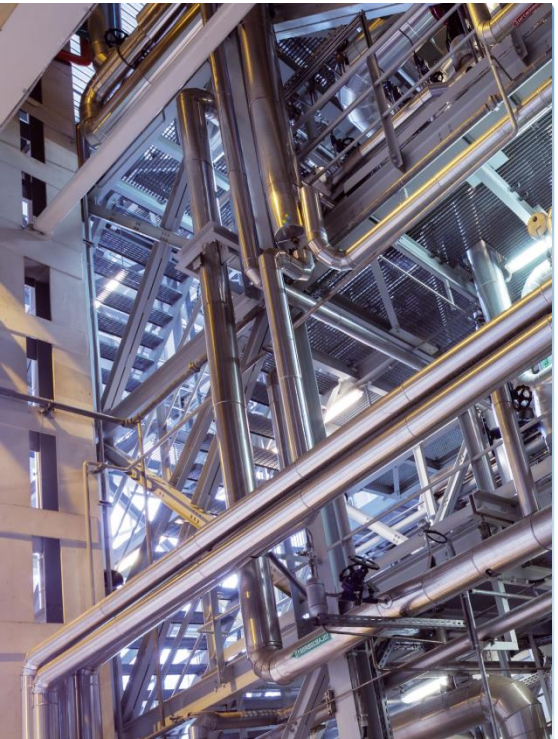
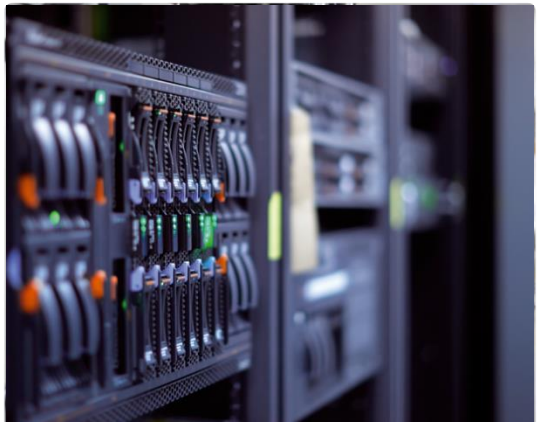


3. Kooperations- Veranstaltung

„Industrial Security in der Automatisierungspraxis“

4. Oktober 2018 bei der Hosokawa Alpine AG in Augsburg



VIDEC.

„Produktions-IT überwachen - Risiken einfach managen“

ACHT:WERK

Jens Bußjäger · Geschäftsführer

Achtwerk GmbH & Co KG
Am Mohrenshof 11a
D-28277 Bremen

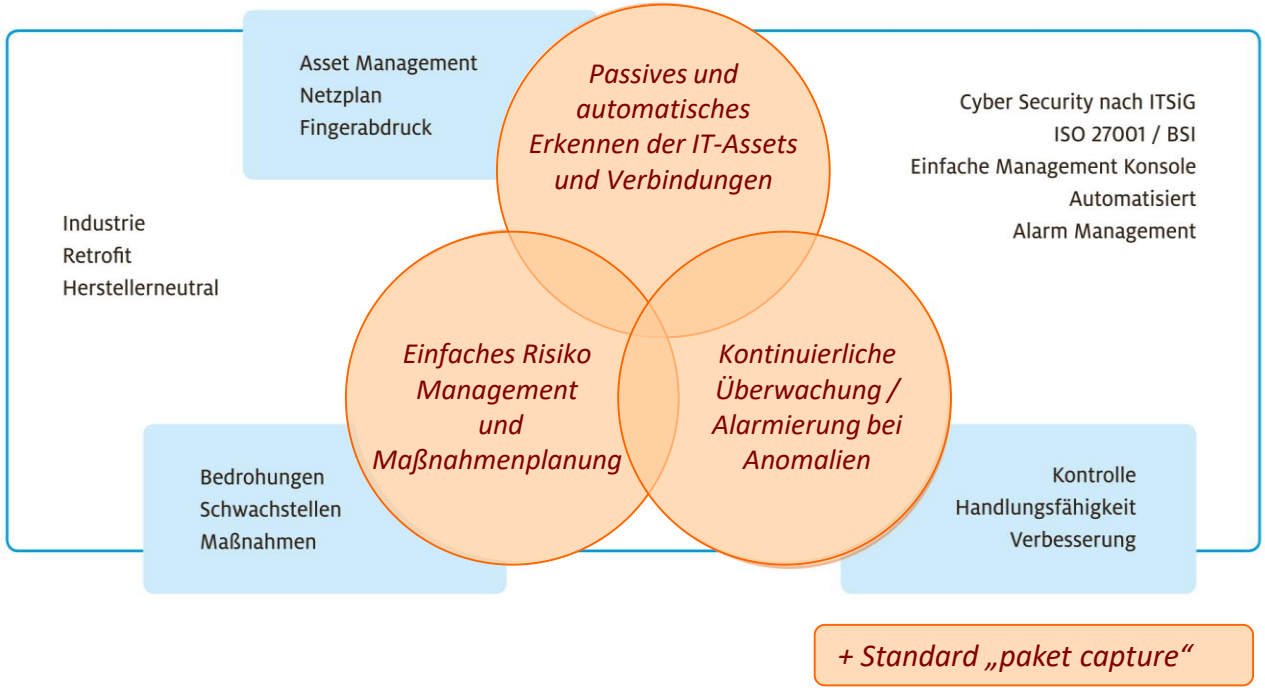
T +49 175 81 61 704
jens.bussjaeger@acht-werk.de
www.acht-werk.de

