IBM Software Partner Academy

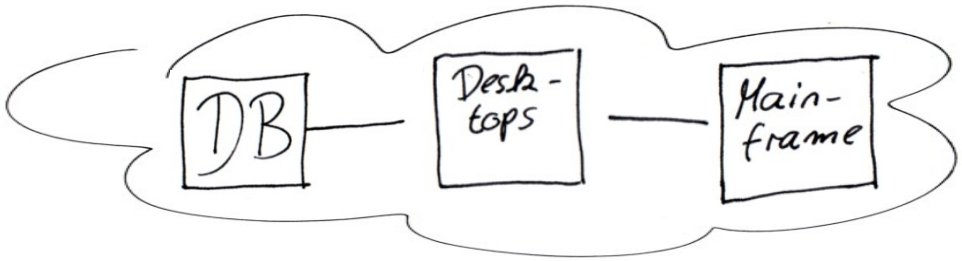
Tivoli Brand

Whiteboarding- Positionierung des Tivoli Security Produkte

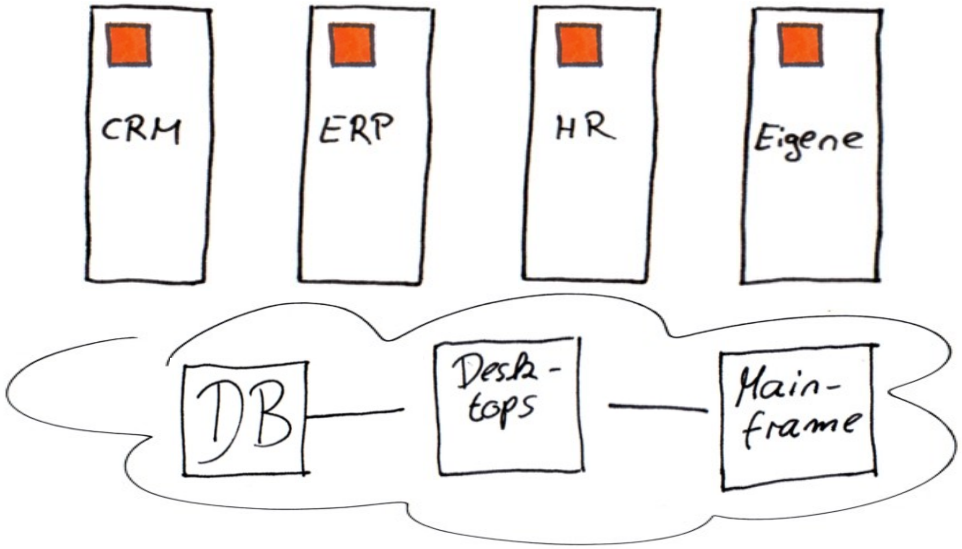
3. Tag, Donnerstag der 09.10.2008

Hans-Joachim Lorenz
Teamleiter Software Sales GB LE Süd
hans.lorenz@de.ibm.com

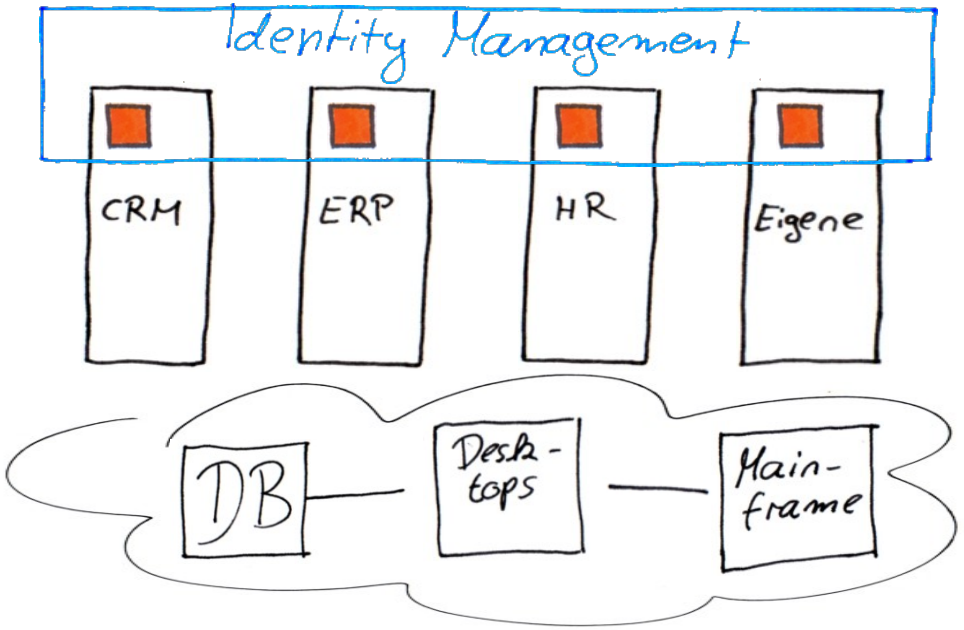
Zu Beginn betrachten wir als Beispiel Ihre Datenbanken, Desktops
und den Mainframe, welche Ihre unternehmenseigene IT-Infrastruktur bilden!



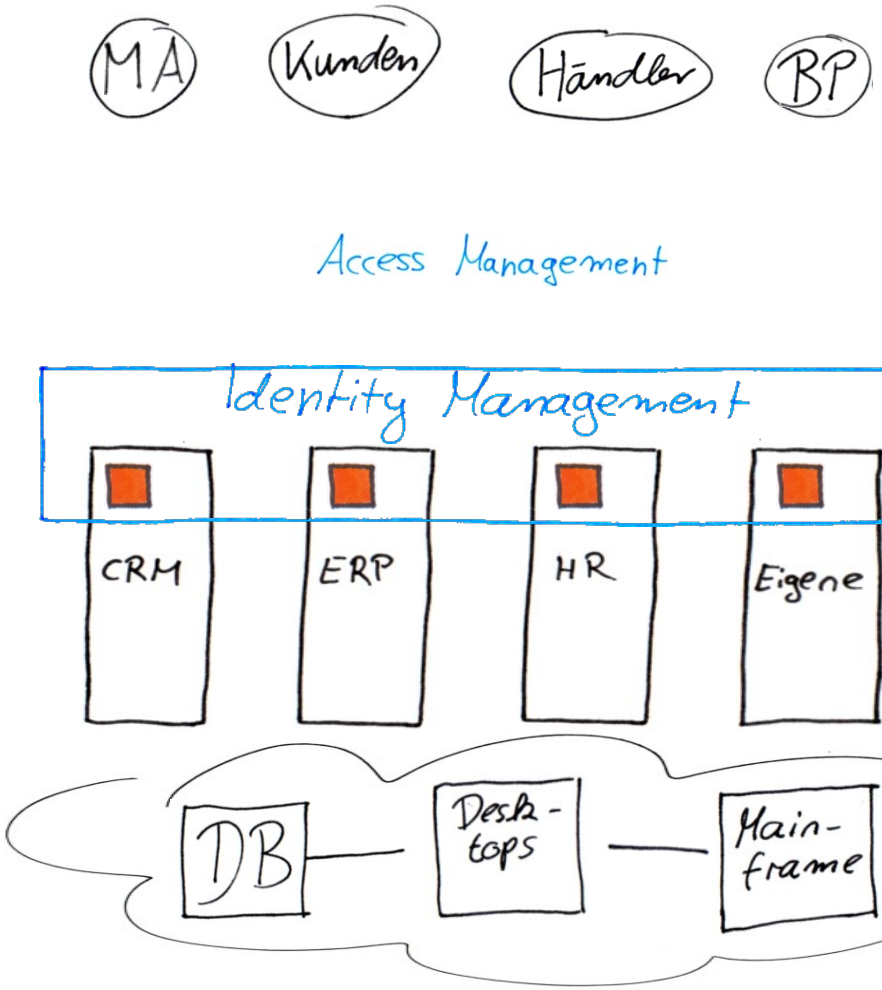
Zudem laufen bei Ihnen eine Vielzahl von Systemen, wie CRM, ERP, HR oder auch eigene Applikationen, welche allesamt eigene Benutzerverwaltungen durchführen.



