Klaus Mochalski | CEO

Integration 4.0

Cybersicherheit & Stabilität durch Monitoring vernetzter Industrieanlagen

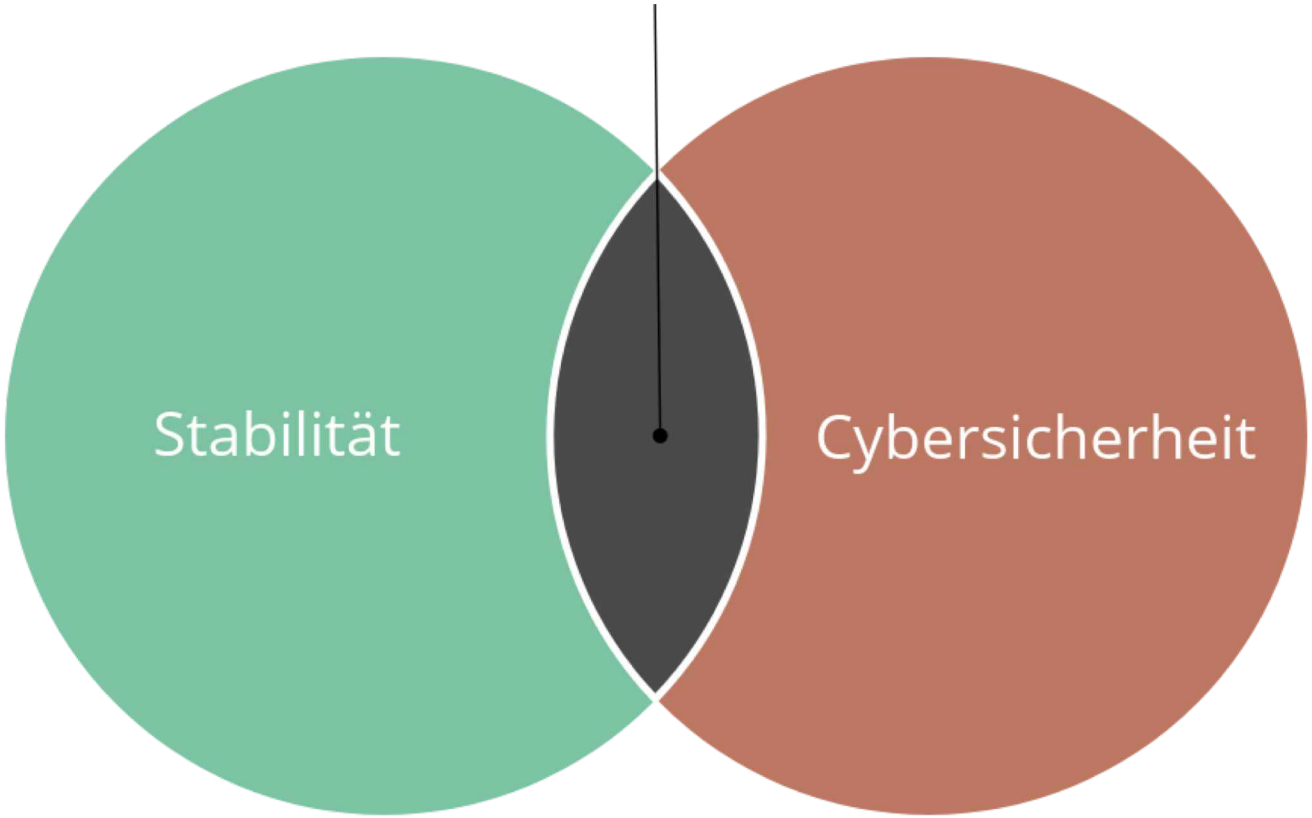

WISSEN SIE, WER SICH
IN IHRER INFRASTRUKTUR
HERUMTREIBT?