VIDEC.

INDUSTRIE RISIKO MANAGEMENT AUTOMATISIERUNG

VIDEC.

Vertrauen ist gut, Kontrolle ist wesentlich.

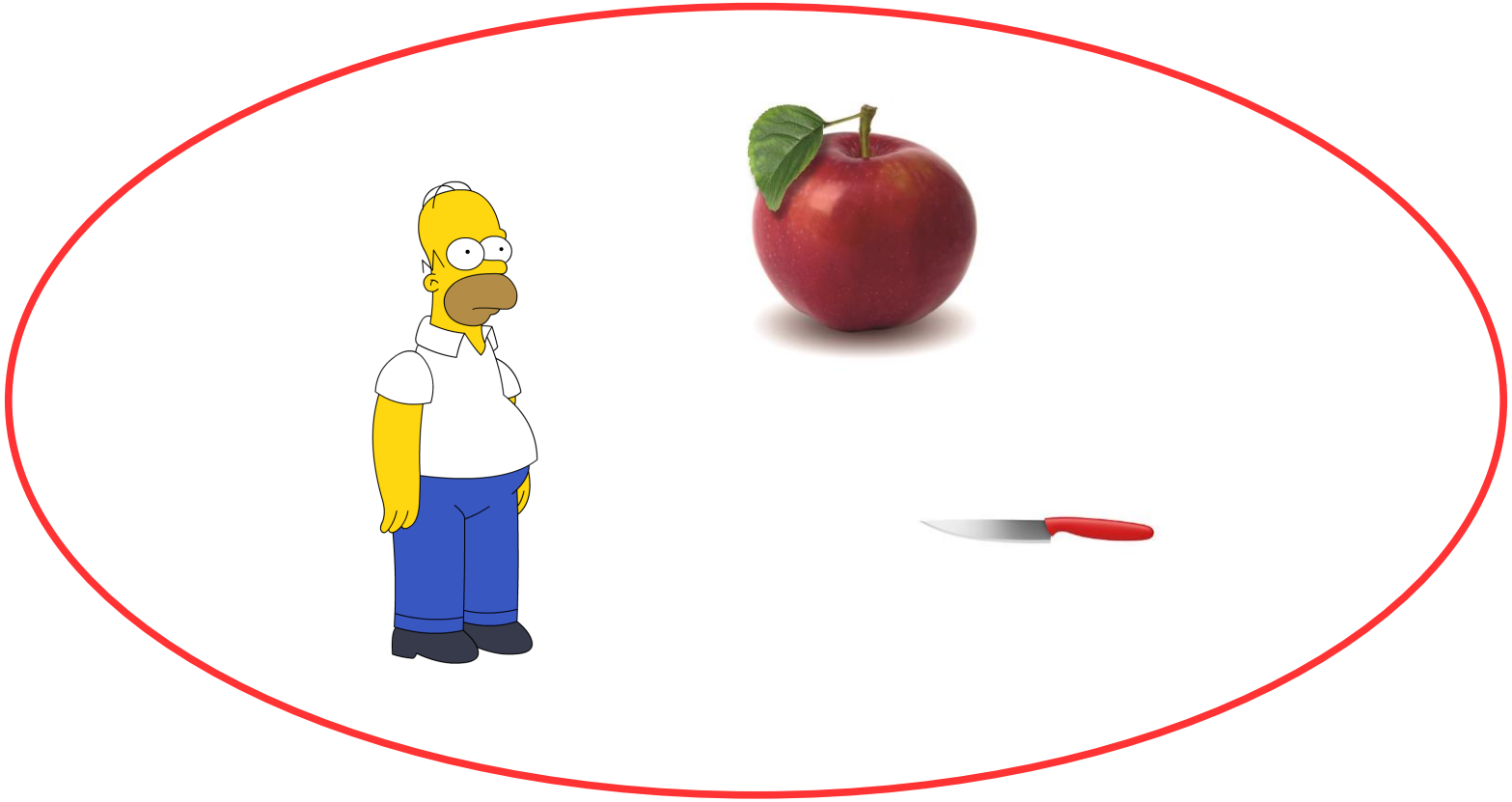


Integriert von der passiven Erkennung „Assetregister“,

