Hochschule Düsseldorf
University of Applied Sciences

HSD

DISM
HSD

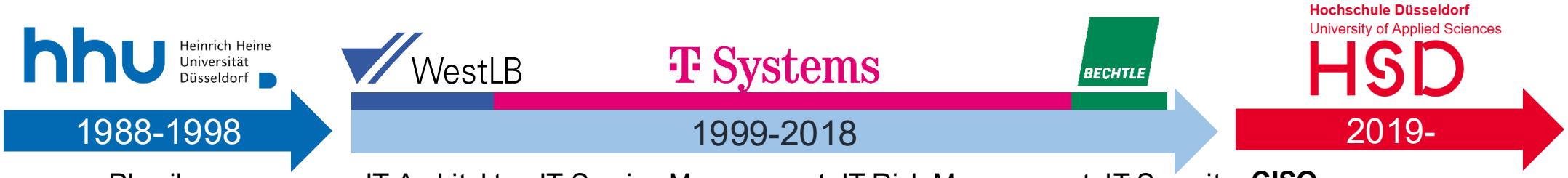
Informationssicherheit an der HSD

Teil 1: Das DISM an der HSD
Teil 2: Auf dem Weg zu SIEM, XDR und SOC

Christoph Glowatz – CISO HSD

CISO und Stabsstelle 3

Dr. Christoph Glowatz
Stabsstelle 3 Informationssicherheit (2 MA)
christoph.glowatz@hs-duesseldorf.de



Erster Teil

Das DISM an der HSD

Ab 2019: Datenschutz- und Informationssicherheits-Management @HSD

Auftrag:

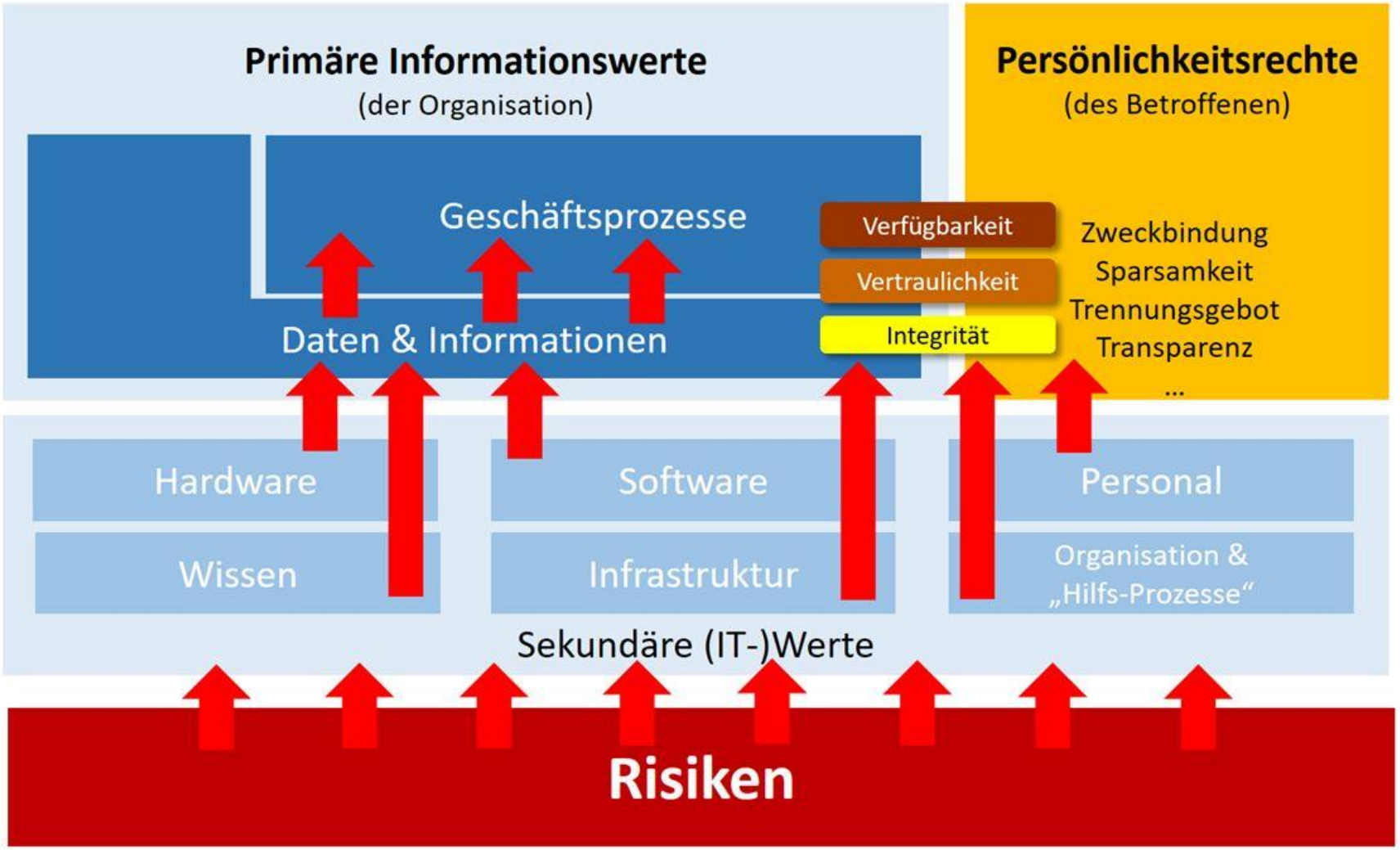
- Aufbau eines integrierten **Datenschutz- und Informationssicherheits-Management**;
- Informationssicherheit in **„Anlehnung“ an BSI-Grundschutz**;

Hochschule Düsseldorf
University of Applied Sciences
HSD

2019-

CISO
stellv. DSB
Datenschutz &
Informationssicherheits-Management

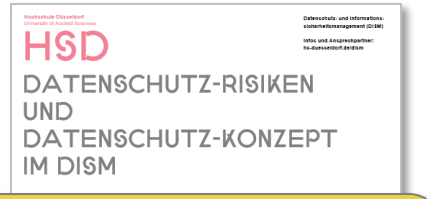
Stelle Datenschutz & Informationssicherheit nebeneinander



Zur Illustration: Behandlung von „Verfahren“ im DISM

„Anmeldung“ des Verfahrens im DISM (Inventarisierung und Aufnahme ins VVT)

Dokumentation des Verfahrens nach Art. 30 DSGVO
Welche Rechtsgrundlage?
Welche Daten?
Wer ist betroffen?
Wer verarbeitet?
Wie wird geschützt?



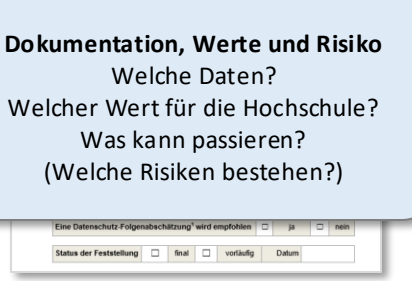
Risiken für den Betroffenen
Wert der Daten für den Betroffenen?
Risiken für den Betroffenen?

Technisch-Organisatorische Maßnahmen
Was unternimmt die Hochschule zum Schutz der Rechte der Betroffenen?

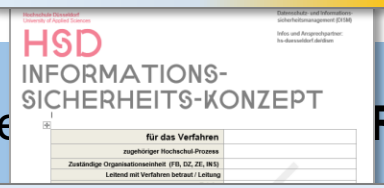
Datenschutz: Schutz **VOR** den **personenbezog**

Welche Risiken bestehen?
Wie hoch ist der Schutzbedarf?

Dokumentation, Werte und Risiko
Welche Daten?
Welcher Wert für die Hochschule?
Was kann passieren?
(Welche Risiken bestehen?)



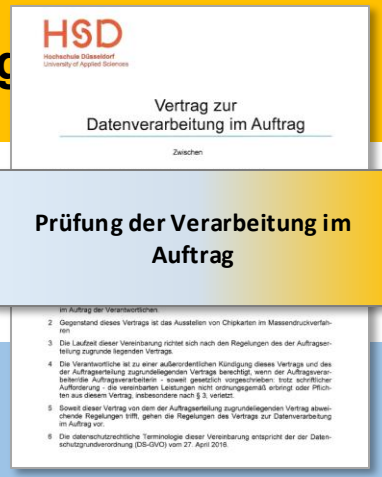
Wie reduziere ich die Risiken?
Wie schütze ich die Betroffenen und die Hochschule?



