….
- Application/Transaction
- Vulnerabilities

Data from
- Passive OT Monitoring
- Security Infrastructure
- Application/Transaction
- Vulnerabilities

Data from
- Passive OT Monitoring
- Security Infrastructure
- Vulnerabilities

›

Asset Discovery

Communication Profile

Threat Detection

Threat Response

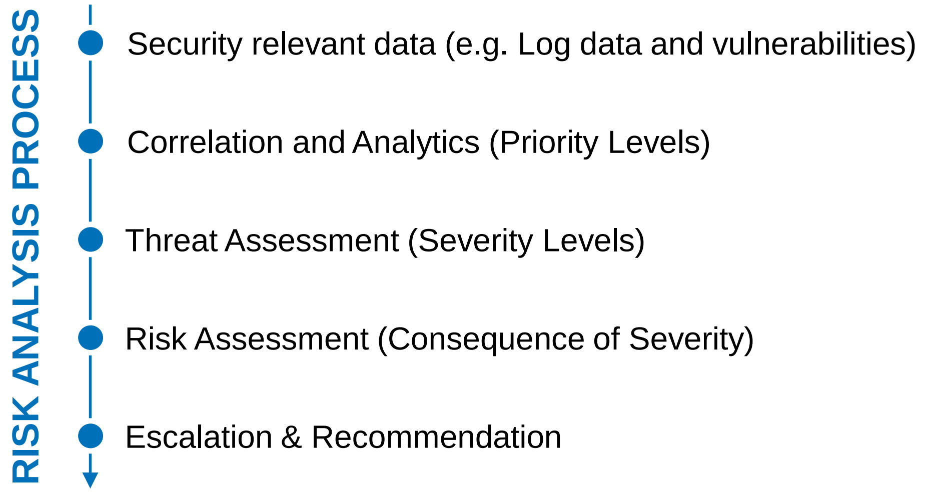
Vulnerability Response

Efficient Compliance

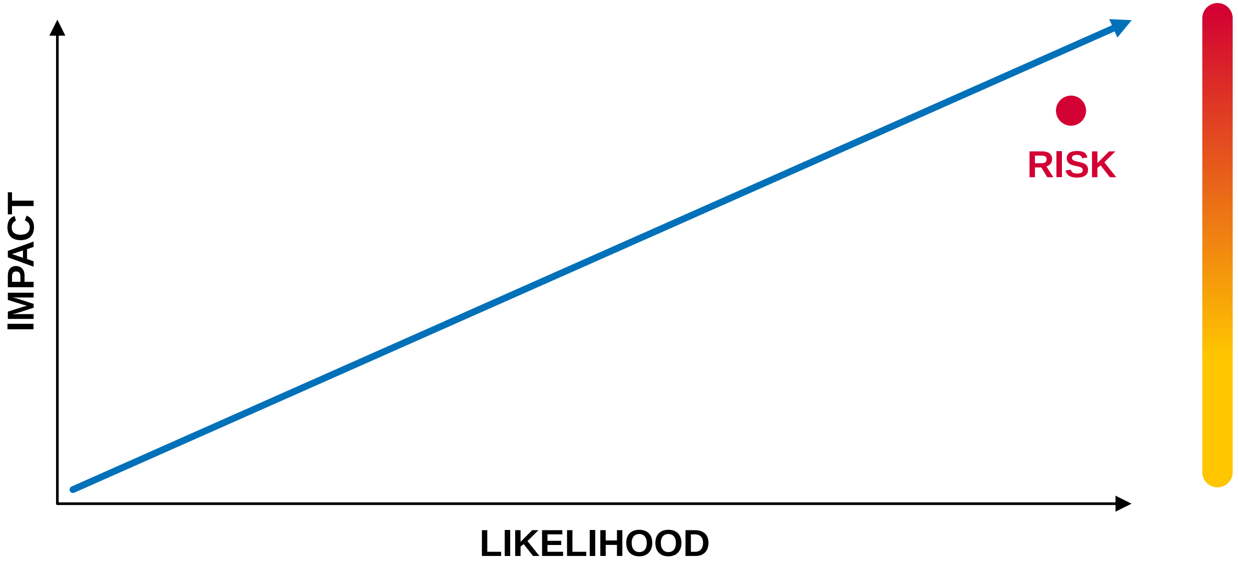
SOC – Defense Center

How are attacks detected?