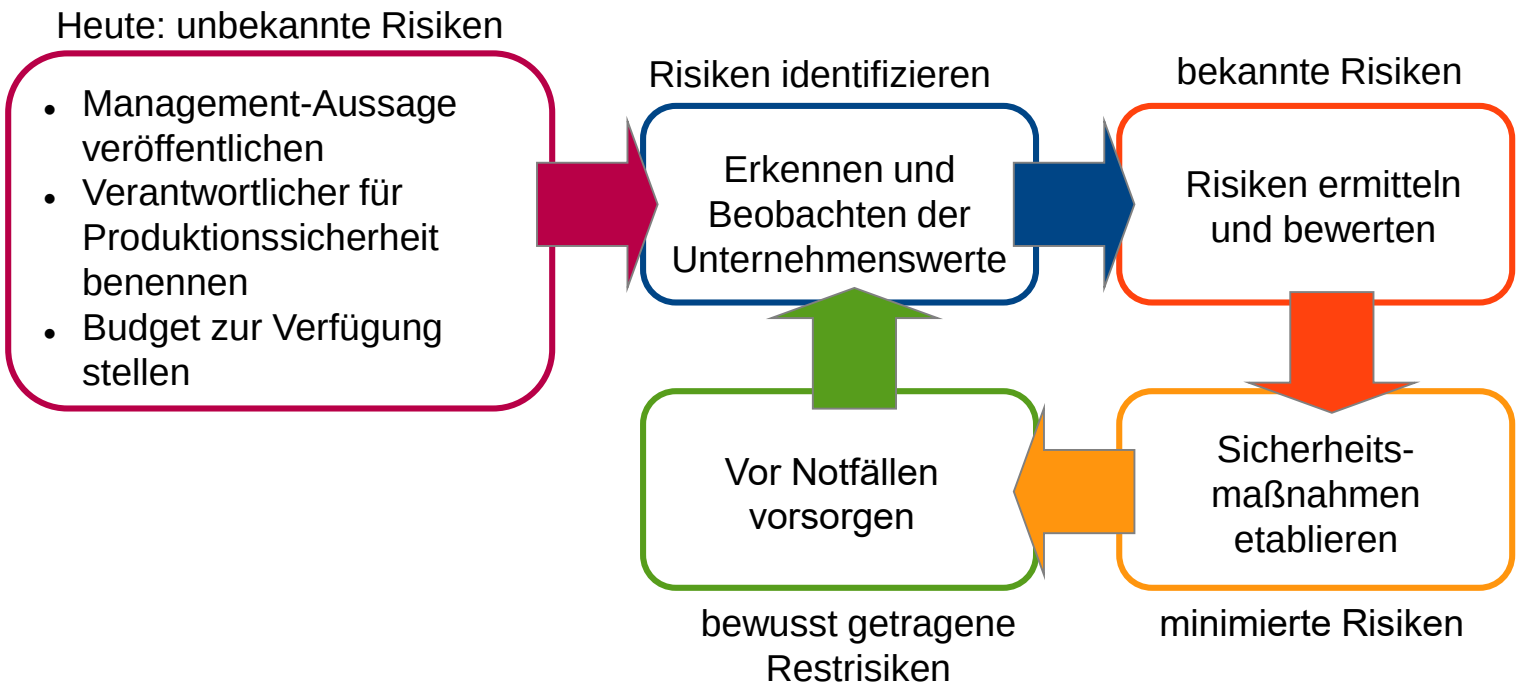
der automatisierten und kontinuierlichen Überwachung „Angriffserkennung“

sowie der aktuellen Beurteilung und Behandlung der Risiken „Security Management Prozess“.

