Leibniz Supercomputing Centre

of the Bavarian Academy of Sciences and Humanities

Transition zur neuen ISO/IEC 27001

30. DFN-Konferenz | 10.02.2023 | Miran Mizani, Michael Schmidt

Der Zweck des ISMS

Strategische Steuerung

Regulatorische Anforderungen

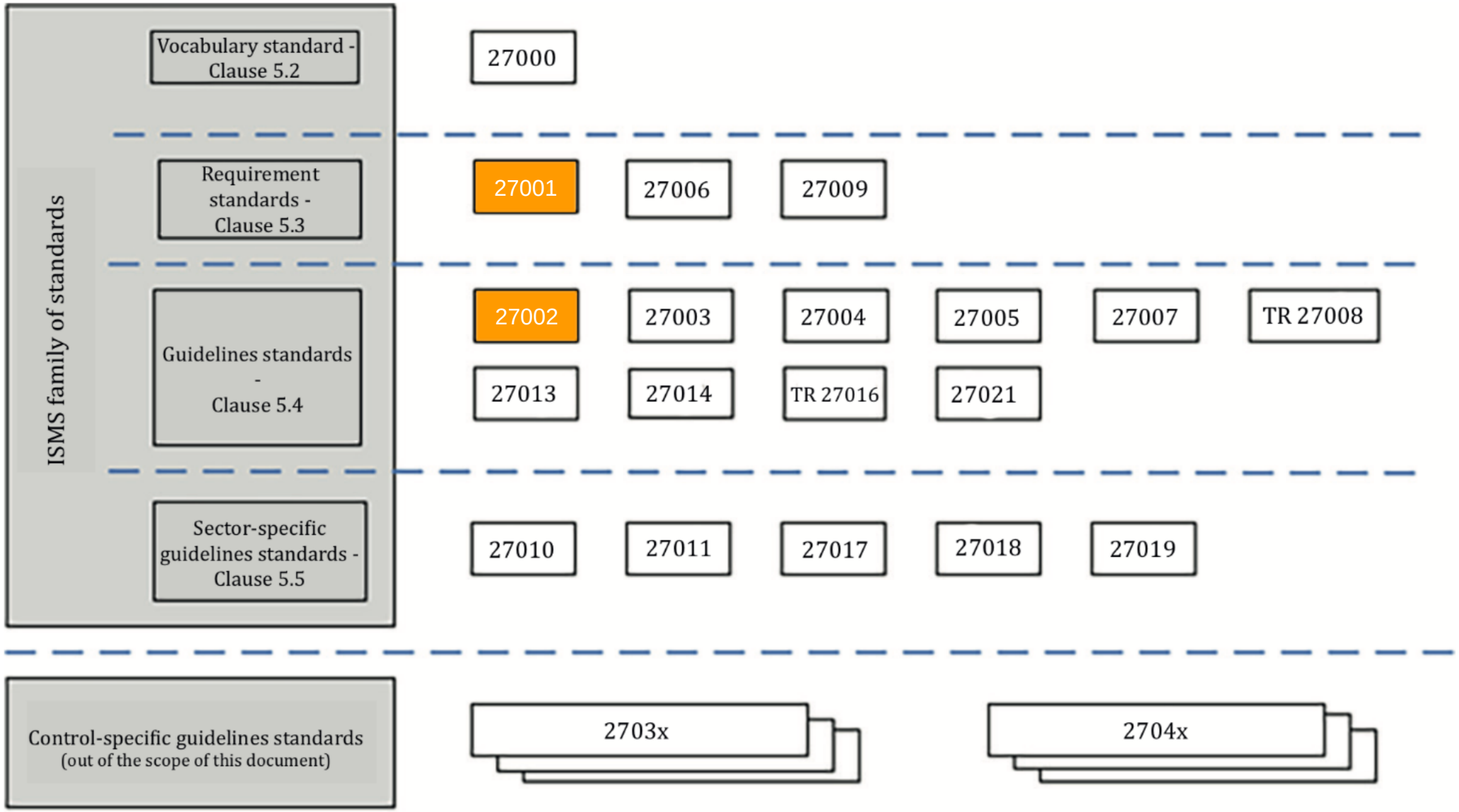
Anforderungen von Partnern

Umgang mit Risiken

Erreichen von Zielen

Die erste Überarbeitung des Standards nach 9 Jahren!