Vulnerability Information is most important for prioritization of threats



- Security relevant data (e.g. Log data and vulnerabilities)
- Correlation and Analytics (Priority Levels)
- Threat Assessment (Severity Levels)
- Risk Assessment (Consequence of Severity)
- Escalation & Recommendation

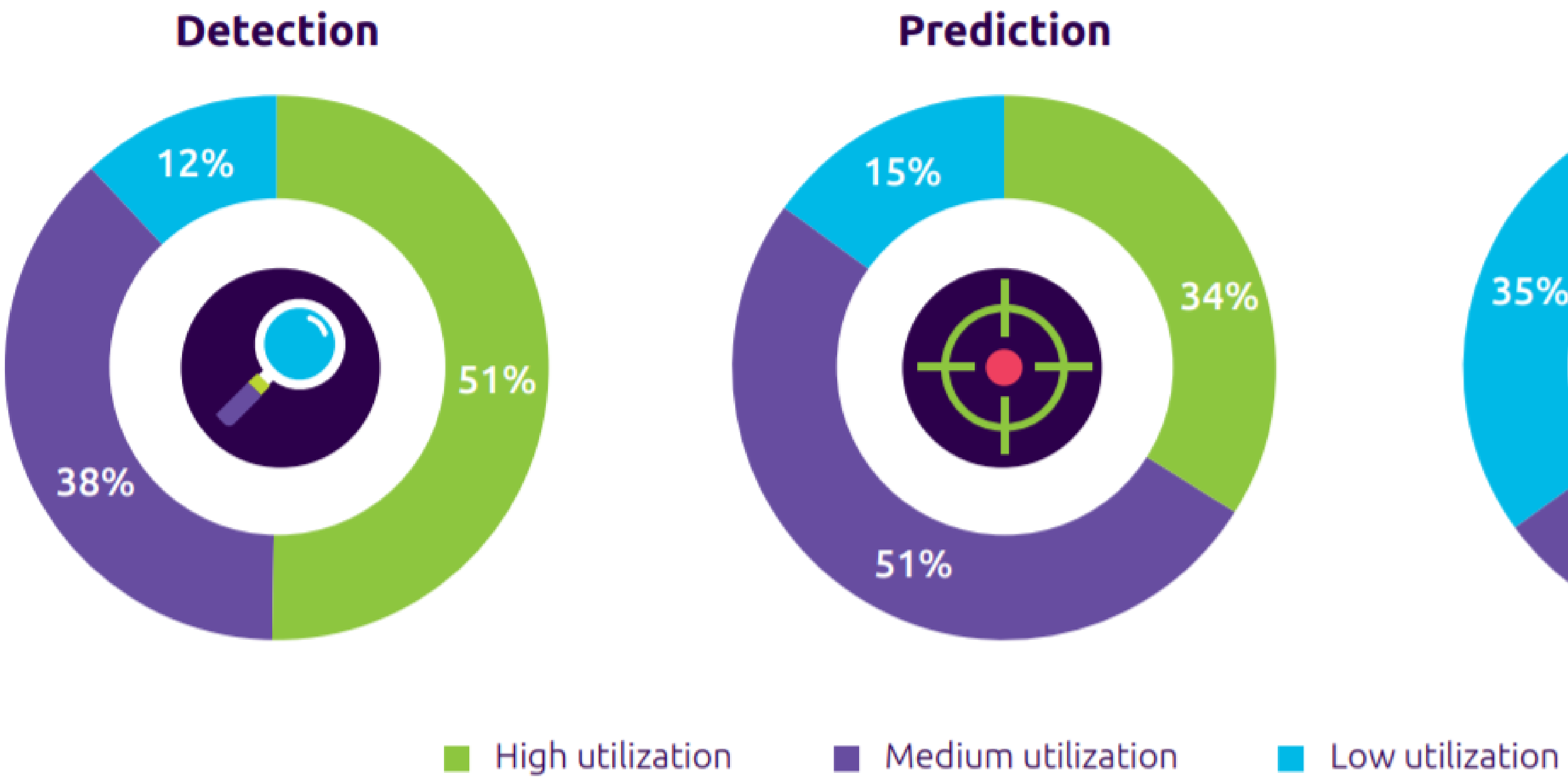


RISK = LIKELIHOOD (THREAT × VULNERABILITIES × COMPENSATING CONTROLS) × **IMPACT** (ASSET VALUE/CRITICALITY)

! Prioritized security incidents enable smart/focused budget and resource allocation.

Artificial Intelligence-enabled cybersecurity is increasingly necessary

Higher utilization of AI for detection than prediction or response



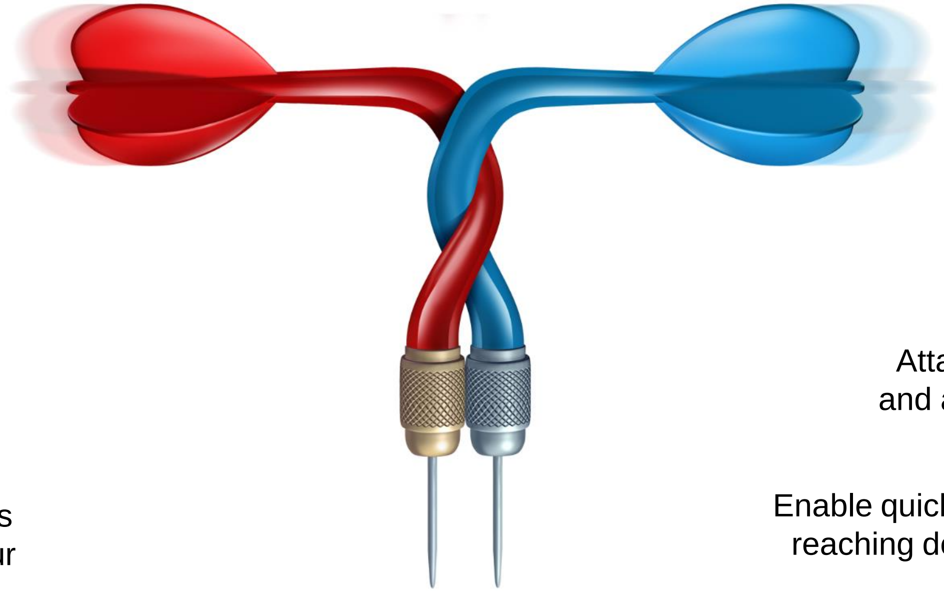
Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

AI is used on both sides

Offense and defence race is entering another round

Attackers automate and scale attacks?

- Malware continuously transforms
- Malware continuously adapts its behavior
- Malware learns to remain inconspicuous
- Malware imitates human behaviour



Defenders detect and respond faster?

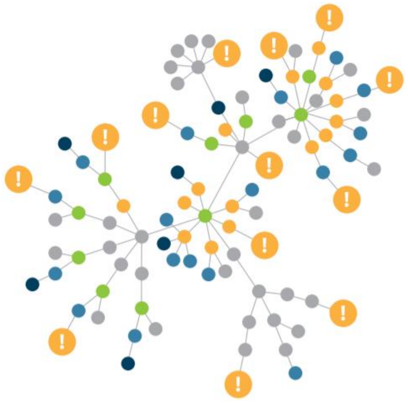
- Reliable and rapid contextual intelligence on new threats.
- Support more and more expert tasks
- Attacks can be detected and analyzed more quickly
- Enable quick and far-reaching decisions

Example
Trickbot - Originally launched as a banking Trojan, Trickbot is increasingly evolving into a multi-purpose weapon ranging from ransomware and data theft to targeted attacks.

TÜVRheinland®
Precisely Right.

