Capgemini

Intelligente Verteidigung gegen Cyber-Angriffe

FROM MONITOR TO DEFEND

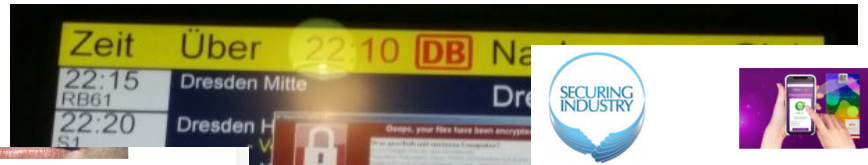
Change the behavior

REACTIVE TO PROACTIVE

Ralph Hünten

https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions#gao

(Industry) players were hit by several cyber attacks and will remain crucial targets



Hohe DSGVO-Strafe für die AOK wegen werblicher Verwendung von Gewinnspieldaten

NEWS 06.07.2020 Schwerer Datenschutz-Verstoß in Baden-Württemberg

Haufe Online Redaktion

Bild: Gerd Altmann/ pixabay.com

Bei der Datenschutzgrundverordnung ist die Zeit der Eingewöhnung vorbei – die Datenschutzbeauftragten langen hin.

Die AOK Baden-Württemberg muss nach einem DSGVO-Verstoß eine Geldbuße ihn Höhe von 1,24 Millionen Euro zahlen. Die zuständige Landesbehörde verhängte die Buße, weil die Krankenkasse Daten von Gewinnspielteilnehmern auch ohne deren Zustimmung zu Werbezwecken verwendete. Ohne AOK-Schadensbegrenzung wäre die Strafe noch höher ausgefallen.

ZUM HAUFE SHOP

ZUM THEMA RECHT & POLITIK

Datenschutzgrundverordnung: Es kommen schnell viele Tausend Euro zusammen

SECURING INDUSTRY

Home | News Archive | Events | Supplier Directory | Pharmaceuticals | Food & Beverage | Electronics & Industrial | Cosmetics

Fresenius says cyber-attack led to release of patient data

...nius has confirmed that a ransomware attack earlier ...the publication of confidential patient data.

– which is Europe's largest private hospital operator – ...at data theft had occurred after a cyberattack that ...nSecurity.com blog had affected "every part of the

BUSINESS

Bayer points finger at Wicked Panda in cyberattack

German chemicals giant Bayer claims it has fou... China which attacked the company in early 201... cyberattacks worrying firms.

Bayer factory

A group of hackers known ...

The New York Times

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

ISS World hack leaves thousands of employees offline

By Joe Tidy & David Molloy
BBC News

20 February 2020 Share

2,3 Terabit pro Sekunde: AWS meldet größten DDoS-Angriff aller Zeiten

Facebook | Twitter | WhatsApp | Pocket | E-Mail

(Foto: Beppe Castro / Shutterstock)

Kim Rixecker
News-Redakteur

Verwandte Themen

AWS | Amazon | Cloud-Computing | GitHub | Server

ThePrint

POLITICS | GOVERNANCE | ECONOMY | DEFENCE | INDIA | FEATURES | OPINION | EVENTS | VIDEO | MORE

World

Hackers target supercomputers researching Covid-19 in Switzerland, Germany, UK

Agencies investigating the hacking say potential theft of information could jeopardise the delivery of secure, effective, and efficient treatment options.

WILLIAM TURTON 16 May, 2020 2:09 pm IST

Most Popular

How India can end Chinese transgressions: Take conflict to a place Beijing is worried about

China's 'bat woman' warns coronavirus is just the tip of the iceberg

Schools from green, orange zones likely to reopen first, students of classes 8-12 to attend

CERT Bund

Home
Über CERT-Bund
Links
Warn- und Informationsdienste
Meldungen Suchen
Übersicht Meldungen
Kurzinfos
Infomeldungen
Hersteller-Meldungen
Digitale Signatur
Fragen und Antworten

// home / Warn- & Informationsdienste / Übersicht Meldungen / Ki

Kurzinfos

Datum: von bis 1000 Meldi
Einträge pro Seite: 20 Seite:

Datum	Risiko	ID #	Titel
07.07.20	2	CB-K20/0673	Red Hat OpenShift: Schwachstelle ermöglicht Denial of Service
07.07.20	3	CB-K20/0672	TYPO3 Extension: Mehrere Schwachstellen
07.07.20	4	CB-K20/0671	Android/Pixel Patchday Juli
07.07.20	3	CB-K20/0650 Update 3	Mozilla Firefox/Thunderbird: Mehrere Schwachstellen
07.07.20	5	CB-K20/0647 Update 2	F5 BIG-IP: Mehrere Schwachstellen
07.07.20	4	CB-K20/0574 Update 3	Linux Kernel: Schwachstelle ermöglicht Denial of Service
07.07.20	3	CB-K20/0573 Update 4	Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff

EasyJet Says Cyberattack Stole Data Million Customers

The low-cost airline said that email addresses and itineraries were hacked, and that the credit card details of 2,200 travelers were revealed.

© Capgemini 2018. All rights reserved |

Cyber Killchain

RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOITATION	INSTALLATION	COMMAND & CONTROL	ACTIONS ON OBJECTIVES
Harvesting email addresses, conference information, etc.	Coupling exploit with backdoor into deliverable payload	Delivering weaponized bundle to the victim via email, web, USB, etc.	Exploiting a vulnerability to execute code on victim's system	Installing malware on the asset	Command channel for remote manipulation of victim	With 'Hands on Keyboard' access, intruders accomplish their original goals

Attacker Categories: Nation State, Hackers, Insiders, cybercriminals: Intentional or not

IDENTIFY → PROTECT → DETECT → RESPOND → RECOVER

© 2020 Capgemini. All rights reserved.
© Capgemini 2018. All rights reserved |

Risk assesment is based on the results of professional business and technical evaluations

Excursus loss and probability of occurrence

Risk Assessment

Loss

Subject Area

Determination of the **financial business loss**

+

IT

Determination of the **financial technical loss**

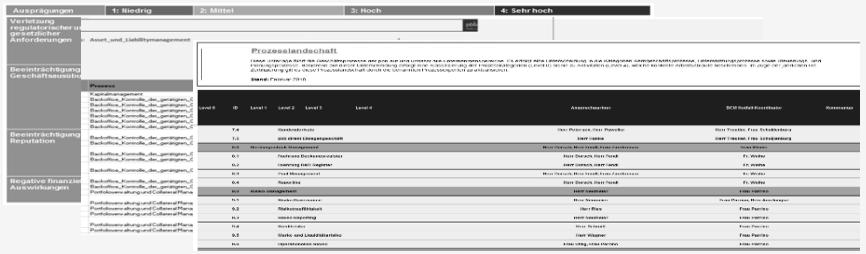
x

Probability of Occurrence

Determination of the probability of occurrence on the basis of
- **Expert estimate and**
- **risk scenarios**

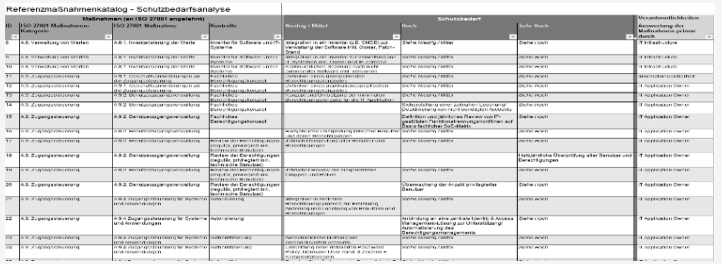
Business assessment of protection requirements

Determination of the **potential loss amount** on the base of a business assessment of the **protection requirement**



Technical protection requirements analysis

Probability of occurrence and loss in IT depending on the implementation status of the reference measures



