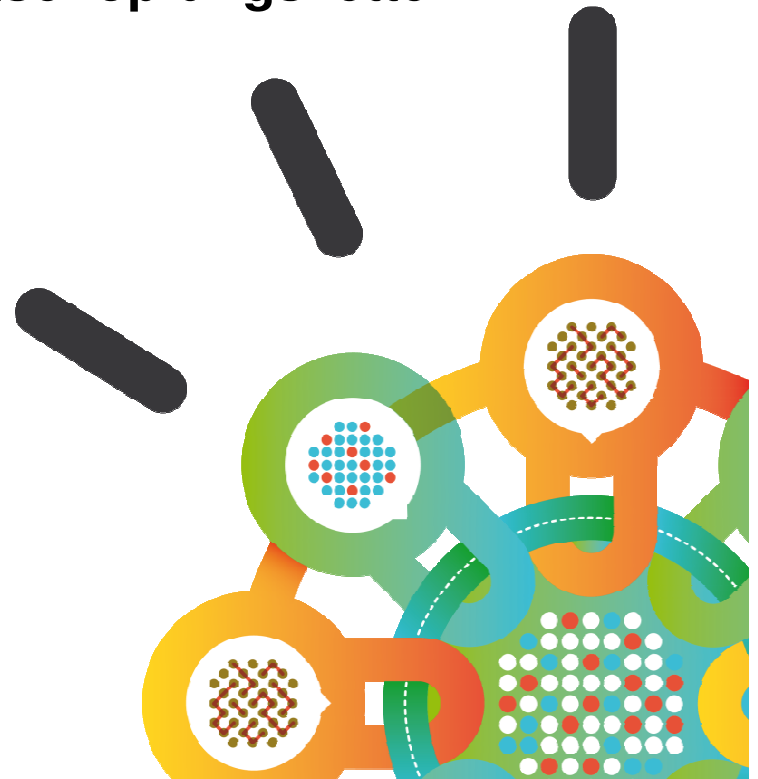


Security Intelligence.
Think Integrated.

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

26.07.2010, 08:43
Siemens: Viren-Update kann Fabriken lahm legen

Siemens warnt seine Industriekunden vor einem neuen Wurm, der ihre Kontrollsysteme befällt. Gleichzeitig verwies der Konzern darauf, dass selbständiges Removal die IT-gestützten Prozesse lahm legen könnte.

Der SCADA-Wurm (Supervisory, Control and Data Acquisition) - "VirusBlokAda" oder "Stuxnet" genannt - betrifft industrielle Kontrollsysteme in Produktionsanlagen aller Größe. "Da jede Fabrik individuell konfiguriert ist, können wir die Möglichkeit nicht ausschließen, dass die Entfernung des Virus Ihre Anlagen in irgendeiner Weise in Mitleidenschaft zieht", hieß es in einem Statement von Siemens Industry.

Datenkrake: Virus Stuxnet ist erstmals aktiv.

CHIP ONLINE

Iran im Krieg 2.0

Der Computerwurm Stuxnet befällt eine iranische Atomanlage – sehen so die Schlachten der Zukunft aus?

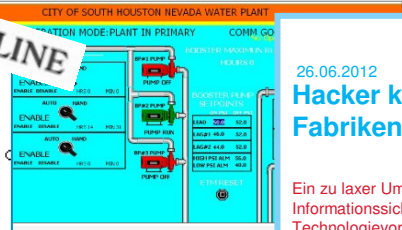


Das iranische Kernkraftwerk Buschehr wurde bereits in den siebziger Jahren geplant und wird voraussichtlich Anfang November durch russische Hilfe ans Netz gehen.

ZEITUNG ONLINE

20.11.2011
Ferngesteuertes Wasserwerk
Hacker führen US-Behörden vor

Von Ole Reißmann



CITY OF SOUTH HOUSTON NEVADA WATER PLANT

ANSHOT eines Wasserwerks: Hacker brüstet sich mit

staat Illinois wurde ein Wasserwerk offenb.

