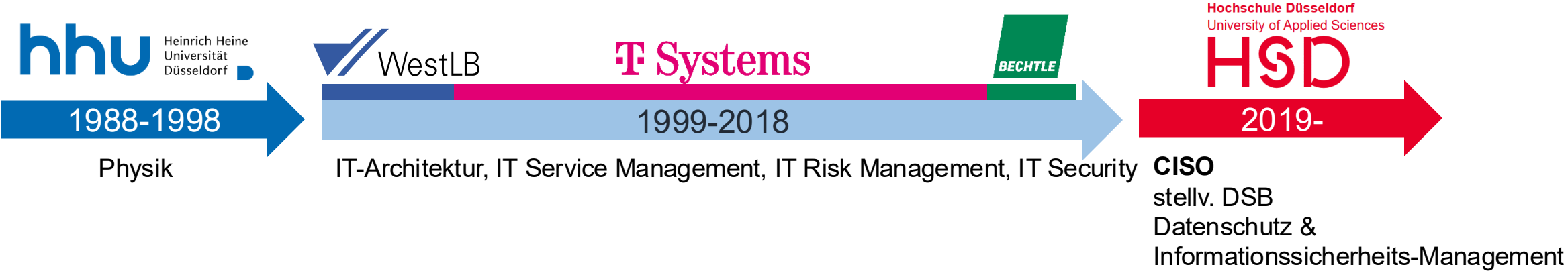


# Informationssicherheit an der HSD

Teil 1: Das DISM an der HSD

Teil 2: Auf dem Weg zu SIEM, XDR und SOC

**Dr. Christoph Glowatz**  
Stabsstelle 3 Informationssicherheit (2 MA)  
[christoph.glowatz@hs-duesseldorf.de](mailto:christoph.glowatz@hs-duesseldorf.de)



Erster Teil

# Das DISM an der HSD

# Ab 2019: Datenschutz- und Informationssicherheits-Management @HSD

## Auftrag:

- Aufbau eines integrierten **Datenschutz- und Informationssicherheits-Management**;
- Informationssicherheit in „**Anlehnung**“ an **BSI-Grundsatz**;