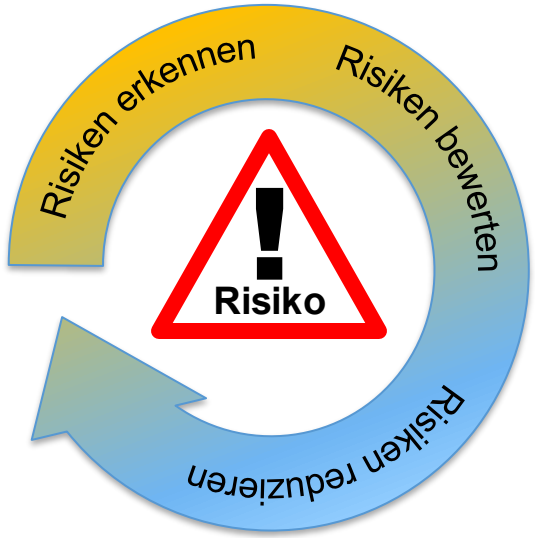
Technisch-Organisatorische Maßnahmen
Was unternimmt die Hochschule zum Schutz der Informationswerte?

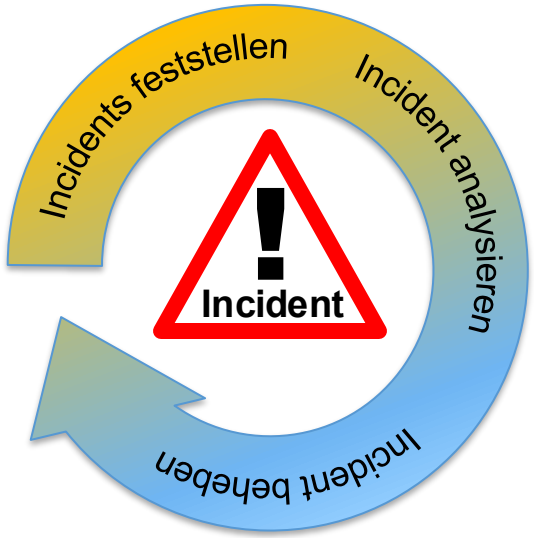
ationssiche R Daten

Prüfung der Verarbeitung im Auftrag



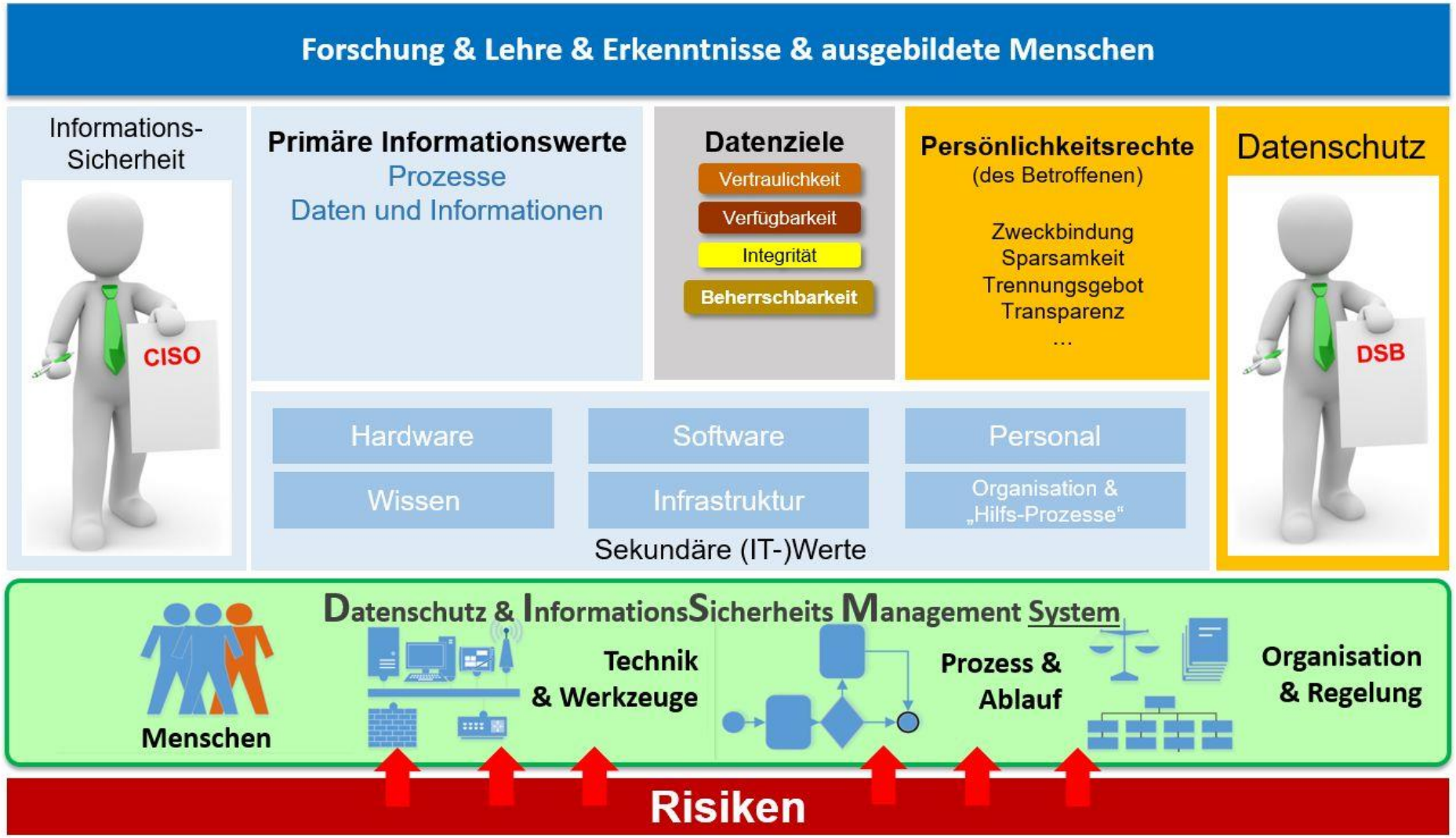
Übergang in den kontinuierlichen DISM-Betrieb



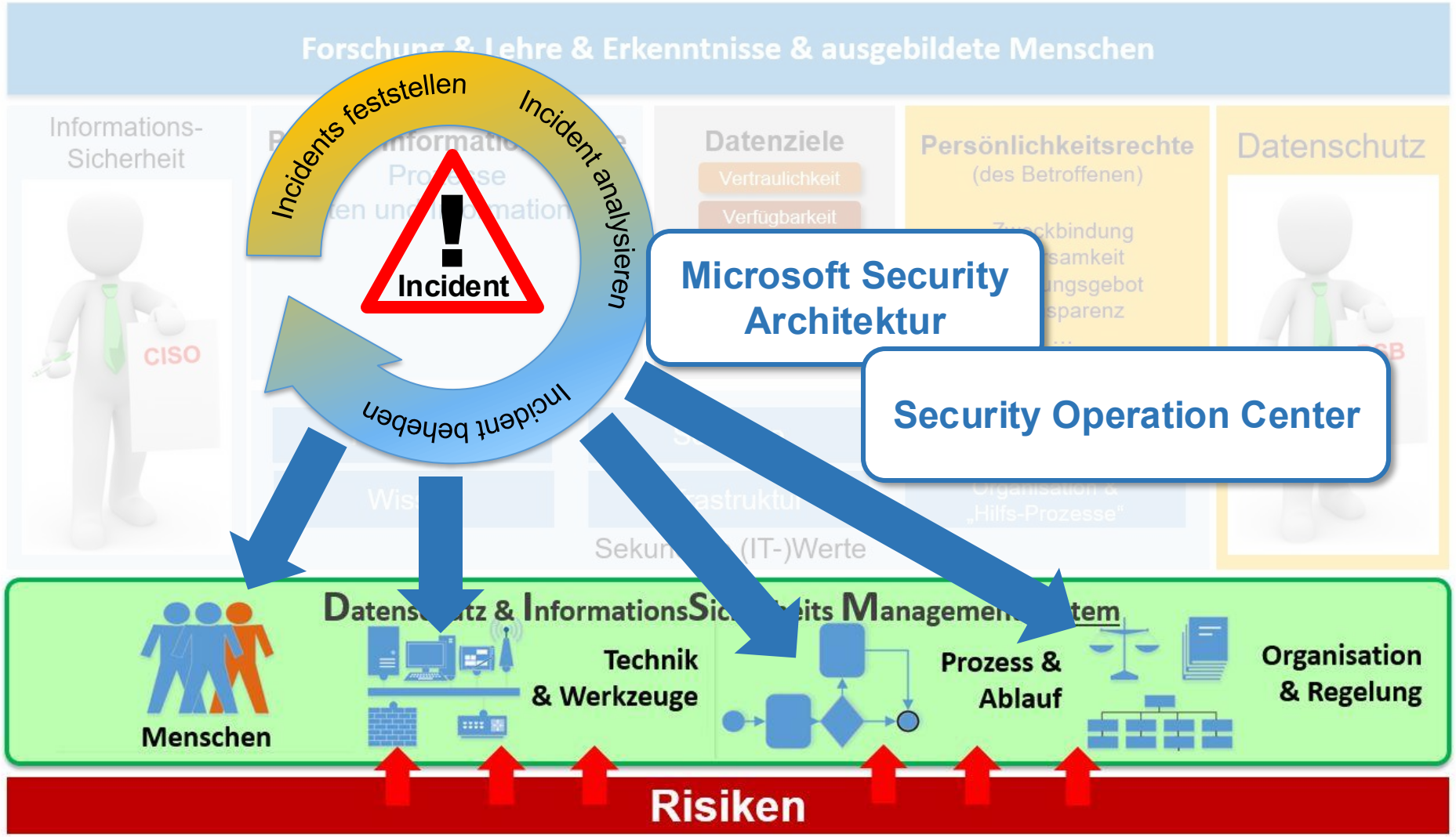


Initiale Behandlung im DISM — Zyklisches **Risiko-Management** — **Incident-Management**