© 2020 Capgemini. All rights reserved.
© Capgemini 2018. All rights reserved |

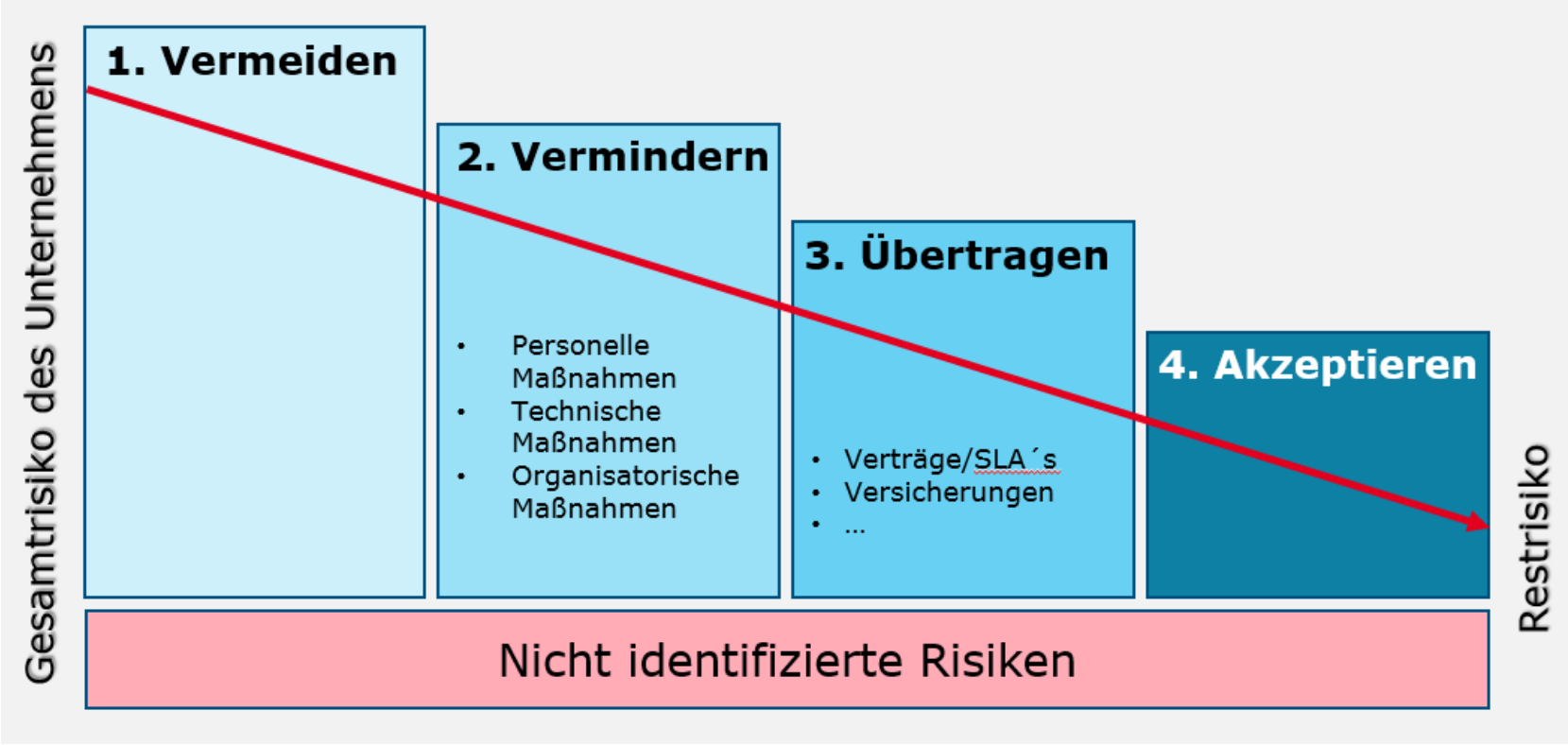
You and I – the new Risk

	Access	Productivity & Collaborative apps	Business apps	Support
1 Use own device 1. Users uses own device to access Office productivity suite	Split tunnelling VPN	Office 365 zoom 1. Collaboration & Productivity • O365 Assess and Deploy • Teams/Skype Assess and Deploy 2. Digital adoption to aid user uptake	SaaS *Non-VPN only* Web enabled business apps	1. Service Desk hypercare support 2. Field Services hypercare support 3. O365/Teams/Skype Workplace services hypercare support 4. User experience analytics *5.Potential for additional cross functional support; Cybersecurity, Svc Mgt functions, project management*