Hochschule Düsseldorf  
University of Applied Sciences

**HSD**

2019- 

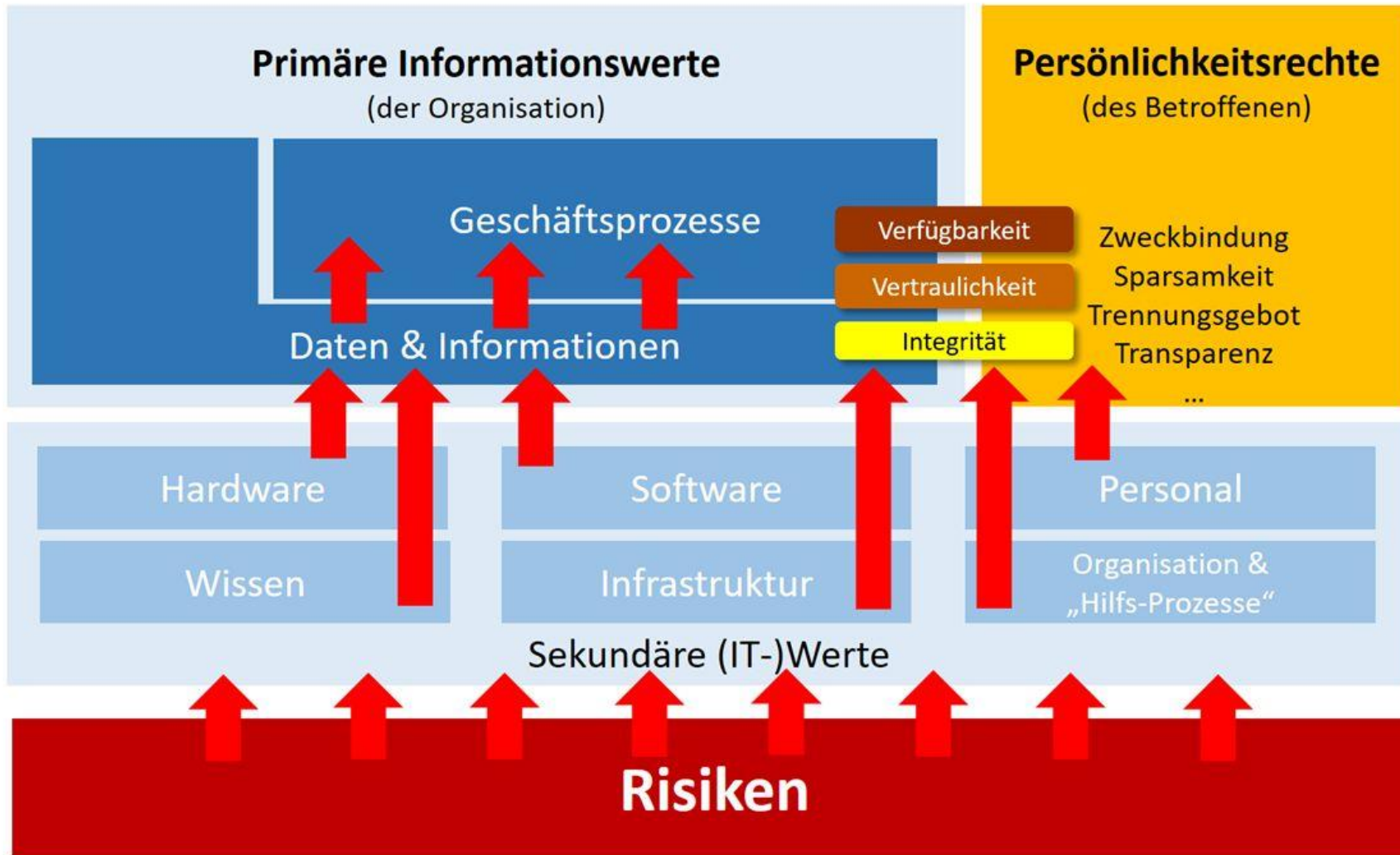
**CISO**

stellv. DSB

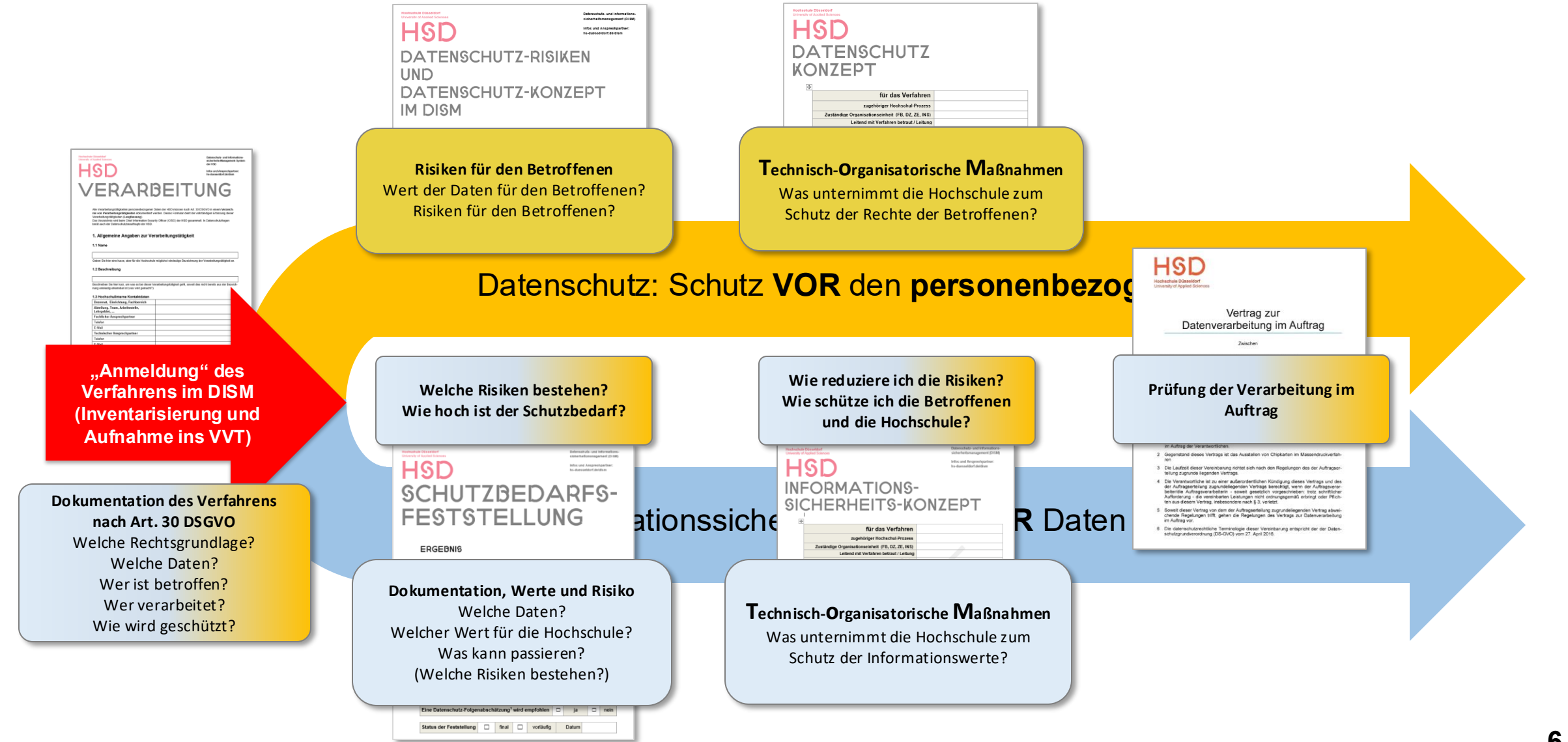
Datenschutz &

Informationssicherheits-Management

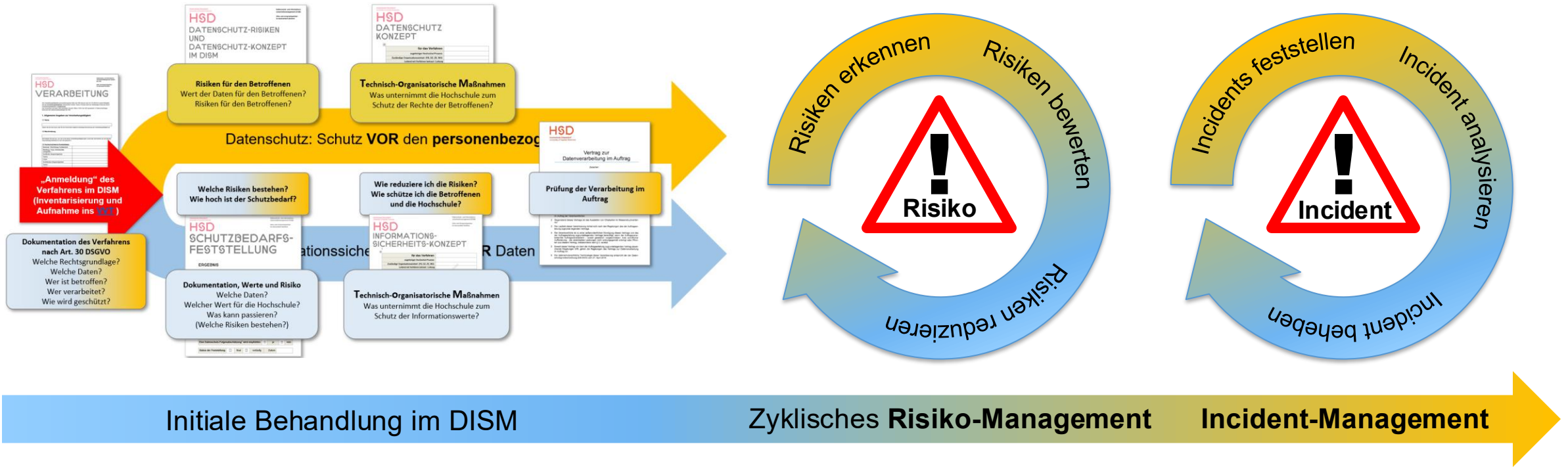
# Stelle Datenschutz & Informationssicherheit nebeneinander



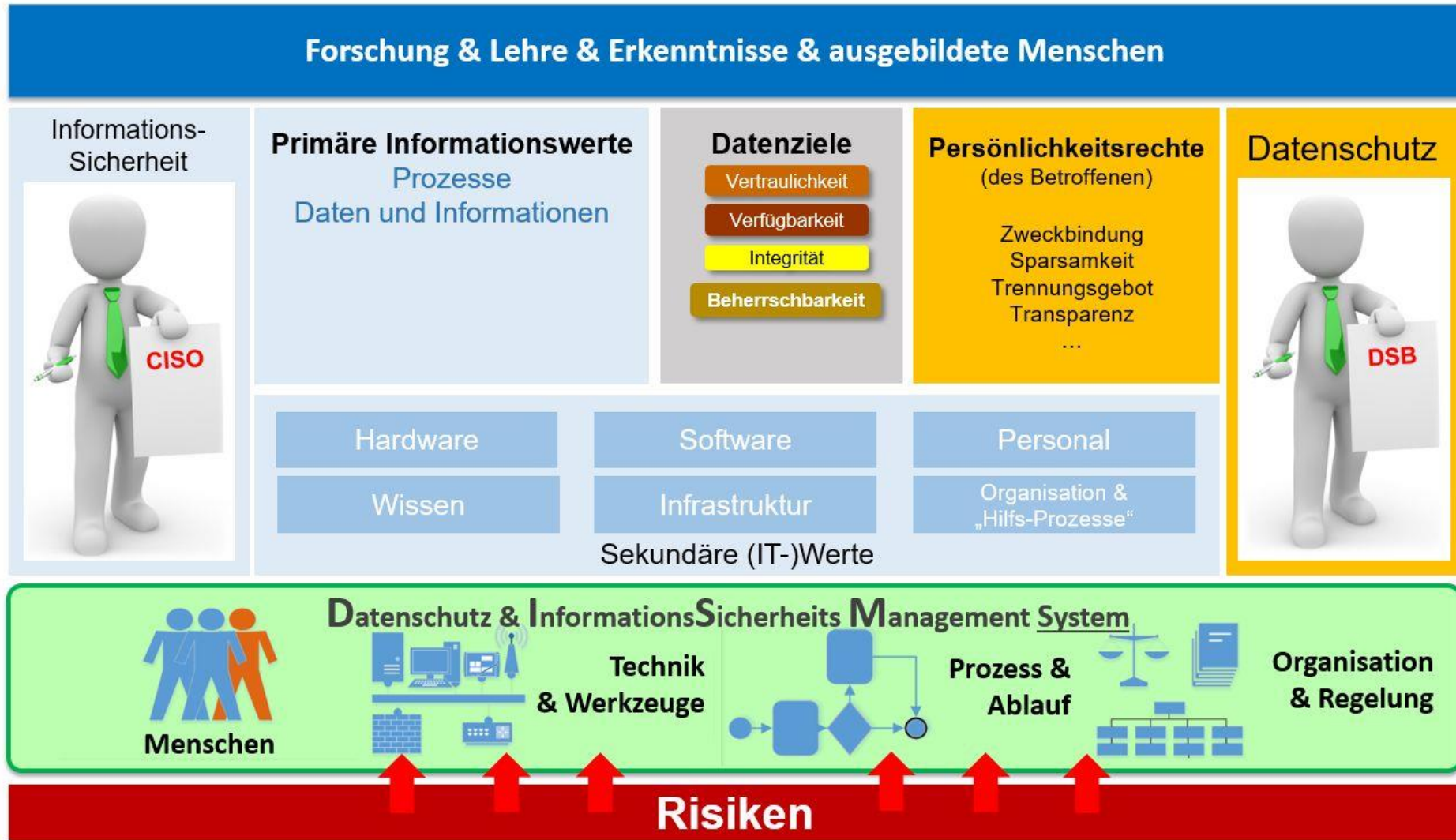
# Zur Illustration: Behandlung von „Verfahren“ im DISM



