FACE THE UNPREDICTABLE

TEHTRIS XDR Lösung für KRITIS 2.0, TISAX, BAIT, …

Olaf Müller-Haberland

Head of Germany

TEHTRIS

Our Mission

PROTECT YOU AGAINST

CYBER ESPIONAGE

& **CYBER SABOTAGE**

THROUGH

REAL-TIME

AUTOMATIZED

INCIDENT RESPONSE

TEHTRIS

Innovation, Performance and Trust Provider

€20M
Record Series A
Nov. 2020

Ace · Open CNP · NACO · Business Angels

12 Years of **R&D**

360°
cyber-protection
& visibility
on the
hyper-automatized

eXtended Detection
and Response
(XDR) Platform

Artificial Intelligence
Deep Learning

+10.000
Virus analyzed
per minute

Only
XDR & EDR solutions

100%
developed and hosted
in Europe

La seule plateforme XDR Européenne
The only European XDR Platform

5/5
Gartner Peer Insights
Clients ratings

Gartner peerinsights
TEHTRIS XDR Platform Ratings Overview
5.0 ★★★★★ 12 Reviews (All Time)

Security software deployed in
more than 100 countries
& across all industries

100% client loyalty

INDUSTRY · TRANSPORT · EDUCATION · RETAIL · PUBLIC ADMINISTRATION

HEALTHCARE · SERVICES PROVIDERS · BANKS INSURANCE · CRITICAL INFRASTRUCTURES

TEHTRIS *belongs to*

ACN · amtso · La French Tech · European Champions Alliance · CYBER THREAT ALLIANCE

Awards and Distinctions

Gartner · OPSWAT · Cyber Defense Magazine Winner · Open Trusted Cloud OVHcloud · SECURITY

