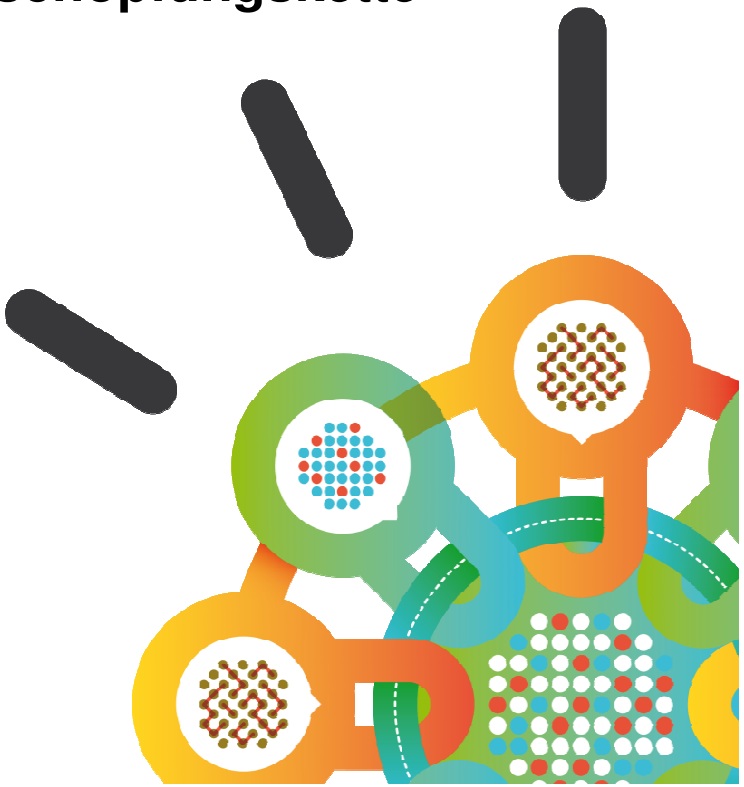
Security Intelligence.
Think Integrated.

# IBM Security Systems

## Sicherheitsaspekte in Produktion und Wertschöpfungskette

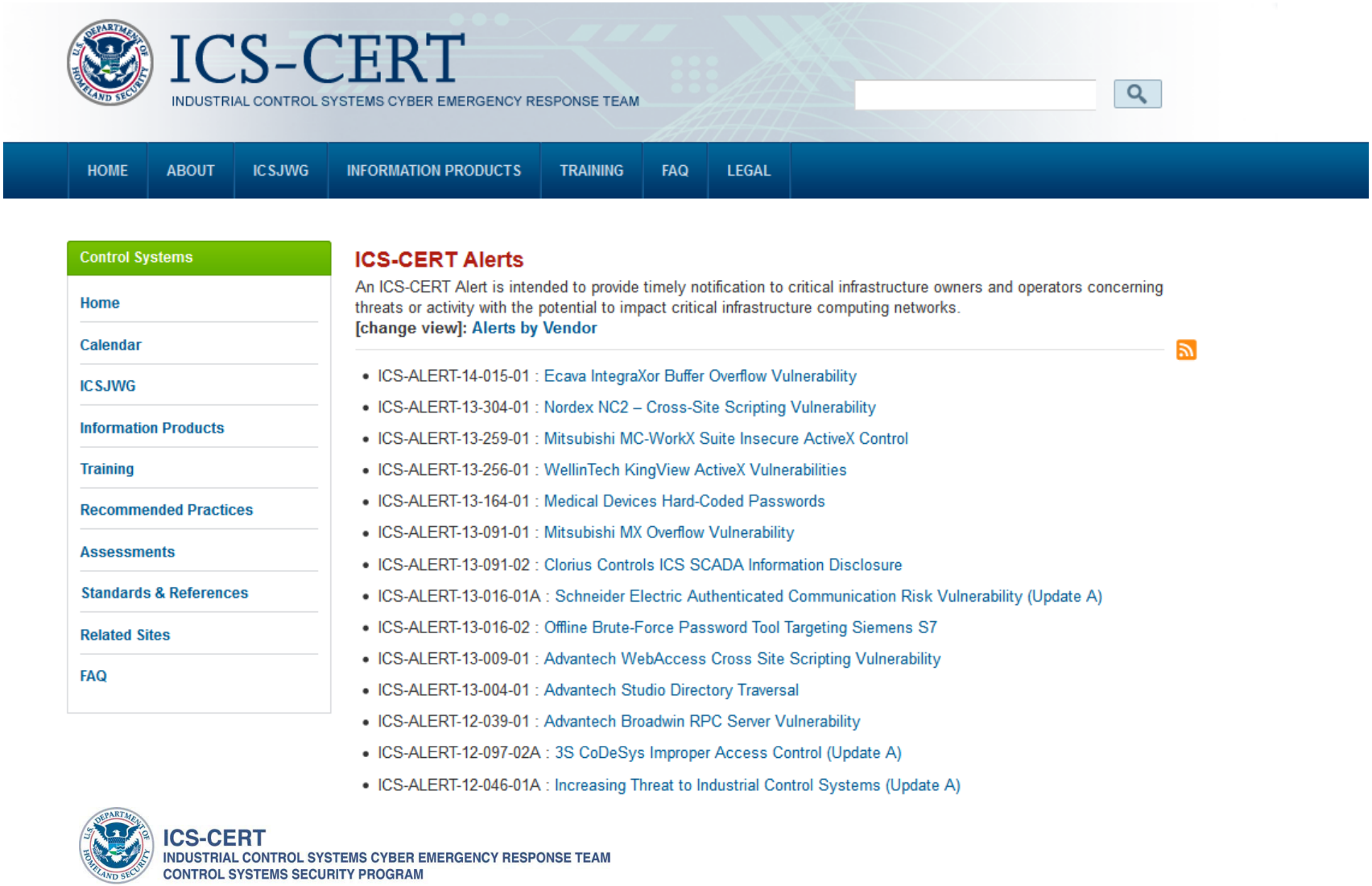
Gerd Rademann
IBM Security Systems
Business Unit Executive DACH
gerd.rademann@de.ibm.com