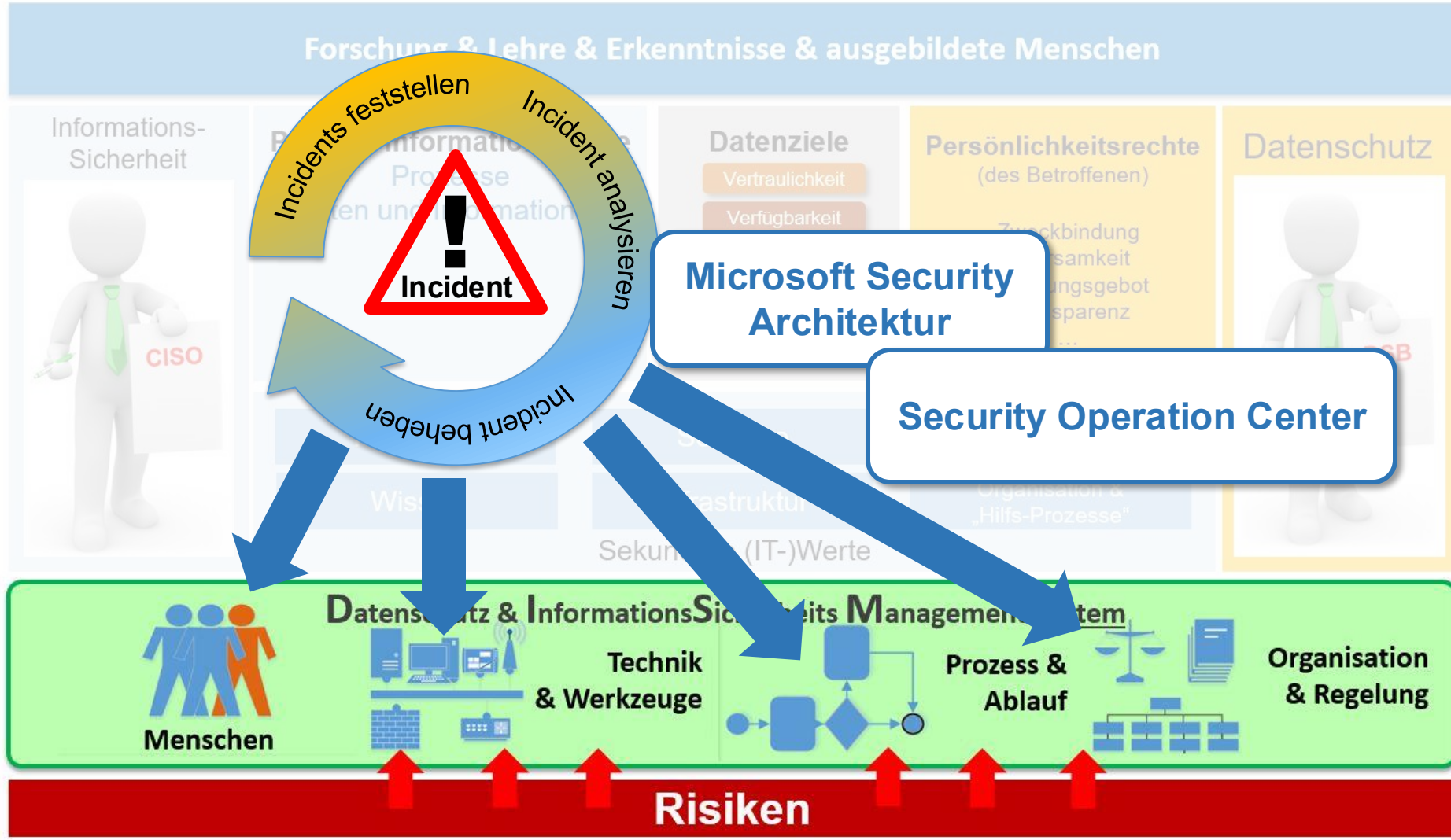
# Übergang in den kontinuierlichen DISM-Betrieb



# Das DISM zwischen Werten und Risiken



# Incident Management im DISM



# BSI-Grundschutz im DISM: Von der „Anlehnung“ zur VzC...

HSD  
INFORMATIONSSICHERHEITS-KONZEPT

Datenschutz- und Informations-sicherheitsmanagement (DISM)  
Info- und Ansprechpartner:  
hs-dism@hsd.duisburg

für das Verfahren	
Zugehöriger Hochschul-Prozess	
Zuständige Organisationseinheit (FB, DZ, ZF, INS)	
Leitend mit Verfahren betraut / Leitung	
Telefon	
E-Mail	
Fachlich mit Verfahren betraut / Fachadministration	
Telefon	
E-Mail	
Technisch mit Verfahren betraut / IT-Administration	
Telefon	
E-Mail	
Ansprechpartner für DSB und CSO	
Telefon	
E-Mail	

Schutzbedarf des Verfahrens  gering  normal  hoch  sehr hoch

Kronjuwel-Status  ja  nein

Status des Verfahrens  in Planung  im Aufbau  im Betrieb

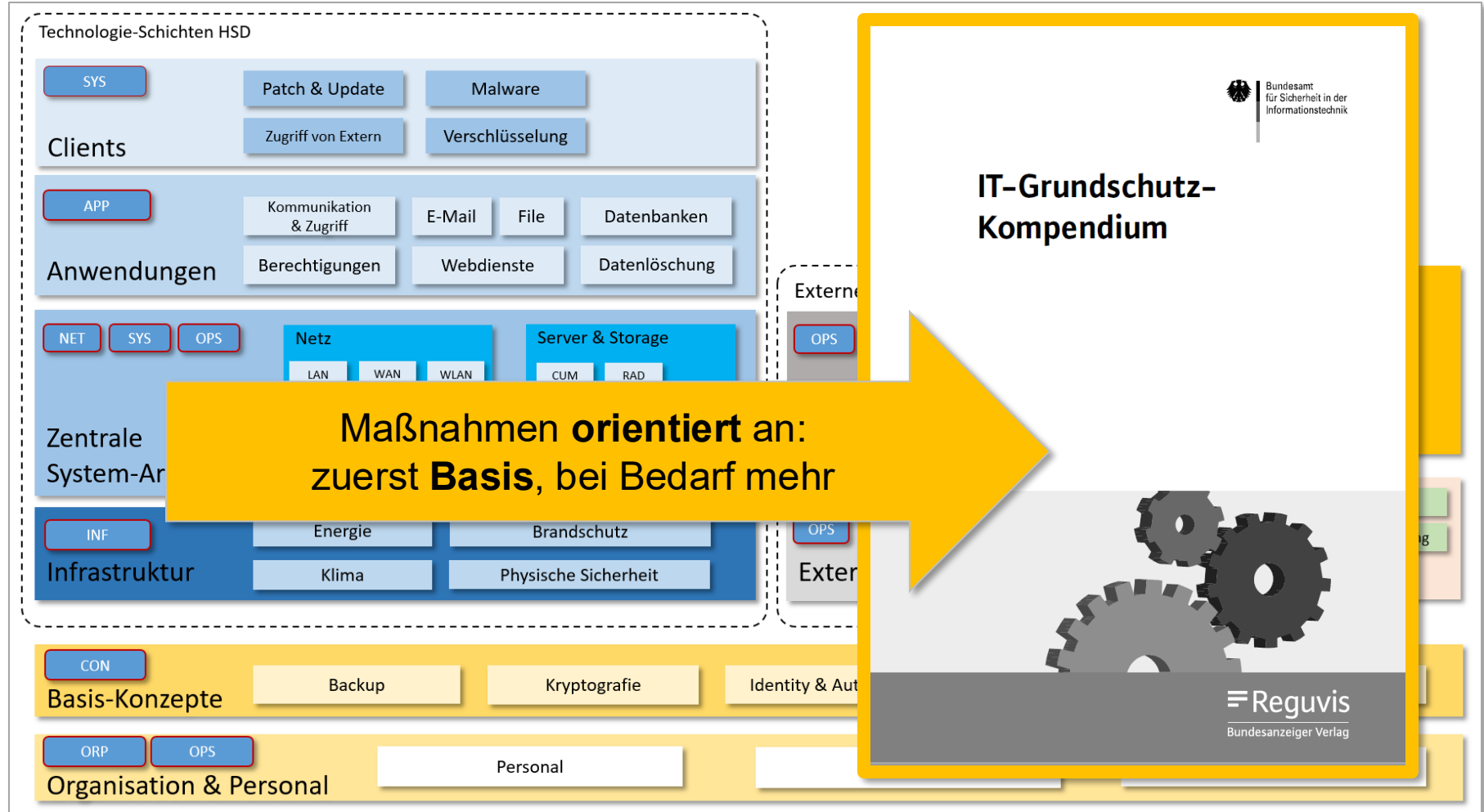
Ansprechpartner und Adressat von Informationssicherheits-Konzepten an der HSD ist im Rahmen des Datenschutzes- und Informationssicherheitsmanagement (DISM):  
Dr. Christoph Glowatz  
Beauftragter für Informationssicherheit  
Chief Information Security Officer  
Münsterstraße 156  
Gebäude 2, Etage 3, Raum 02.03.028  
40476 Düsseldorf