In the Media

BBC · Forbes · Business Insider · ZDNet · BFM Business · Challenges · Les Echos

L3 LIMITED

Committed to the fight against cyberattacks

and editor of innovative solutions since 2012

April 2010

TEHTRIS Foundation

2012

Software Editor

R&D and development of Cybersecurity proprietary solutions

2015

Automatic neutralization

Without human action

2020

20 Million Euros Series A

2021

200 employees

2010-2012

Vulnerability search

Pentests and consulting

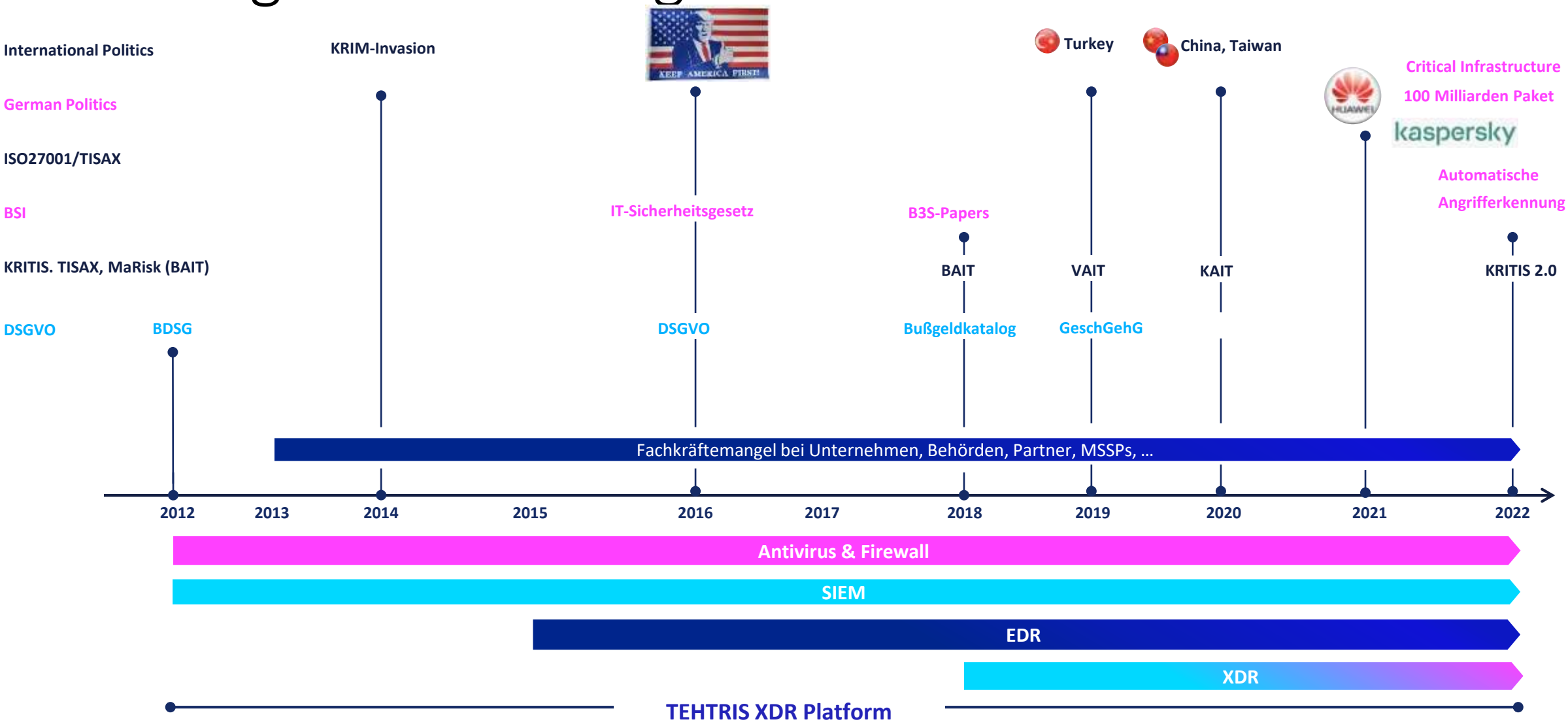