BSI: Industrial Control System Security
Top 10 Bedrohungen und Gegenmaßnahmen 2019

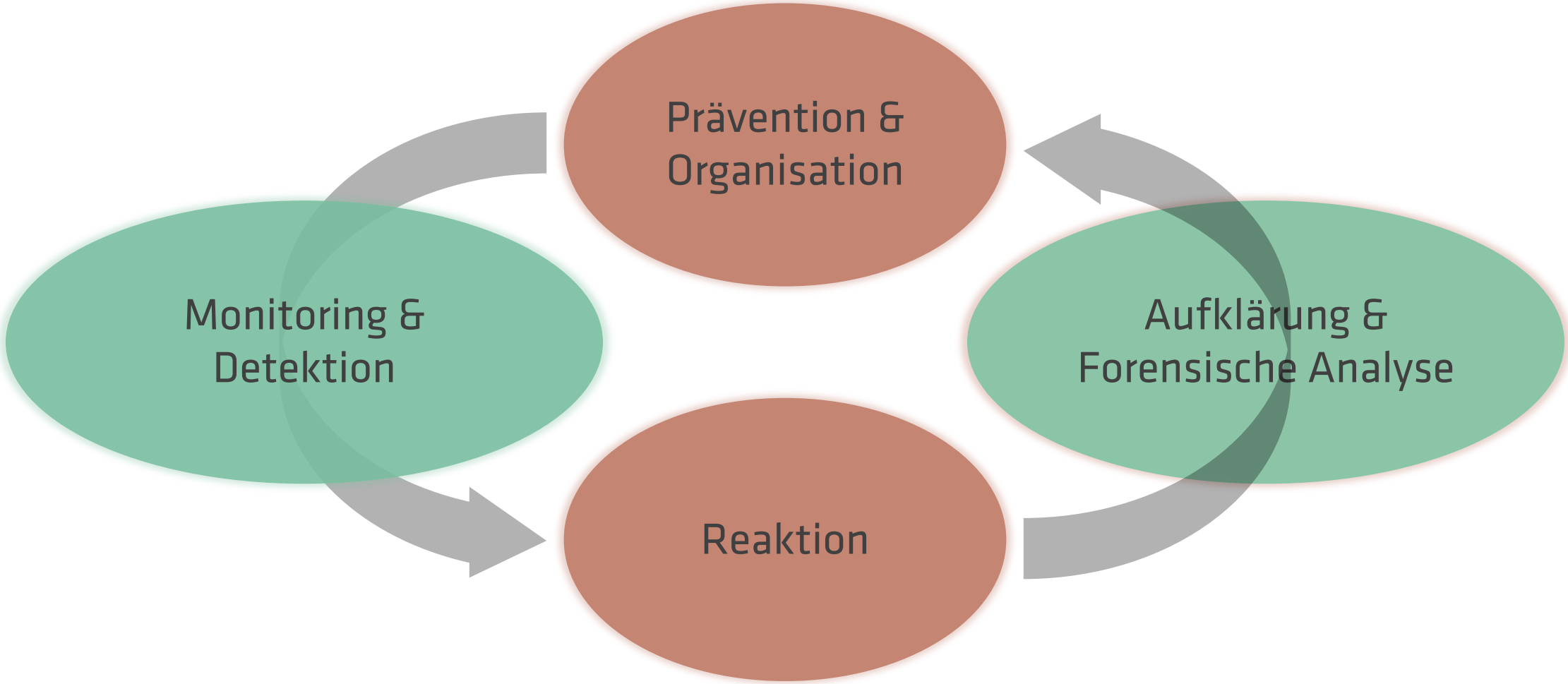
Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	
Infektion mit Schadsoftware über Internet und Intranet	
Menschliches Fehlverhalten und Sabotage	
Kompromittierung von Extranet und Cloud-Komponenten	
Social Engineering und Phishing	
(D)DoS Angriffe	
Internet-verbundene Steuerungskomponenten	
Einbruch über Fernwartungszugänge	
Technisches Fehlverhalten und höhere Gewalt	
Kompromittierung von Smartphones im Produktionsumfeld	