DIGITALE HOCHSCHULE NRW  
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

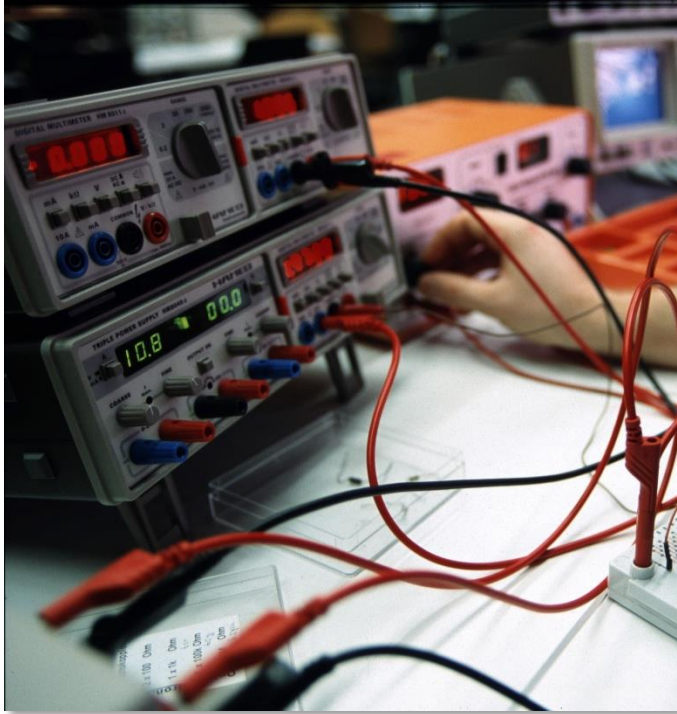
Vereinbarung zur Cybersicherheit an den Hochschulen (VzC)

**VzC-Projekt @ HSD:  
Gestartet im April 2025**

im Einvernehmen mit der Digitalen Hochschule NRW (DH.NRW)



# Prinzip 1: Hochschule bleibt Hochschule



Daten



Informationen

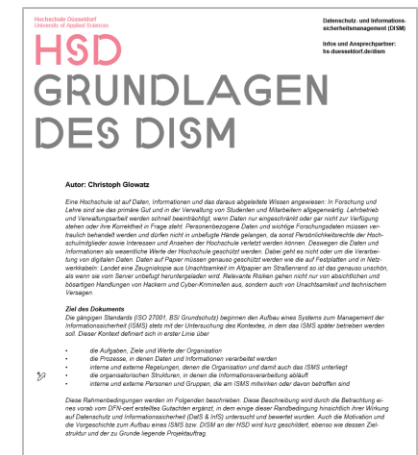
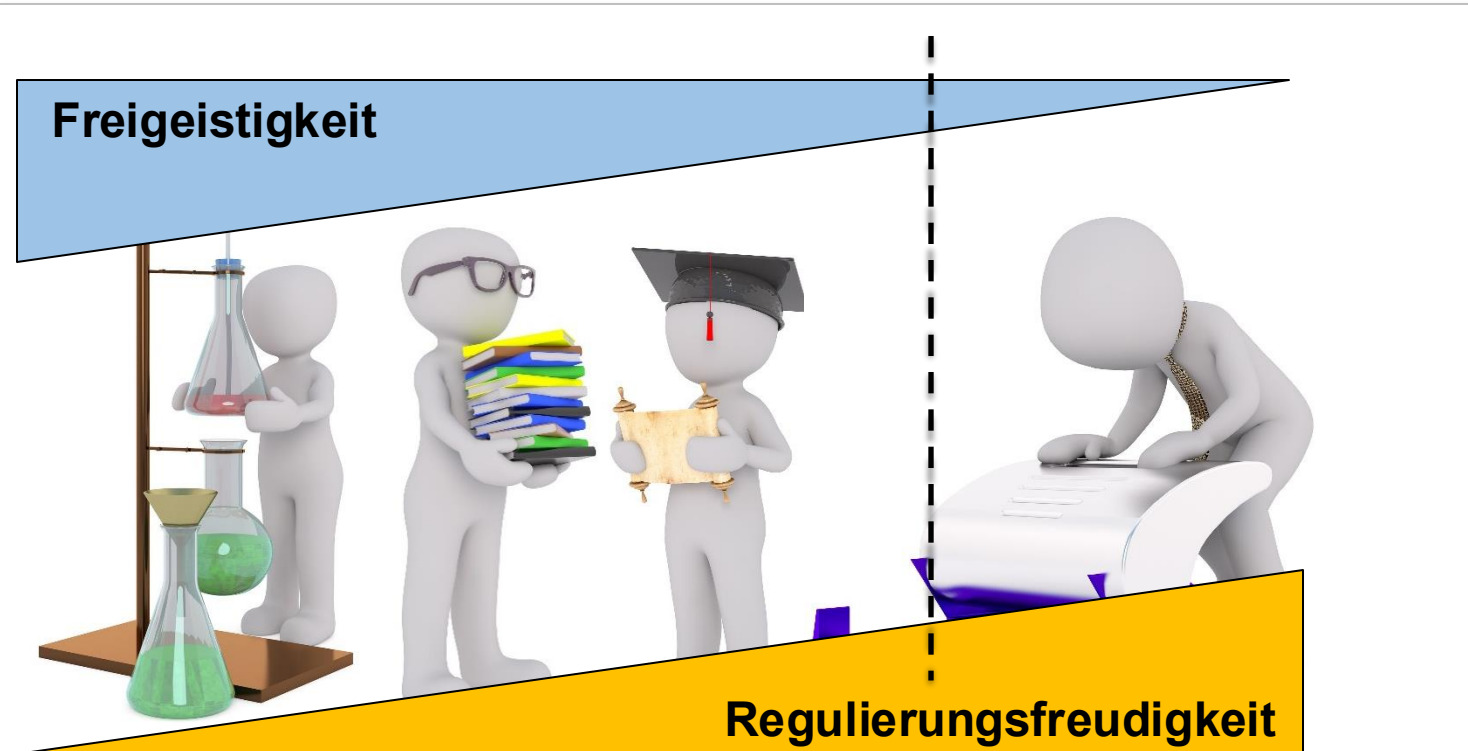


Wissen

Das Ziel einer Hochschule ist die **Weitergabe** von Informationen, **nicht** deren **Geheimhaltung**.

