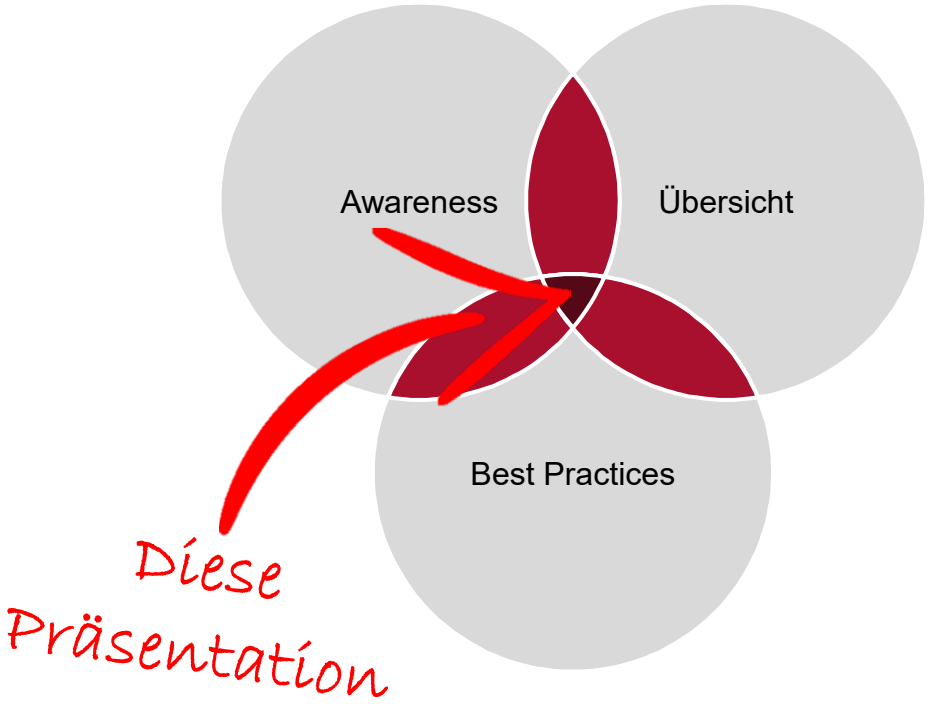

Cyberangriffe auf
SAP-Systeme


Awareness
Übersicht
Best Practices
Diese Präsentation

Cybersecurity Herausforderungen

Umgang mit Komplexität und Fachkräftemangel

62’954

Bekannte Cyberangriffe in der Schweiz im letzten Jahr[1]

Nur 1/3

der Datenverletzungen werden vom eigenen Security-Team oder den eigenen Tools entdeckt[2]

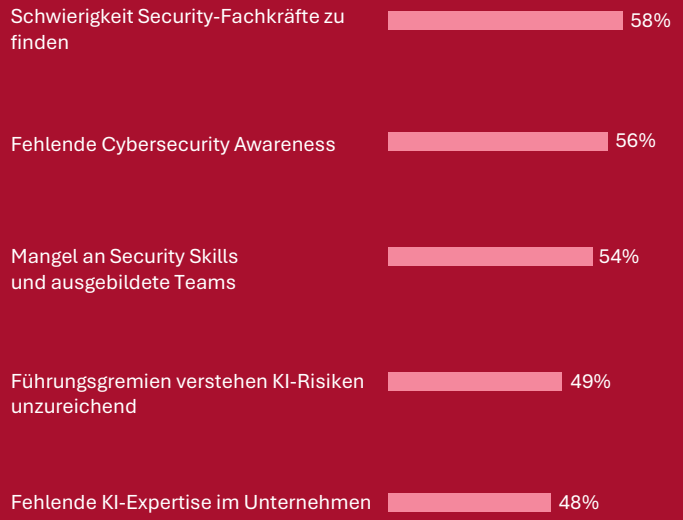
40’000

Fehlende IT/Security Fachkräfte bis 2026[3]