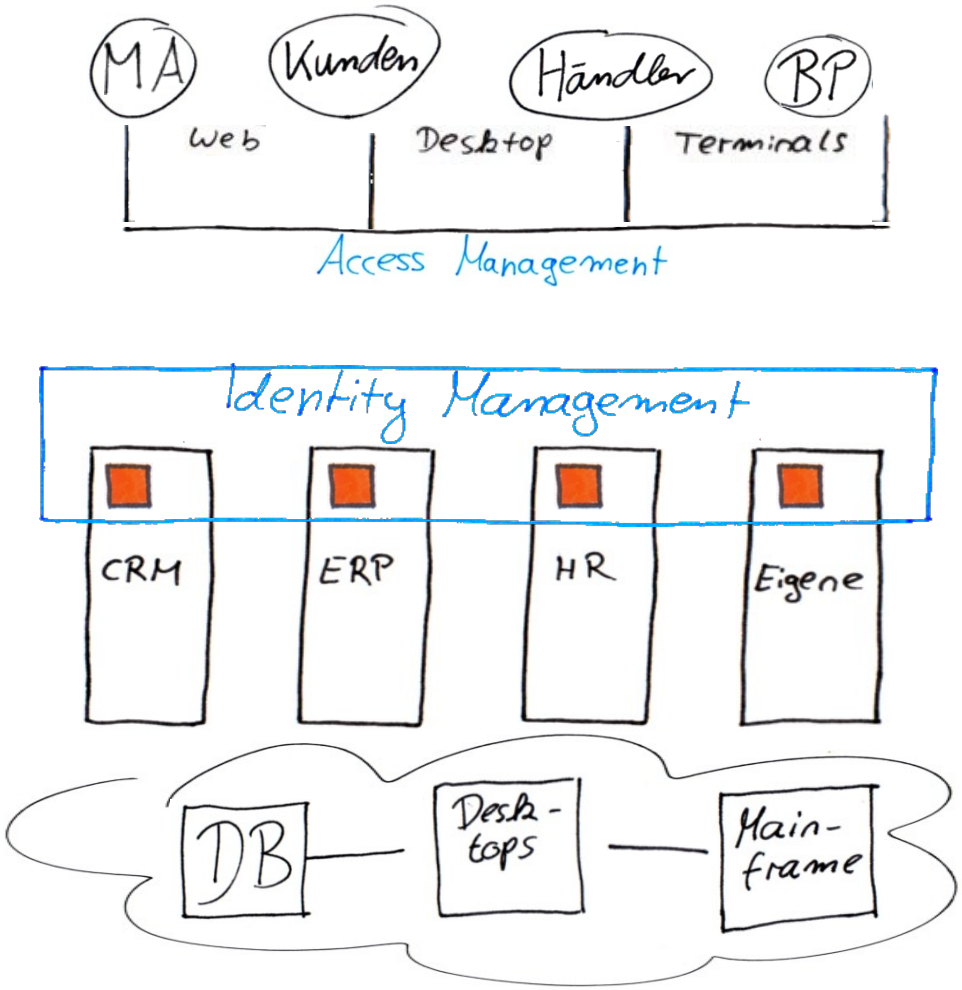
Dieser Administrationsaufwand wird mit Hilfe des Identity Managements durch eine automatische, zentrale Benutzerdefinition und Bereitstellung von Benutzerdiensten minimiert. Dadurch werden Kosten gespart.



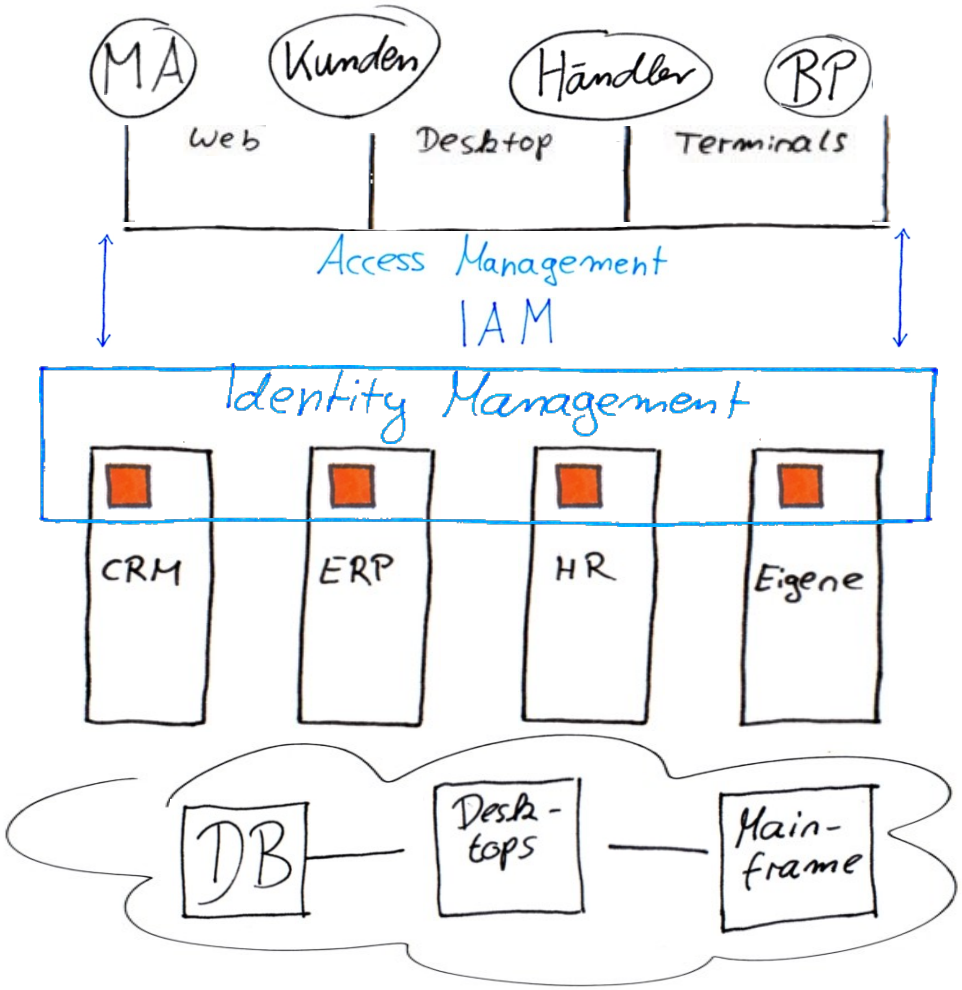
Der Zugang von z.B. Ihren Mitarbeitern, Kunden, Händlern und Business Partnern erfolgt über das Access Management…