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.html

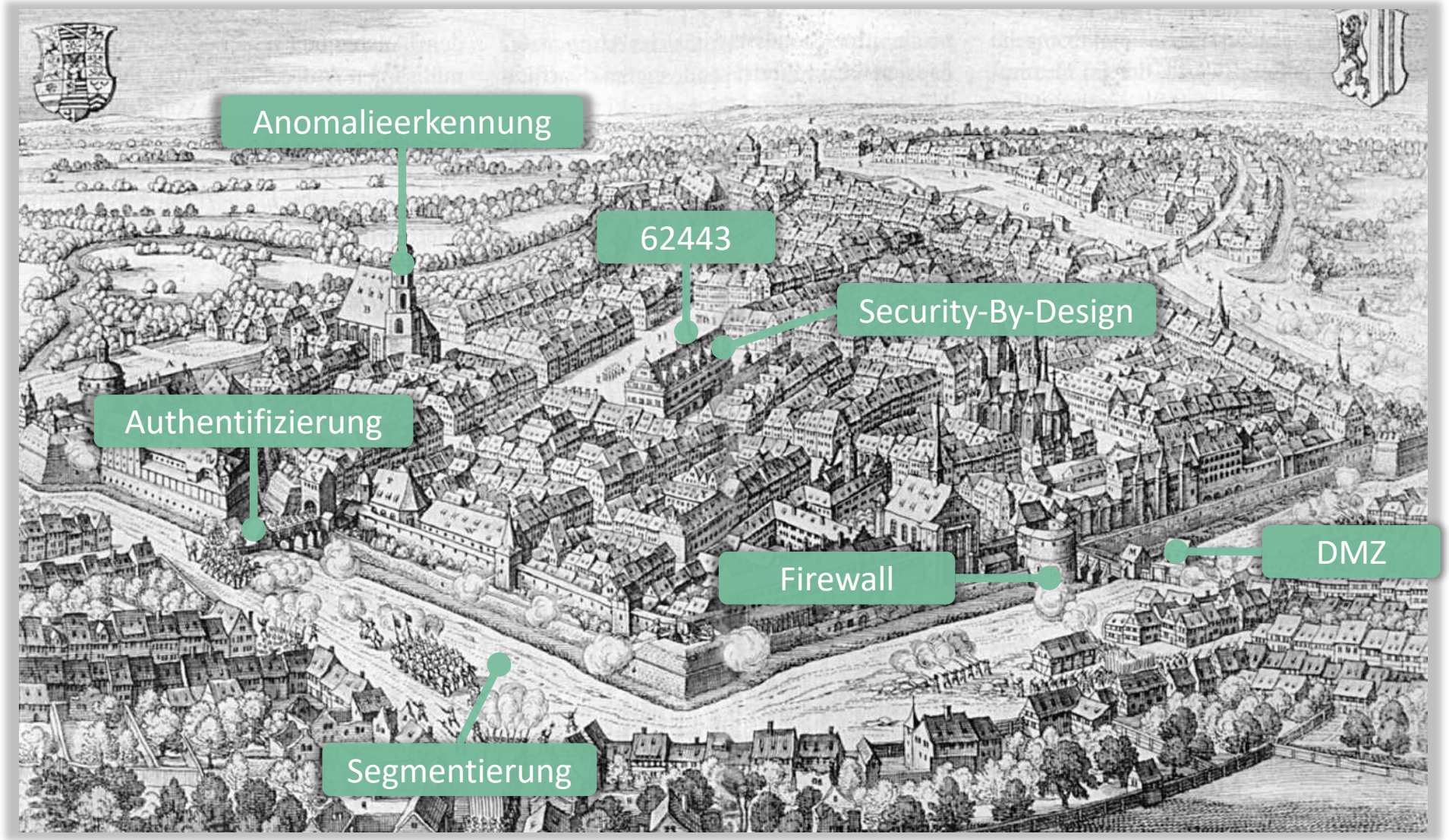
Produktivität & Anlagenverfügbarkeit



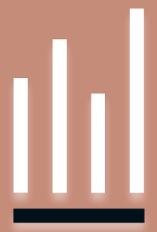
Sicherheit & Stabilität in der Industrie 4.0