Neue Version der Dokumente 27001/27002



Minimale Änderungen am Managementsystem selbst

4 Context of the Organisation

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance Evaluation

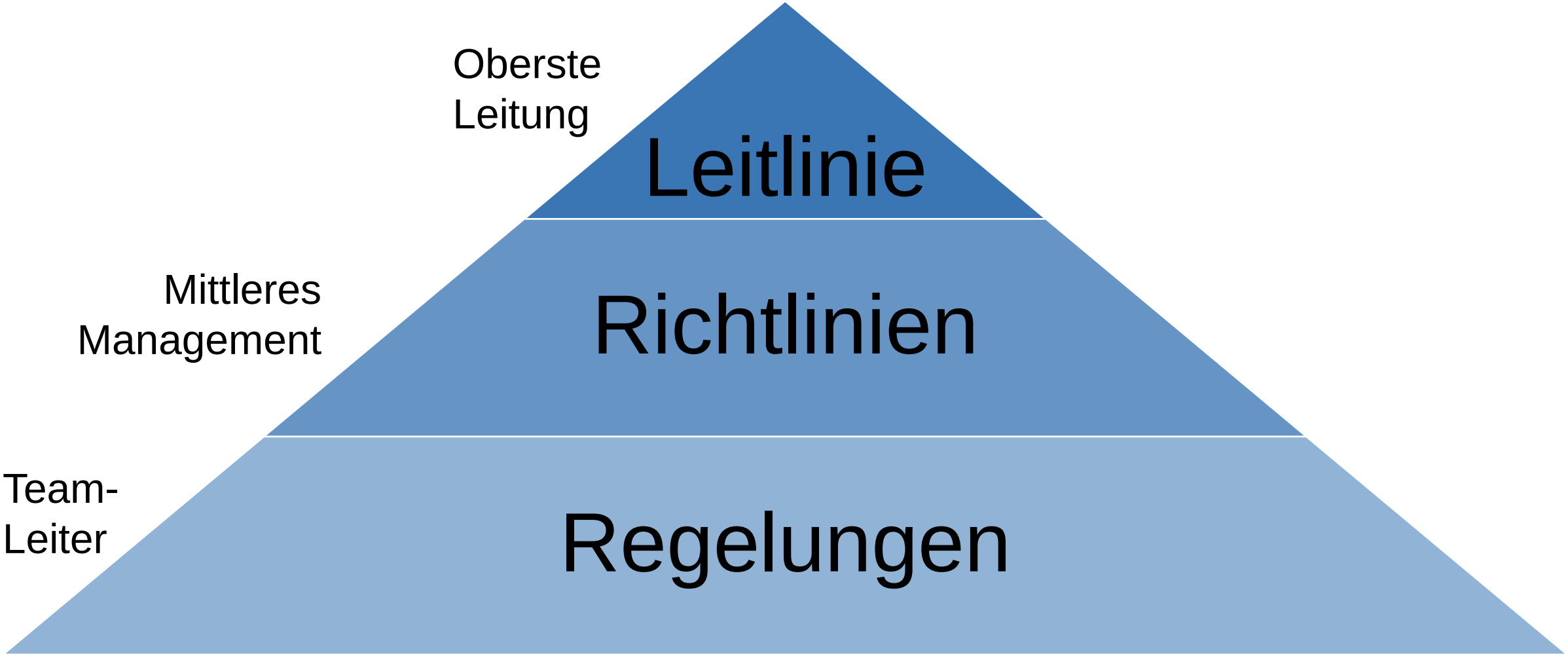
10 Improvement

Kaum Anpassungen am ISMS notwendig

Minimale Überarbeitung einzelner Paragraphen

Hauptsächlich Änderungen am Anhang A

Präzisierung des Begriffs „Policy“ in der neuen Version



Größtenteils Änderungen an den Controls des Anhang A

Anpassungen existierender Controls

Version 2013

- 14 Kategorien
- 114 Controls
  - Teilweise sehr kleinteilig
  - Manche inhaltlich überlappend
    z.B. Kryptografie ↔ Kommunikation

⇒ Komplizierte Zusammenhänge zwischen den Controls

Version 2022

- 4 Kategorien, neue Struktur
- 82 Controls + 11 neue Controls
  - 56 zu 24 Stück konsolidiert
  - 23 umbenannt
  - 35 unverändert