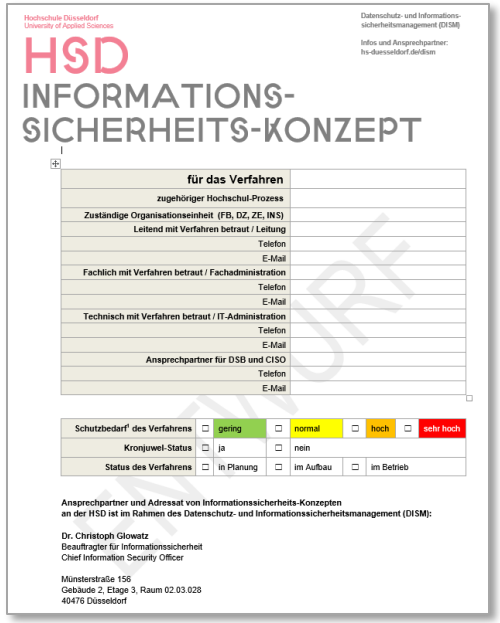
Das DISM zwischen Werten und Risiken

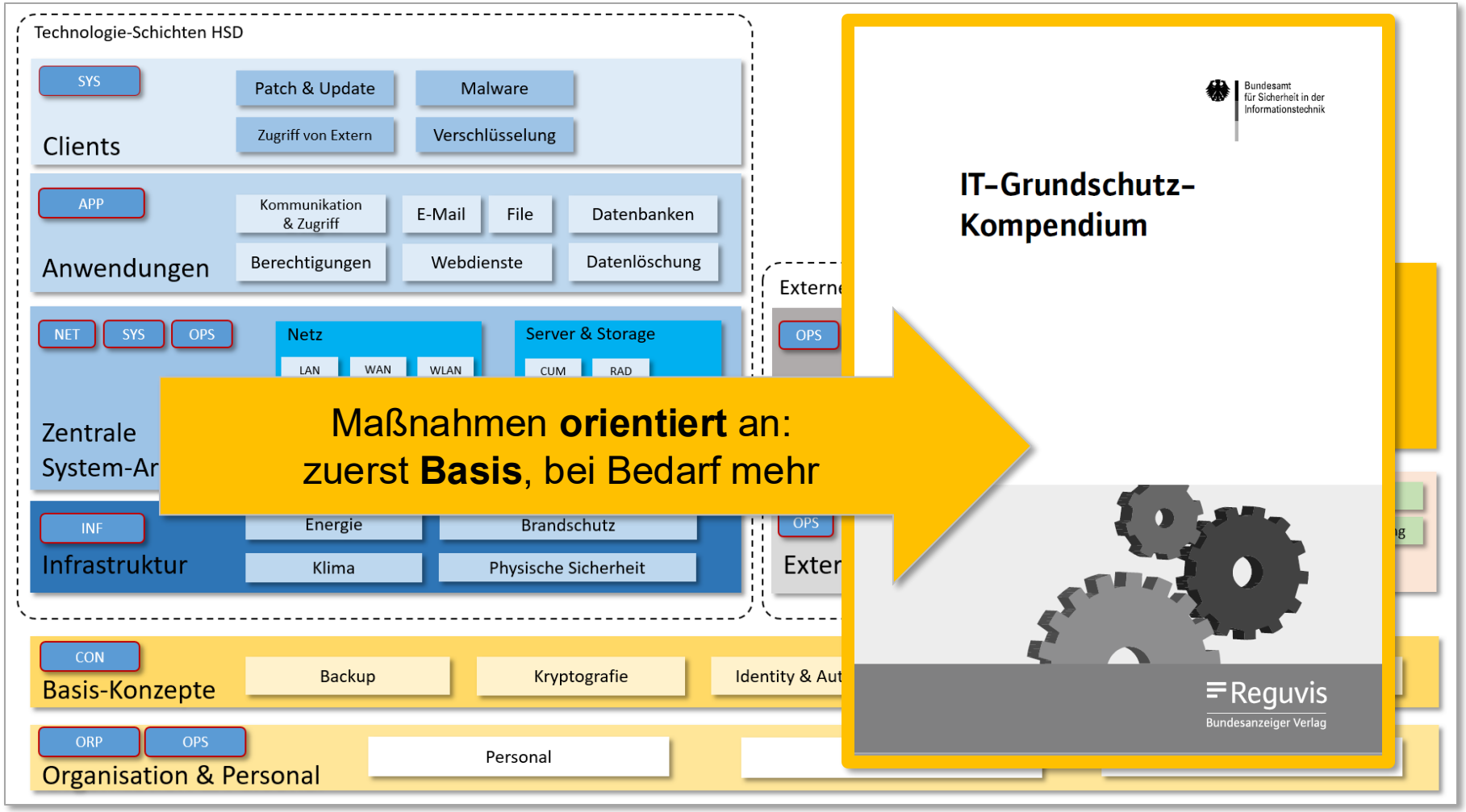


Incident Management im DISM

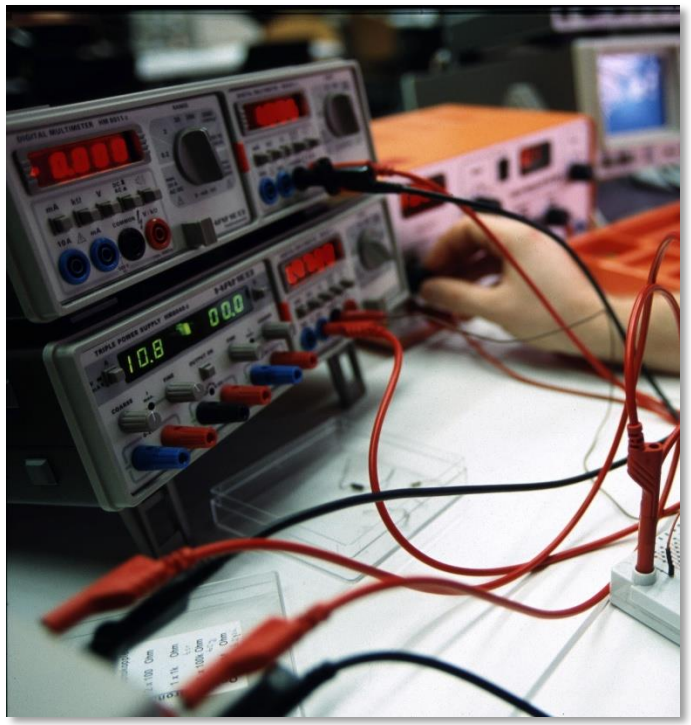


BSI-Grundschutz im DISM: Von der „Anlehnung“ zur VzC…





Prinzip 1: Hochschule bleibt Hochschule