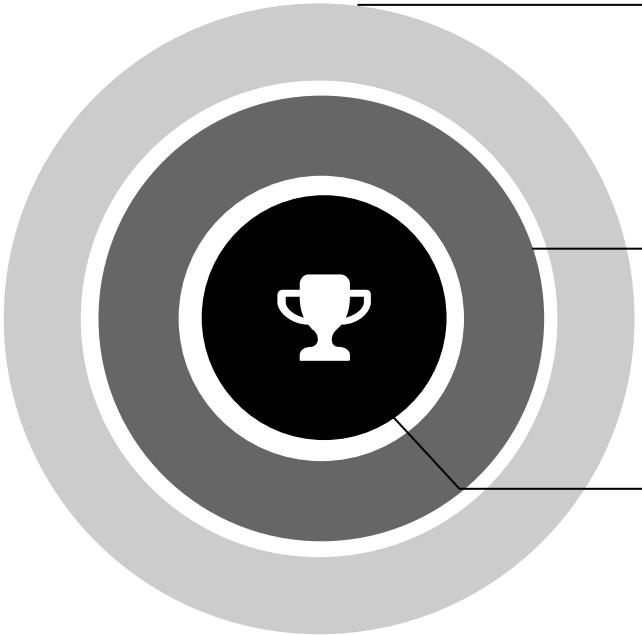
[1] BACS Halbjahresbericht | [2] IBM Cost of a Data Breach Report | [3] Source Group International

Chronischer Fachkräftemangel

fördert Cyberrisiken



[4] Fortinet Global Cybersecurity Skills Gap Report



Schutz vor Cyberangriffen

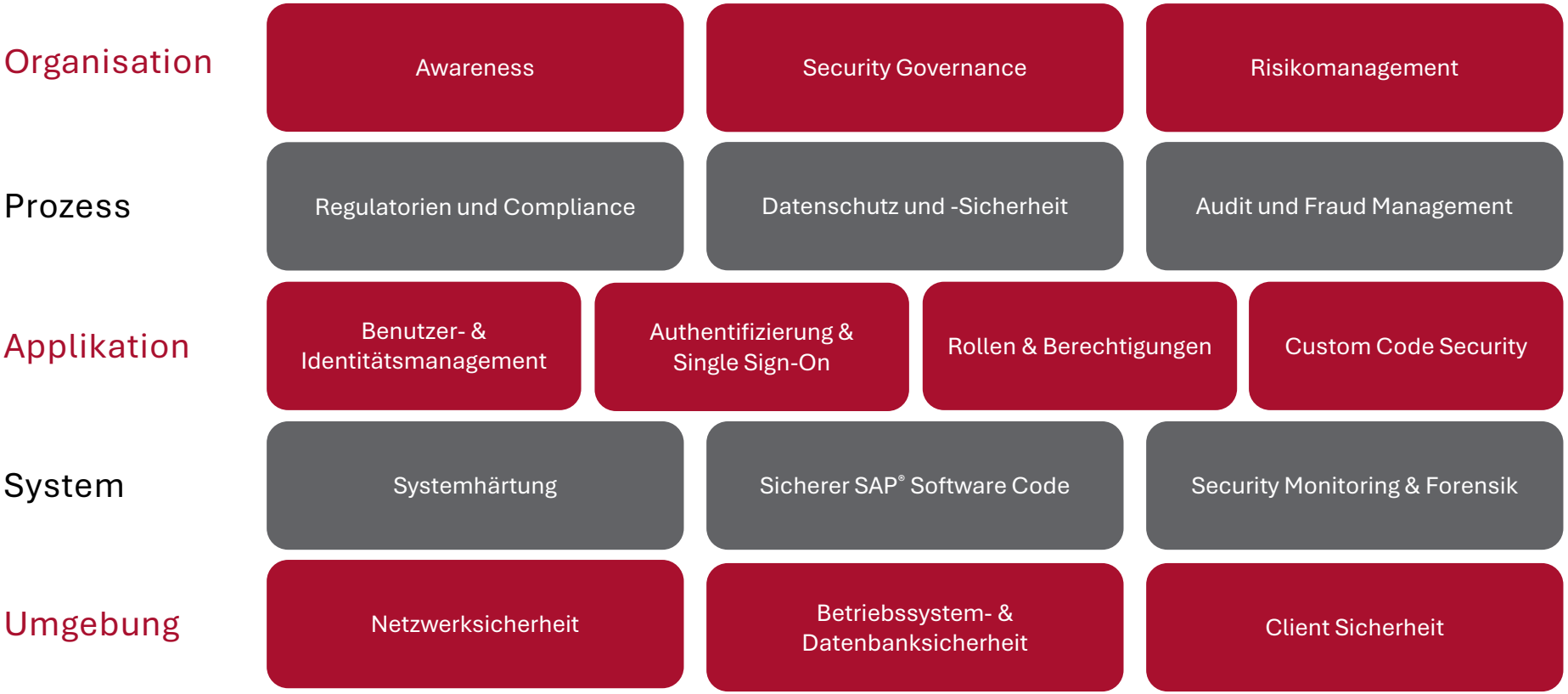
- Angriffe in immer mehr Varianten inkl. Ransomware, Social Engineering, DDoS
- Bedrohungen entwickeln sich durch KI schnell weiter