⇒ Insgesamt deutlich übersichtlicher und einfacher

Die Aufteilung der Controls ist nun deutlich übersichtlicher

Veränderte Taxonomie des Anhang A

Organizational Controls (37 Controls)

u.a. Umgang mit Informationen, Identitätsmanagement, Rollen

People Controls (8 Controls)

u.a. On- und Offboarding von Personal, Remote Work

Physical Controls (14 Controls)

u.a. Zutrittskontrolle und Objektschutz, Geräte und Betriebsmittel

Technological Controls (34 Controls)

u.a. Endgeräte, Softwareentwicklung, Monitoring

Neue Attribute liefern zusätzliche Informationen zu den Controls

Drei Kategorien von Attributen

Anwendbarkeit

Control type

Beschreibt, wann das Control im Vergleich zur Bedrohung wirkt.

#Preventive, #Detective, #Corrective

Information security properties

Möglichkeit, Controls nach Schutzziel auszuwählen

#Confidentiality, #Integrity, #Availability

Framework-Referenzen

Cybersecurity concepts

Funktionen des NIST Cybersecurity Frameworks

#Identify, #Protect, #Detect, #Respond, #Recover

Security-Bereiche

Operational capabilities

Unterbereiche des IS-Managements

#Governance,#Asset_management, #Information_protection, uvm.

Security domains

Bereiche der Security

#Defense, #Protection, #Resilience, #Governance_and_Ecosystem

Die neuen Controls

Threat intelligence	IS for use of cloud services	ICT Readiness for BCM	Configuration management
Physical security monitoring	Monitoring activities	Web filtering	Secure coding
Information deletion	Data masking	Data leakage prevention	

Vorbereitung und Durchführung

Vorbereitung in drei Schritten

SoA aktualisieren → Gap-Analyse durchführen → Neue Controls implementieren

Zertifizierung im Transition Audit

- Innerhalb von zwei Jahren
- Risiken überprüfen
- Geänderte Controls

Die risikobasierte Priorisierung rückte vier neue Controls in den Fokus des LRZ

Erfahrung aus der Umsetzung der neuen Controls

5.23
Cloud Services

7.4
Physical Security Monitoring

5.7
Threat Intelligence

8.16
Monitoring Activities

Cloud Services

5.23 Information security for use of cloud services: Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den IS-Anforderungen der Organisation festgelegt werden.

LRZ ist bislang völlig on-premises – wie lange geht das noch?

Cloud-Dienstleister behandeln wie jeden anderen Dienstleister auch

vgl. Umgang mit Lieferanten (27001:2013 A15)

Kritikalität und Sicherheitsrelevanz
SUPPM

Risikomatrix
RM

Schatten-IT?!
Unkoordinierte Wahl von Cloud-Dienstes

Nutzen privater Cloud-Dienste?
geschäftliche Daten via privater Dropbox teilen?

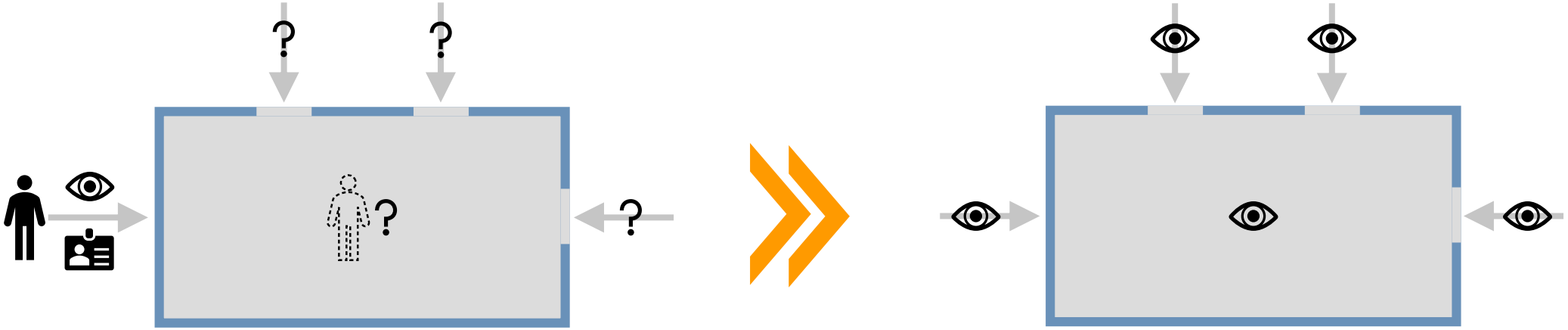
Nutzung von Cloud Diensten ermöglichen, ohne zentrale Kontrolle zu verlieren!

angemessene Richtlinien & Awareness-Maßnahmen

Zutrittsüberwachung ist kontinuierlich und allseitig erforderlich!