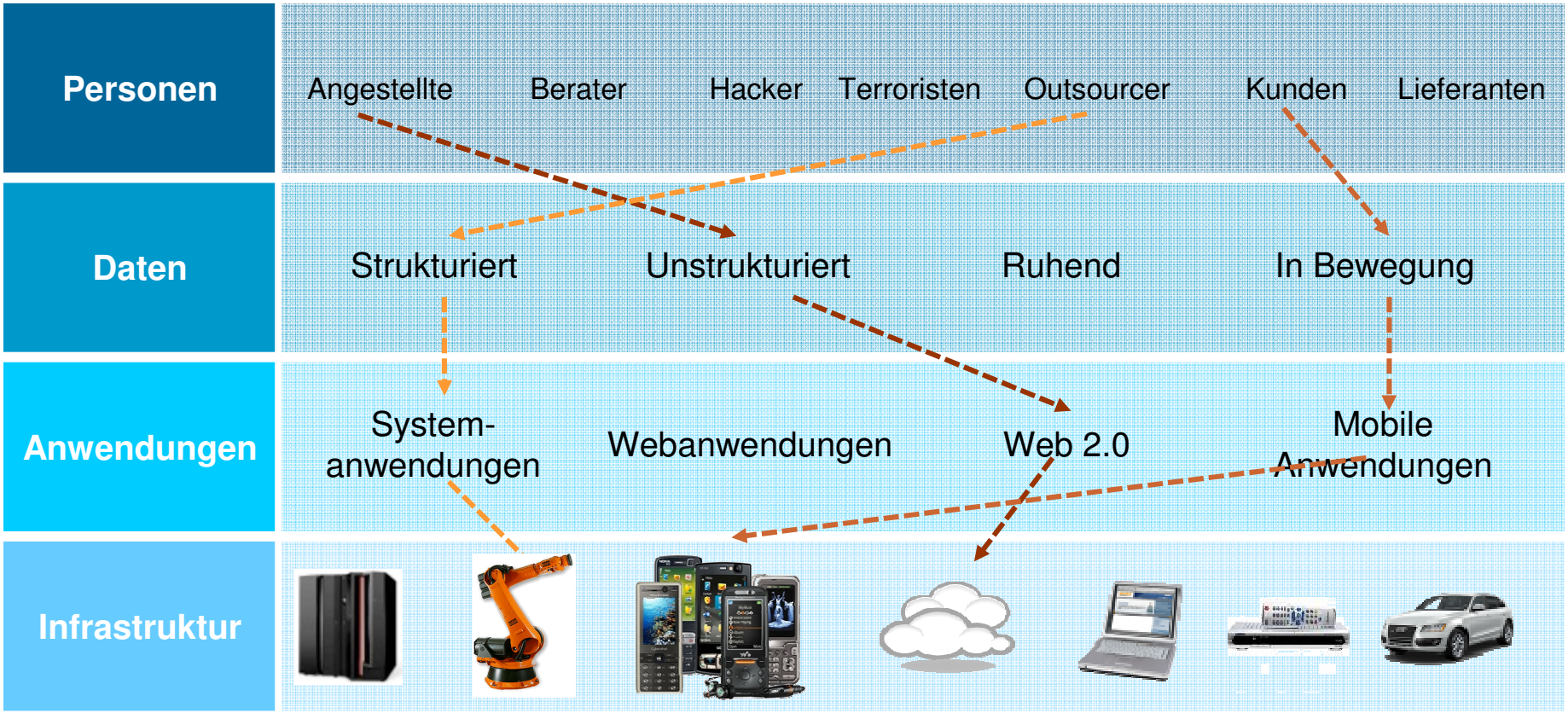
# Aktuelle Situation

- shopfloor rückt zunehmend in den Fokus von Angriffen
- Produktionsausfälle durch Virenbefall an Produktionsanlagen, z.B. Robotern
- Experten werten das Risiko von Produktionsnetzwerken als hoch und sehen Schadenspotentiale in Millionenhöhe
- Risiko ist hoch, weil das Thema Security in der Konzeptphase der Fabriken selten eine Rolle gespielt hat