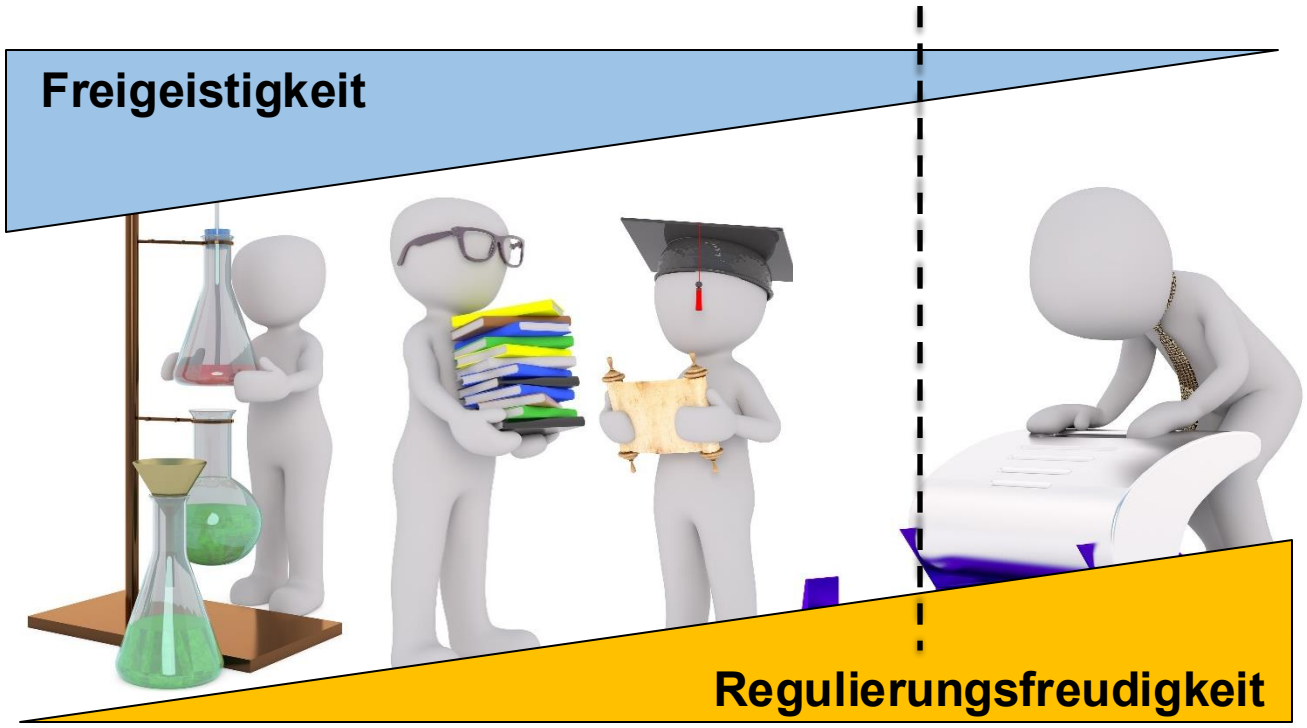


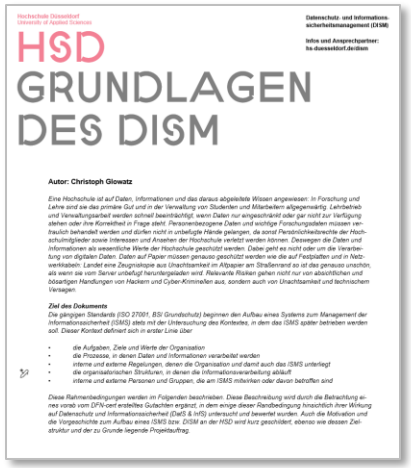
Daten → Informationen → Wissen

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“

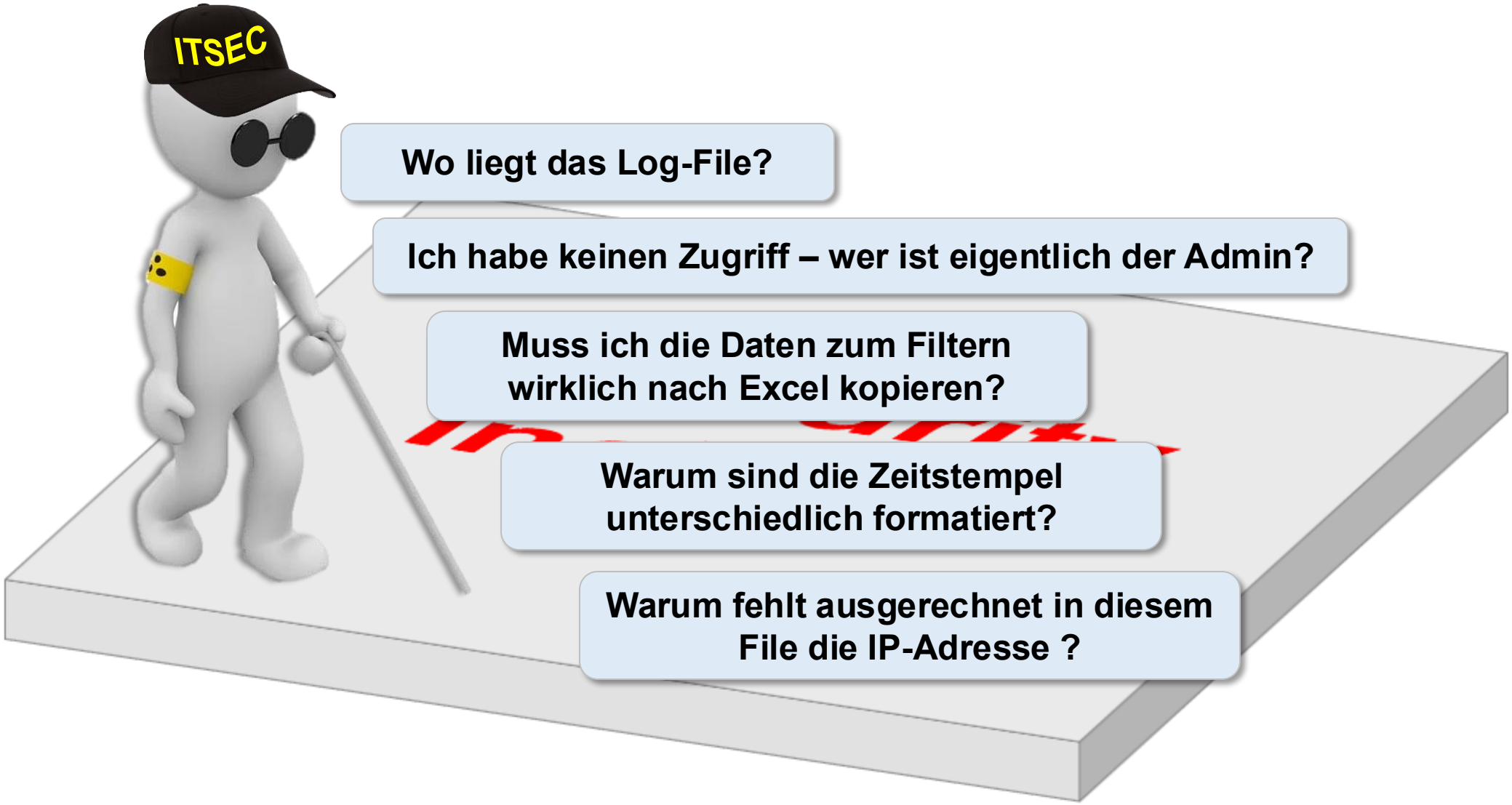
Der spezielle Risiko-Kontext „Hochschule“ muss stets berücksichtigt werden!