Fehlende Security Skills reduzieren

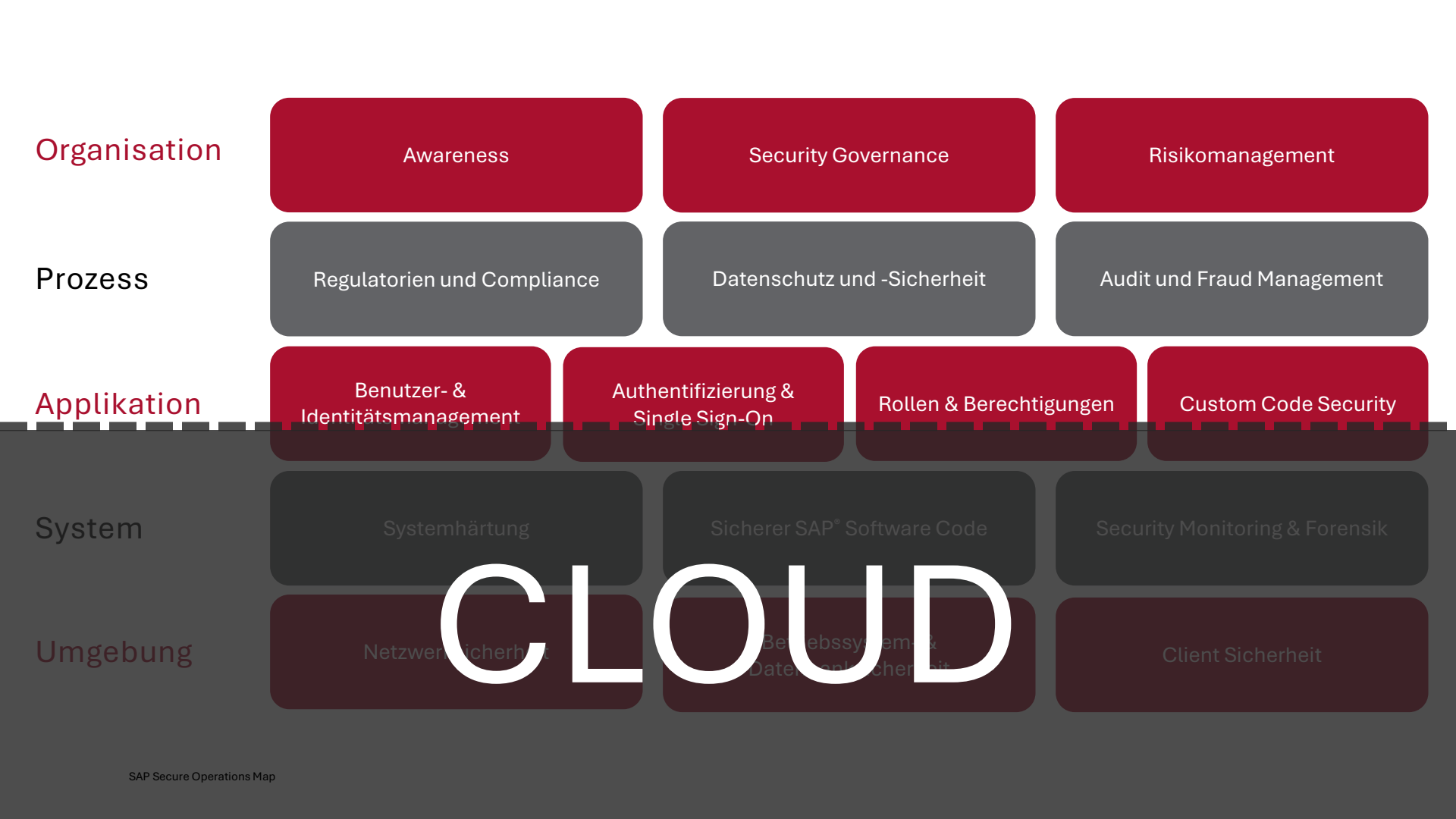
- Schwierige Rekrutierung von Security-Experten
- Teams gebunden durch manuelle operative Aufgaben
- Folge: Erhöhtes Risiko und verzögerte Innovation