# Auszug: Warnmeldungen und Hinweise des ICS-CERT



# Die Lösung eines Sicherheitsproblemes ist komplex

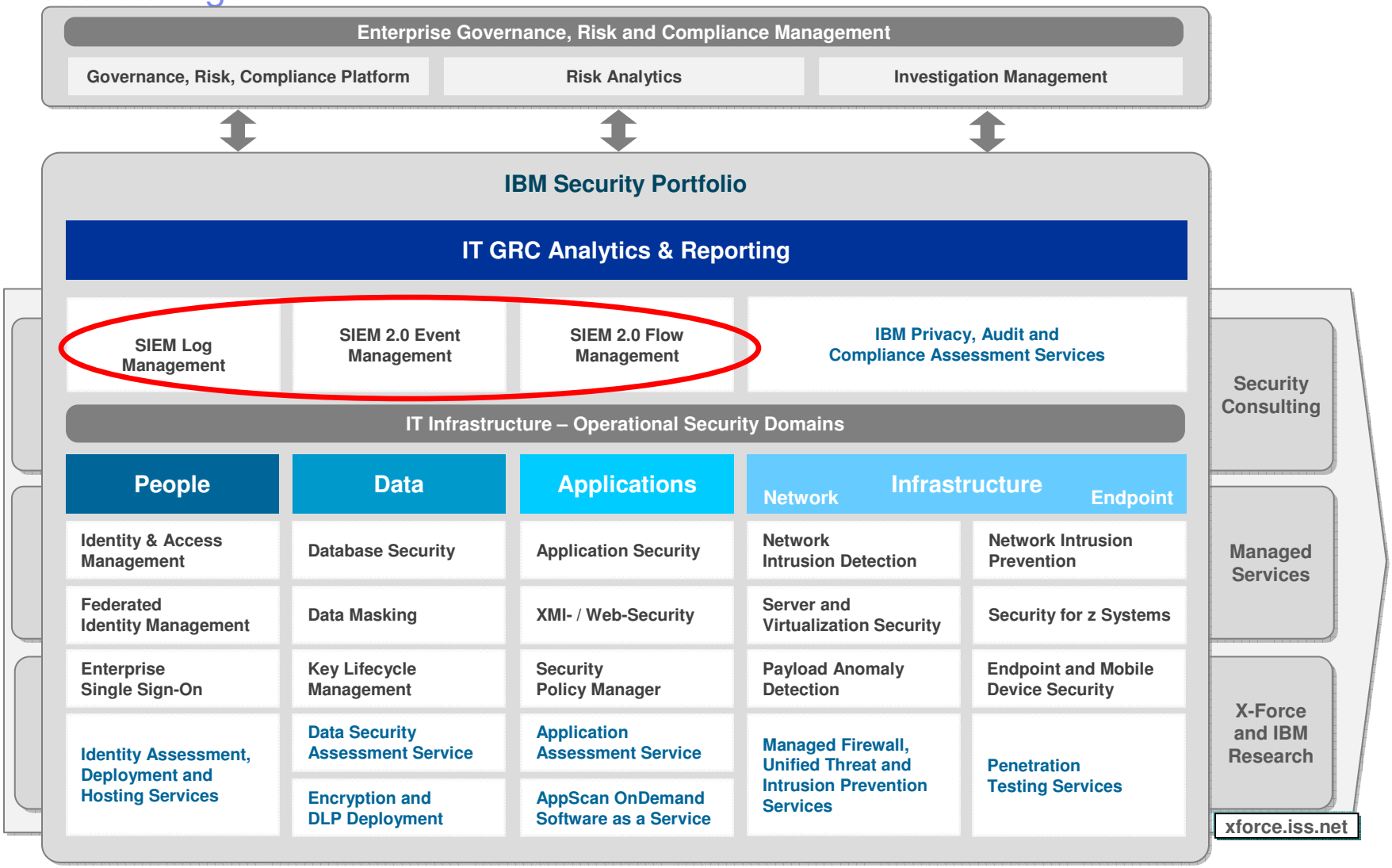



**Es reicht nicht länger aus die Grenzen zu schützen - Insellösungen und Einzelkomponenten werden das Unternehmen nicht schützen**

# Einige konkrete Ansatzpunkte im industriellen Umfeld

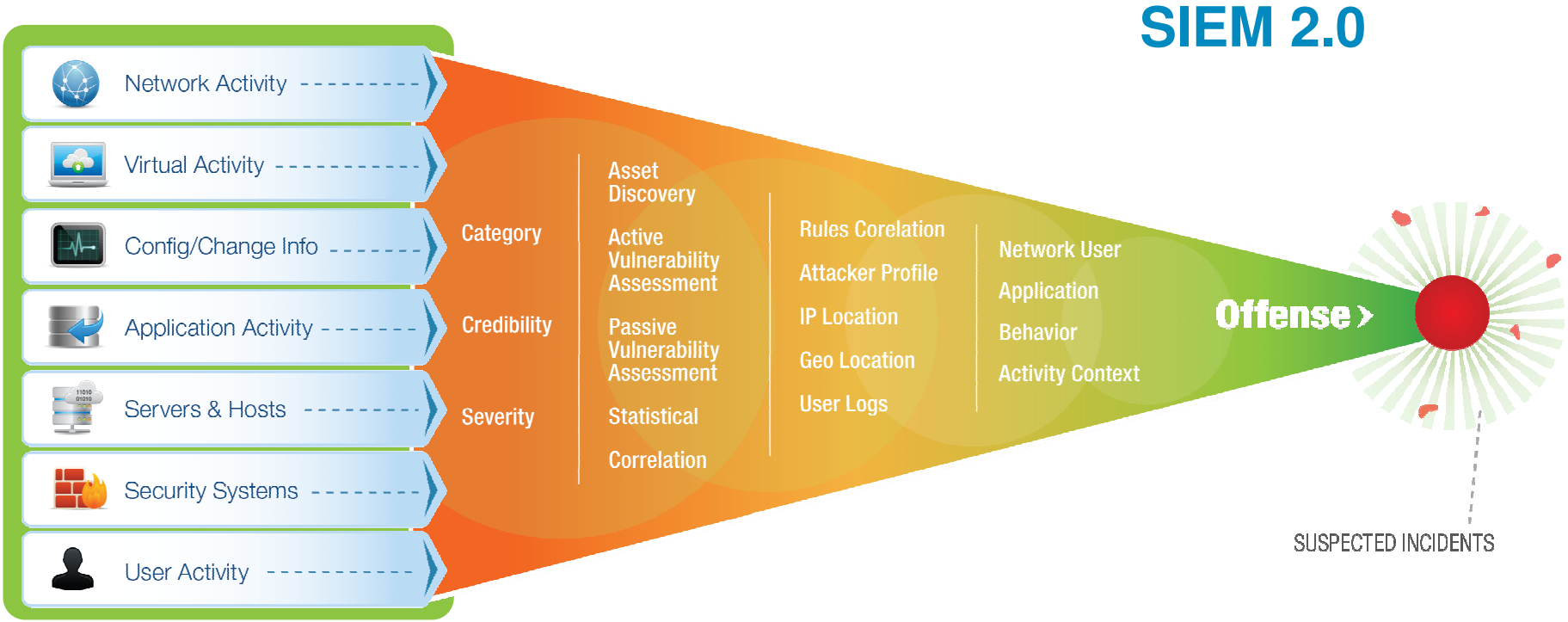
- Die Bedrohung durch Insider macht einen erheblichen Anteil der Bedrohungen aus.
  - **Privileged User Management**
- Unternehmensübergreifende Wertschöpfungsketten erfordern den Austausch sicherer, vertrauenswürdiger Identitätsinformationen
  - **Identity Federation**
- Security muß bei der Entwicklung der Systeme von Beginn an mitgedacht werden (Secure by Design)
  - **Application Security**
- Immer neue Angriffstechniken erfordern stetige Aktualisierung des Schutzes.
  - **Intrusion Detection/Prevention** auf Basis ständiger Analyse der Bedrohungen
- In einer industriellen Produktionsumgebung darf eine Überwachung der Kommunikation keine Eingriffe in die Systeme verursachen (rückwirkungsfreie Überwachung)
  - **Security Intelligence**