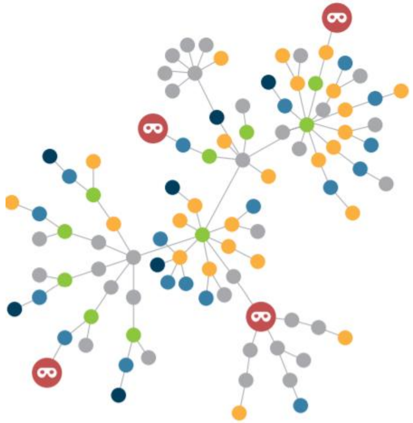
AI in Detection and Response

Where are we in detection & prediction? – an example for combined supervised and unsupervised ML



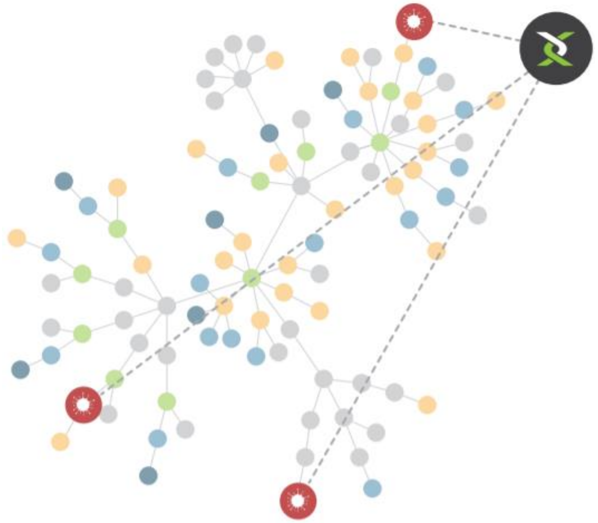
Unsupervised ML for Anomalies

- What is weird in my environment?



Supervised ML for Threat Detection

- What is bad in my environment?



Combined Anomalies & Threat Detection

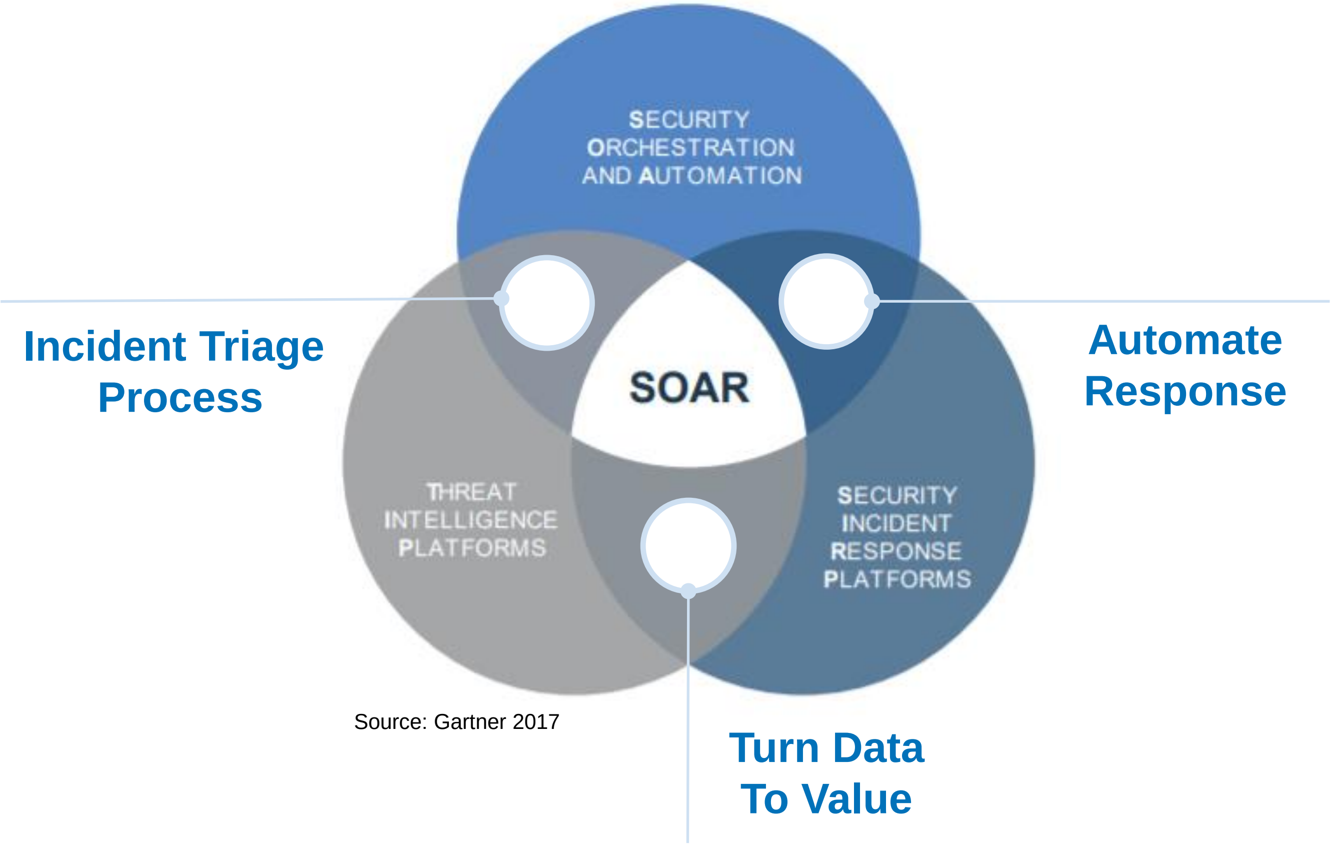
- What is the impact of this intrusion?