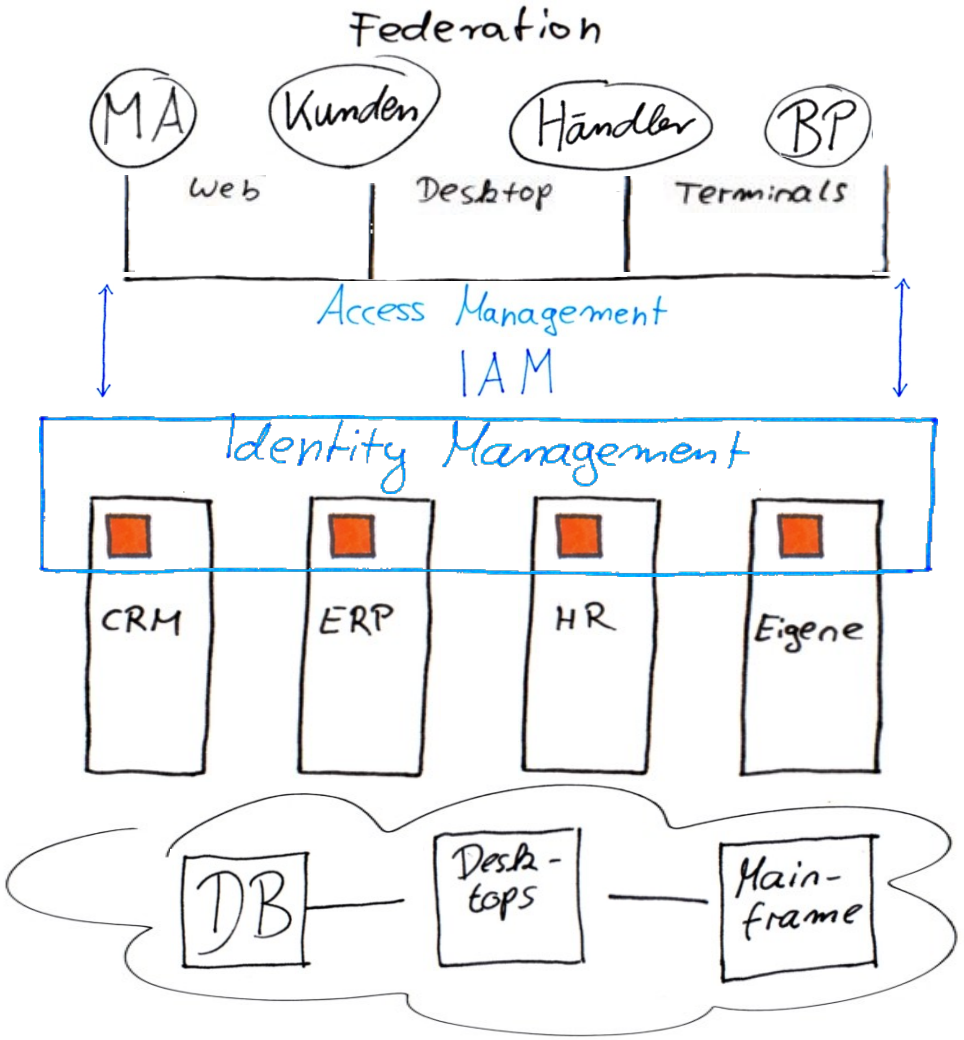
Als Zugangswege bieten sich hier beispielsweise Desktops, Terminals und das Web an



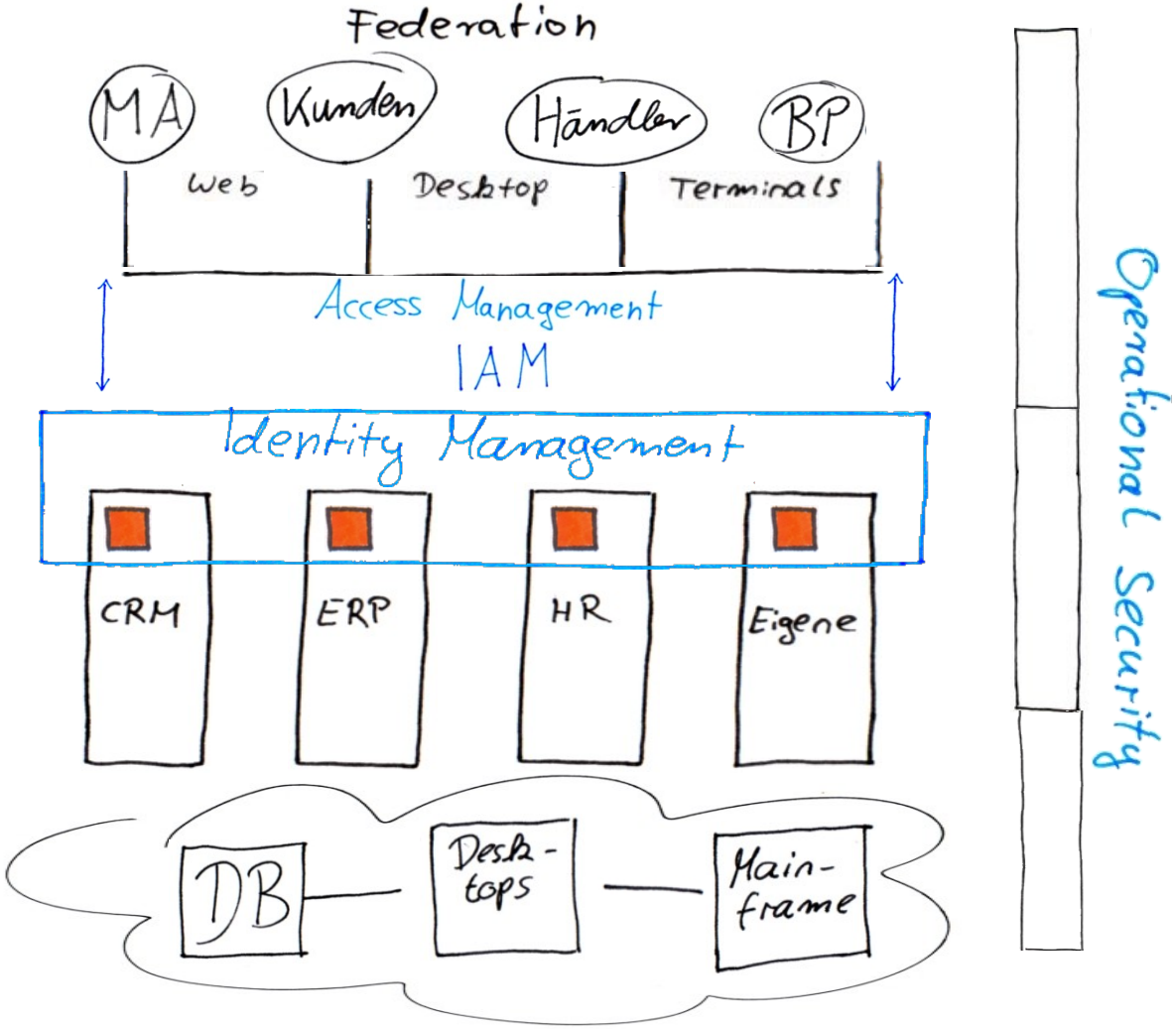
Der gesamte Themenkomplex wird als Identity & Access Management, kurz IAM bezeichnet.