# IBM bietet zur Lösung ein umfassendes Security Portofolio - insbesondere auch für Industrieanlagen




blue = services offerings

# Security Intelligenz korrelliert die Informationen aller relevanten Systeme und liefert klare Hinweise für Handlungsbedarf




Log-Quellen + Security Intelligenz = genaueste & umsetzbare Erkenntnisse

# Besondere Rahmenbedinungen von Industrieanlagen

- Höchste Priorität haben Taktzeiten und Produktionsmengen
- Massnahmen zur Security dürfen dies nicht beeinträchtigen
- Produktionsnetzwerke aktuell sind im Gegensatz zur Office IT relativ statisch; Kommunikation zwischen unbekannten oder nicht berechtigten Partnern deuten auf ein Sicherheitsrisiko hin
- Visionen der Fertigung zielen auf die Kommunikation zwischen Anlagen- (teilen) zur intelligenten Steuerung

# Ein Kundenbeispiel

*Ausgangssituation:*

- Automatisierungssysteme sind geschäftskritisch
- Fertigungssysteme haben ein relativ statisches Kommunikationsverhalten
- Netzwerkbelastung durch nicht benötigte Services
- Suche nach einer **rückwirkungsfreien** Sicherheits-Lösung, die verdächtige Kommunikation erkennt, nicht benötigte Services eliminiert, alle Assets erkennt

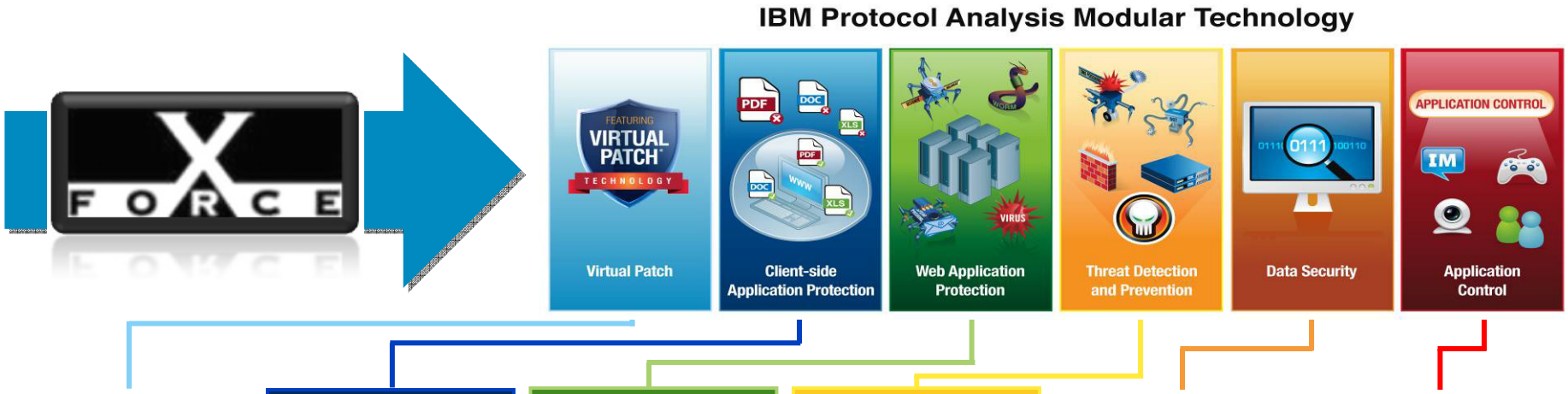
*Beobachtungen:*

- Firewalls können die Verfügbarkeit von Fertigungssystemen reduzieren
- Aktivierter Virenschutz kann cycle times erhöhen
- Software Patches können
  - den Boot-Vorgang erheblich verlängern
  - den Wiederanlauf beeinträchtigen oder verhindern
- Aktive Scan-Vorgänge können zum Systemausfall führen