Werte sind **Offenheit, Transparenz, Kreativität, Spontanität** und die **Freiheit von Forschung und Lehre**

# Unser Risiko-Kontext ist wie er ist



„organisierte Anarchie“  
„Bruch zwischen geistig-akademischer  
und rechtlich-wirtschaftlicher Sphäre“

**Der spezielle Risiko-Kontext „Hochschule“ muss stets berücksichtigt werden!**

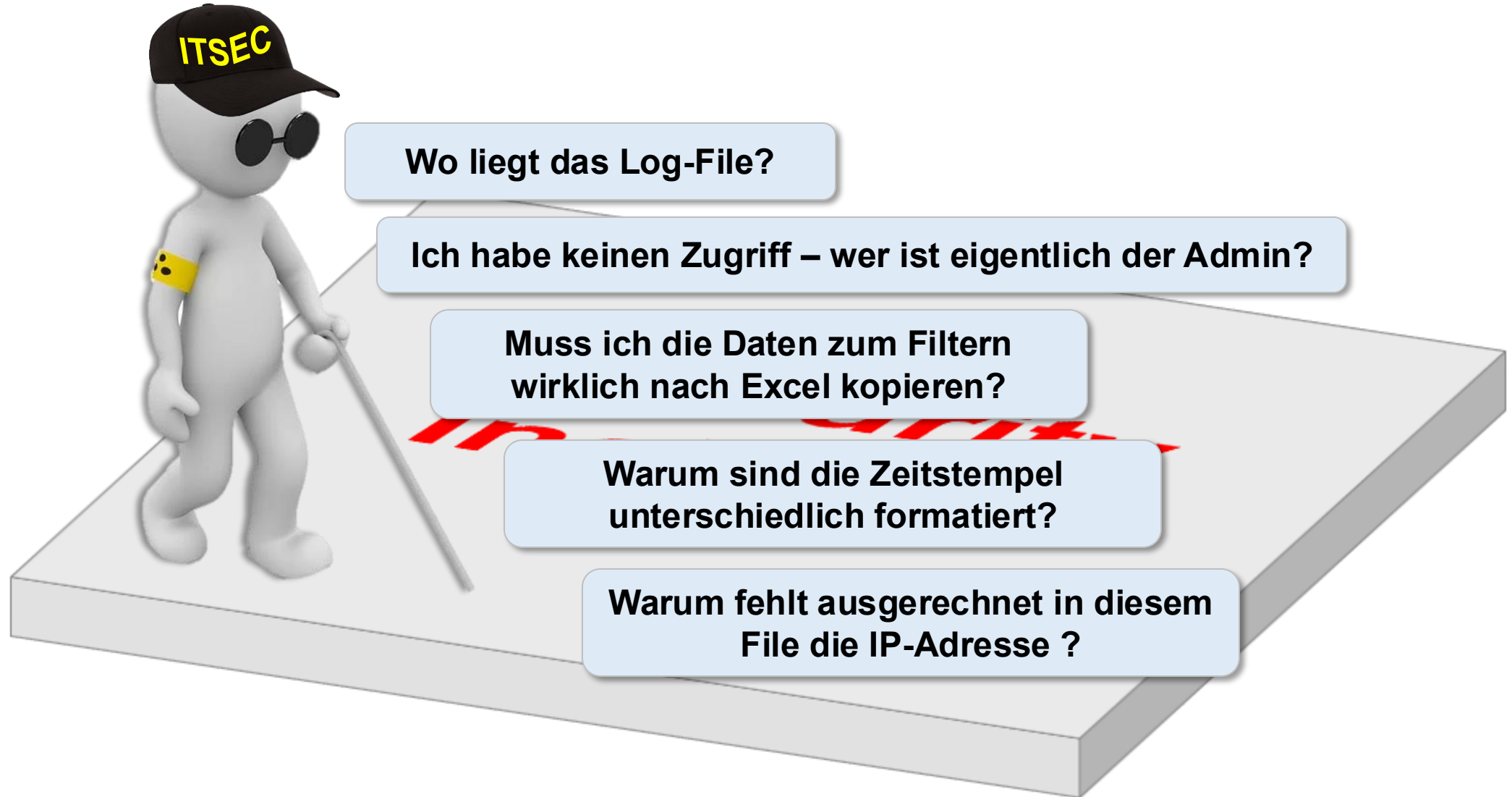
# Prinzip 2: Fokus - Wo und wie werden wir konkret angegriffen?