Physical Security Monitoring

7.4 Physical Security Monitoring:
Die Räumlichkeiten sollten kontinuierlich auf unbefugten physischen Zutritt überwacht werden.



Zutrittskontrolle
(einmalig) am Haupteingang

Zutrittsüberwachung
allseitig und kontinuierlich

Einbruchmeldeanlagen mit Anbindung an die Polizei sind i.d.R. die beste Wahl

Kontinuierliche Detektion unbefugten Zutritts

regelmäßige
Rundgänge

sehr aufwändig

Besser:
Awareness der Beschäftigten

(VdS-attestierte)
Einbruchmeldeanlage

intensive Planung im Vorfeld (DS, Betrieb, baulich, organisatorisch)
→ zuverlässig
Anwesenheit detektieren

flächendeckende
Videoüberwachung

Dienstvereinbarung
Allein wenig Detektion

Forensik im Nachhinein,
Live-Unterstützung

Detektion ohne Reaktion ist beinahe wertlos

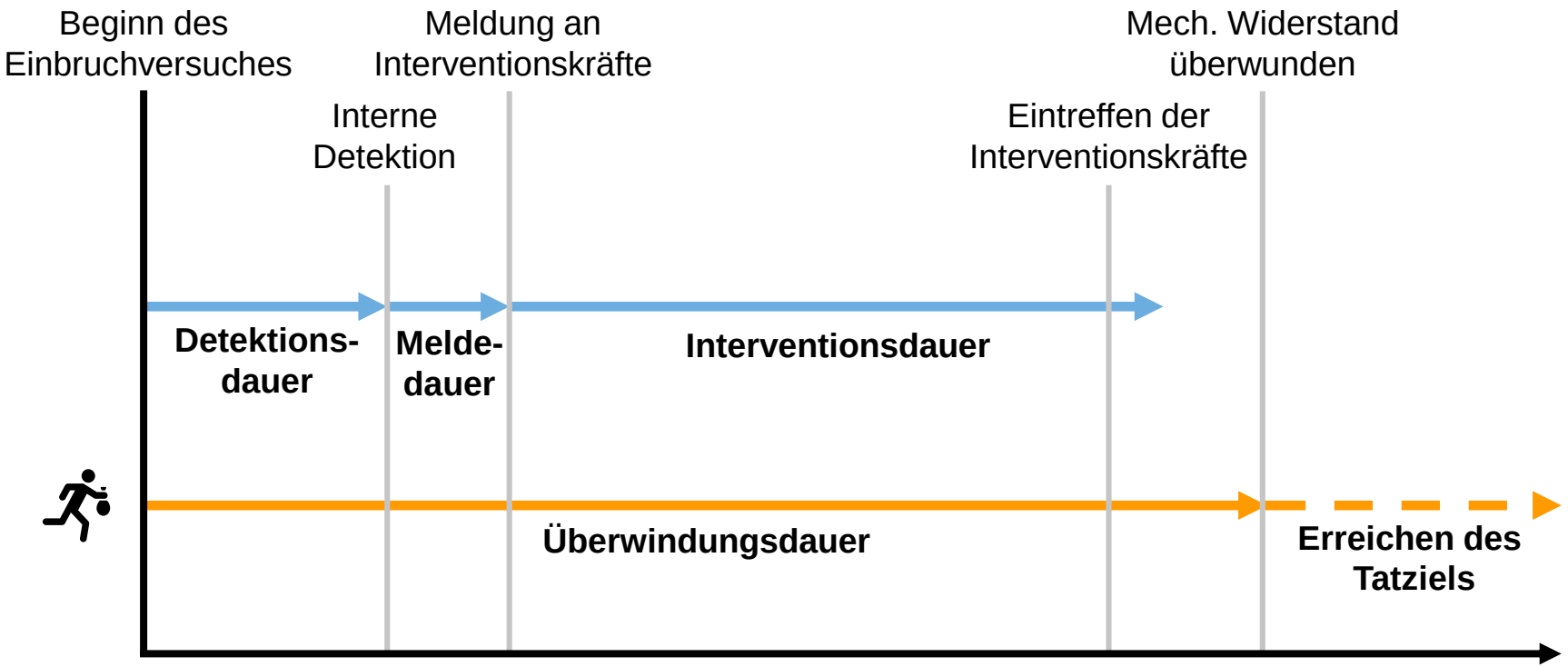
Reaktion auf physische Angriffe nicht ohne ausgebildete Kräfte!