Risikomanagement *und* Schwachstellen und Bedrohungen



Ein pragmatischer Ansatz...



Risiken erkennen, Risiken bewerten,

Risiken identifizieren!

1. Erkennen und Beobachten der Unternehmenswerte

- Aktuelle Liste der IT-Systeme und installierten Anwendungen (inkl. SW-Stände)
- Aktueller, physischer und logischer Netzplan
- Richtlinie zu Dokumentations-vorgaben
- Handlungsanweisung zum Umgang mit Sicherheitsvorfällen

IRMA:

Passiv & Automatisch Scannen

IT Assets und Verbindungen analysieren

Validierung der IT

Kontinuierliche Überwachung

Risiken bekannt!

2. Risiken ermitteln und bewerten

- Bedrohungen- und Schwachstellen-identifizierung
- Risikobewertung
- Risikobehandlung festlegen
- Jährliche Auditierung

IRMA:

Passiv & Automatisch Scannen

Schwachstellen

Ungenutzte Dienste

Risiko Management nach ISO27000

Kontinuierliche Überwachung

VIDEC.

Risiken Managen und somit minimieren

3. Sicherheits-Maßnahmen etablieren

- Dokumentation des Sicherheitskonzeptes
- Administrations- und Benutzerhandbücher für alle Systeme vorhanden
- Festlegung der betrieblichen Aufgaben von Betreiber, Integrator und Hersteller
- Handlungsanweisung zum sicheren Betrieb für Mitarbeiter
- Training des Personals

IRMA:

Maßnahmen aus dem Risiko Mgmt.

Validierte Verbindungen für Firewallregeln und Netzsegmentierung

Ungenutzte Dienste

Schwachstellen

(...)

4. vor Notfällen vorsorgen

- Festlegen der kritischen Geschäftsprozesse (Business Impact Analyse)
- Datensicherungs-konzept
- Notfallvorsorge-Konzept
- Notfall- und Wiederherstellungs-plan (Business Continuity Plan)

IRMA:

Benachrichtigungen und Alarme

Status Reports

Akzeptierte Bedrohungen aus dem Risiko Management

Daten zur Analyse bei Fehlerfällen (Forensik)

Risiken minimieren

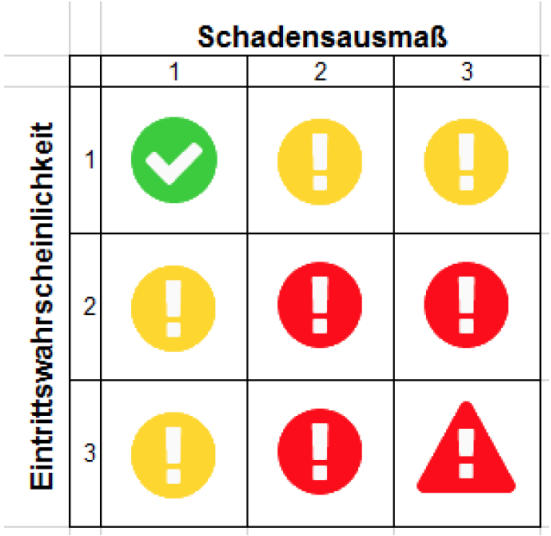
bewusst getragene Restrisiken

VIDEC.