Behörden spielen den Fall herunter, Exper

Kriminelle könnten per Fernsteuerung in

sein. Zum Beweis knackte ein Unbekannter

SPIEGEL ONLINE

26.06.2012
Hacker kopieren komplette Fabriken

Ein zu laxer Umgang mit dem Thema Informationssicherheit bedroht den Technologievorsprung deutscher Unternehmen - vom Produktdesign und der Produktion bis zur carIT. Im Round-Table-Gespräch mit automotiveIT diskutieren Berufshacker Felix „FX“ Lindner und Sandro Gaycken, Sicherheitsforscher an der Freien Universität Berlin, die aktuelle Bedrohungslage.



automotiveIT

Auszug: Warnmeldungen und Hinweise des ICS-CERT



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME

ABOUT

ICSJWG

INFORMATION PRODUCTS

TRAINING

FAQ

LEGAL

Control Systems

Home

Calendar

ICSJWG

Information Products

Training

Recommended Practices

Assessments

Standards & References

Related Sites

FAQ

ICS-CERT Alerts

An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.
[\[change view\]: Alerts by Vendor](#)



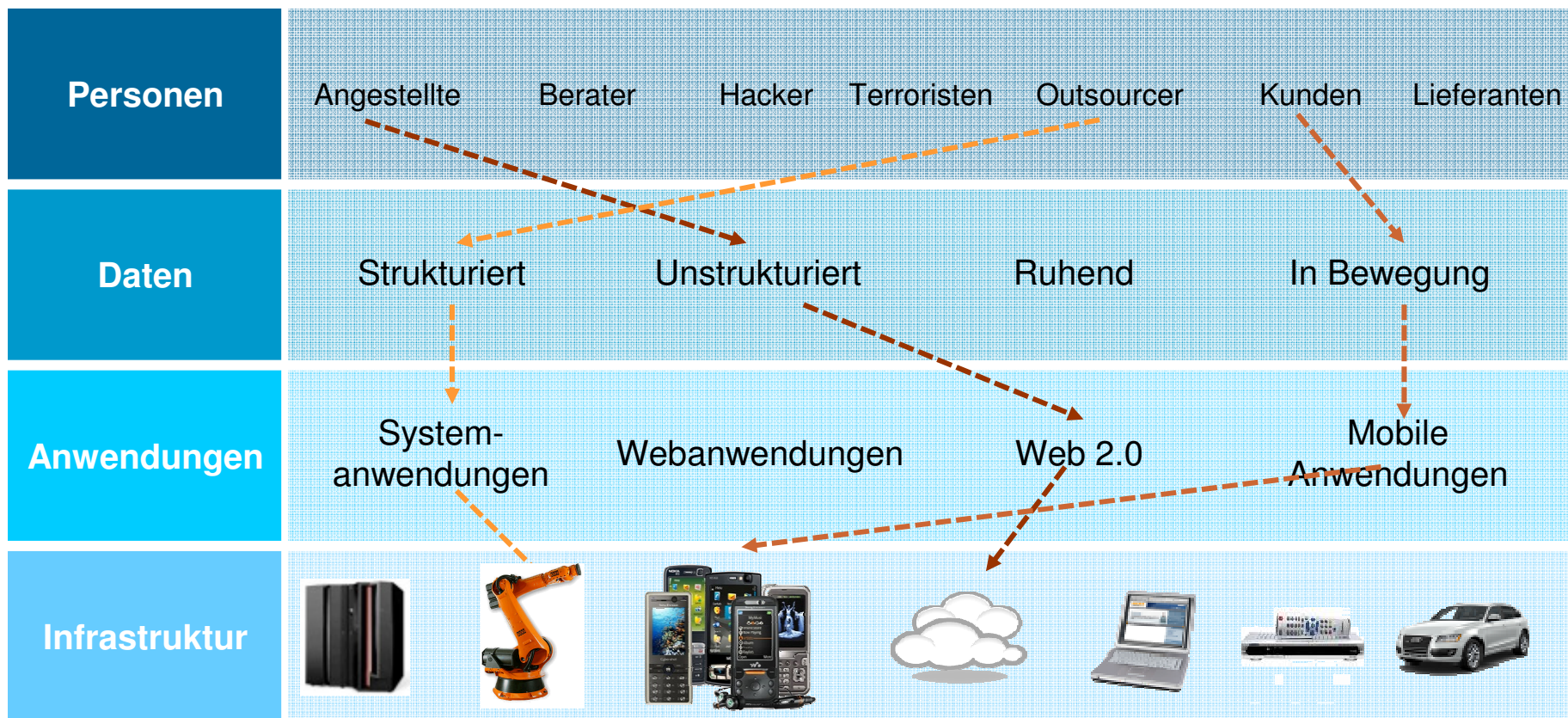
- ICS-ALERT-14-015-01 : Ecava IntegraXor Buffer Overflow Vulnerability
- ICS-ALERT-13-304-01 : Nordex NC2 – Cross-Site Scripting Vulnerability
- ICS-ALERT-13-259-01 : Mitsubishi MC-WorkX Suite Insecure ActiveX Control
- ICS-ALERT-13-256-01 : WellinTech KingView ActiveX Vulnerabilities
- ICS-ALERT-13-164-01 : Medical Devices Hard-Coded Passwords
- ICS-ALERT-13-091-01 : Mitsubishi MX Overflow Vulnerability
- ICS-ALERT-13-091-02 : Clorius Controls ICS SCADA Information Disclosure
- ICS-ALERT-13-016-01A : Schneider Electric Authenticated Communication Risk Vulnerability (Update A)
- ICS-ALERT-13-016-02 : Offline Brute-Force Password Tool Targeting Siemens S7
- ICS-ALERT-13-009-01 : Advantech WebAccess Cross Site Scripting Vulnerability
- ICS-ALERT-13-004-01 : Advantech Studio Directory Traversal
- ICS-ALERT-12-039-01 : Advantech Broadwin RPC Server Vulnerability
- ICS-ALERT-12-097-02A : 3S CoDeSys Improper Access Control (Update A)
- ICS-ALERT-12-046-01A : Increasing Threat to Industrial Control Systems (Update A)