→ Alarmweiterleitung direkt an die Polizei

Hoher mechanischer Widerstand, frühe Detektion, unmittelbare Meldung und schnelle Intervention!

Für eine erfolgreiche Intervention muss gelten:

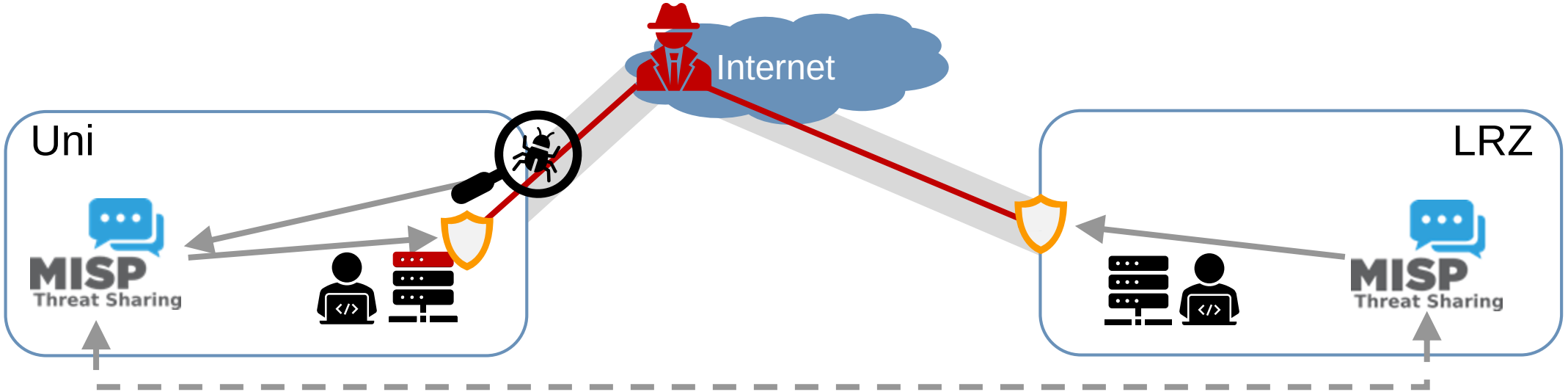
Detektionsdauer + Meldedauer + Interventionsdauer < *Überwindungsdauer (+ Erreichen des Tatziels)*



Idealer Ablauf einer erfolgreichen Intervention. Frei ausgehend von VdS 2311

Sharing is caring!

5.7 Threat Intelligence: Informationen über Bedrohungen der Informationssicherheit sollten gesammelt und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.