Defence-In-Depth



Automatische Anomalieerkennung



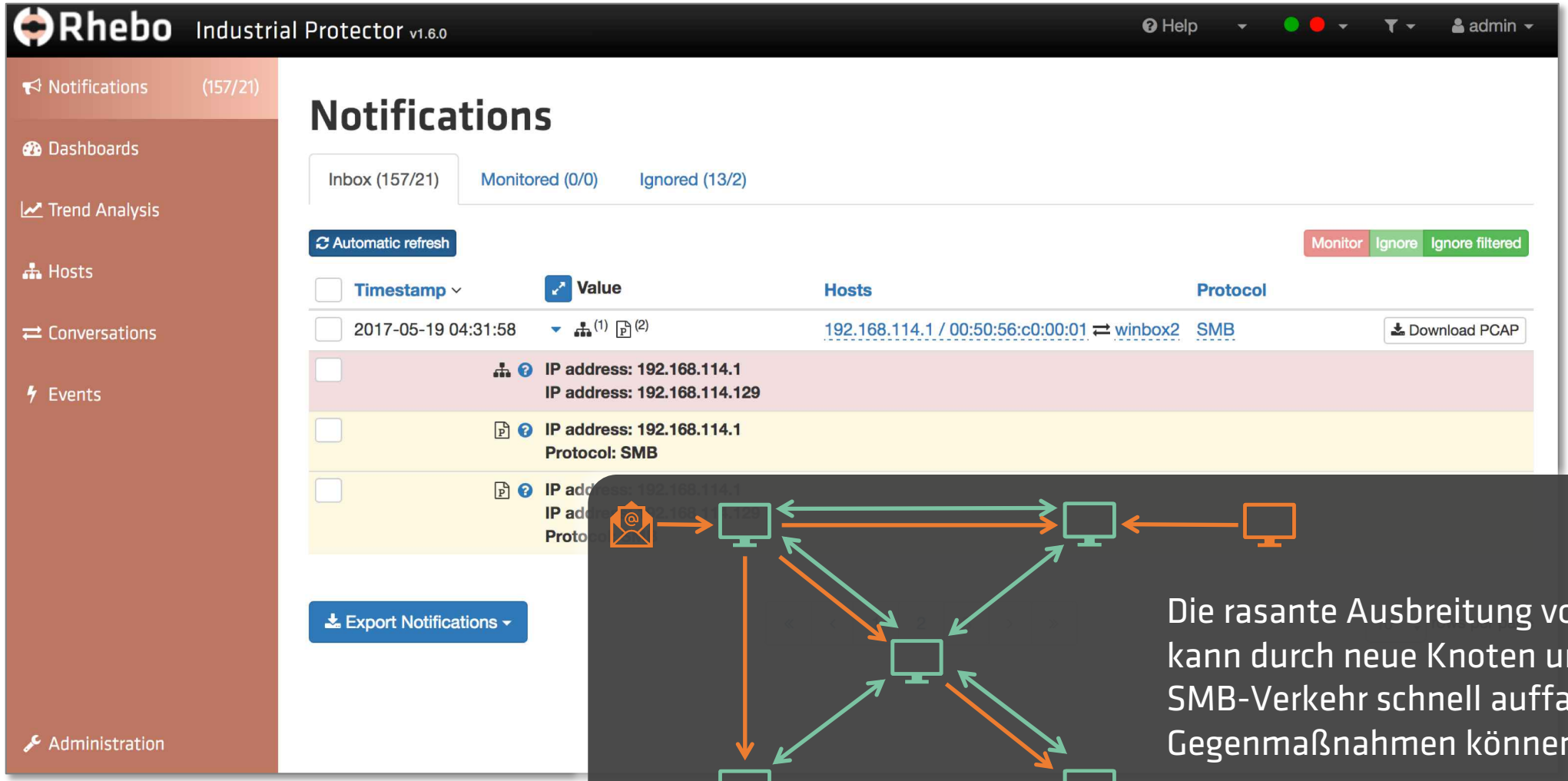
ANALYSIEREN

LERNEN

SCHÜTZEN

Praxisbeispiel: WannaCry

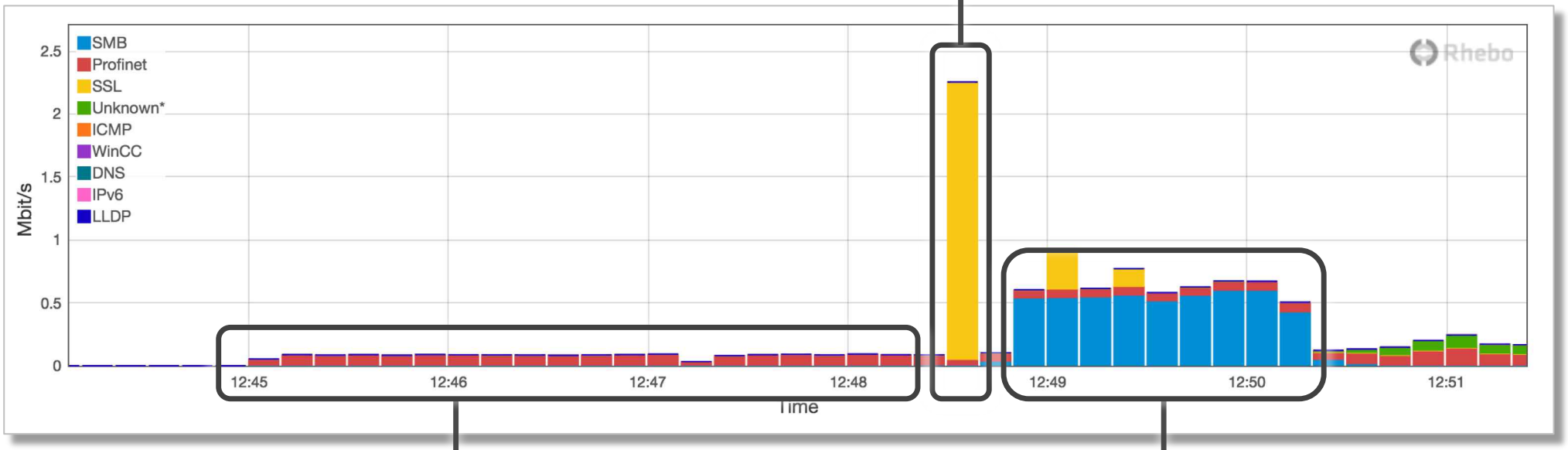
WannaCry – Funktionsweise



Die rasante Ausbreitung von WannaCry kann durch neue Knoten und anomalen SMB-Verkehr schnell auffallen und Gegenmaßnahmen können greifen.