Source: Using AI to Detect and Contain Cyberthreats, Lastline Whitepaper

TÜVRheinland®
Precisely Right.

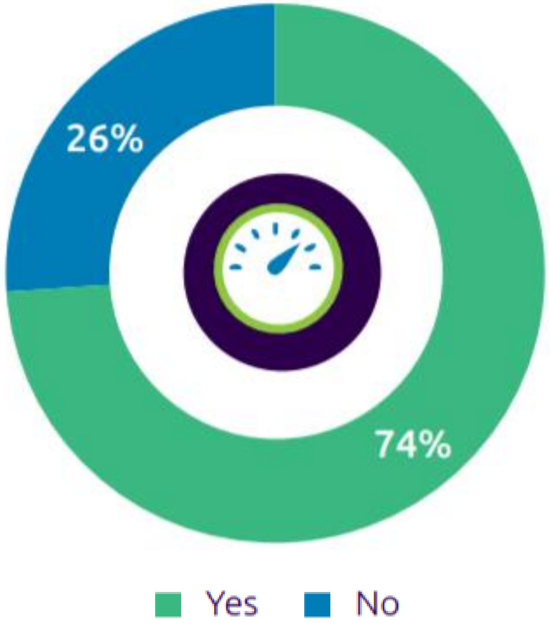
AI in Detection and Response

Where are we in response? – AI in SOAR for effective and impactful response


SECURITY ORCHESTRATION AND AUTOMATION
SOAR
THREAT INTELLIGENCE PLATFORMS
SECURITY INCIDENT RESPONSE PLATFORMS
Incident Triage Process
Automate Response
Turn Data To Value