Compliance im Griff behalten

- Laufend neue Vorgaben: nDSG, ISO, DORA, NIST 2.0, EU-CSRD
- Schwierige Gesamtbeurteilung in hybriden SAP-Landschaften



SAP Secure Operations Map



SAP Secure Operations Map

Zero Trust

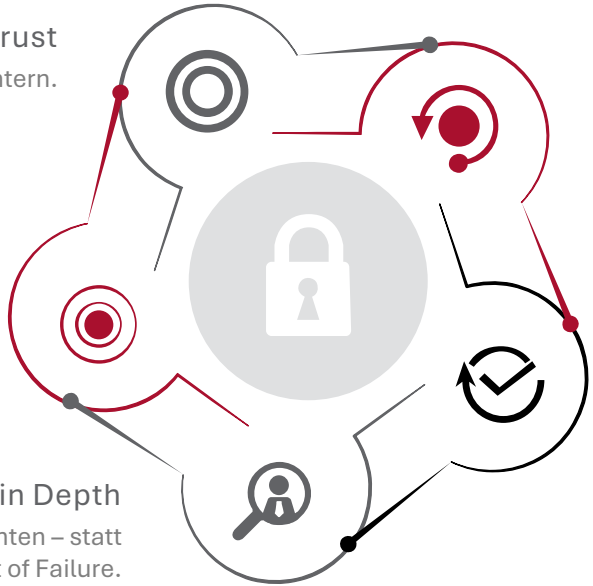
Jeder Zugriff wird geprüft – auch intern.

4-Augen-Prinzip

Kritische SAP-Aktionen brauchen Kontrolle – immer.

Defense in Depth

Mehrere Schutzschichten – statt einem Single Point of Failure.