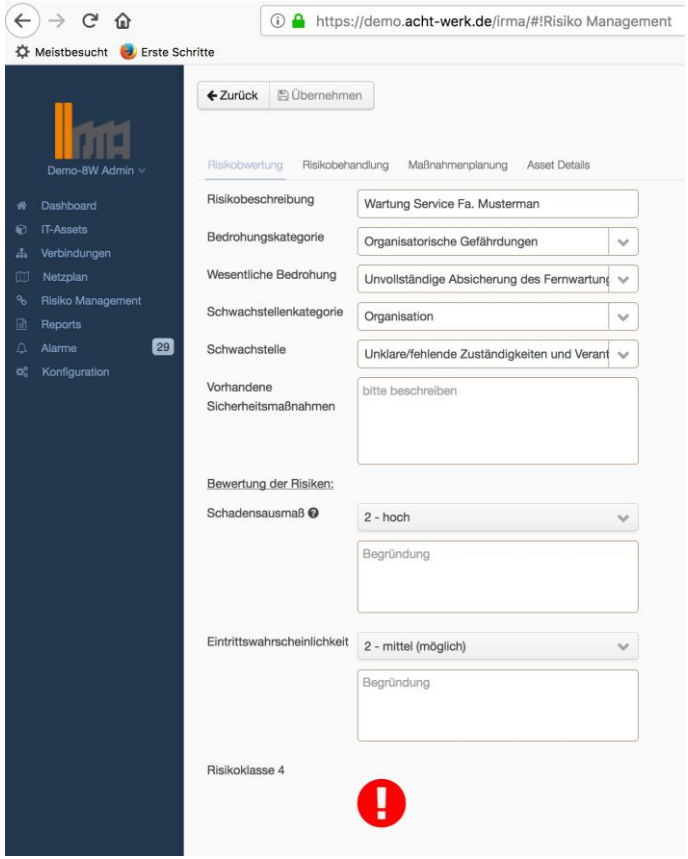
Risikobewertung

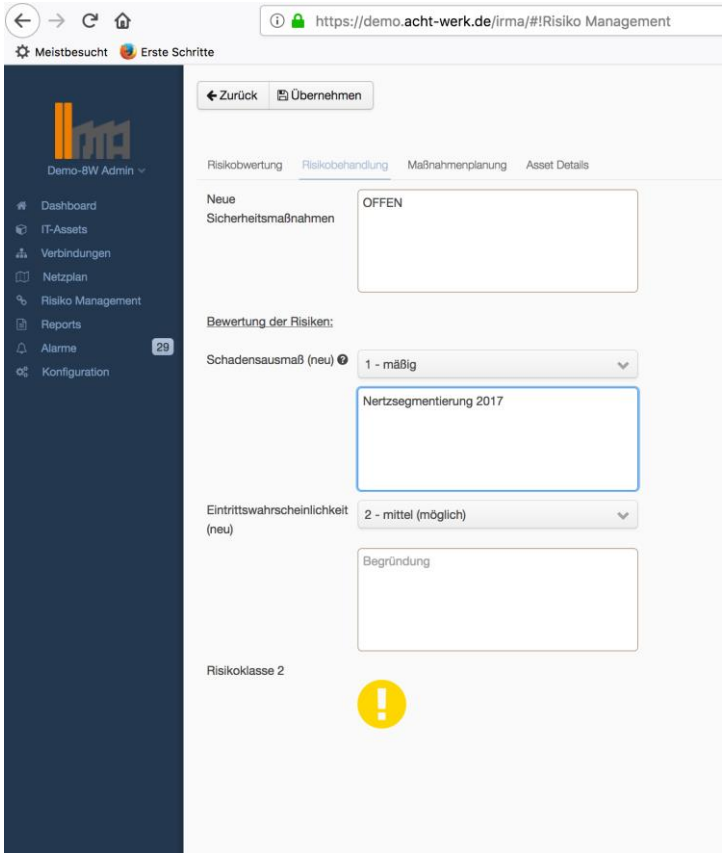
Risiko = Eintrittswahrscheinlichkeit * Schadenshöhe

Risikoklasse	Über eine Schadensausmaß-Eintrittswahrscheinlichkeits-Matrix wird die Risikoklasse bestimmt und durch ein Symbol dargestellt.