Source: Gartner 2017

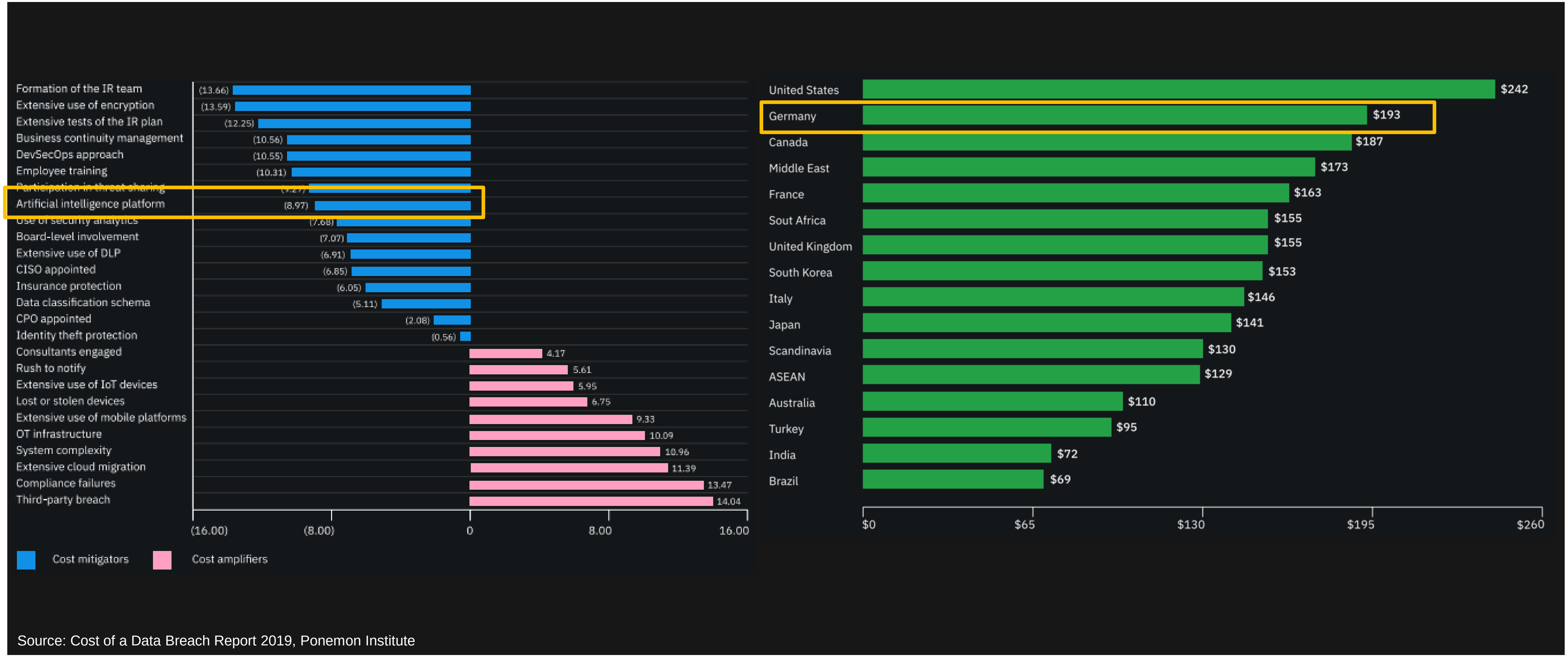
AI enables a faster response to breaches



Source: Using AI to Detect and Contain Cyberthreats, Lastline Whitepaper

AI in Detection and Response

Factors impacting the per record cost of a data breach



Source: Cost of a Data Breach Report 2019, Ponemon Institute

Key Takeaway

Cybersecurity must be a business innovator – not a cost driver.

You do need brakes to drive fast and save!

Questions?

Wolfgang Kiener

Global Head Advanced Threat Center

Phone: +49 174 1880217

Industrial Security in 2019:
A TÜV Rheinland Perspective

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Industrial Security in 2019: A TÜV Rheinland Perspective

www.tuv.com/ot-security19

Cybersecurity Trends 2019

New thinking on cybersecurity and privacy in
a world where digital transformation beckons.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Cybersecurity Trends 2019

www.tuv.com/cybersecuritytrends2019

LEGAL DISCLAIMER
This document remains the property of TÜV Rheinland. It is supplied in confidence solely for information purposes for the recipient. Neither this document nor any information or data contained therein may be used for any other purposes, or duplicated or disclosed in whole or in part, to any third party, without the prior written authorization by TÜV Rheinland. This document is not complete without a verbal explanation (presentation) of the content.
TÜV Rheinland AG

TÜVRheinland®
Precisely Right.