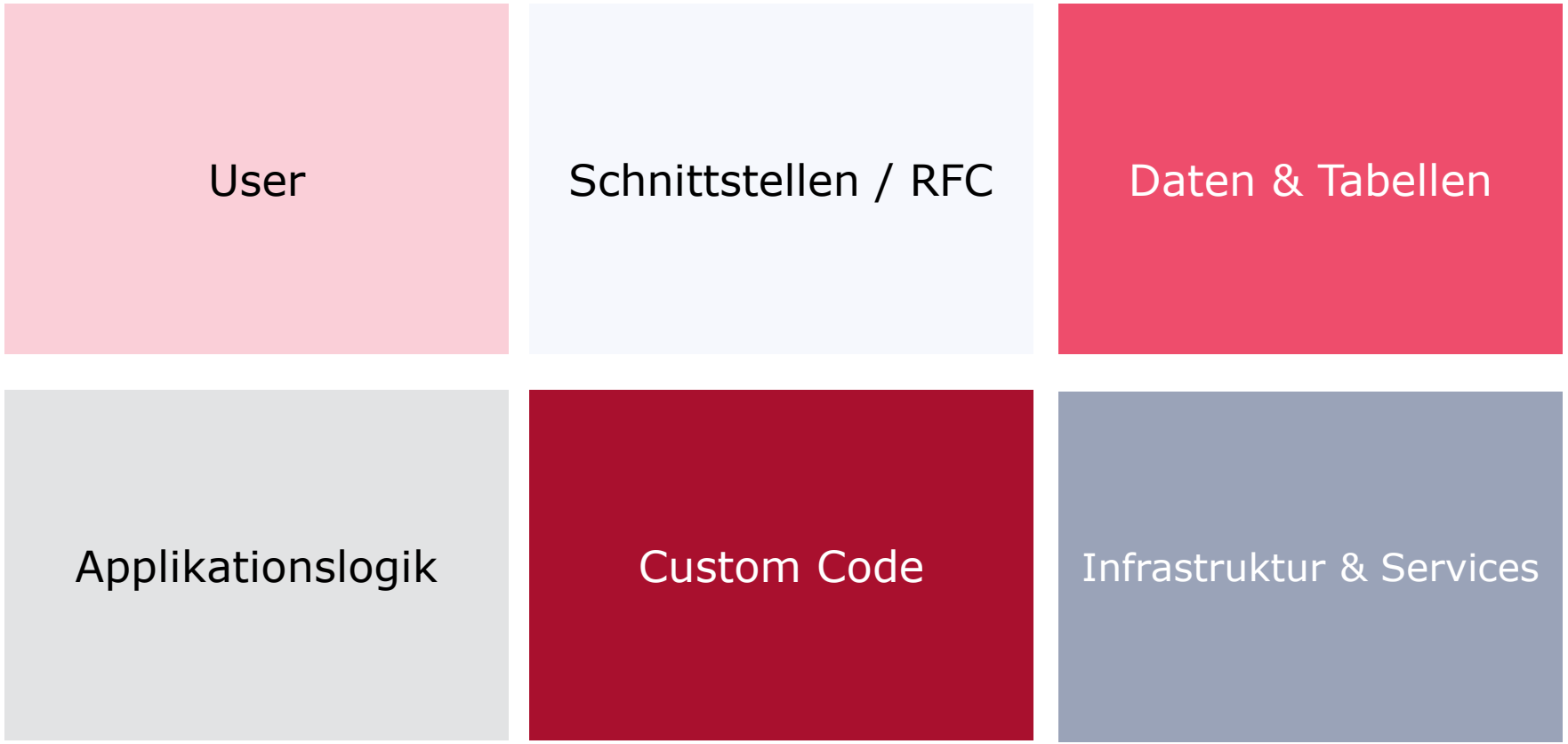


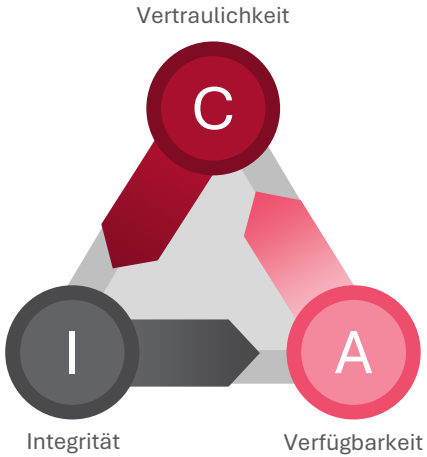
Least Privilege

Verhindert 80% aller SAP-Missbräuche

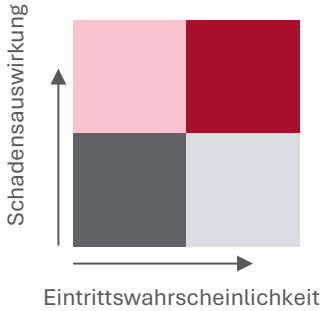
Security By Design

Sicherheit beginnt nicht erst im Betrieb – sondern beim Design.