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

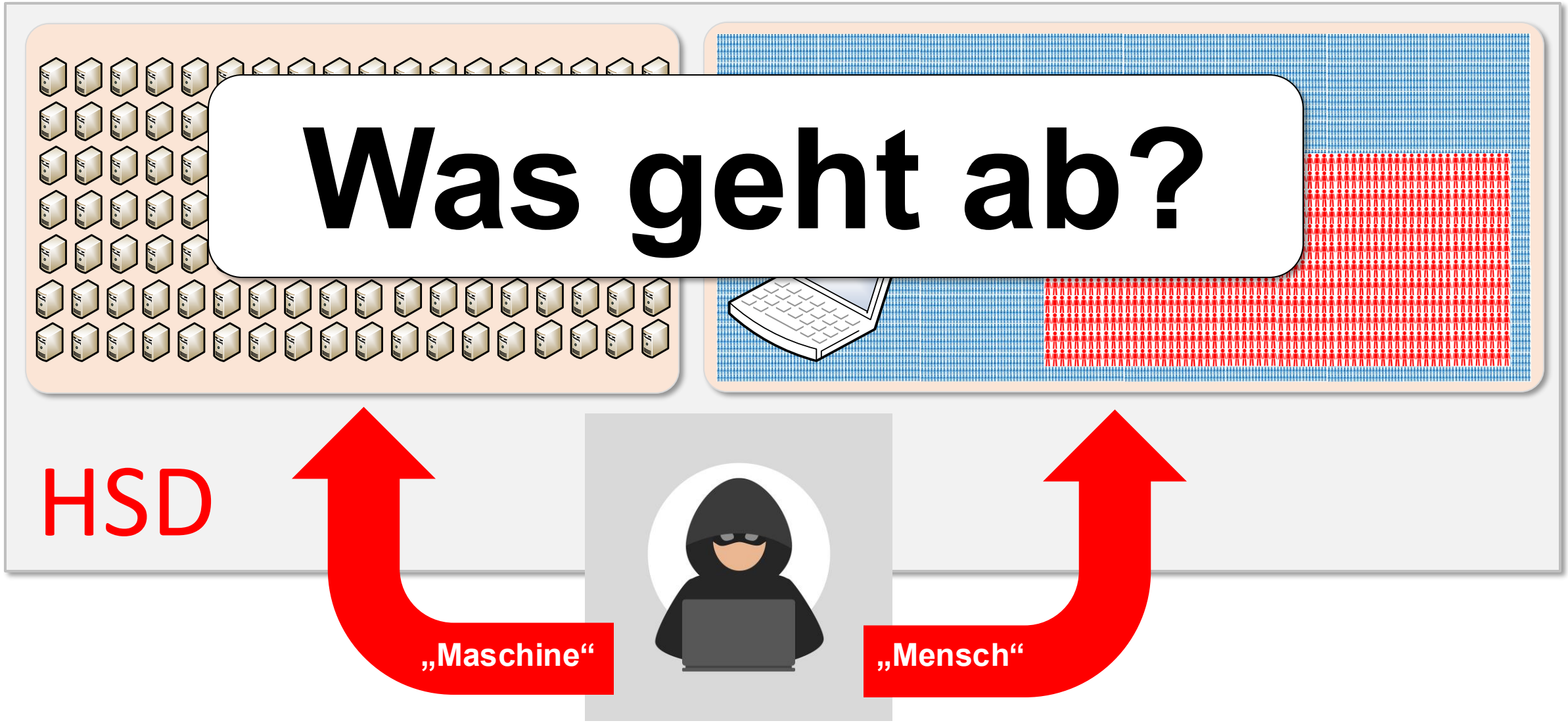
Zweiter Teil

Auf dem Weg zu SIEM, XDR und SOC

Was den CISO (und seine Kolleg*innen) nervös macht…

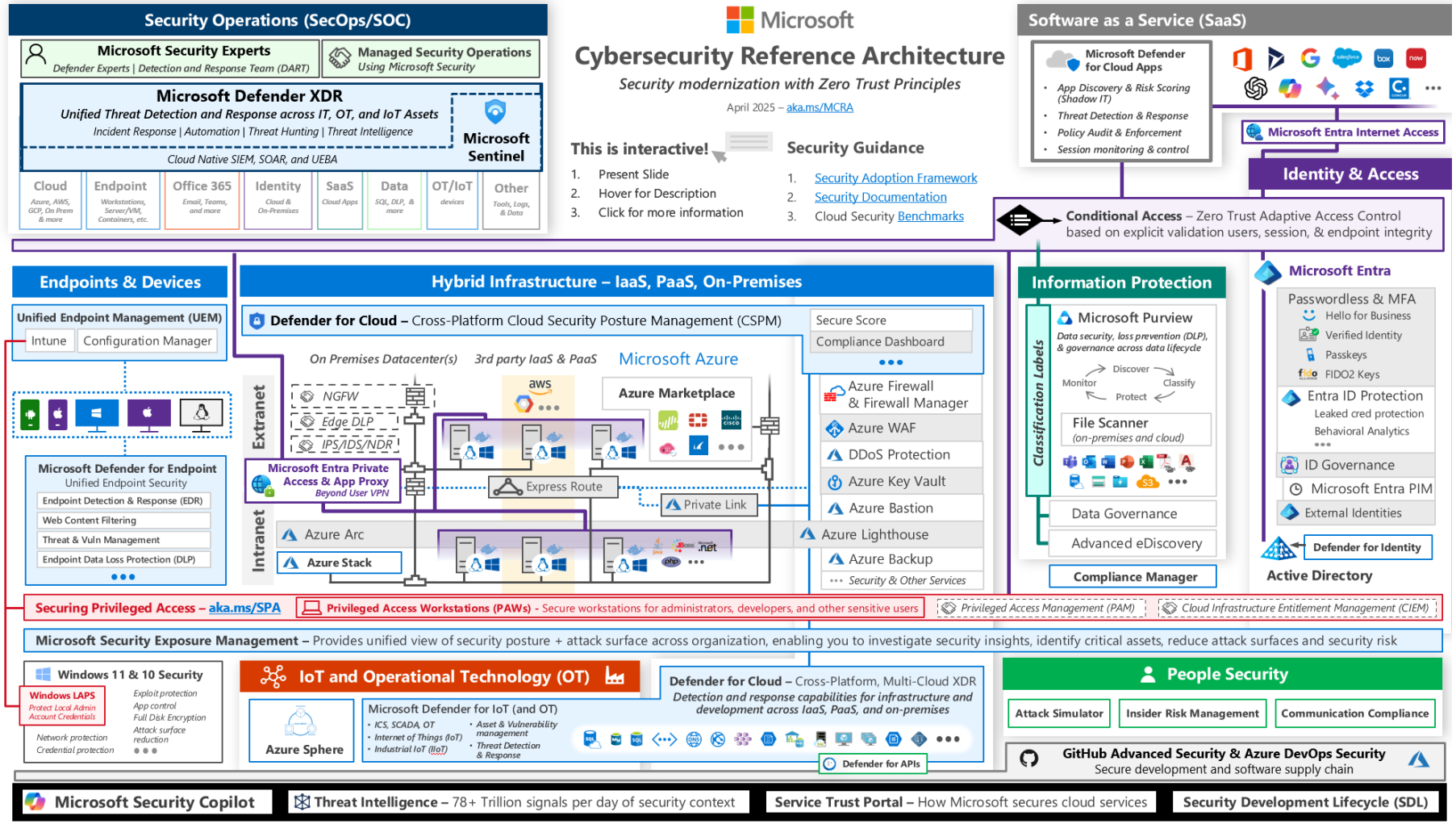


Ich brauche Daten zur „Attack Surface“



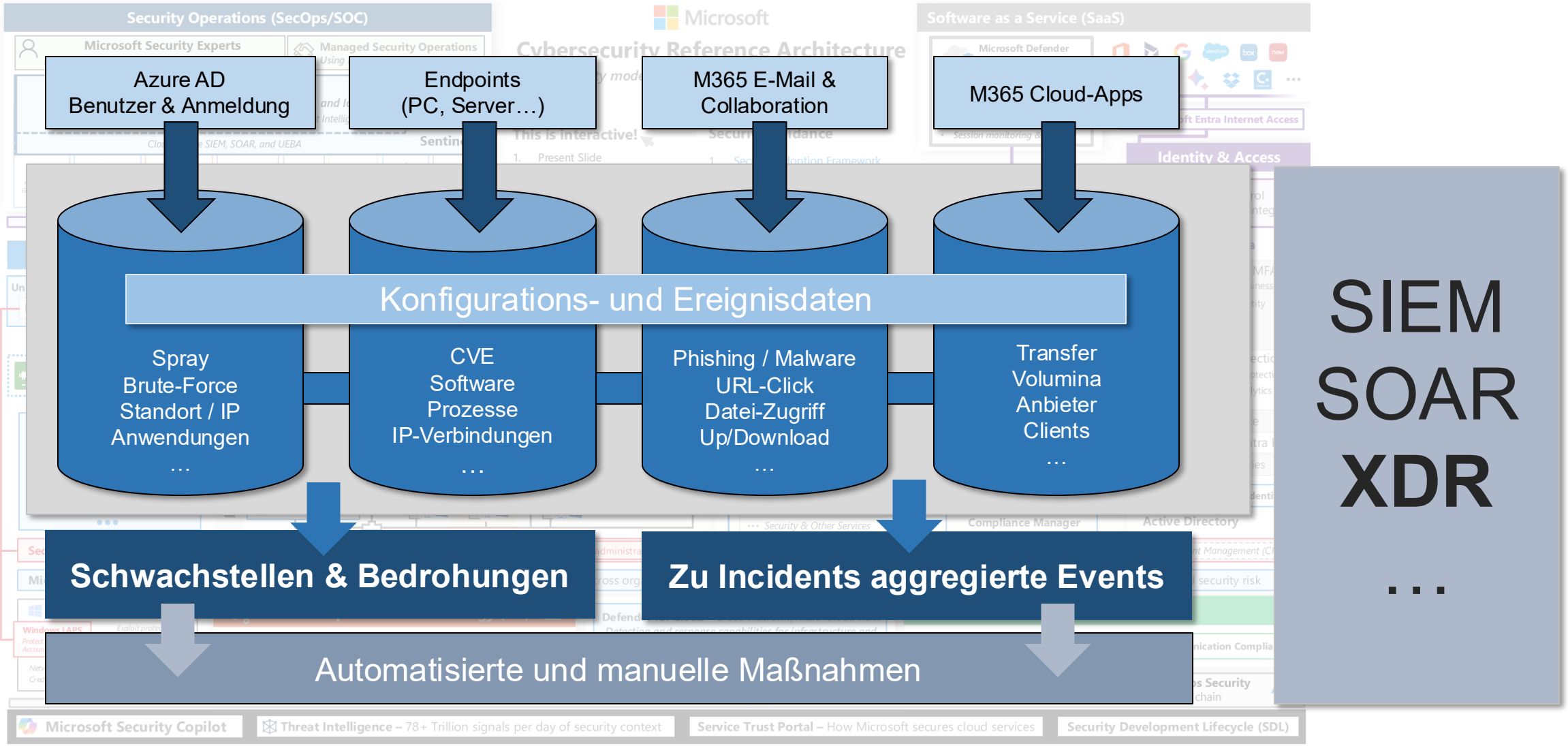
Auf dem Weg zu SIEM, XDR und SOC

Die „Lösung“ in der Microsoft-Welt:

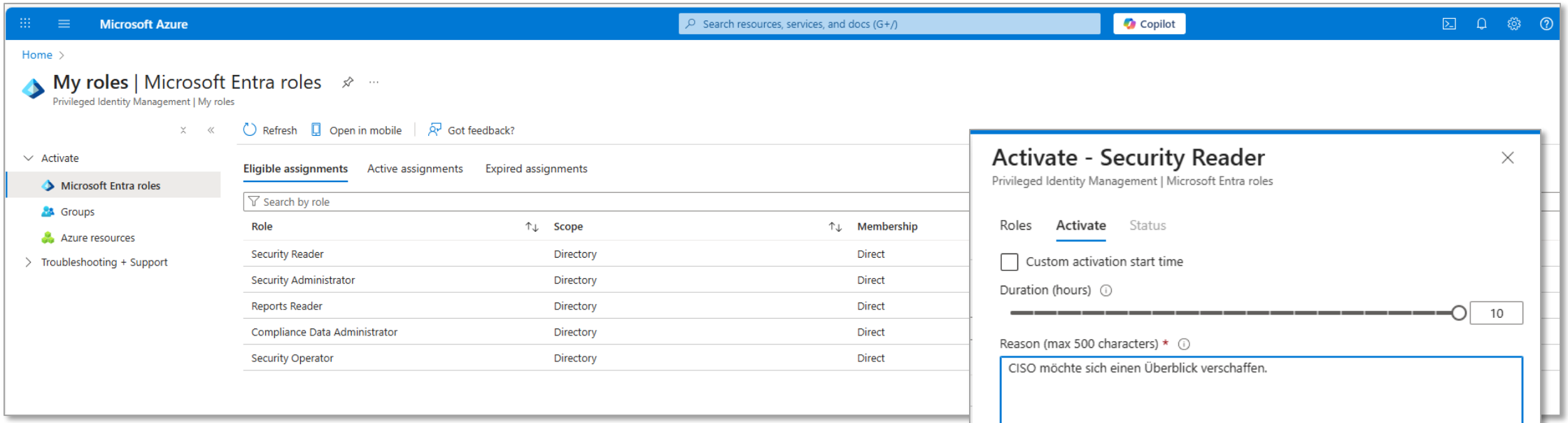


Auf dem Weg zu SIEM, XDR und SOC

Daten, Daten, Daten

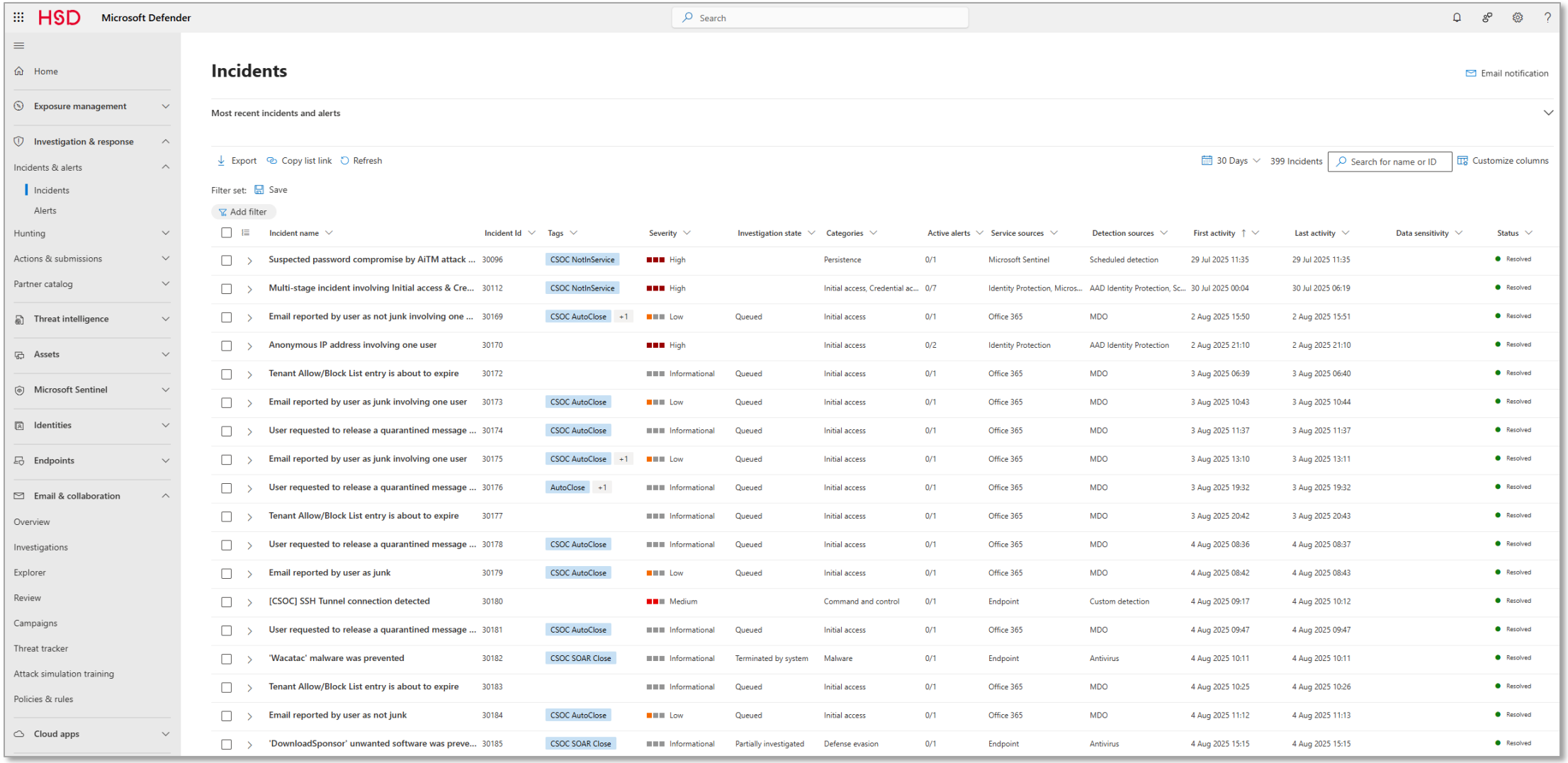


Start in den CISO-Tag



Auf dem Weg zu SIEM, XDR und SOC

Was ist denn so passiert?



Dashboard Benutzer-Angriffe

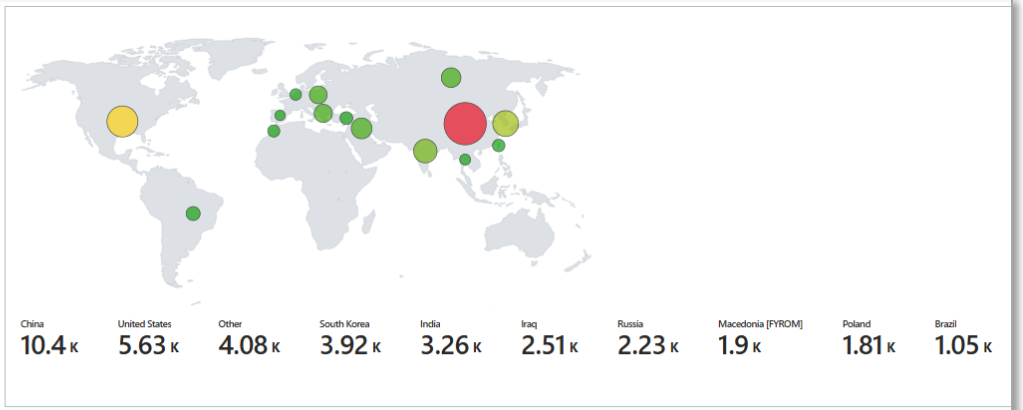
Logins nach Lokalisierung der IP-Adresse

Verteilung der Login-Versuche auf Standorte.

vermuteter Anmelde-Standort	Login not ok	Login ok	%ok
CN	10408	0	0
US	5631	1138	16.8
KR	3915	162	4
IN	3259	76	2.3
IQ	2505	9	0.4
RU	2231	0	0
MK	1899	258	12
PL	1813	632	25.8
BR	1054	53	4.8
TR	853	2665	75.8
TW	798	39	4.7