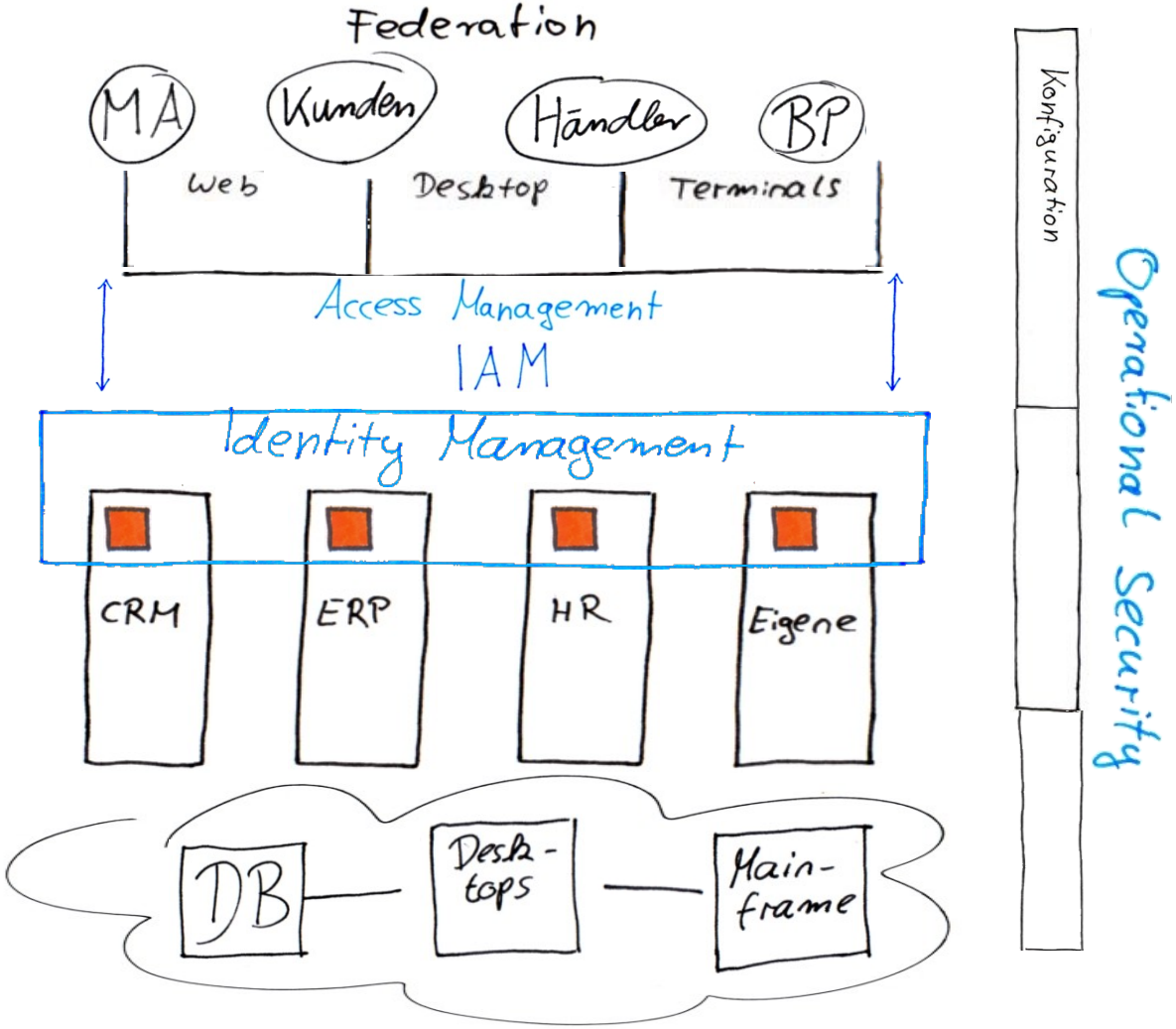
Soll IAM über Unternehmensgrenzen hinweg zum Einsatz kommen (z.B. bei Herstellern, Zulieferern, Händlern), so spricht man von Federation



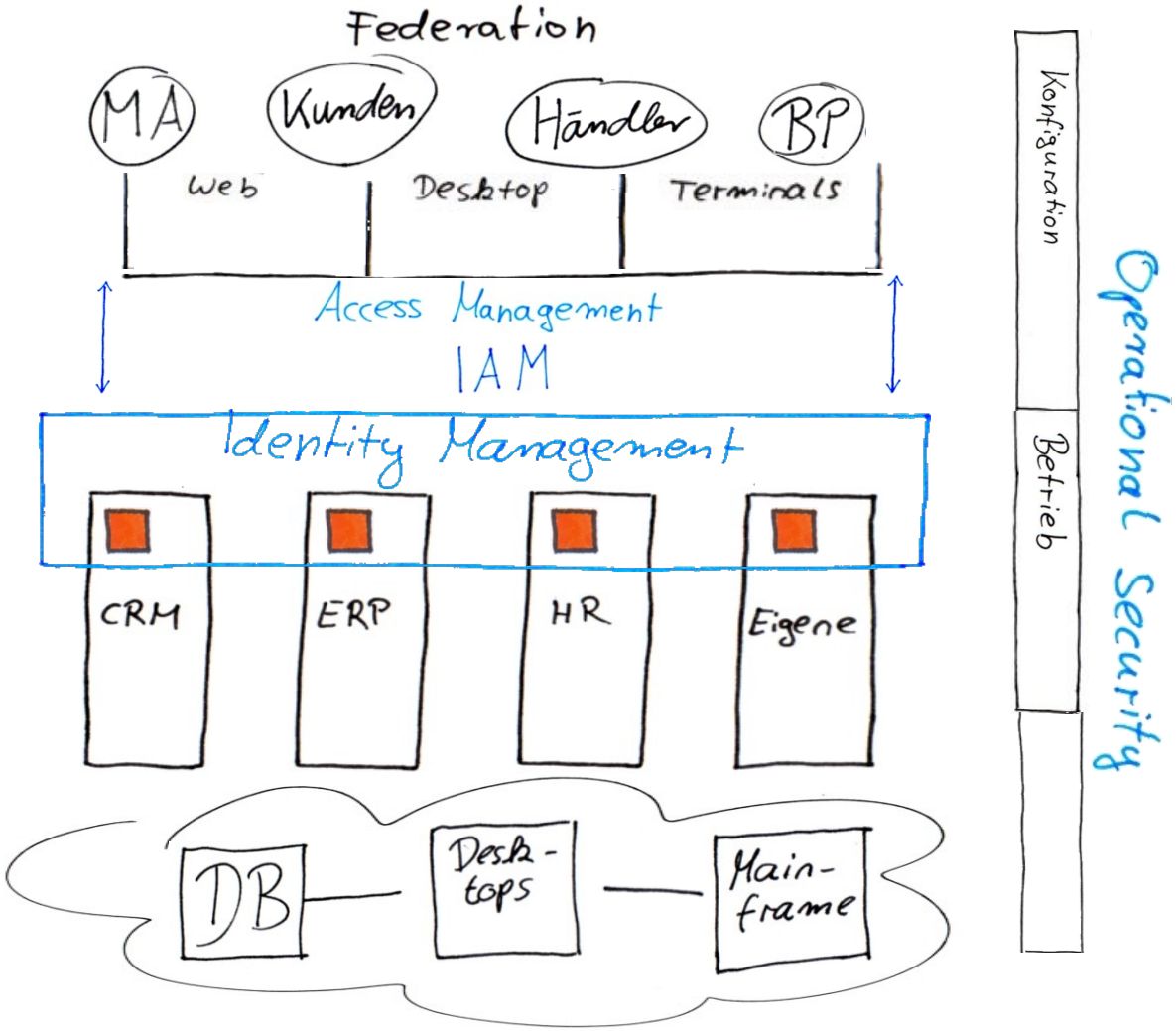
Neben IAM ist Operational Security ein weiterer Themenkomplex, der sich aus 3 Bestandteilen zusammensetzt