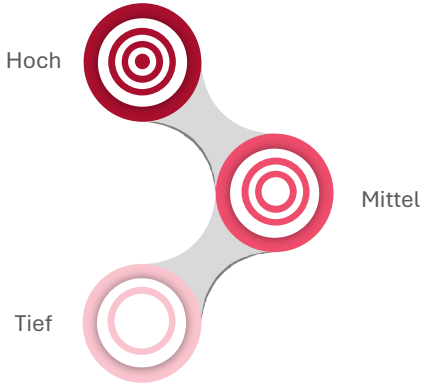

User
Schnittstellen / RFC
Daten & Tabellen
Applikationslogik
Custom Code
Infrastruktur & Services



Schutzbedarf



Risikoanalyse



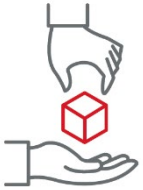
Priorisierung

Abschalten
unnötiger Services

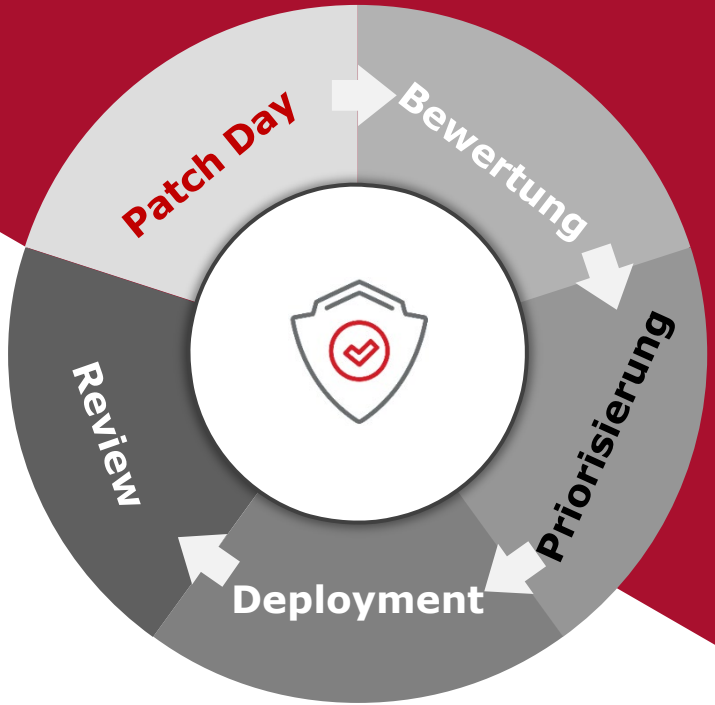
Sichere
Standardkonfiguration

Verschlüsselung
(TLS / SNC / SSFS)