IP-Standorte im ausgewählten Land und Anzahl der Login-Versuche von dort

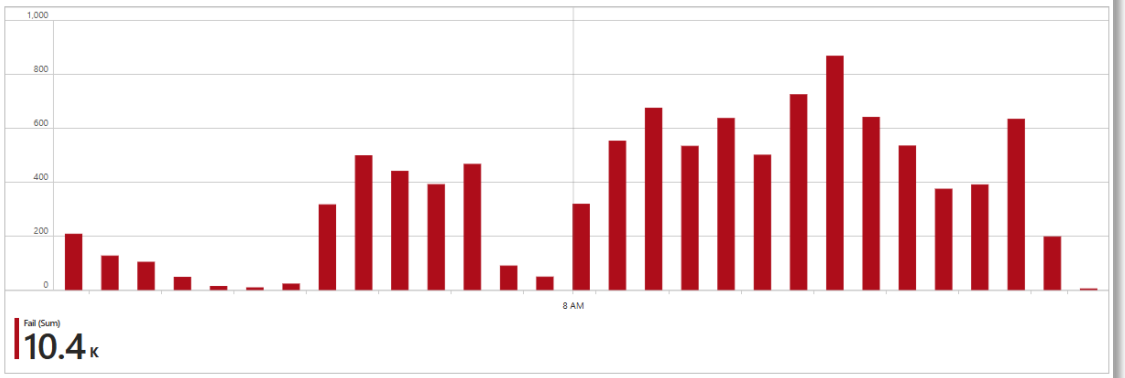
Geografische Verteilung der Login-Versuche



Erfolglose (rot) und erfolgreiche (grün) Login-Versuche aus im Zeitraum

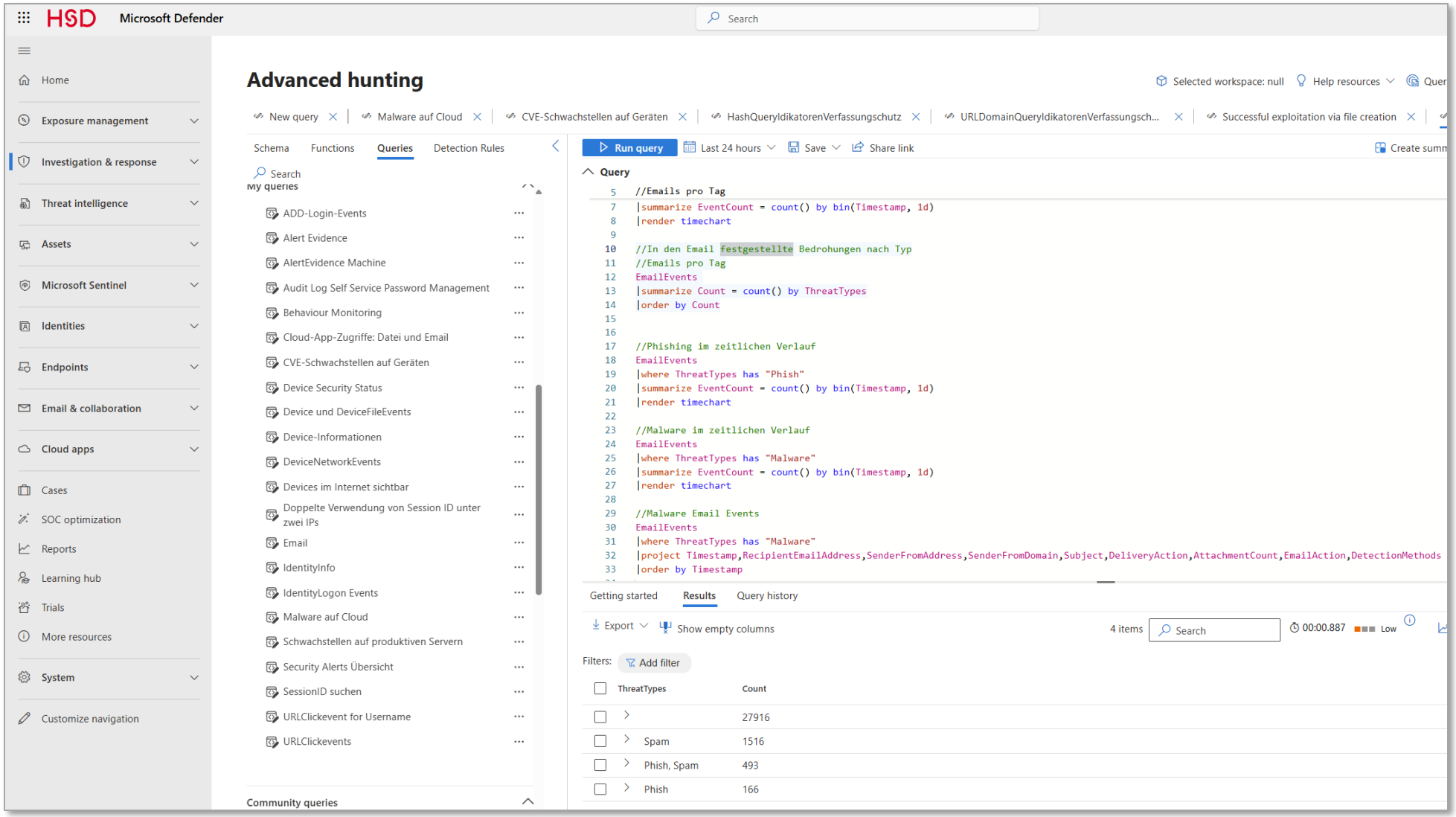
IP-Standort	IP-Adresse	Ch...	Marked Malic...	Login not ok	ok
CN - Nehezhen - Heilongjiang	221.209.48.203	Abuse?	ja	86	0
CN - Wuhan - Hubei	58.49.113.138	Abuse?	ja	78	0
CN - Shapingba Qu - Chongqing	218.76.73.4	Abuse?	ja	66	0
CN - Guangzhou - Guangdong	157.122.198.35	Abuse?	ja	61	0
CN - Zhengzhou - Henan	39.165.183.70	Abuse?	ja	59	0
CN - Beijing - Beijing Shi	118.188.18.25	Abuse?	ja	55	0
CN - Nanchang - Jiangxi	182.106.213.108	Abuse?	ja	55	0
CN - Guangzhou - Guangdong	120.238.23.168	Abuse?	ja	55	0
CN - Wuchang - Heilongjiang	116.113.193.70	Abuse?	ja	55	0
CN - Lhasa - Xizang	220.182.17.122	Abuse?	ja	53	0
CN - Zhengzhou - Henan	39.165.154.222	Abuse?	ja	52	0

⚠ Results were limited to the first 1000 rows.