2 Virtual Desktop Browser only IGEL Secure endpoint connection 1. Browser only access with Citrix secure configurations 2. Users given IGEL UD Pocket; USB turns almost any x86 device to a WVD ready iGel managed device	Micro-VPN tunnel Direct Access to cloud services	Office 365 zoom 1. Collaboration & Productivity ▪ O365 Assess and Deploy ▪ Teams/Skype Assess and Deploy 2. Digital adoption to aid user uptake	Windows 10 · Microsoft Azure · SaaS · Citrix Cloud 1. My Workspace • Deploy Citrix Cloud • Citrix security analytics • Package and deploy apps into virtualized environment • Scale apps for users	1. Service Desk hypercare support 2. Field Services hypercare support 3. O365/Teams/Skype Workplace services hypercare support 4. Citrix and Microsoft management 5. User experience analytics *6.Potential for additional cross functional support; Cybersecurity, Svc Mgt functions, project management*
3 Corporate Laptop 1. Provision of corporate laptop	Full VPN	Office 365 zoom 1. Collaboration & Productivity ▪ O365 Assess and Deploy ▪ Teams/Skype Assess and Deploy 2. Digital adoption to aid user uptake	Windows 10 · SaaS 1. Windows 10 deployment - Set-up Windows Auto pilot	1. Service Desk hypercare support 2. Field Services hypercare support 3. O365/Teams/Skype Workplace services hypercare support 4. Windows 10 Evergreen support 5. User experience analytics 6. End point management *7.Potential for additional cross functional support; Cybersecurity, Svc Mgt functions, project management*

© 2020 Capgemini. All rights reserved.

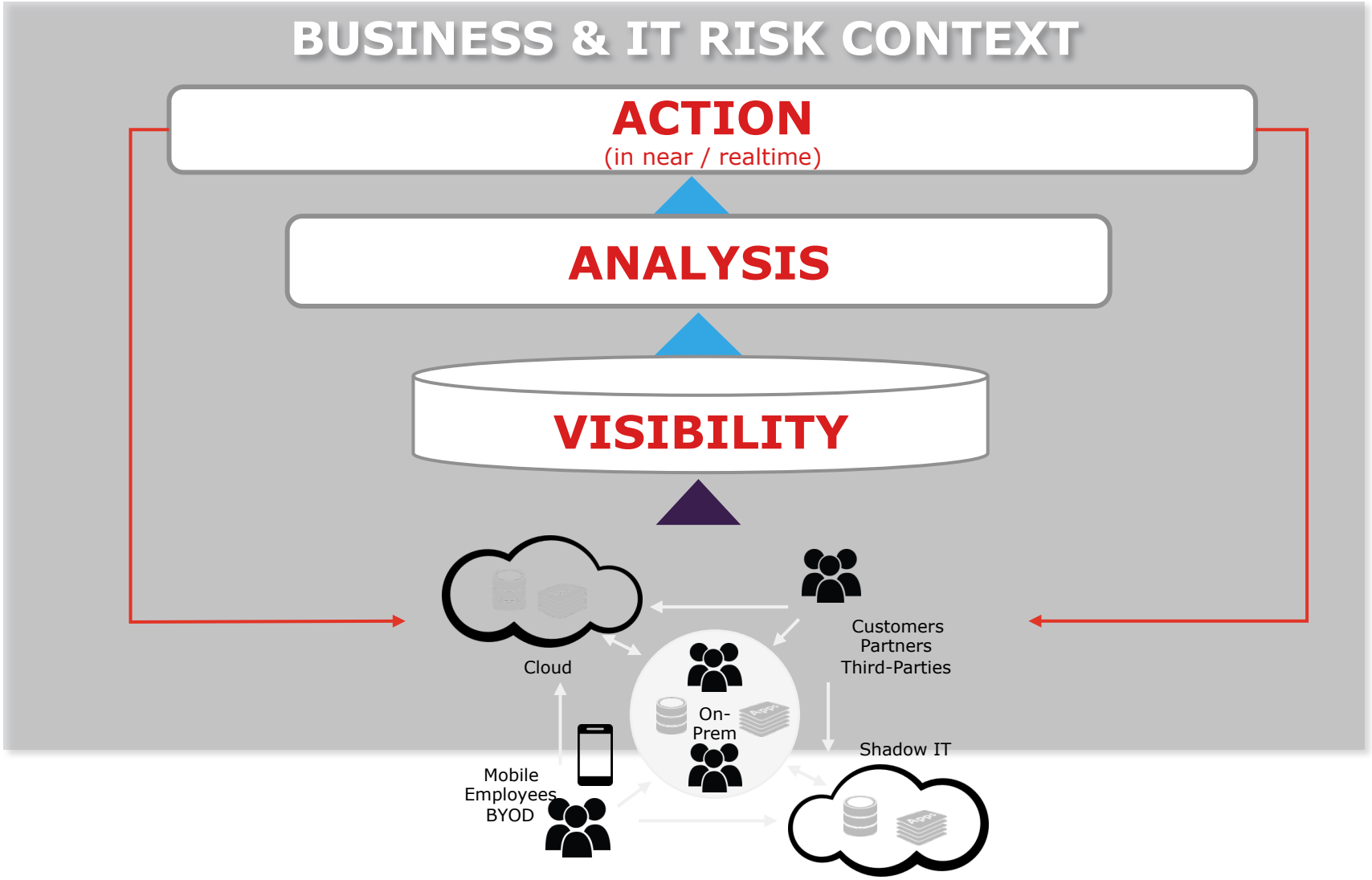
© Capgemini 2018. All rights reserved |
6