Sichere Parameter

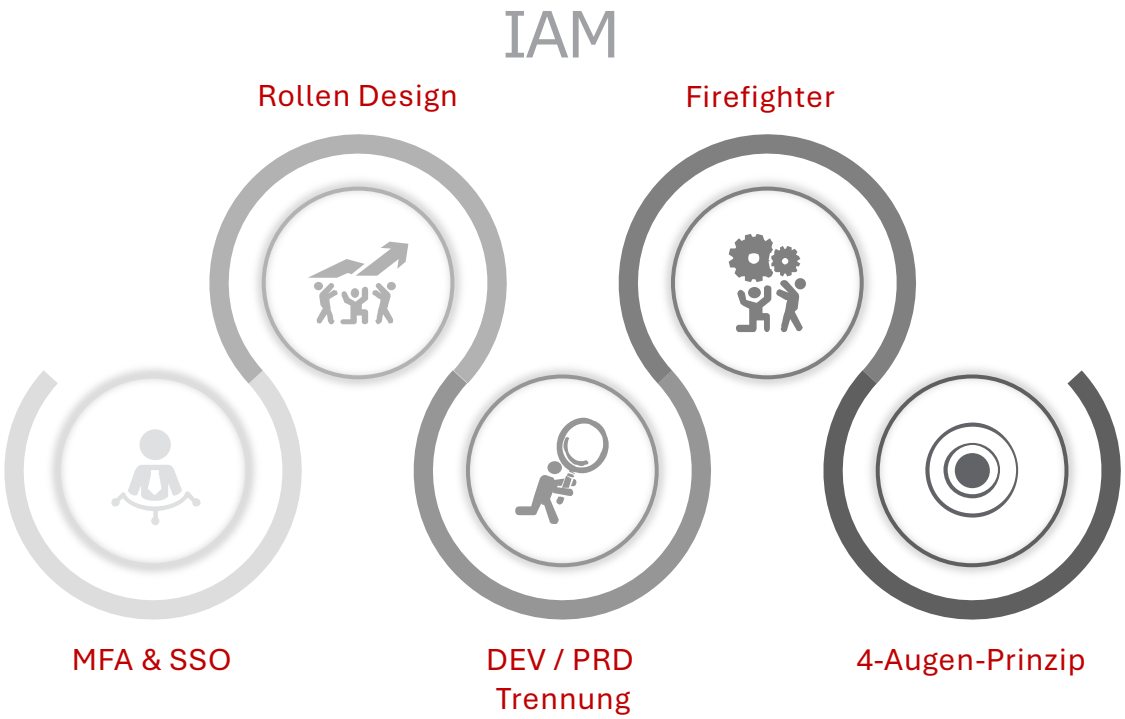


Minimal Attack Surface



Systemhärtung

Wer bist du?
Wie beweist du es?
Was darfst du?



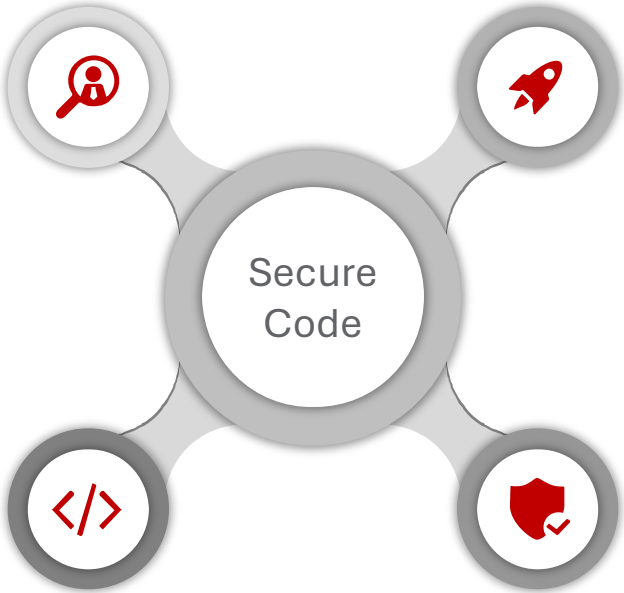
SAP <-> Non-SAP <-> Cloud

ATC / Code Scan

Unsichere Code-Stellen automatisch erkennen.

Transportprozess

Nur kontrollierte Transporte, nie direkt in Prod.



Kein PRD Code

Keine spontanen Änderungen in Produktivsystemen.