WannaCry – Detektion & Gegenmaßnahmen

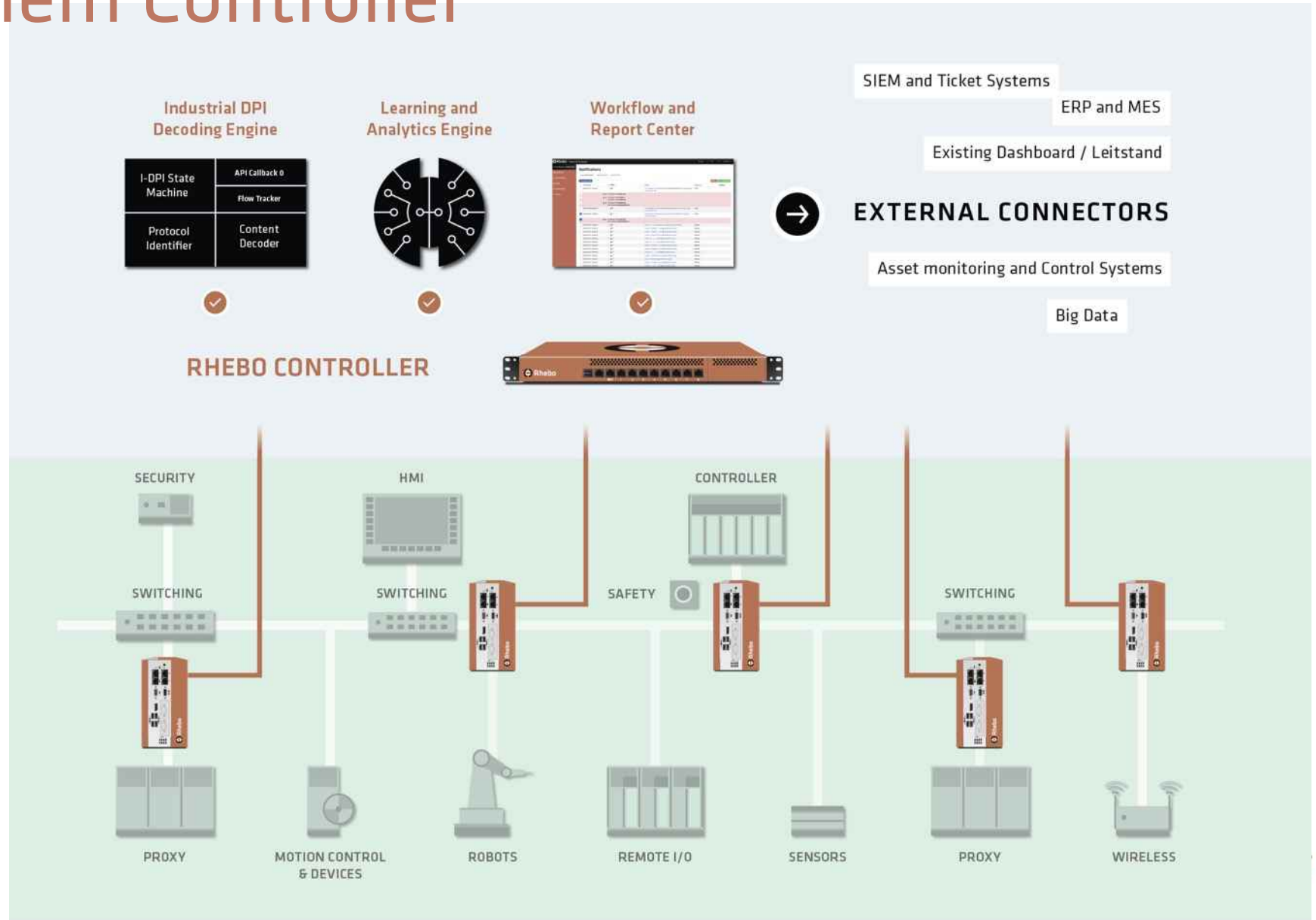
Schadcode-Download über SSL



normaler Profinetverkehr

anomal hoher SMB-Verkehr

Typische Installation mit verteilten Datensensoren und zentralem Controller

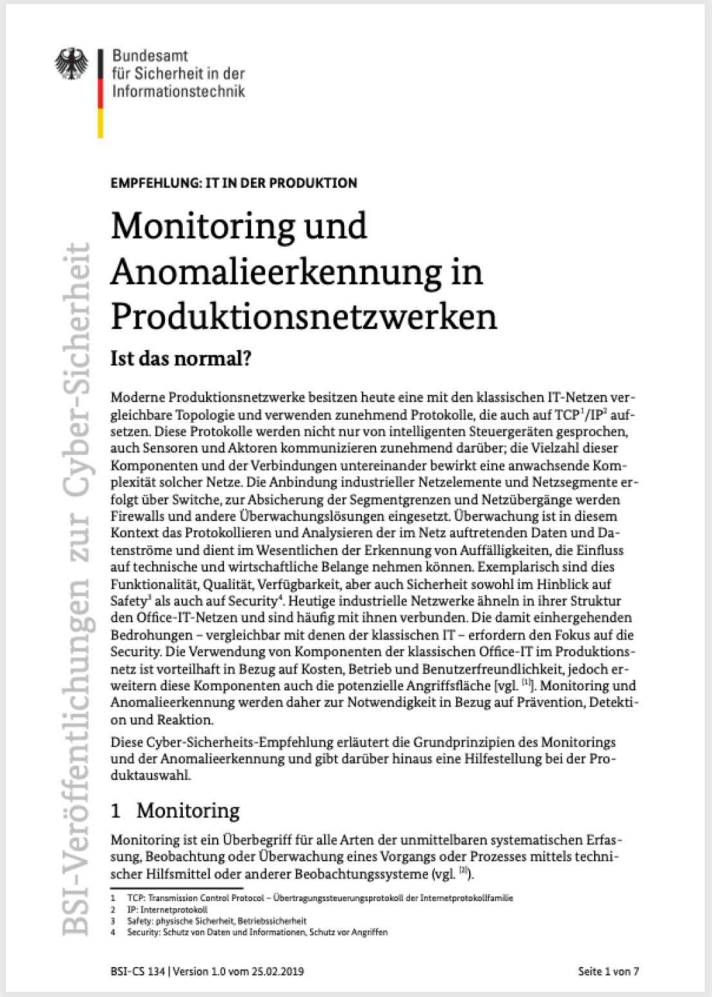


Rhebo

IEC 62443 Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component & Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		

Empfehlung von BSI & Allianz für Cyber-Sicherheit



Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IN DER PRODUKTION

Monitoring und Anomalieerkennung in Produktionsnetzwerken

Ist das normal?