Since 2012

TEHTRIS XDR Platform

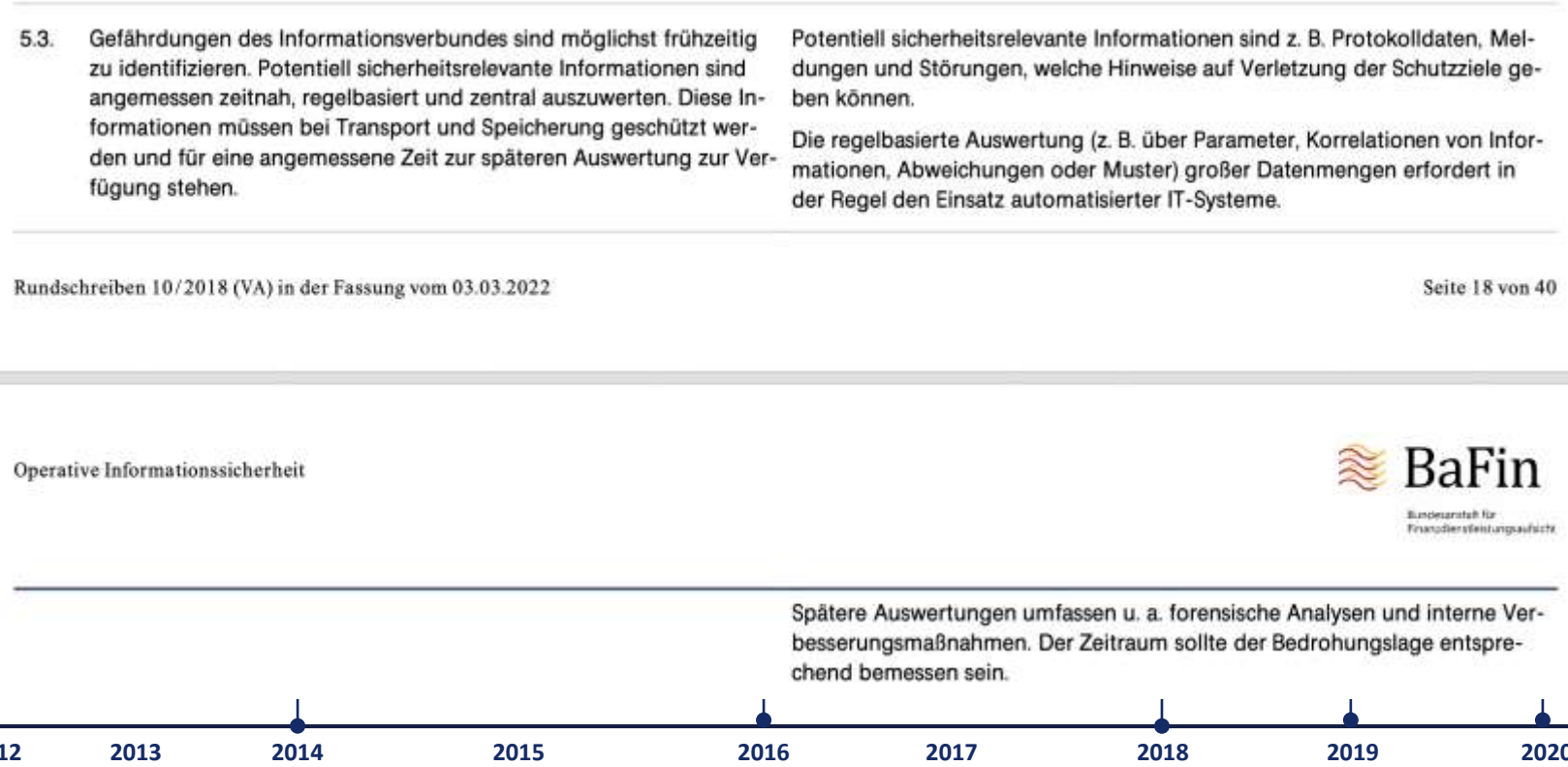
Remediation of 100% threats

R&D of EDR, EPP, MTD, CTI, SIEM, Deceptive Response, SOAR…
to protect all systems, networks, data flows, cloud

Heutige Anforderungen versus Stand der Technik



Heutige Anforderungen versus Stand der Technik



5.3. Gefährdungen des Informationsverbundes sind möglichst frühzeitig zu identifizieren. Potentiell sicherheitsrelevante Informationen sind angemessen zeitnah, regelbasiert und zentral auszuwerten. Diese Informationen