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
 CONTROL SYSTEMS SECURITY PROGRAM

Die Lösung eines Sicherheitsproblem es ist komplex

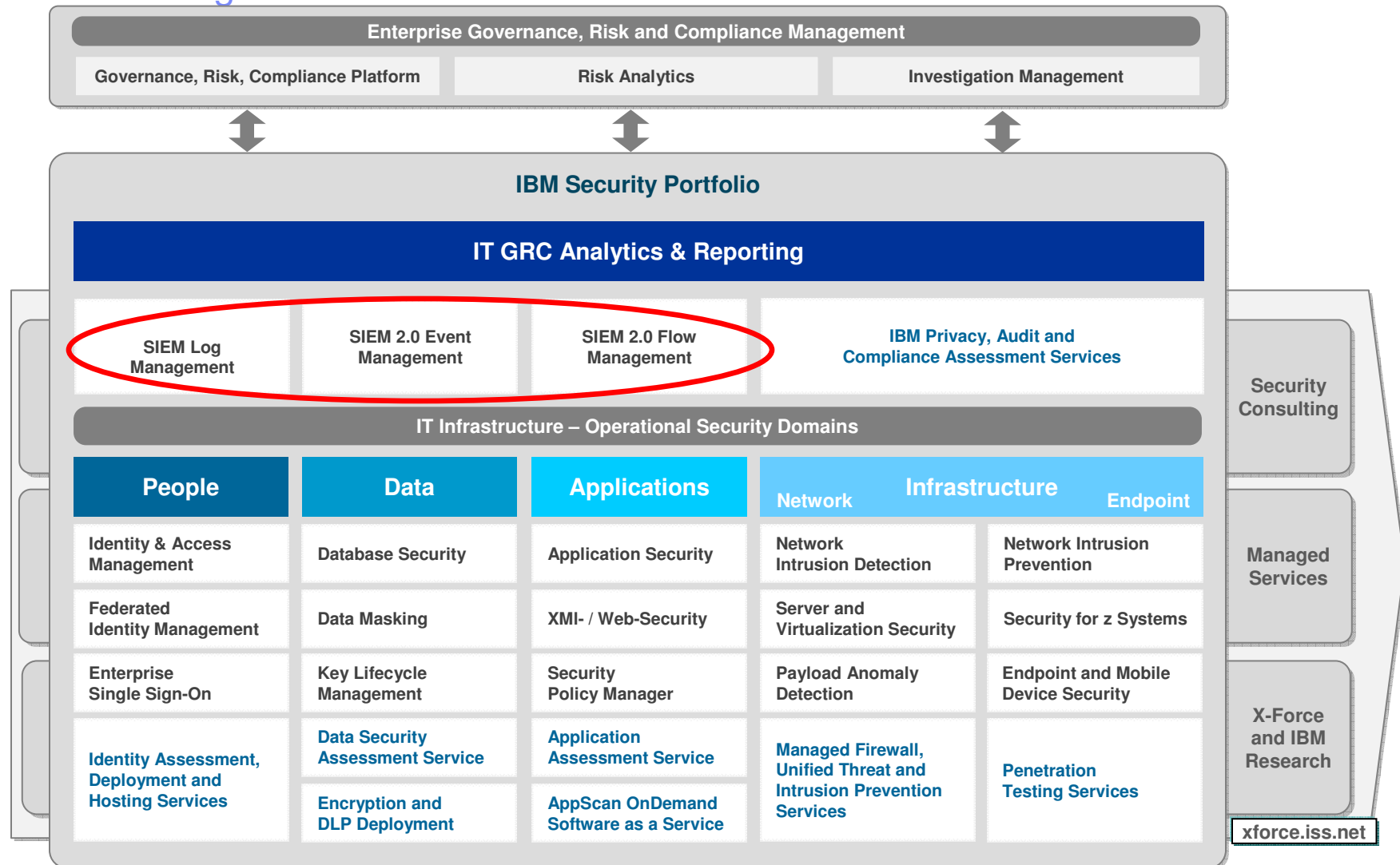


Es reicht nicht länger aus die Grenzen zu schützen -
Insellösungen und Einzelkomponenten werden das
Unternehmen nicht schützen

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**