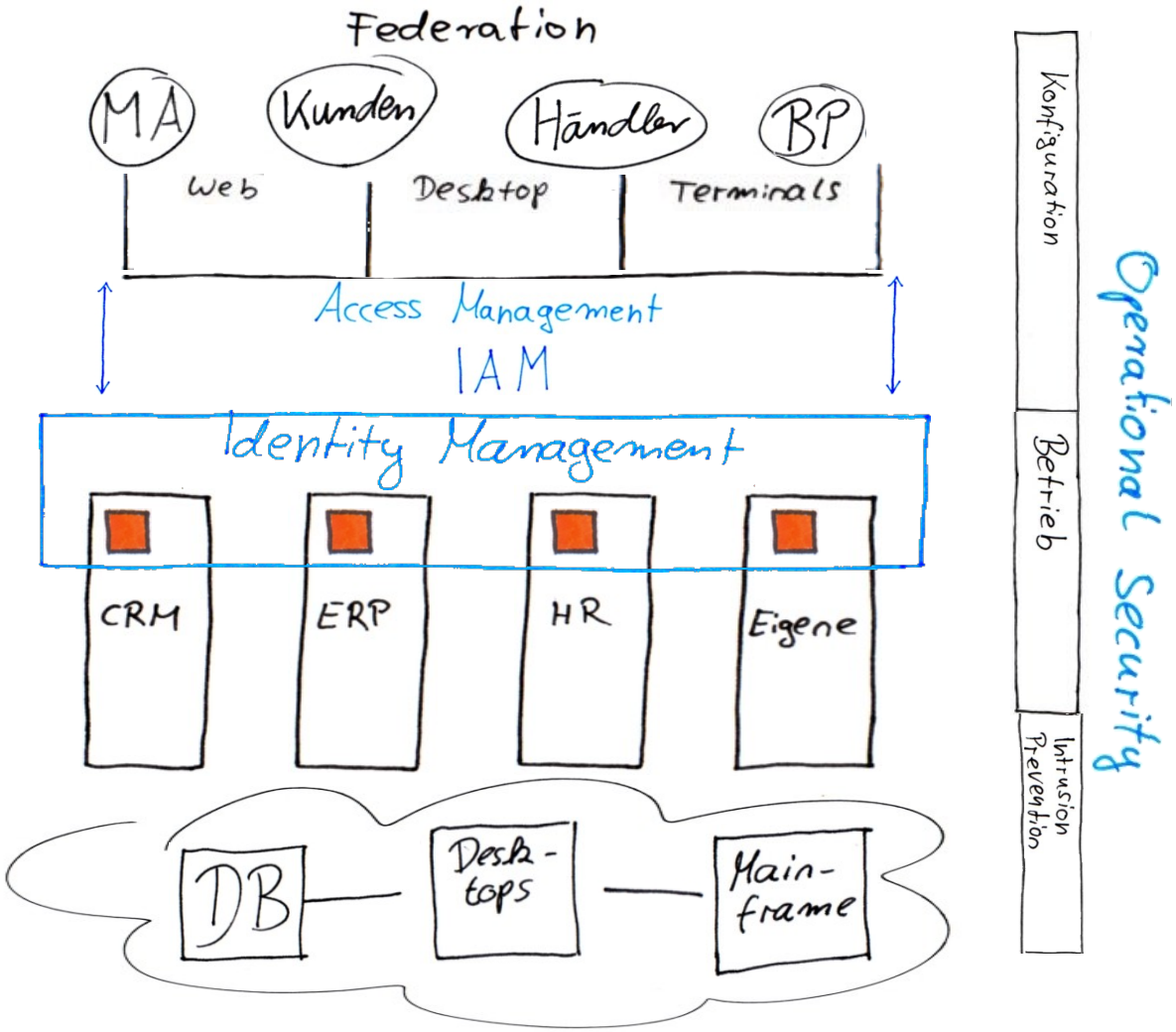
In Ihrem IT-Umfeld sollte Ihre Konfiguration in Hinblick auf die Erfüllung von Sicherheitsrichtlinien beurteilt werden…



…Kritische Sicherheitsinformationen sollten in Echtzeit überwacht werden (Security Event Logs)…