müssen bei Transport und Speicherung geschützt werden und für eine angemessene Zeit zur späteren Auswertung zur Verfügung stehen.

Potentiell sicherheitsrelevante Informationen sind z. B. Protokolldaten, Meldungen und Störungen, welche Hinweise auf Verletzung der Schutzziele geben können.

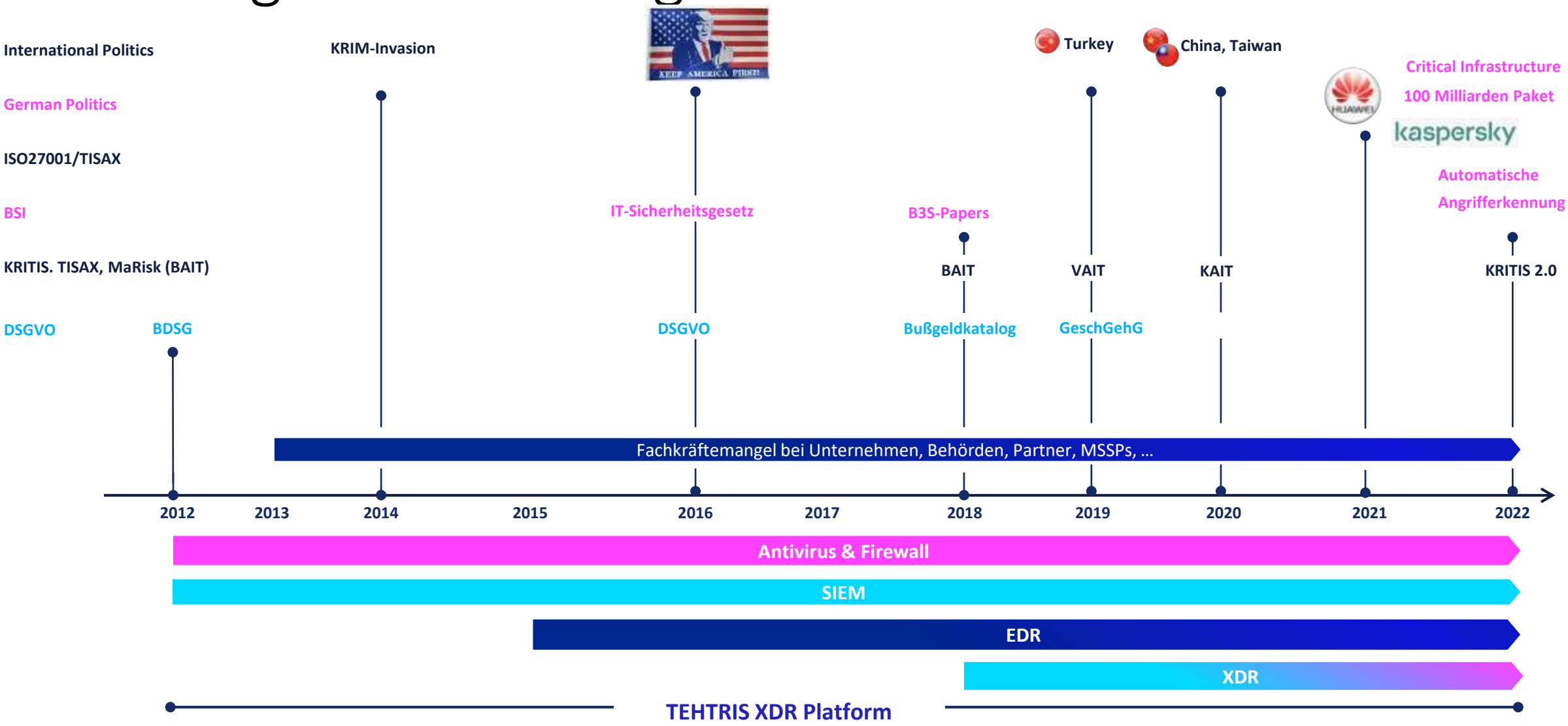
Die regelbasierte Auswertung (z. B. über Parameter, Korrelationen von Informationen, Abweichungen oder Muster) großer Datenmengen erfordert in der Regel den Einsatz automatisierter IT-Systeme.