Moderne Produktionsnetzwerke besitzen heute eine mit den klassischen IT-Netzen vergleichbare Topologie und verwenden zunehmend Protokolle, die auch auf TCP[1]/IP[2] aufsetzen. Diese Protokolle werden nicht nur von intelligenten Steuergeräten gesprochen, auch Sensoren und Aktoren kommunizieren zunehmend darüber; die Vielzahl dieser Komponenten und der Verbindungen untereinander bewirkt eine anwachsende Komplexität solcher Netze. Die Anbindung industrieller Netzelemente und Netzsegmente erfolgt über Switche, zur Absicherung der Segmentgrenzen und Netzübergänge werden Firewalls und andere Überwachungslösungen eingesetzt. Überwachung ist in diesem Kontext das Protokollieren und Analysieren der im Netz auftretenden Daten und Datenströme und dient im Wesentlichen der Erkennung von Auffälligkeiten, die Einfluss auf technische und wirtschaftliche Belange nehmen können. Exemplarisch sind dies Funktionalität, Qualität, Verfügbarkeit, aber auch Sicherheit sowohl im Hinblick auf Safety[3] als auch auf Security[4]. Heutige industrielle Netzwerke ähneln in ihrer Struktur den Office-IT-Netzen und sind häufig mit ihnen verbunden. Die damit einhergehenden Bedrohungen – vergleichbar mit denen der klassischen IT – erfordern den Fokus auf die Security. Die Verwendung von Komponenten der klassischen Office-IT im Produktionsnetz ist vorteilhaft in Bezug auf Kosten, Betrieb und Benutzerfreundlichkeit, jedoch erweitern diese Komponenten auch die potenzielle Angriffsfläche [vgl. [1]]. Monitoring und Anomalieerkennung werden daher zur Notwendigkeit in Bezug auf Prävention, Detektion und Reaktion.

Diese Cyber-Sicherheits-Empfehlung erläutert die Grundprinzipien des Monitorings und der Anomalieerkennung und gibt darüber hinaus eine Hilfestellung bei der Produktauswahl.

1 Monitoring

Monitoring ist ein Überbegriff für alle Arten der unmittelbaren systematischen Erfassung, Beobachtung oder Überwachung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme (vgl. [3]).

1 TCP: Transmission Control Protocol – Übertragungssteuerungsprotokoll der Internetprotokollfamilie
2 IP: Internetprotokoll
3 Safety: physische Sicherheit, Betriebssicherheit
4 Security: Schutz von Daten und Informationen, Schutz vor Angriffen