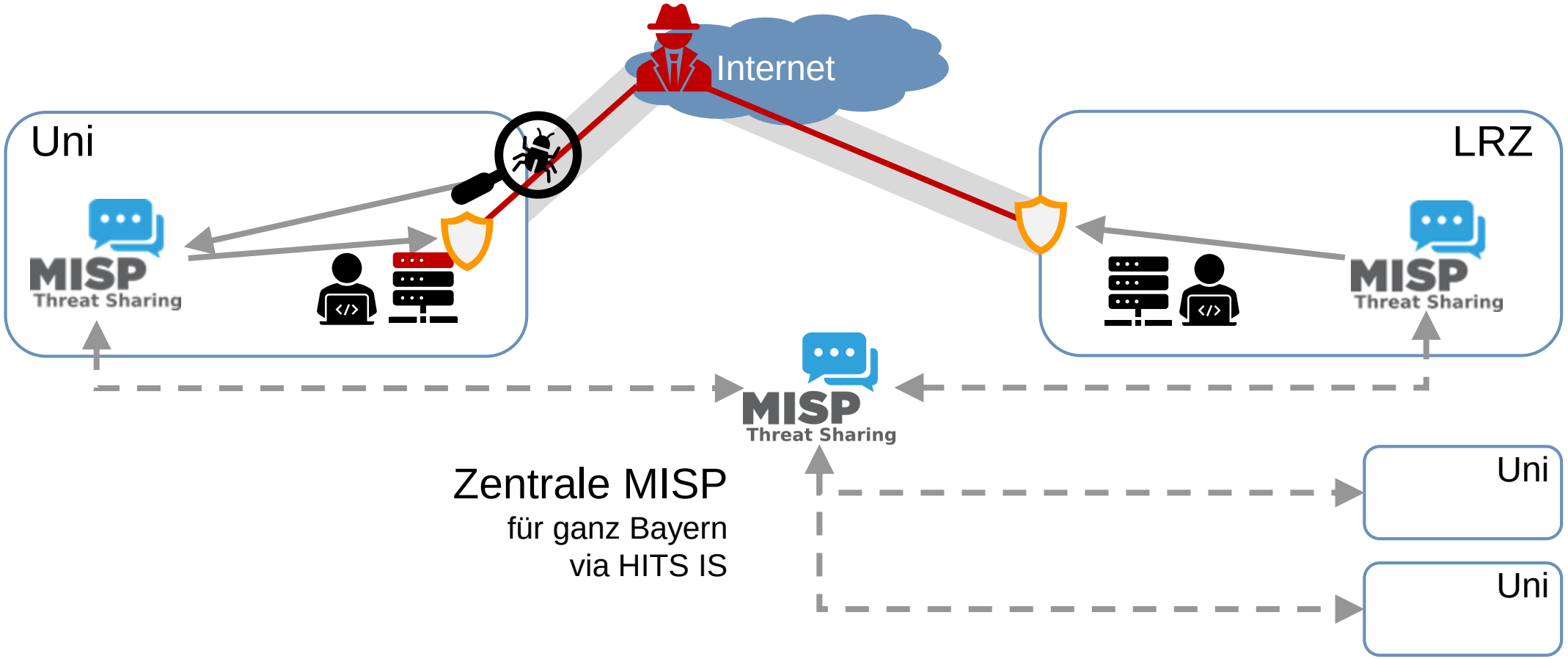


via Mail zu unstrukturiert

→ MISP als TI-Sharing-Plattform

Sharing is caring!

5.7 Threat Intelligence: Informationen über Bedrohungen der Informationssicherheit sollten gesammelt und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.



Überwachung von Aktivitäten

8.16 Monitoring Activities: Netze, Systeme und Anwendungen sollten auf anormales Verhalten hin überwacht und geeignete Maßnahmen ergriffen werden, um potenzielle Informationssicherheitsvorfälle zu bewerten.

Infrastruktur- und Applikations-Monitoring + nun zusätzlich **IT-Security**-Monitoring