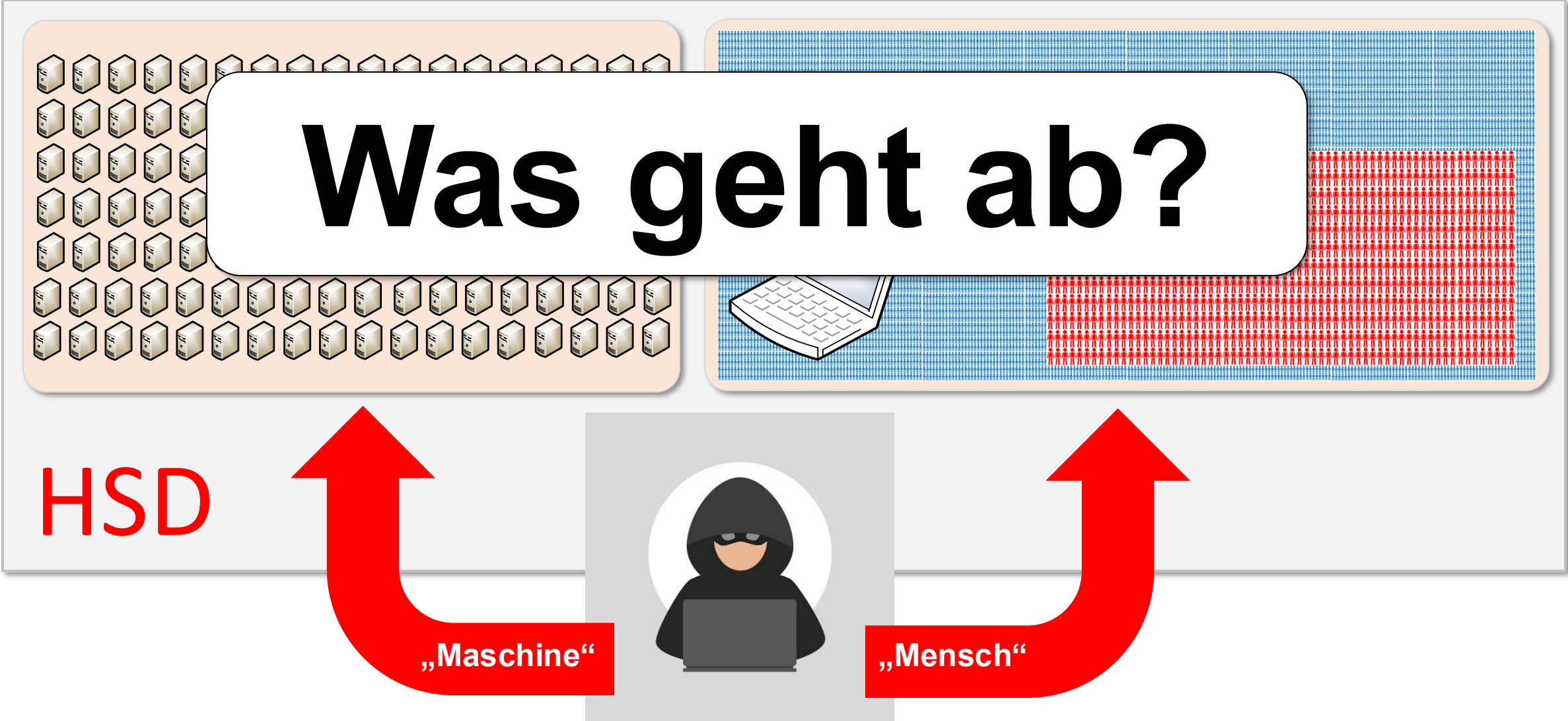
Zweiter Teil

# Auf dem Weg zu SIEM, XDR und SOC

## Was den CISO (und seine Kolleg\*innen) nervös macht...

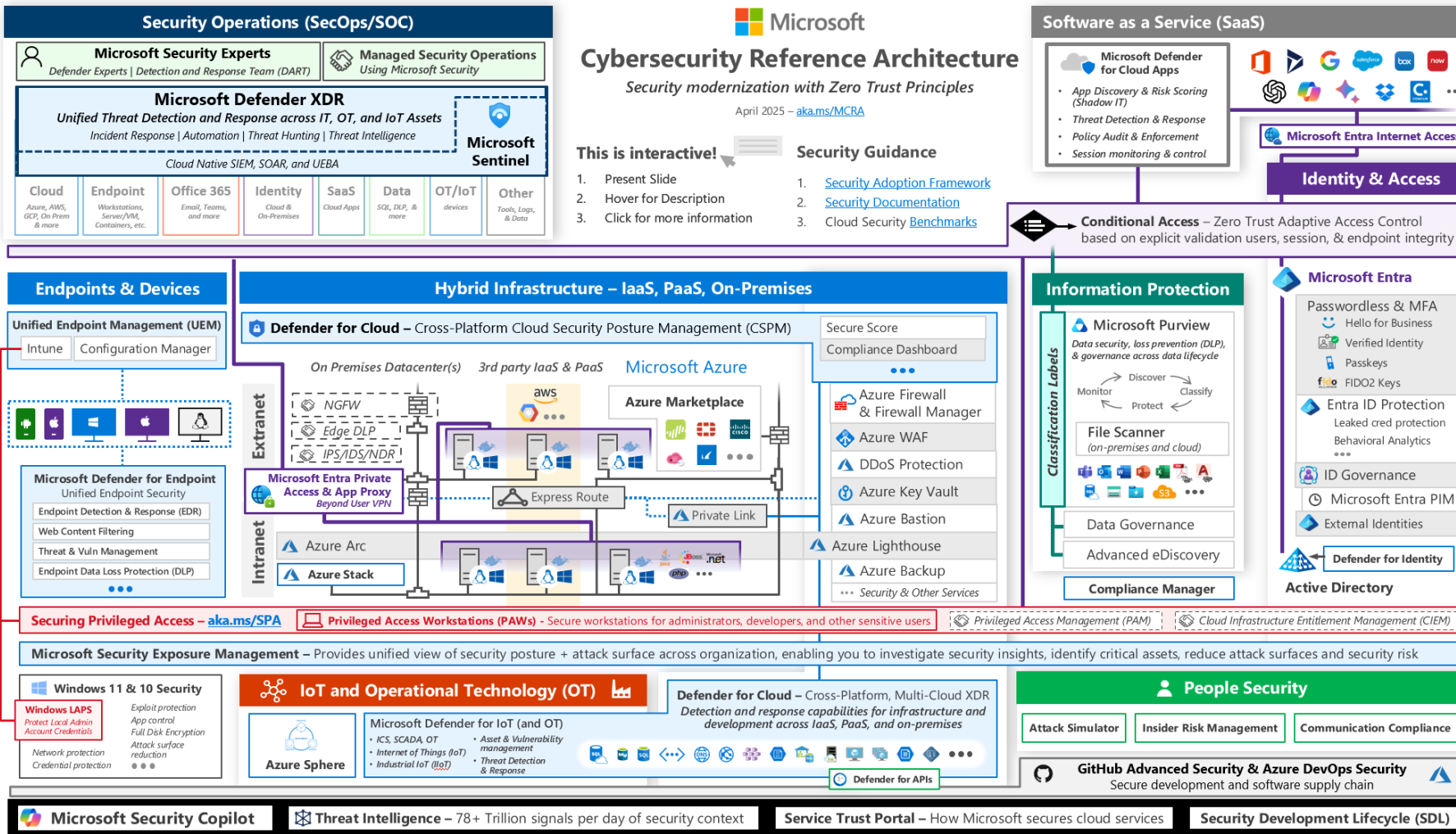


# Ich brauche Daten zur „Attack Surface“



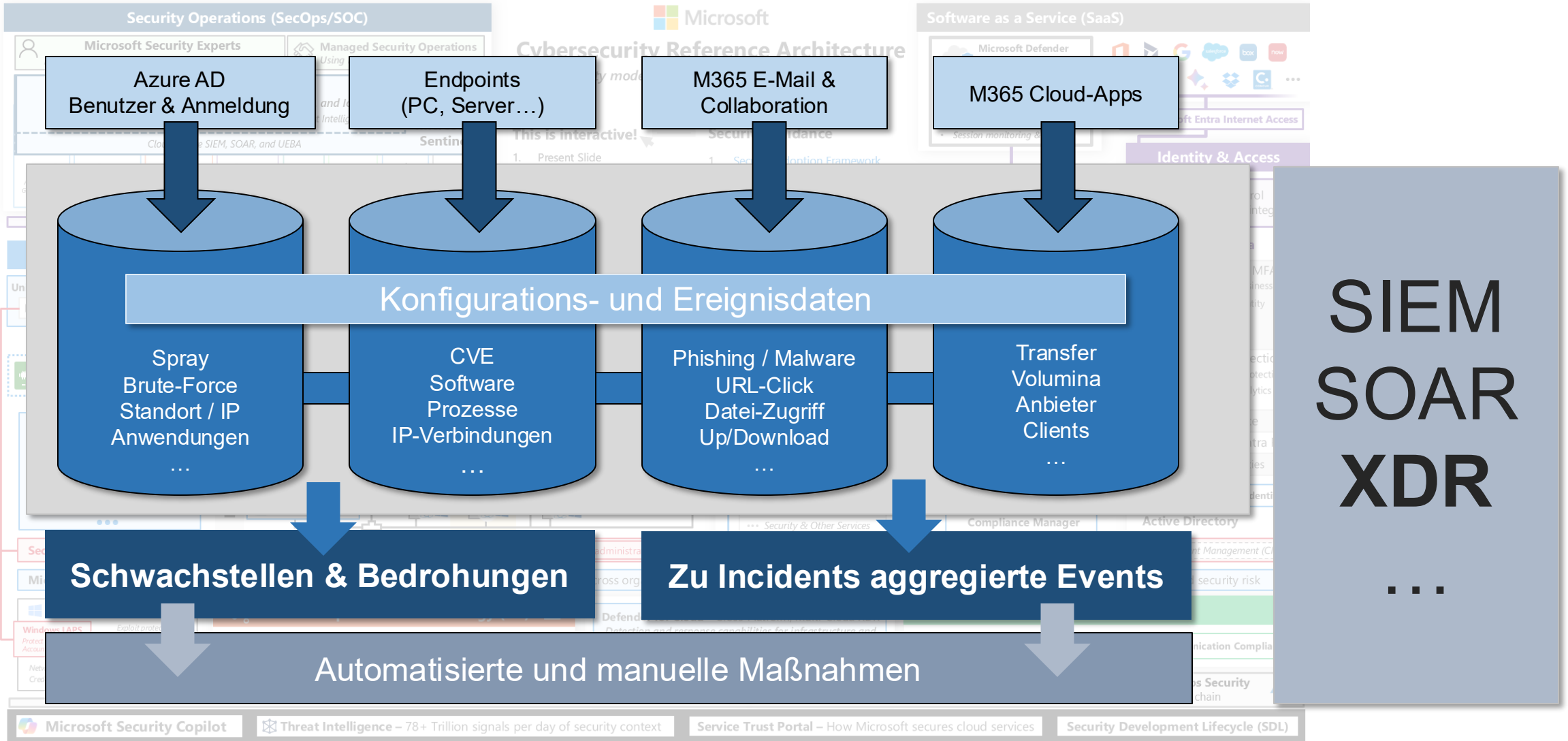
# Auf dem Weg zu SIEM, XDR und SOC

## Die „Lösung“ in der Microsoft-Welt:



# Auf dem Weg zu SIEM, XDR und SOC

## Daten, Daten, Daten



# Auf dem Weg zu SIEM, XDR und SOC

## Start in den CISO-Tag

The screenshot shows the Microsoft Azure portal interface. The main content area displays 'My roles | Microsoft Entra roles' with a table of eligible assignments. A dialog box titled 'Activate - Security Reader' is open, showing options for activation, duration, and a reason for activation.