IRMA – Risiko Management



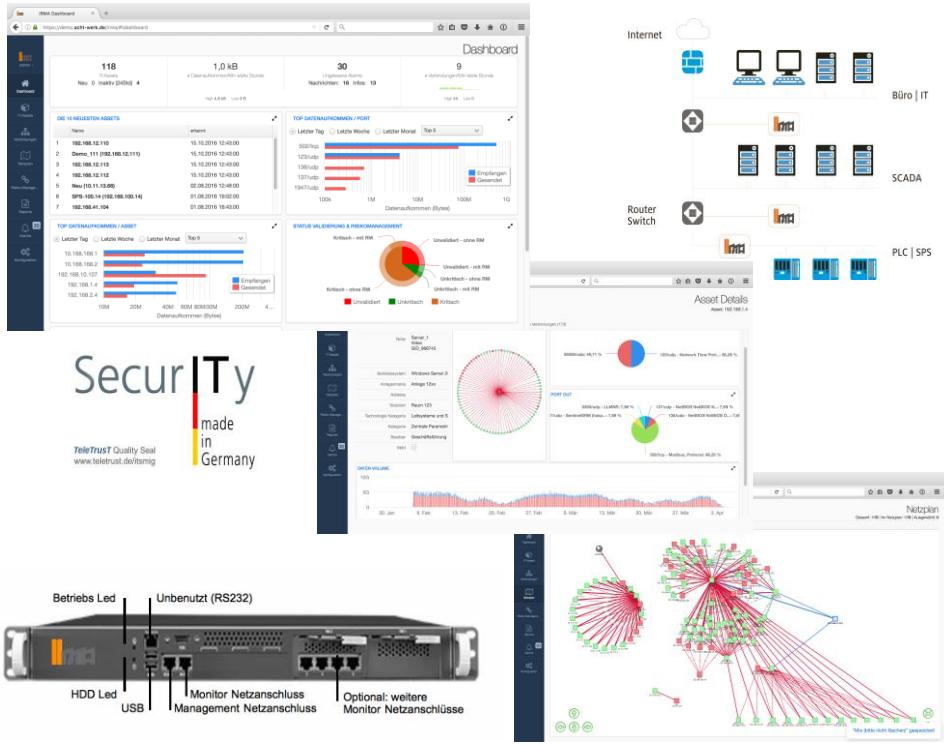


IRMA Funktionen

Überwachung und Kontrolle in Echtzeit

IRMA ist ein Industrie-Computersystem zur Identifikation und Abwehr von Cyberangriffen in Produktionsnetzwerken. IRMA überwacht kontinuierlich Ihre Produktionsanlagen, liefert Informationen zu Cyberangriffen und ermöglicht die Analyse und intelligente Alarmierung mittels einer übersichtlichen Management-Konsole. *So können verzögerungsfrei Aktionen gestartet werden, um den Angriff zu stoppen oder seine Folgen wirkungsvoll zu entschärfen*

Passiv, IRMA verhält sich ausschließlich passiv im Netz, nur Metadaten von Datenpakete filtert und aufgezeichnet. Es erfolgt keine Beeinflussung oder Aktivität im gescannten Netz. Die IRMA TAP Clients (Sensoren) kommunizieren ausschließlich abgesichert und verschlüsselt über das IT-Managementnetz.



Vielen Dank …

Vertrauen ist gut, Kontrolle ist wesentlich.

INDUSTRIE

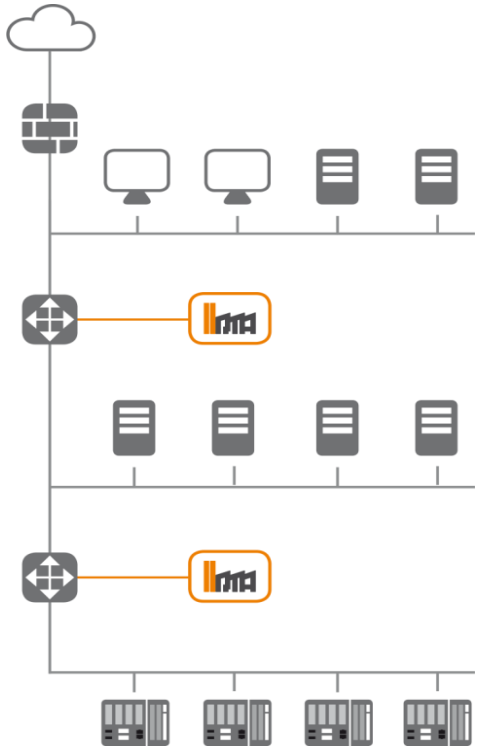
Speziell für die Steuerungs-, Automatisierungs- und Informations-Technik von Produktionsanlagen wurde IRMA entwickelt!

RISIKO MANAGEMENT

Nur durch das integrierte Risiko Management in IRMA ist eine effiziente Behandlung der Bedrohungen möglich!

AUTOMATISIERUNG

Assets werden automatisiert erfasst, im Risiko Management klassifiziert und mit der fortlaufenden Kontrolle geprüft.



VIDEC.