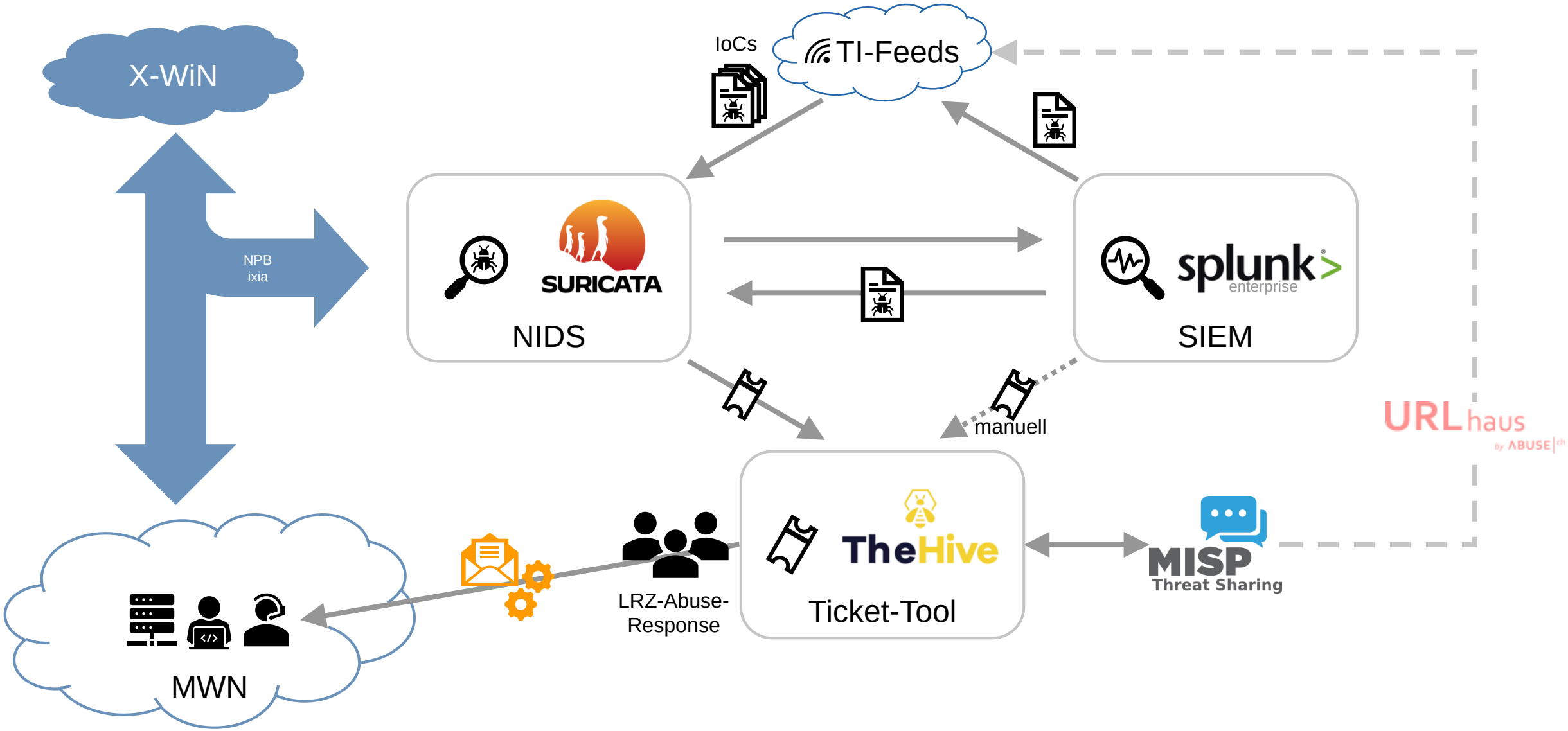
Anomalien auf Relevanz, Klassifikation und Kritikalität bewerten

→ Automatisierung lohnt sich

+ Integration in organisatorische Abläufe
+ Case-/Ticket-System
+ Threat Intelligence
+ Incident Response Plattform

Abhängigkeit zu Control 5.7 Threat Intelligence und 8.23 Web Filtering

NIDS und Meldungsverarbeitung im MWN



IDS und Meldungsverarbeitung im MWN

Meldungsverarbeitung

Prozesse und Verfahren zur
Bearbeitung von Monitoring-Events nötig!

Filtern, Aufbereiten, Melden an Betroffene
→ qualitative Meldungen mit Handlungsanweisungen

SHADOWSERVER

Scan des gesamten IPv4-Adressraums
auf bekannte Fehlkonfigurationen
vom Internet aus erreichbarer Systeme
→ Automatisierte Verarbeitung ✓

Roadmap

SURICATA

IDS → IPS
inline schalten &
Verbindungen blockieren
(vgl. NGFW) → Web Filtering

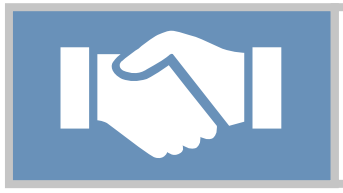
Manuellen Aufwand der
Meldungsverarbeitung reduzieren!

Die neue Version erweitert die Norm sinnvoll, die meisten Themen sind bereits Realität

Keine Panik – einfach weitermachen!

Nur wenige Änderungen am Managementsystem

Die neuen Controls sind längst Realität



Kooperationen können bei der Umsetzung helfen

Fragen zum ISMS?
Gerne melden!

Normen
Michael Schmidt
Michael.Schmidt@lrz.de

Architekt
Miran Mizani
Miran.Mizani@lrz.de