Role	Scope	Membership
Security Reader	Directory	Direct
Security Administrator	Directory	Direct
Reports Reader	Directory	Direct
Compliance Data Administrator	Directory	Direct
Security Operator	Directory	Direct

**Activate - Security Reader**  
Privileged Identity Management | Microsoft Entra roles

Roles **Activate** Status

Custom activation start time

Duration (hours) 10

Reason (max 500 characters) \*  
CISO möchte sich einen Überblick verschaffen.



# Auf dem Weg zu SIEM, XDR und SOC

## Was ist denn so passiert?

**HSD** Microsoft Defender

Search

Home

Exposure management

Investigation & response

Incidents & alerts

Incidents

Alerts

Hunting

Actions & submissions

Partner catalog

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Overview

Investigations

Explorer

Review

Campaigns

Threat tracker

Attack simulation training

Policies & rules

Cloud apps

### Incidents

Most recent incidents and alerts

Export Copy list link Refresh

30 Days 399 Incidents Search for name or ID Customize columns

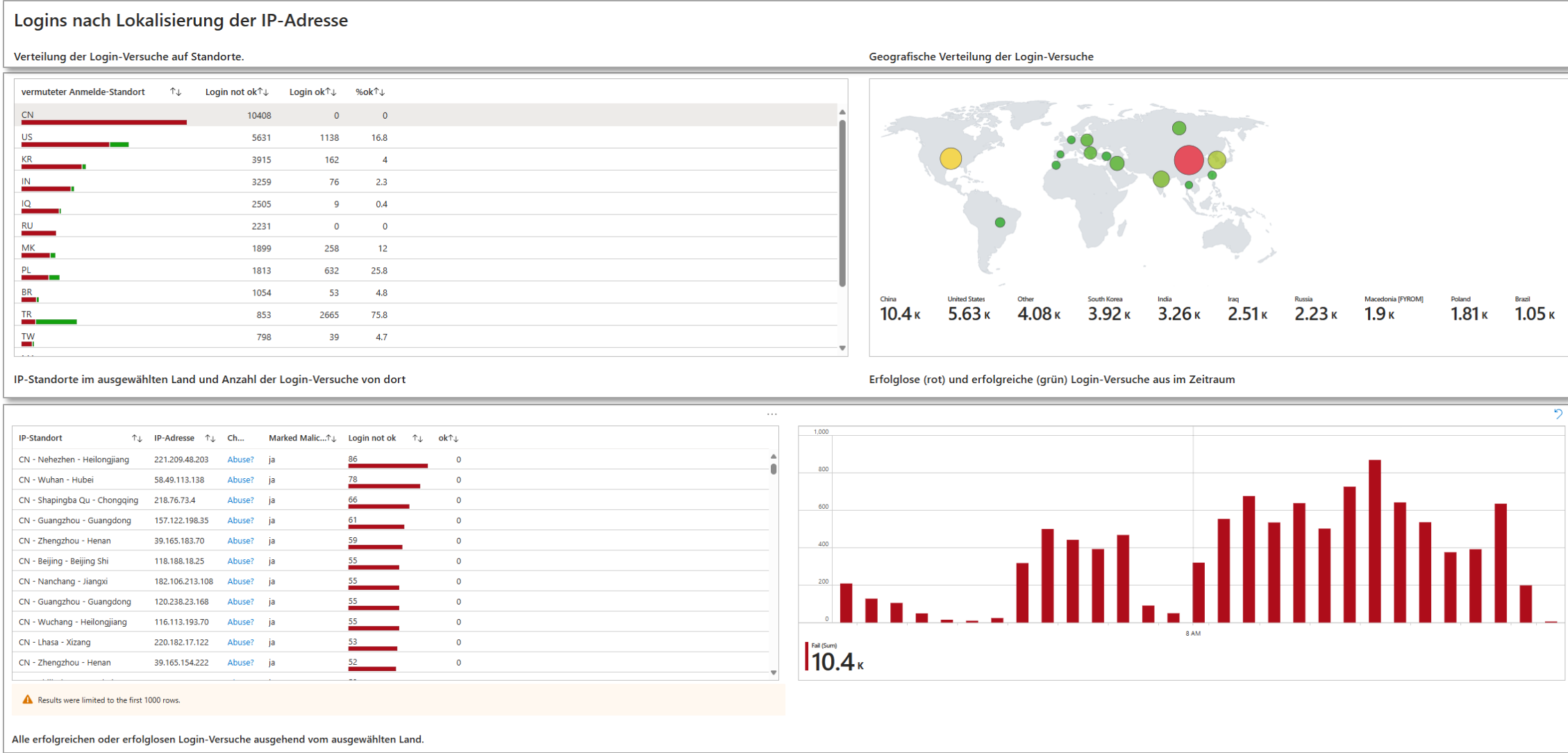
Filter set: Save

Add filter

Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Active alerts	Service sources	Detection sources	First activity	Last activity	Data sensitivity	Status
> Suspected password compromise by AiTM attack ...	30096	CSOC NotInService	High		Persistence	0/1	Microsoft Sentinel	Scheduled detection	29 Jul 2025 11:35	29 Jul 2025 11:35		Resolved
> Multi-stage incident involving Initial access & Cre...	30112	CSOC NotInService	High		Initial access, Credential ac...	0/7	Identity Protection, Micros...	AAD Identity Protection, Sc...	30 Jul 2025 00:04	30 Jul 2025 06:19		Resolved
> Email reported by user as not junk involving one ...	30169	CSOC AutoClose +1	Low	Queued	Initial access	0/1	Office 365	MDO	2 Aug 2025 15:50	2 Aug 2025 15:51		Resolved
> Anonymous IP address involving one user	30170		High		Initial access	0/2	Identity Protection	AAD Identity Protection	2 Aug 2025 21:10	2 Aug 2025 21:10		Resolved
> Tenant Allow/Block List entry is about to expire	30172		Informational	Queued	Initial access	0/1	Office 365	MDO	3 Aug 2025 06:39	3 Aug 2025 06:40		Resolved
> Email reported by user as junk involving one user	30173	CSOC AutoClose	Low	Queued	Initial access	0/1	Office 365	MDO	3 Aug 2025 10:43	3 Aug 2025 10:44		Resolved
> User requested to release a quarantined message ...	30174	CSOC AutoClose	Informational	Queued	Initial access	0/1	Office 365	MDO	3 Aug 2025 11:37	3 Aug 2025 11:37		Resolved
> Email reported by user as junk involving one user	30175	CSOC AutoClose +1	Low	Queued	Initial access	0/1	Office 365	MDO	3 Aug 2025 13:10	3 Aug 2025 13:11		Resolved
> User requested to release a quarantined message ...	30176	AutoClose +1	Informational	Queued	Initial access	0/1	Office 365	MDO	3 Aug 2025 19:32	3 Aug 2025 19:32		Resolved
> Tenant Allow/Block List entry is about to expire	30177		Informational	Queued	Initial access	0/1	Office 365	MDO	3 Aug 2025 20:42	3 Aug 2025 20:43		Resolved
> User requested to release a quarantined message ...	30178	CSOC AutoClose	Informational	Queued	Initial access	0/1	Office 365	MDO	4 Aug 2025 08:36	4 Aug 2025 08:37		Resolved
> Email reported by user as junk	30179	CSOC AutoClose	Low	Queued	Initial access	0/1	Office 365	MDO	4 Aug 2025 08:42	4 Aug 2025 08:43		Resolved
> [CSOC] SSH Tunnel connection detected	30180		Medium		Command and control	0/1	Endpoint	Custom detection	4 Aug 2025 09:17	4 Aug 2025 10:12		Resolved
> User requested to release a quarantined message ...	30181	CSOC AutoClose	Informational	Queued	Initial access	0/1	Office 365	MDO	4 Aug 2025 09:47	4 Aug 2025 09:47		Resolved
> 'Wacatac' malware was prevented	30182	CSOC SOAR Close	Informational	Terminated by system	Malware	0/1	Endpoint	Antivirus	4 Aug 2025 10:11	4 Aug 2025 10:11		Resolved
> Tenant Allow/Block List entry is about to expire	30183		Informational	Queued	Initial access	0/1	Office 365	MDO	4 Aug 2025 10:25	4 Aug 2025 10:26		Resolved
> Email reported by user as not junk	30184	CSOC AutoClose	Low	Queued	Initial access	0/1	Office 365	MDO	4 Aug 2025 11:12	4 Aug 2025 11:13		Resolved
> 'DownloadSponsor' unwanted software was preve...	30185	CSOC SOAR Close	Informational	Partially investigated	Defense evasion	0/1	Endpoint	Antivirus	4 Aug 2025 15:15	4 Aug 2025 15:15		Resolved