Rundschreiben 10/2018 (VA) in der Fassung vom 03.03.2022 Seite 18 von 40

Operative Informationssicherheit

Spätere Auswertungen umfassen u. a. forensische Analysen und interne Verbesserungsmaßnahmen. Der Zeitraum sollte der Bedrohungslage entsprechend bemessen sein.

Heutige Anforderungen versus Stand der Technik



Heutige Anforderungen versus Stand der Technik

International Politics

German Politics

ISO27001/TISAX

BSI

KRITIS. TISAX, MaRisk (BAIT)

DSGVO

BDSG

Weiterführende Informationen

Weitere Orientierung zum Thema Angriffserkennung bietet der IT-Grundschutz des BSI, dort unter anderem die Bausteine

- OPS.1.1.4 Schutz vor Schadprogrammen,
- OPS.1.1.5 Protokollierung
- NET.1.2 Netzmanagement
- NET.3.2 Firewall
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1: Behandlung von Sicherheitsvorfällen

(www.bsi.bund.de/dok/531534)

Auf die Methodik des IT-Grundschutz baut auch der Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen auf. (www.bsi.bund.de/dok/886714)

Critical Infrastructure

100 Milliarden Paket

kaspersky

Automatische Angrifferkennung

KRITIS 2.0

2012 20 2021 2022

Antivirus & Firewall

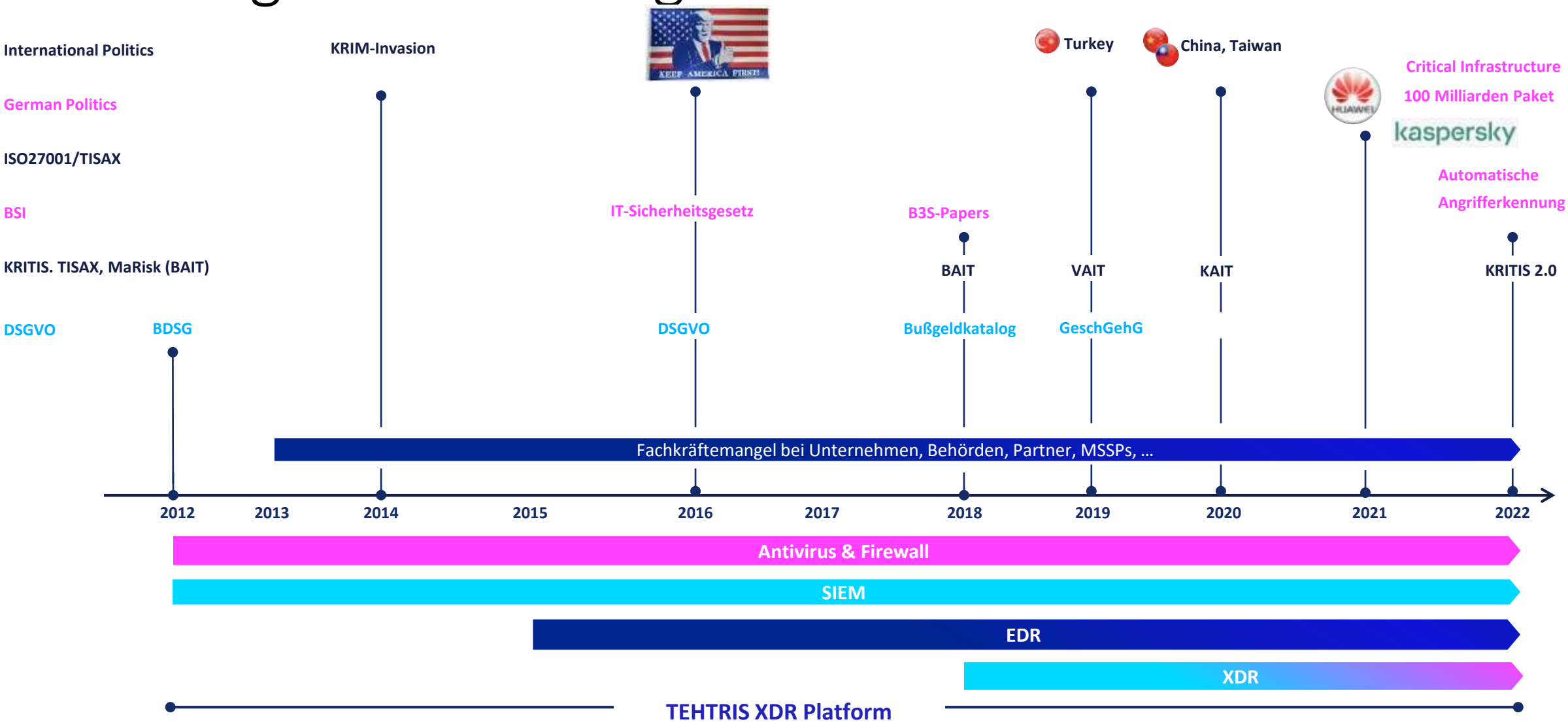
SIEM

EDR

XDR

TEHTRIS XDR Platform

Heutige Anforderungen versus Stand der Technik



TEHTRIS XDR Platform

REAL-TIME REMEDIATION
NO LAST CLICK REQUIRED

Cyberattacks

Ransomware

Protect your IT & OT

La seule plateforme XDR Européenne

The only European XDR Platform

The only native cyber defense platform

A complete and modular protection of your systems

Partner Services

Governance | Risk Management | Compliance

Security Operations Center

Managed Security Services | Managed Detection Response | CERT/CSIRT

TEHTRIS

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence	Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

TEHTRIS Products

SIEM | DNS FW | EDR | EPP | MTD | ZTR | NTA | DECEPTIVE RESPONSE

Technical Landscapes

CLOUD	SYSTEMS	NETWORKS
Microsoft AZURE | O365 Amazon AWS Salesforce OVH Cloud Workload	Endpoints | Servers Mobile devices OT / SCADA IoT	SD-Wan, Firewalls, VPN, Network flows

TEHTRIS XDR für kritische Infrastrukturen

Unser Angebot

360° intervention and monitoring of your endpoints

Thanks to the hyper automation and intelligence of TEHTRIS

Detection and neutralization of known and unknown threats

In remediation mode, the TEHTRIS OPTIMUS agent blocks known signatures, identifies malicious behavior and neutralizes unknown cyberattacks automatically

Embedded TEHTRIS artificial intelligence

TEHTRIS CTI, Sandbox, more than 15 analysis engines (signature database), innovative neural networks (Cyberia) and behavioral analysis module

Industrialized and turnkey solution for IT/OT Security

Functional, efficient and autonomous protection with TEHTRIS professional and managed services from TEHTRIS/Partner

Final Documentation with the target person « Auditor »

We pick you up where you are and finalize

FACE THE UNPREDICTABLE

Danke! Fragen?

olaf.mueller-haberland@tehtris.eu

ITSA Halle 7A / 429