Risk Management



© 2020 Capgemini. All rights reserved.
© Capgemini 2018. All rights reserved |

Holistic Cyber Security View & intelligent Defense



Act to mitigate business damage or loss

Detect anomalies that indicate risks or threats

Collect data about what matters

Identities - Flow of Data - Transactions

© Capgemini 2018. All rights reserved |

Security Orchestration, Automation and Response (SOAR) Platform

No digitalization without Cybersecurity – automated & intelligent

Guided Response

Threat Intelligence

Threat & Vulnerability Management - Respond to security incidents

Automate security operations - Dynamic policies for steering

Better Compliance

Team Management

© 2020 Capgemini. All rights reserved.
© Capgemini 2018. All rights reserved |

Our End-to-End Portfolio of Offerings: A Closer look

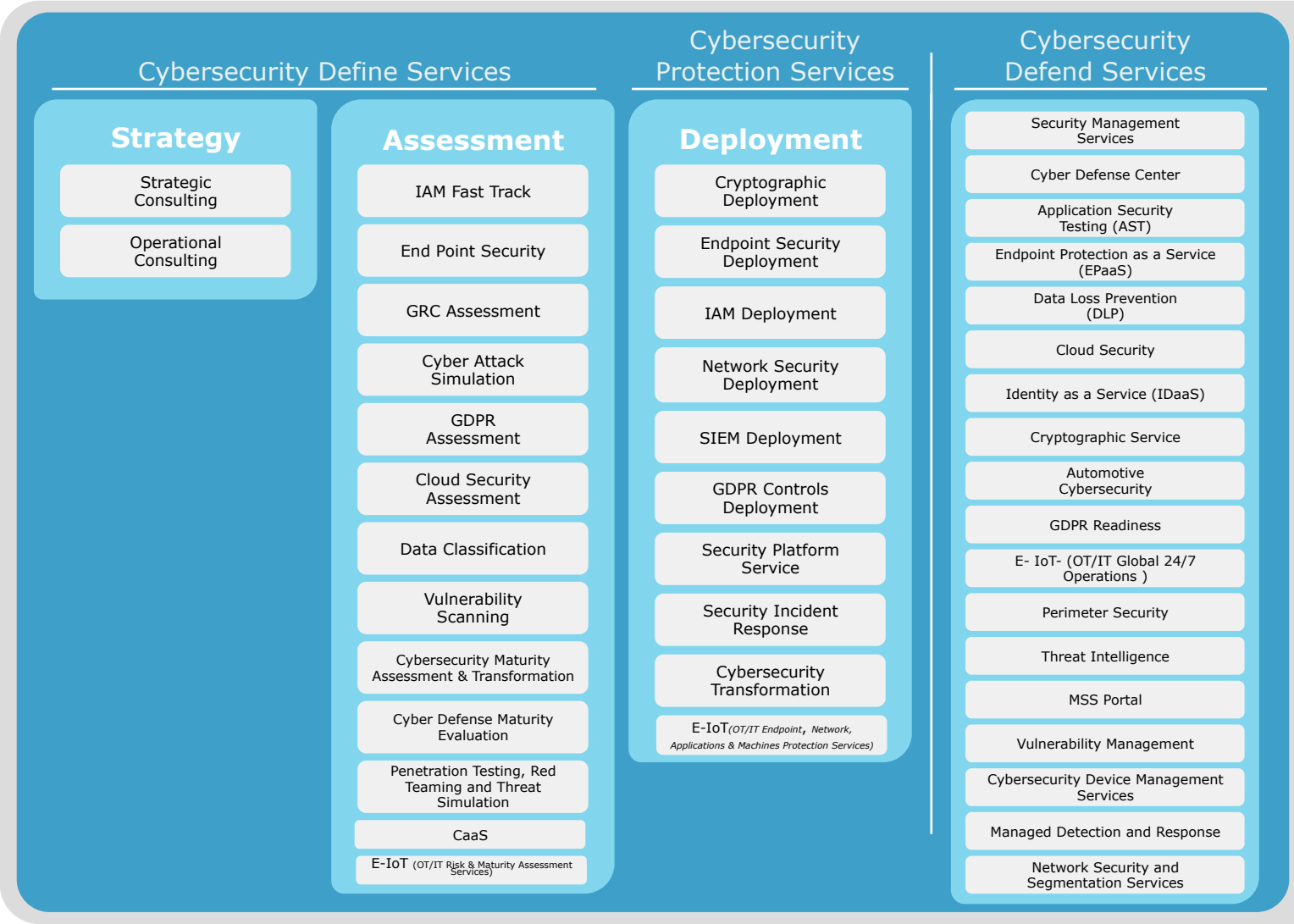
Define Services

- **Strategy Services**
  - Strategic consulting
  - Operational consulting
- **Assessment Services**
  - Security of endpoints to clouds
  - Vulnerabilities
  - Compliance assessment
  - Overall security posture