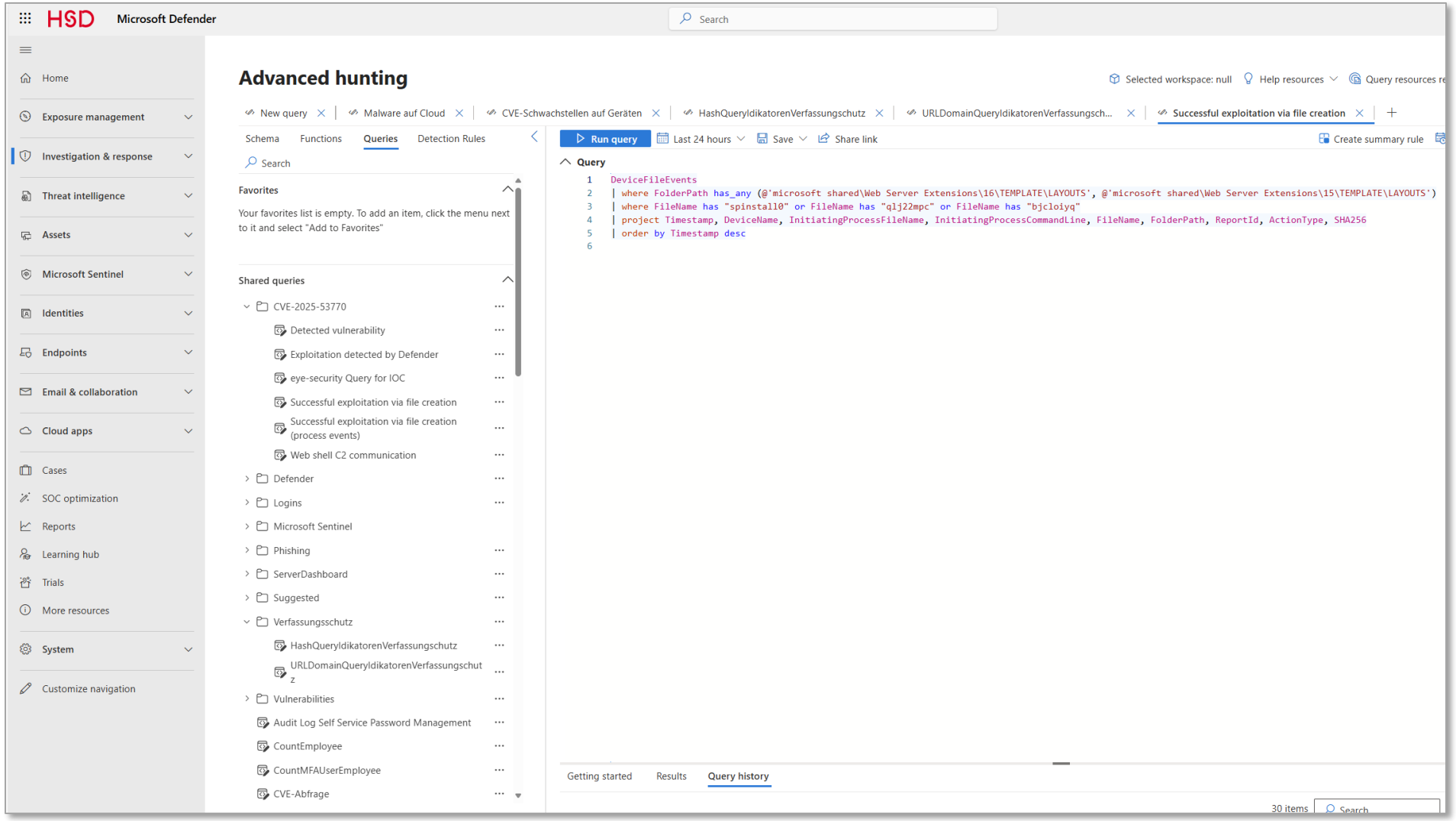


Alle erfolgreichen oder erfolglosen Login-Versuche ausgehend vom ausgewählten Land.

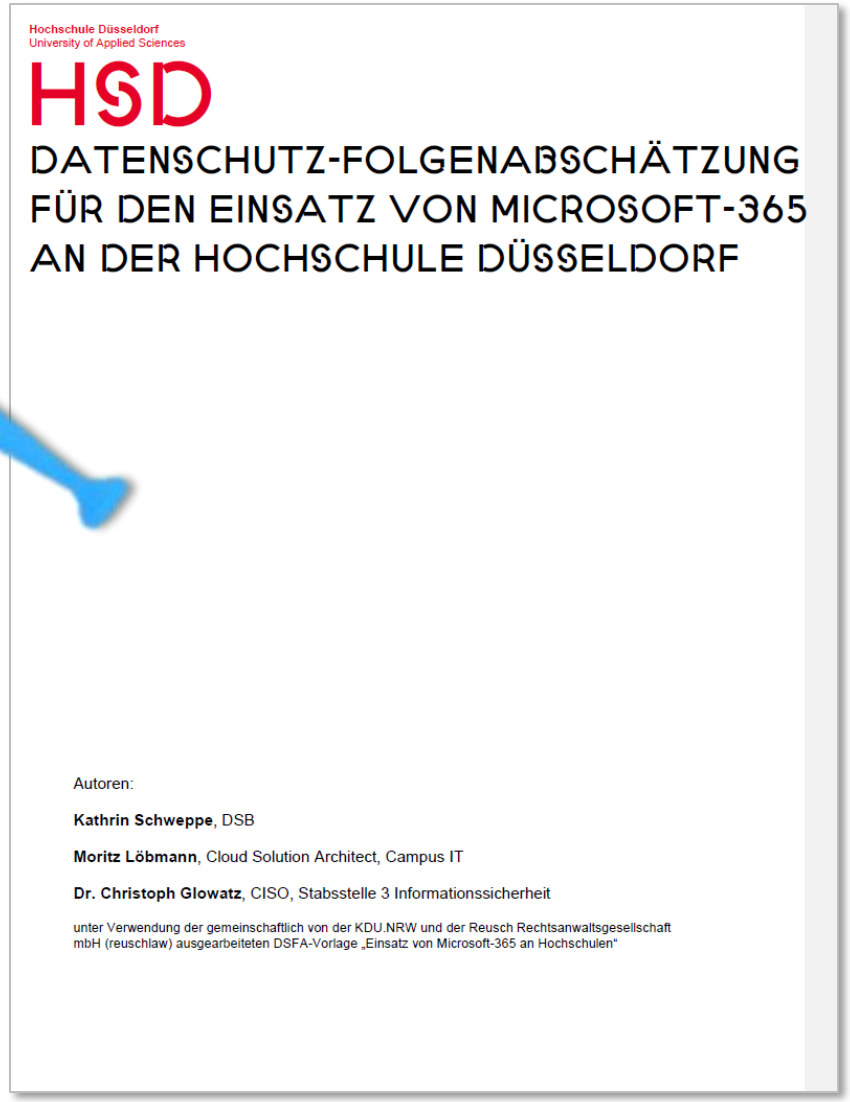
Queries für alle Cyber-Lebenslagen



IOC-Queries & Alarme



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

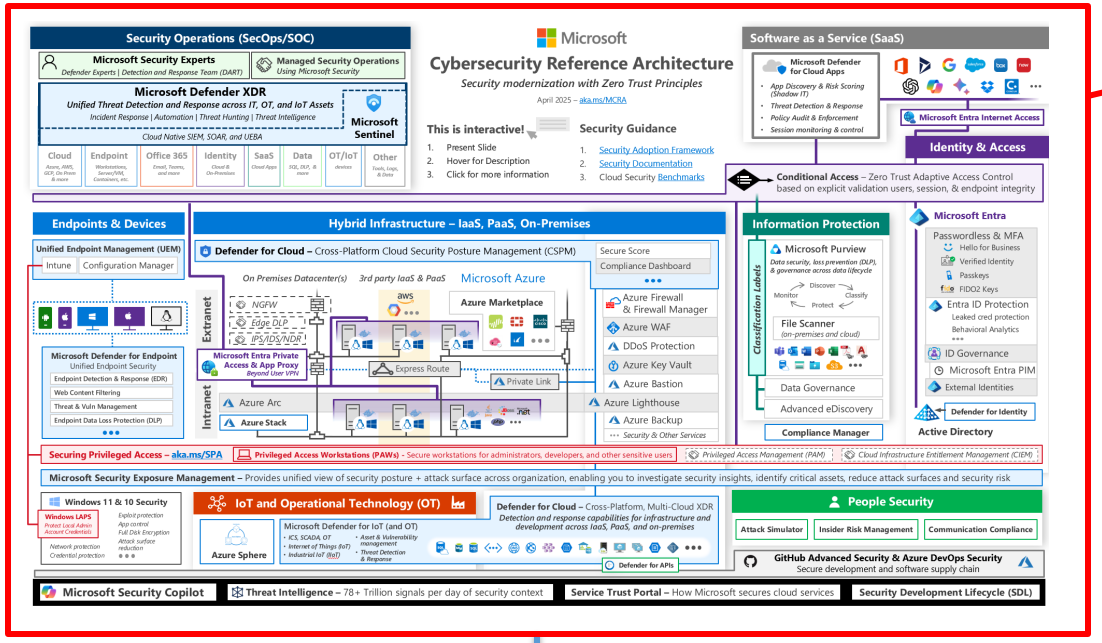
Moritz Löbmann, Cloud Solution Architect, Campus IT

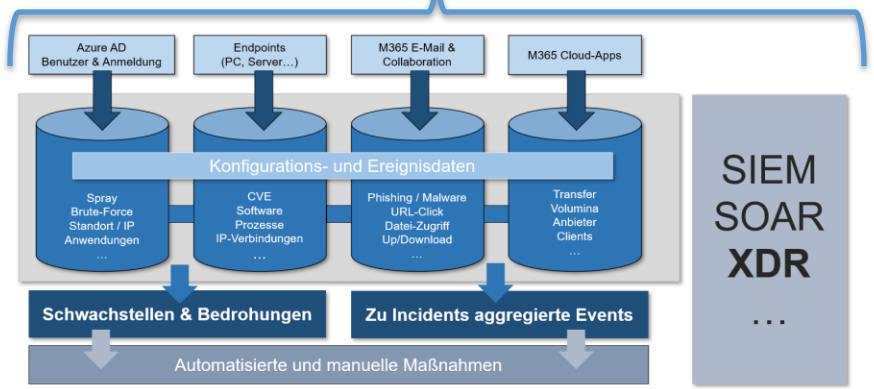
Dr. Christoph Glowatz, CISO, Stabsstelle 3 Informationssicherheit

unter Verwendung der gemeinschaftlich von der KDU.NRW und der Reusch Rechtsanwaltsgesellschaft 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

Danke schön!