*Lösung: SIEM 2.0 (QRadar)*

- Passives Lauschen im Netzwerk
  - Nebeneffekt: Erkennen aller Assets
- Definition von Korrelationsregeln auf Basis von Whitelists (zulässige Kommunikation)
- Überwachung der Kommunikation auf Basis der Regeln
- Analyse der genutzten Services
- Analyse der Kommunkation mit externen Adressen

# Virtual Patch™ zum Schutz von Anlagen, die nicht gepatched werden dürfen




## Virtual Patch

**Was es tut:**
Schützt Schwachstellen vor Angriffen unabhängig vom Softwarepatch und ermöglicht einen verantwortungsvollen Patch Management Prozess.

**Wieso ist es wichtig:**
Nicht jedes System (insbesondere Industrie-Produktionsanlagen darf einfach gepatched werden
Für ca. ein drittel der veröffentlichen Schwachstellen steht zeitnah kein Patch seitens der Hersteller zur Verfügung.

## Client-Side Application Protection

**Was es tut:**
Schützt Endbenutzer vor Angriffen auf täglich genutzte Anwendungen wie MS Office, Adobe PDF, Multimedia Files und Webbrowser.

**Wieso ist es wichtig:**
Schwachstellen in Client Applikationen betreffen regelmäßig eine der größten Kategorien von neu entdeckten Schwachstellen.

## Web Application Protection

**Was es tut:**
Schützt Anwendungen gegen komplexe Angriffe wie SQL Injection, Cross-Site-Scripting, PHP File-Includes, Cross-Site Request Forgery.

**Wieso ist es wichtig:**
Erweitert die Sicherheitsfunktionen um Compliance Anforderungen und die Weiterentwicklung von Bedrohungen abzudecken.

## Threat Detection & Prevention

**Was es tut:**
Erkennt und schützt präventiv vor einer gesamten Klasse von Bedrohungen im Gegensatz zu anderen Lösungen, die lediglich reaktiv spezifische Angriffe erkennen.

**Wieso ist es wichtig:**
Konstante Signatur-Updates sind unnötig. Schutz beinhaltet proprietäre Shellcode Heuristics (SCH) Technologie, die eine konkurrenzlose Erfolgsgeschichte gegen "Zero-Day" Angriffe hat.

## Data Security

**Was es tut:**
Identifiziert unverschlüsselte persönliche Daten und andere vertrauliche Informationen. Bietet auch die Möglichkeit Datenflüsse durch das Netzwerk zu analysieren, um bei dem Aufspüren möglicher Risiken zu helfen.

**Wieso ist es wichtig:**
Flexible und skalierbare Suche nach kundenspezifischen Daten, dient als Ergänzung zur Datensicherheitsstrategie

## Application Control

**Was es tut:**
Verwaltet und kontrolliert unautorisierte Anwendungen und Risiken in definierten Netzwerksegmenten, wie ActiveX Fingerprinting, Peer To Peer, Instant Messaging und Tunneling.

**Wieso ist es wichtig**:
Kontrolle der Netzwerkzugriffe von Anwendungen und Diensten basierend auf Unternehmensrichtlinien.

# Zusammenfassung

- Security Intelligence (QRadar) ist ein nachgewiesen erfolgreiches Mittel, Sicherheitsvorfälle in Produktionsanlagen zu erkennen

- Virtual Patch™ kann Anlagen schützen, die nicht verändert werden dürfen

ibm.com/security



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

# IBM security: research and expertise

**9 Security Operations Centers** + **9 Security Research Centers** + **11 Security Solution Development Centers** + **133 Monitored Countries** + **900+ Professional Services Security Consultants** + **600+ field security specialists** + **4,500 Security Delivery Experts** + **400+ security operations analysts**


**IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security**