Protect Services

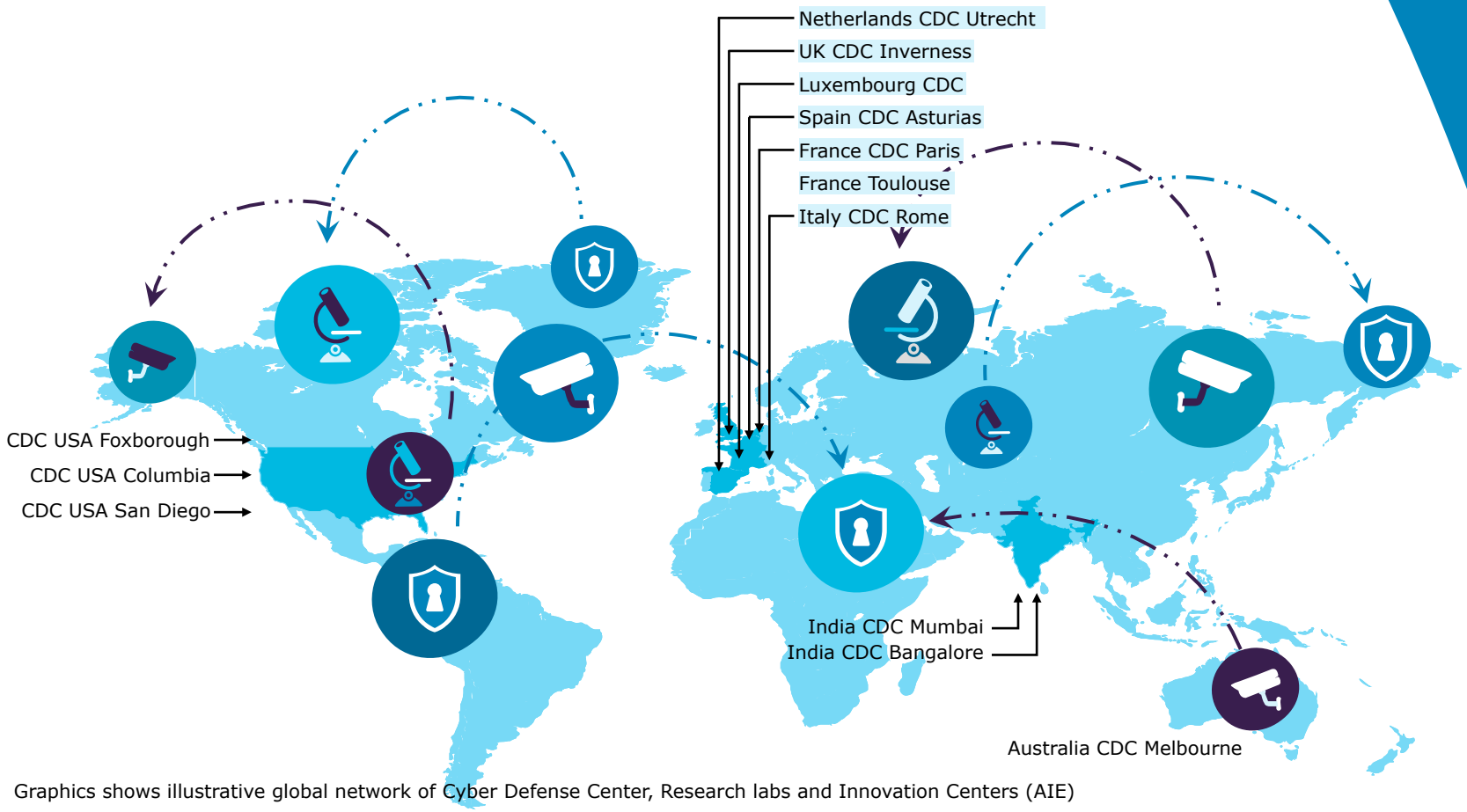
- **Deployment Services**

Defend Services



© 2020 Capgemini. All rights reserved.
© Capgemini 2018. All rights reserved |

Capgemini advantage:
Global Cyber Defense Scale



Graphics shows illustrative global network of Cyber Defense Center, Research labs and Innovation Centers (AIE)

A tangible reduction in both the frequency and duration of major cyber security incidents

Actionable insight on security threats leading to:

Improved defensive posture for new and emerging threats; Ability to conduct advanced analytics on suspect artefacts and proactively protect the technical environments we monitor.

Vast experience with businesses of all types and sizes in every industry

Consistently innovate

Benefits of our global CDC´s

- Expertise of 3000+ security professionals
- Proven processes and technologies
- Complete visibility into IT and security systems
- Advanced analysis of data and threat intelligence

Positive results

- Cyber Attack Platform: We find holes in your security, you didn't see before
- Prevent incidents, detect threats, and respond to attacks like no one else

© Capgemini 2020. All rights reserved

Q&A

Ralph Huenten
Head of Cybersecurity DACH | Cloud Infrastructure Services

Capgemini | Mainzer Landstraße 180 | 60327 Frankfurt am Main, Germany
Tel.: +49 69 95152088 | Mob.: +49 151 40250637

© Capgemini 2018. All rights reserved |