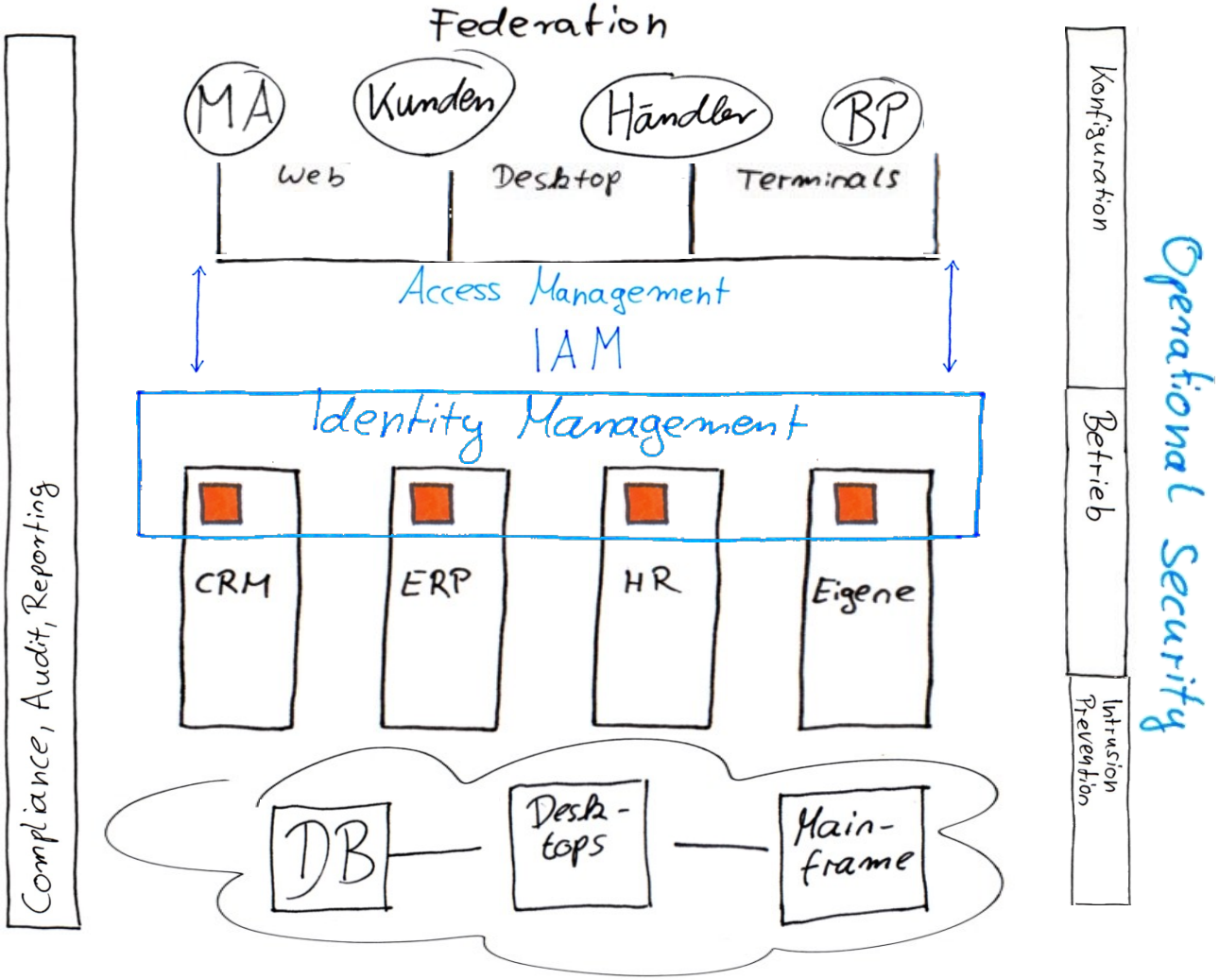


..und mithilfe von Intrusion Prevention werden kritische Sicherheitslücken in Systemen aufgedeckt und geschlossen



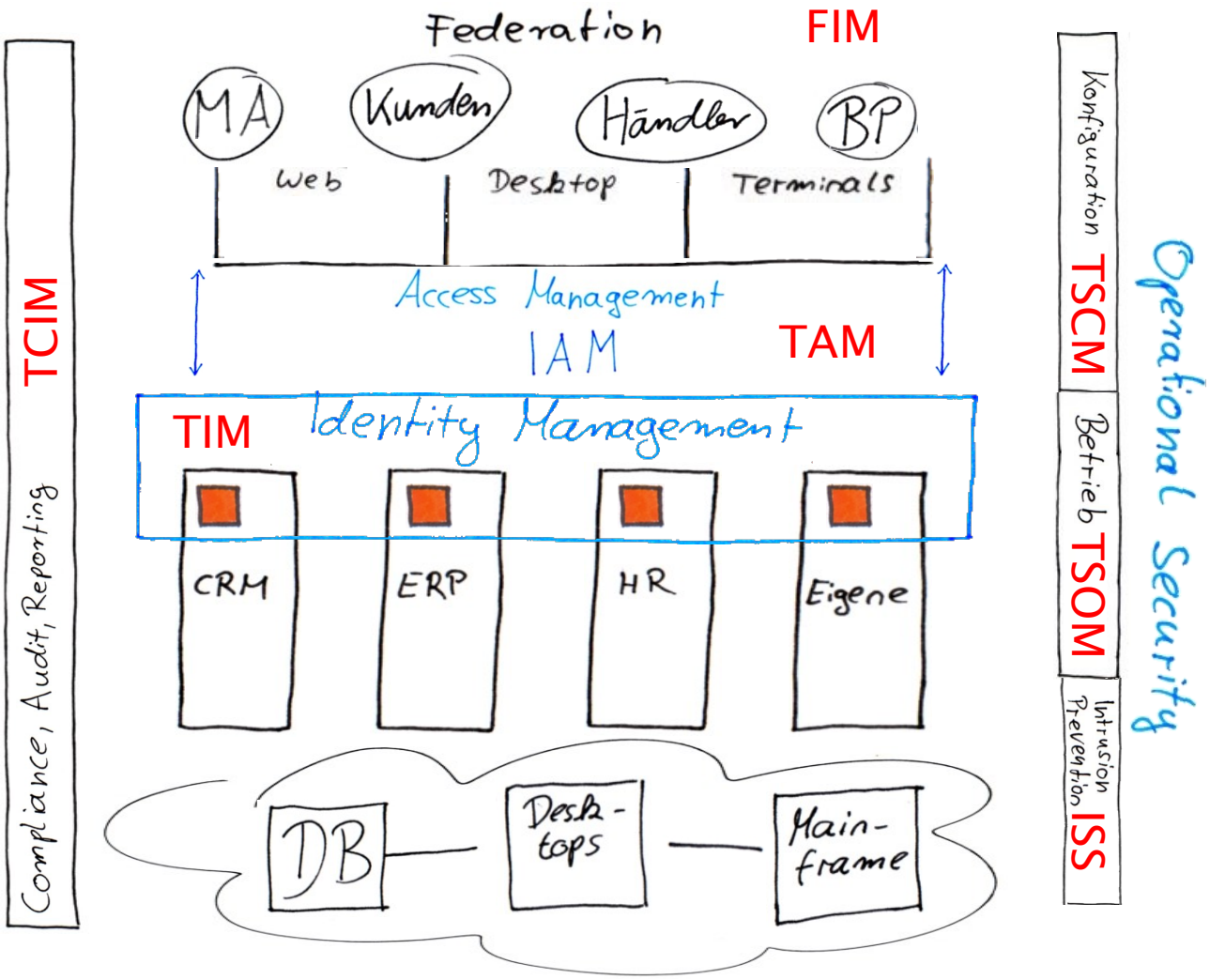
Compliance, Audit und Reporting stellt den 3. Themenkomplex dar.

Wer führte **Welche** Art von Aktion auf **Welchem** System aus?
Wann, Wo, von Wo und **Wohin** wurde es ausgeführt?