# Auf dem Weg zu SIEM, XDR und SOC

## Dashboard Benutzer-Angriffe



# Auf dem Weg zu SIEM, XDR und SOC

## Queries für alle Cyber-Lebenslagen

The screenshot shows the Microsoft Defender Advanced Hunting interface. The left sidebar contains navigation options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, System, and Customize navigation. The main area is titled 'Advanced hunting' and shows a list of queries under 'my queries'. The selected query is 'URLDomainQueryIdkatorenVerfassungsch...' and its code is displayed in the right pane. The query is a Kusto query designed to analyze email events related to phishing and malware. Below the code, the 'Results' tab shows a table with 4 items, including columns for ThreatTypes and Count.

```

5 //Emails pro Tag
7 |summarize EventCount = count() by bin(Timestamp, 1d)
8 |render timechart
9
10 //In den Email festgestellte Bedrohungen nach Typ
11 //Emails pro Tag
12 EmailEvents
13 |summarize Count = count() by ThreatTypes
14 |order by Count
15
16
17 //Phishing im zeitlichen Verlauf
18 EmailEvents
19 |where ThreatTypes has "Phish"
20 |summarize EventCount = count() by bin(Timestamp, 1d)
21 |render timechart
22
23 //Malware im zeitlichen Verlauf
24 EmailEvents
25 |where ThreatTypes has "Malware"
26 |summarize EventCount = count() by bin(Timestamp, 1d)
27 |render timechart
28
29 //Malware Email Events
30 EmailEvents
31 |where ThreatTypes has "Malware"
32 |project Timestamp,RecipientEmailAddress,SenderFromAddress,SenderFromDomain,Subject,DeliveryAction,AttachmentCount,EmailAction,DetectionMethods
33 |order by Timestamp
  
```

ThreatTypes	Count
>	27916
> Spam	1516
> Phish, Spam	493
> Phish	166

# Auf dem Weg zu SIEM, XDR und SOC

## IOC-Queries & Alarme

The screenshot shows the Microsoft Defender Advanced Hunting interface. The left sidebar contains navigation options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, System, and Customize navigation. The main area is titled "Advanced hunting" and shows a list of queries under "Shared queries". The selected query is "Successful exploitation via file creation". The query text is as follows:

```
1 DeviceFileEvents
2 | where FolderPath has_any (@'microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS', @'microsoft shared\Web Server Extensions\15\TEMPLATE\LAYOUTS')
3 | where FileName has "spinstall0" or FileName has "qlj22mpc" or FileName has "bjcloiyq"
4 | project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine, FileName, FolderPath, ReportId, ActionType, SHA256
5 | order by Timestamp desc
6
```

The interface also shows a search bar at the top, a "Run query" button, and a "Query history" tab at the bottom right.

# Auf dem Weg zu SIEM, XDR und SOC Schattenseite der Daten-Vielfalt



Hochschule Düsseldorf  
University of Applied Sciences

## HSD

### DATENSCHUTZ-FOLGENABSCHÄTZUNG FÜR DEN EINSATZ VON MICROSOFT-365 AN DER HOCHSCHULE DÜSSELDORF

Autoren:

**Kathrin Schweppe**, DSB

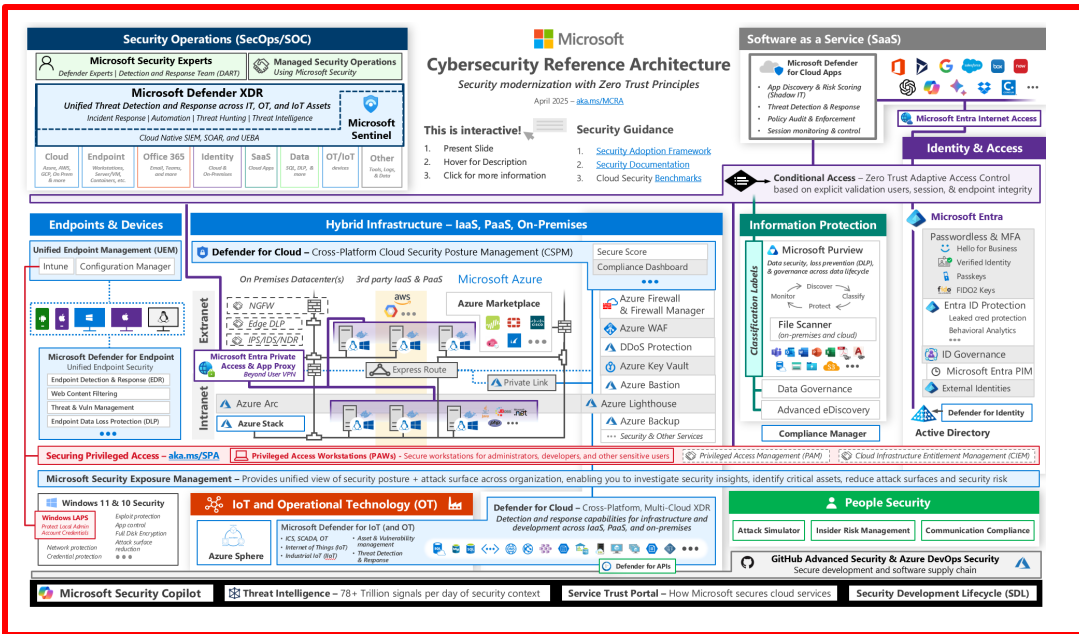
**Moritz Löbmann**, Cloud Solution Architect, Campus IT

**Dr. Christoph Glowatz**, CISO, Stabsstelle 3 Informationssicherheit

unter Verwendung der gemeinschaftlich von der KDU.NRW und der Reusch Rechtsanwalts-Gesellschaft mbH (reuschlaw) ausgearbeiteten DSFA-Vorlage „Einsatz von Microsoft-365 an Hochschulen“

# Auf dem Weg zu SIEM, XDR und SOC

## Wir brauchen Unterstützung



Wie funktioniert das eigentlich alles?

Wie optimiere ich die **Grund-Konfiguration** der Umgebung?

Wie „**onboarde**“ ich die Systeme („Endpoints“) richtig?

Welche **Incidents** sind wirklich **wichtig**?

Wer achtet kontinuierlich auf die Meldungen?

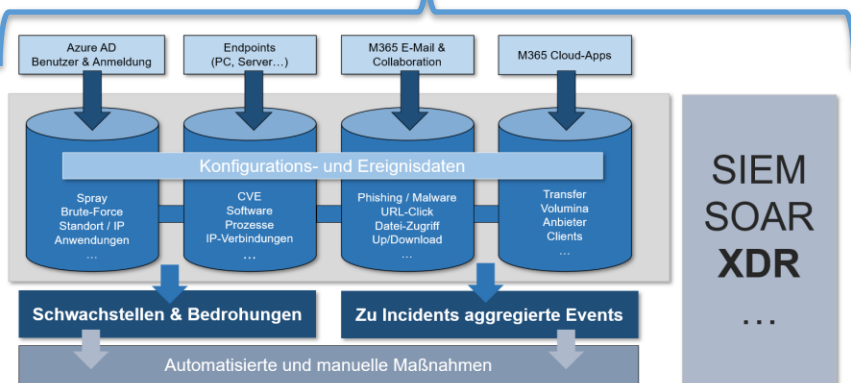
Wo und wie kann ich **automatisieren**?

Wer reagiert wie **nach Dienstschluss**?

Was passiert, wenn es richtig „**knallt**“?

Gesucht:

**Fähige Köpfe zur rechten Zeit**



...und fertig

Danke schön!