BSI-CS 134 | Version 1.0 vom 25.02.2019 Seite 1 von 7

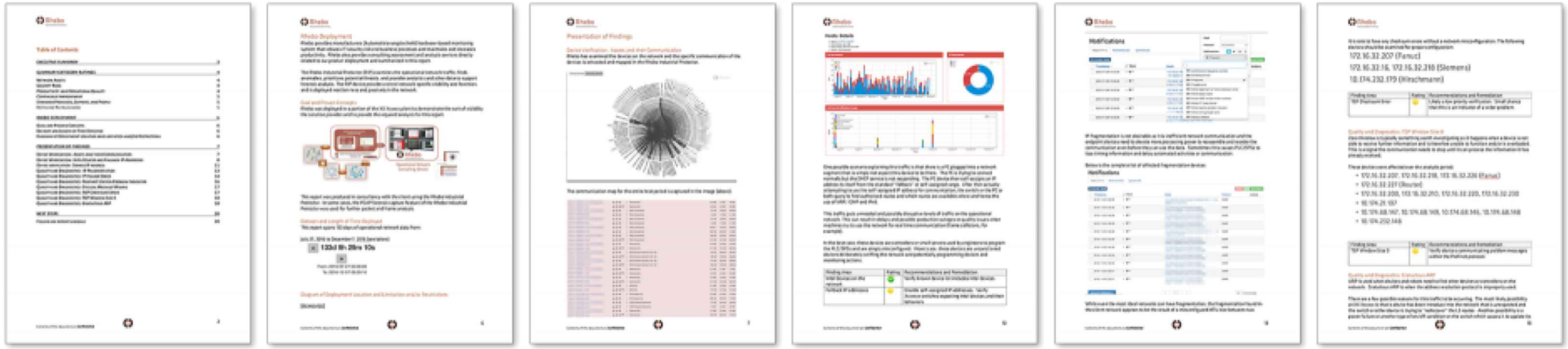
Cyber-Sicherheits-Empfehlung BSI-CS 134

- Grundprinzipien von Monitoring und Anomalieerkennung
- Anforderungen an Systeme

Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit

6 Wochen

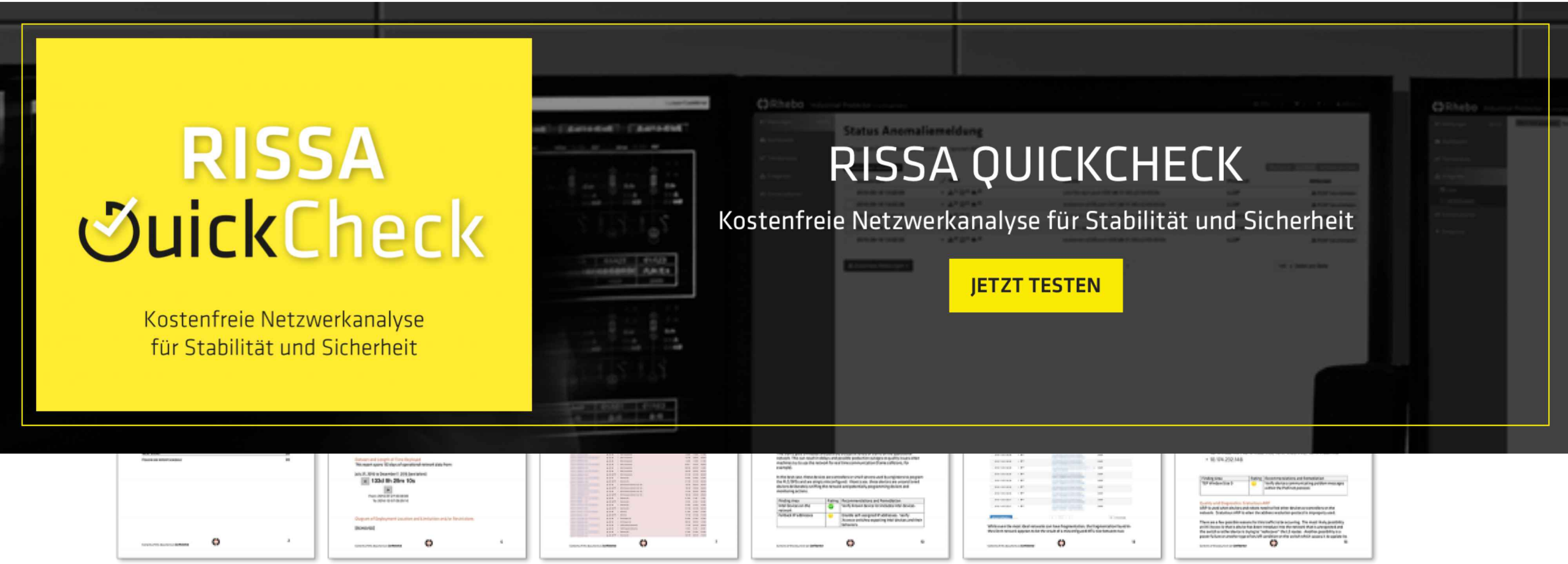
Analyse → Report → Workshop → Operativer Betrieb



Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit

RISSA QuickCheck

Kostenfreie Netzwerkanalyse
für Stabilität und Sicherheit



Rhebo

Industrial Network Continuity

Halle 6, B30