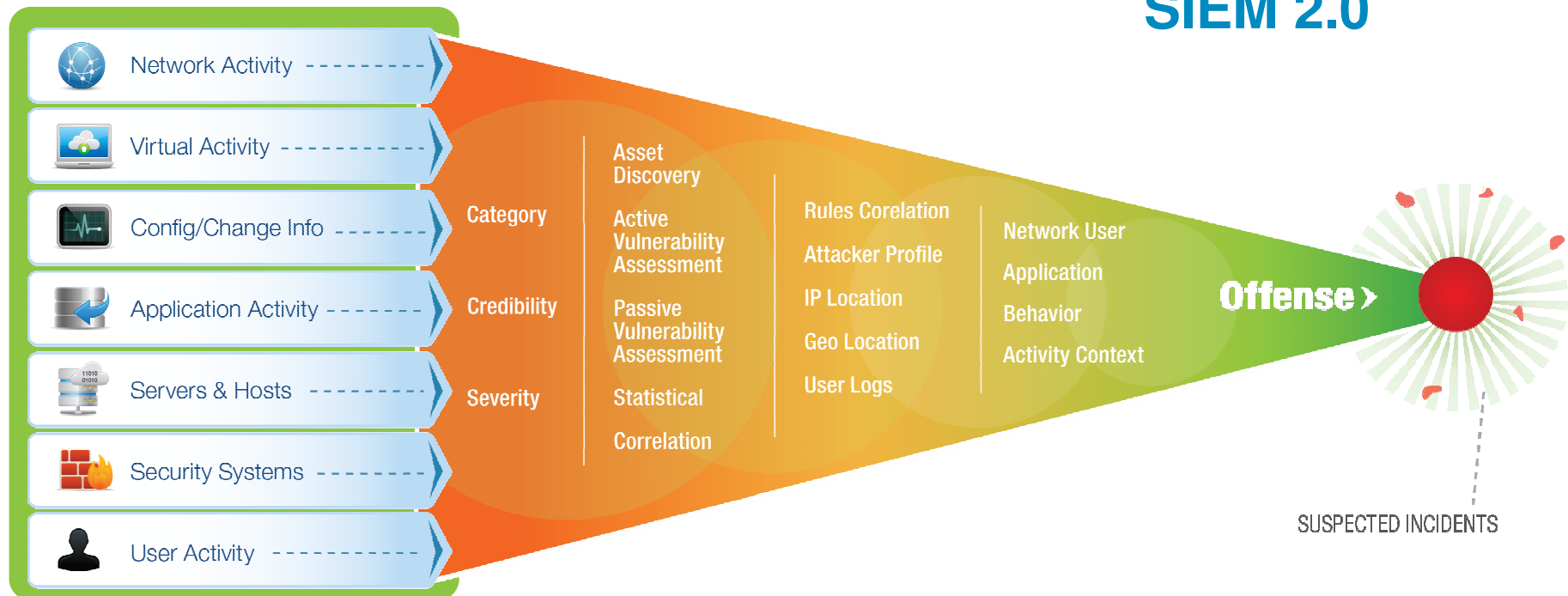
IBM bietet zur Lösung ein umfassendes Security Portfolio - insbesondere auch für Industrieanlagen



blue = services offerings

Security Intelligence korreliert die Informationen aller relevanten Systeme und liefert klare Hinweise für Handlungsbedarf

SIEM 2.0



Besondere Rahmenbedingungen 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:

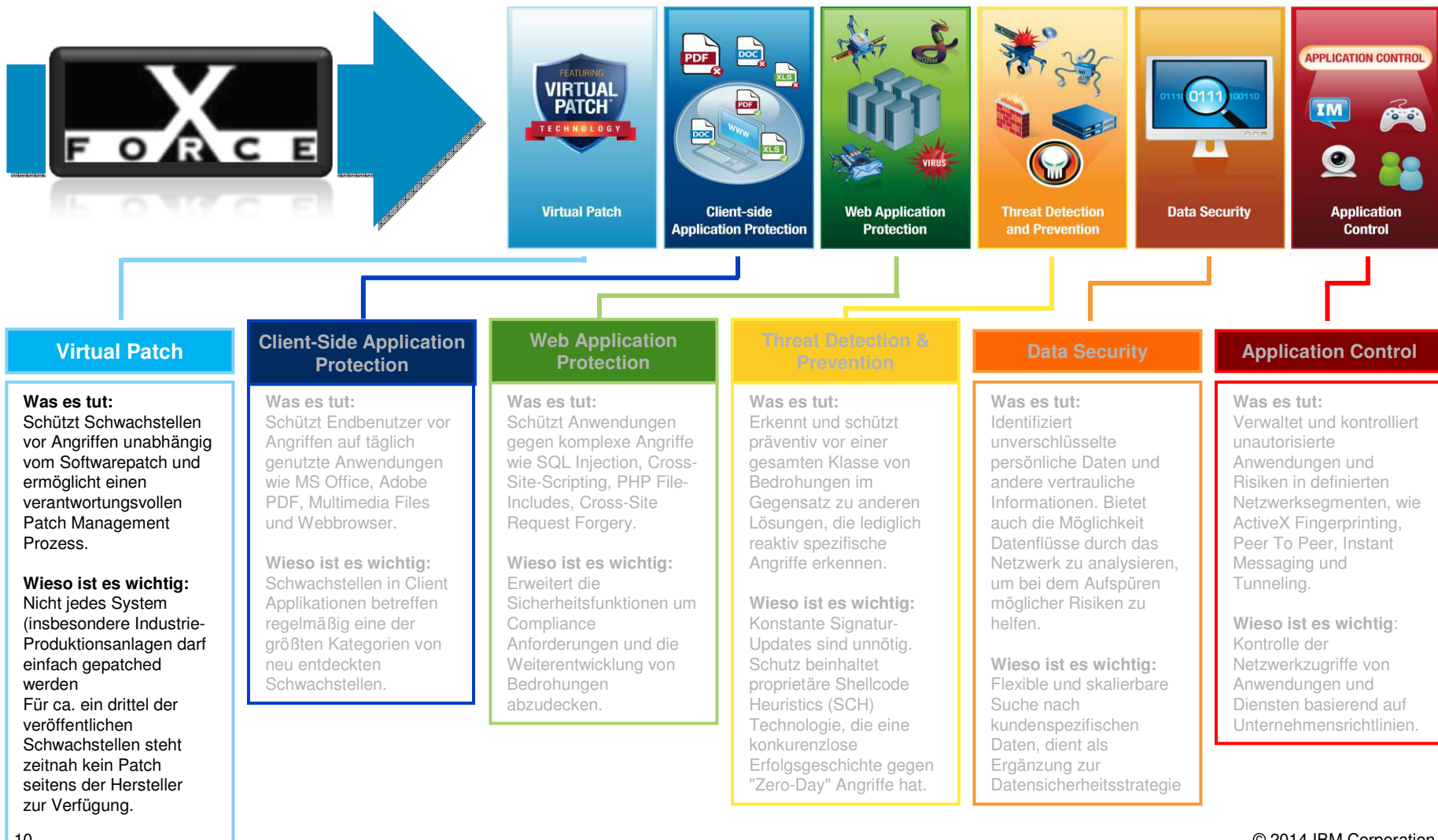
- Firewalls können die Verfügbarkeit von Fertigungssystemen reduzieren
- Aktivierter Virenschutz kann cycle times erhöhen
- Software Patches können
 - den Boot-Vorgang erheblich verlängern
 - den Wiederanlauf beeinträchtigen oder verhindern
- Aktive Scan-Vorgänge können zum Systemausfall führen

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 Kommunikation mit externen Adressen

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

IBM Protocol Analysis Modular Technology



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



© Copyright IBM Corporation 2012. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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



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