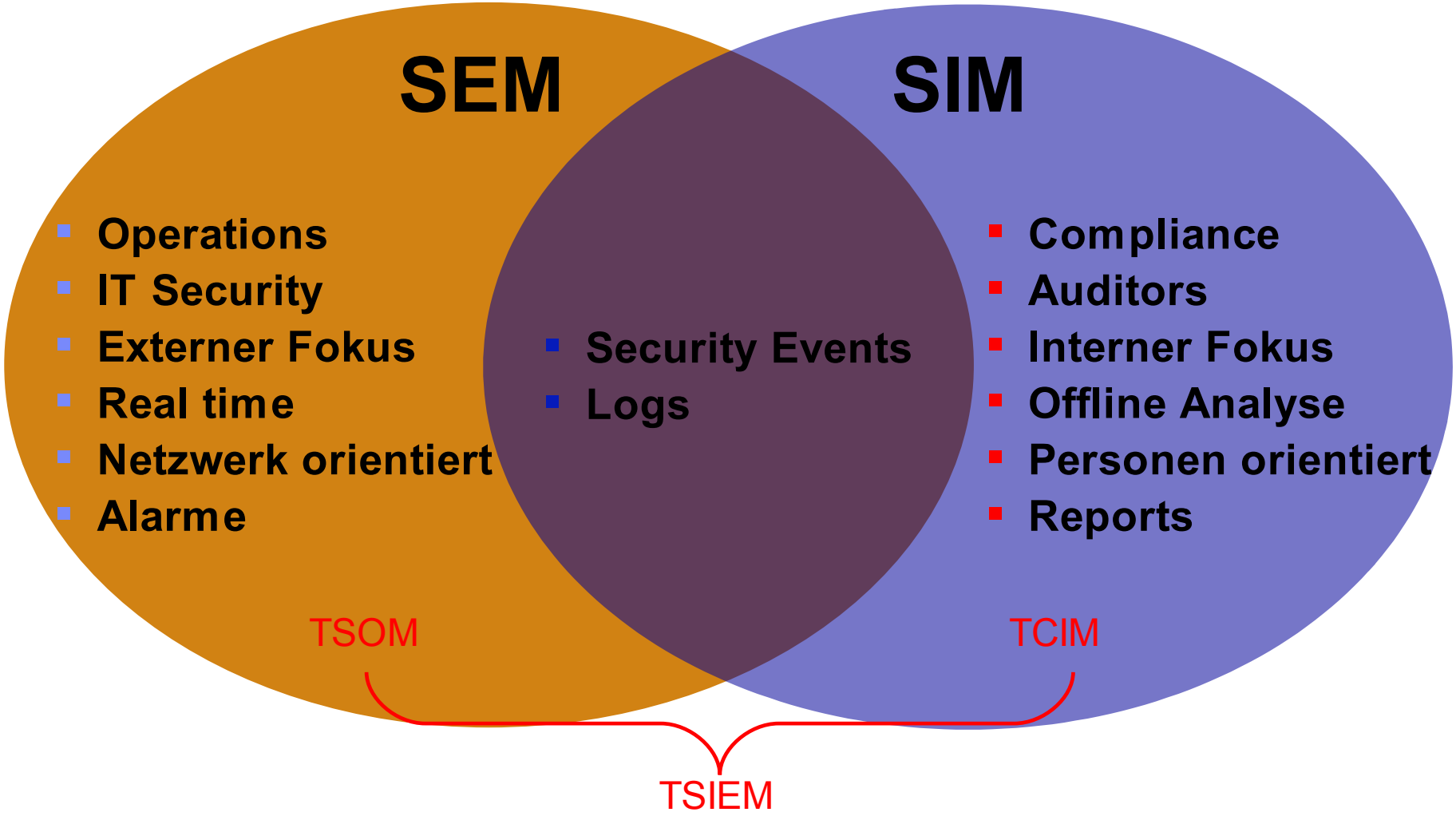
Das IBM Tivoli Security Portfolio stellt für jede Anforderung die passende Lösung zur Verfügung!

- Tivoli Identity Manager
- Tivoli Access Manager
- Tivoli Federated Identity Manager
- Tivoli Security Compliance Manager
- Tivoli Security Operations Manager
- Internet Security Systems
- Tivoli Compliance Insight Manager

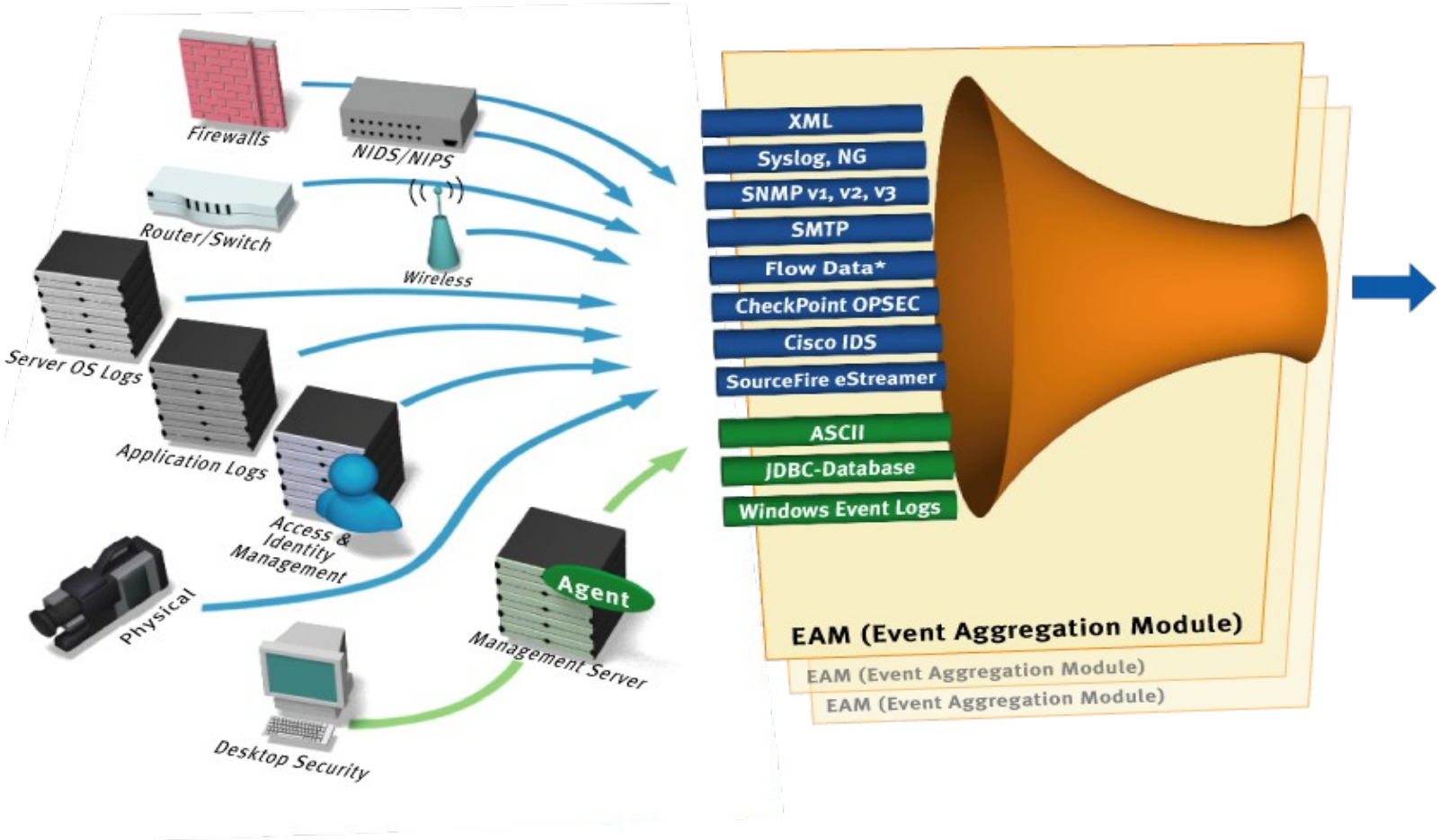


IBM Tivoli Security Information and Event Manager

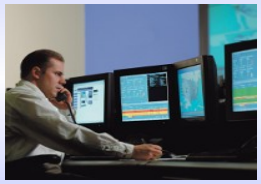
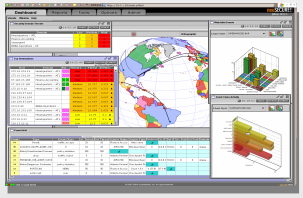
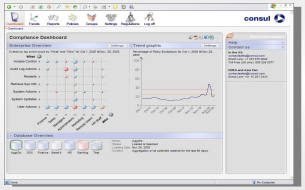
Security Information und Event Management