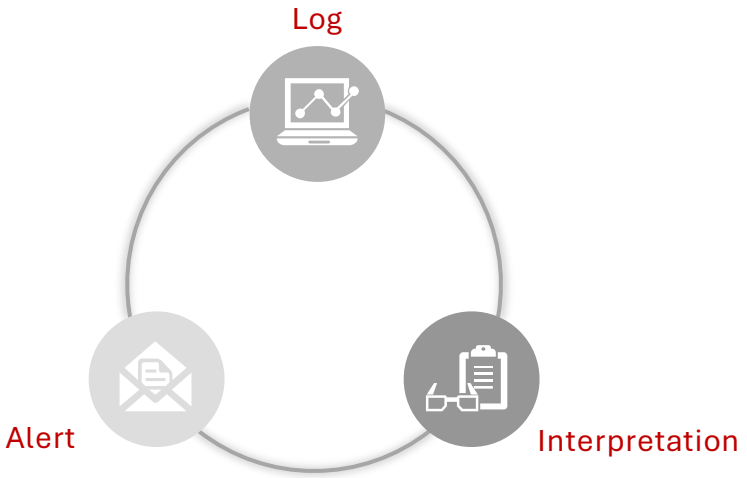
Code Review

4-Augen-Prinzip für heikle Änderungen.

```
2025-03-07 08:12:34 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=BPADMIN  TCODE=SM20   MSG=Security Audit Log gestartet für Mandant 100
2025-03-07 08:12:35 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=BPADMIN  TCODE=SM19   MSG=Änderung Audit-Konfiguration: Objekt=LOG_TYPE, Wert=AL
2025-03-07 08:13:02 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=DDIC     TCODE=SE38   MSG=Programm Z_MIG_RUN gestartet im Dialogmodus
2025-03-07 08:13:05 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=DDIC     TCODE=SE38   MSG=AUTHORITY-CHECK FOR OBJECT S_DEVELOP erfolgreich
2025-03-07 08:13:07 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=DDIC     TCODE=SE38   MSG=Open SQL: SELECT * FROM T000 WHERE MANDT = '100'
2025-03-07 08:15:21 SYS=PRD CLNT=100 MOD=BC-SEC TYP=FAIL  USER=ALERUSER TCODE=SU01   MSG=Anmeldung fehlgeschlagen, falsches Passwort, Terminal=S
2025-03-07 08:15:24 SYS=PRD CLNT=100 MOD=BC-SEC TYP=FAIL  USER=ALERUSER TCODE=SU01   MSG=Anmeldung fehlgeschlagen, falsches Passwort, Terminal=S
2025-03-07 08:15:28 SYS=PRD CLNT=100 MOD=BC-SEC TYP=FAIL  USER=ALERUSER TCODE=SU01   MSG=Anmeldung gesperrt nach 3 Fehlversuchen
2025-03-07 08:17:43 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=RFC_BW   TCODE=/RFC   MSG=RFC-Login von Host BW01 über DEST=PRDCLNT100_BW
2025-03-07 08:17:43 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=RFC_BW   TCODE=/RFC   MSG=Authority-check für Objekt S_RFC: FUNCT=RFC_READ_TABL
2025-03-07 08:17:44 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=RFC_BW   TCODE=/RFC   MSG=RFC_CALL: FUNCT=RFC_READ_TABLE, TABLE=BKPF, ROWS
2025-03-07 08:19:01 SYS=PRD CLNT=100 MOD=BC-SEC TYP=FAIL  USER=RFC_EXT  TCODE=/RFC   MSG=RFC-Login fehlgeschlagen, Kennwort abgelaufen
2025-03-07 08:19:01 SYS=PRD CLNT=100 MOD=BC-SEC TYP=FAIL  USER=RFC_EXT  TCODE=/RFC   MSG=Gateway GWPRD: abgelehnte Registrierung PROGRAM='ext_p
HOST='10.10.10.5'
2025-03-07 08:20:11 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=SAPSYS   TCODE=SM21   MSG=Systemlog: Workprozess abgebrochen, Grund=TIMEOUT, WI
2025-03-07 08:21:55 SYS=PRD CLNT=100 MOD=BC-SEC TYP=INFO  USER=FIUSER01 TCODE=FB60   MSG=Buchungsbeleg angelegt, BELNR=1900002345, BUKRS=100
```

SAP ETD
Splunk
Microsoft Sentinel
ArcSight
Elastic
Qradar
LogPoint

SIEM



SAP Security ist aktueller
als je zuvor

Die Basics einhalten:
Systemhärtung, IAM, Schnittstellen,
Code und sichere Prozesse

Ohne Monitoring bleiben alle
Massnahmen wirkungslos


Vielen Dank

Dario Mandia
Leiter Business Unit
Architecture & Integration
NOVO Business Consultants AG

NOVO Business Consultants AG
Bern, Gutenbergstrasse 50
Zürich, Hofwiesenstrasse 349
www.novo-bc.ch

NOVO
BUSINESS CONSULTANTS