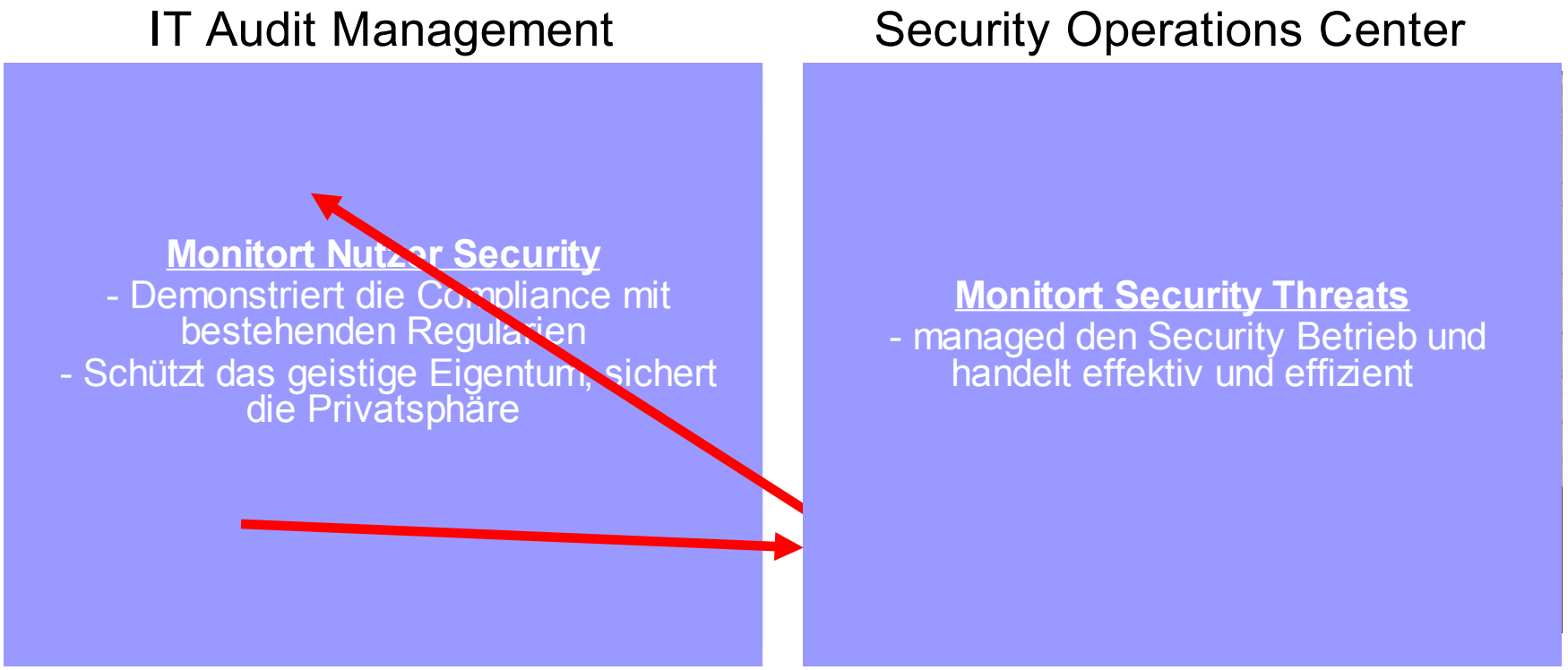
TSOM Log- und Event-Aggregation



TSOM und TCIM

	Security Operations	IT Security Internal Audit
Personen:		
Problem:	Netzwerkzentrische Angriffe Fehlkonfiguration und Mißbrauch Security Data Overload Lindern von Sicherheitsvorfällen	Benutzerzentrische Regelverstöße “Privileged User Audit + Monitoring” Rechtliches Compliance Reporting
Lösung:	Incident Management Security Event Mgmt (SEM)	User Activity Monitoring Security Info Mgmt (SIM)
Produkt:	Tivoli Security Operations Manager (TSOM) 	Tivoli Compliance Insight Manager (TCIM) 

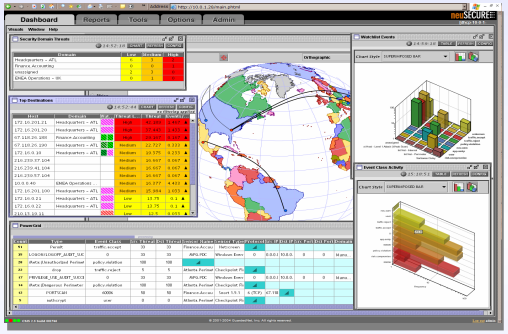
Tivoli Security Information & Event Manager (TSIEM)



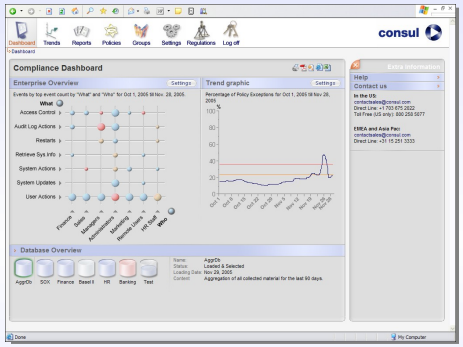
- **Eskaliert kritische/zusammengefasste Events zum Audit/Compliance Modul**
- **Eskaliert Nutzer-Security Warnungen zum Security Betriebs Modul**

Tivoli Security Information und Event Manager Integration

- TSOM korrelliert Events zu TCIM Reports, Steuerkonsole
- TCIM schickt Regelverstöße an die TSOM SOC Konsole



- Regelverstöße bei der Netzwerksicherheit
- Nutzer Zugriffe und administrative Events der Infrastruktur
-Kompromittierte oder angegriffene Assets



Tivoli Security Operations Manager (TSOM)

Tivoli Compliance InSight Manager (TCIM)

Warnungen bei Regelverstößen
- Meldet wenn die Identity des Nutzers, Hosts, oder einer Applikation verletzt wird
- Öffnet Tickets für neue Incidents

Kontaktdaten:

Hans-Joachim Lorenz
Teamleiter Software Sales GB LE Süd

Tel: 0172/7240687
Email: hans.lorenz@de.ibm.com

Happy Selling!