Reduce Time to Detect and Contain Cyber Incidents

Wolfgang Kiener
Business Development Manager

TÜVRheinland®
Precisely Right.

Referent

WOLFGANG KIENER

Business Development Manager
TÜV Rheinland - Cybersecurity
Wolfgang.Kiener@i-sec.tuv.com

TÜVRheinland®
Precisely Right.

Exciting times for threat detection

Offensive Zone

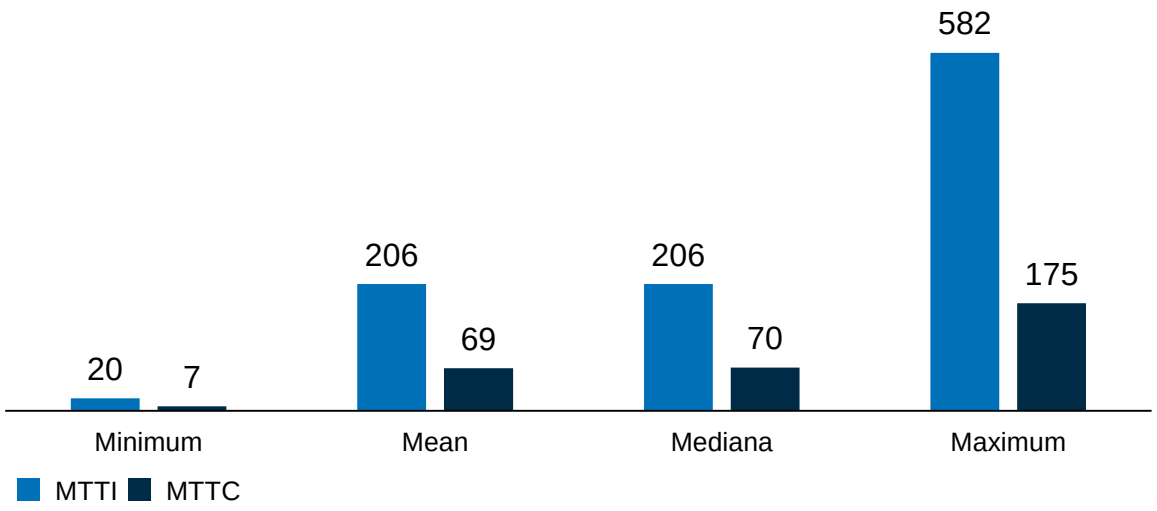
- Explosive growth of cyber crime
- Rapidly expanding attack surface
- Rise of ransomware and attack automation
- Diverse adversaries
- Increasing geopolitical threats

Defensive Zone

- Board level awareness and support
- New and innovative security products
- Emerging technologies
- Rapidly expanding attack surface
- Serious shortage of cyber security talent
- Poor global performance for cyber detection and response
  - >190 days MTTI
  - >66 days MTTC

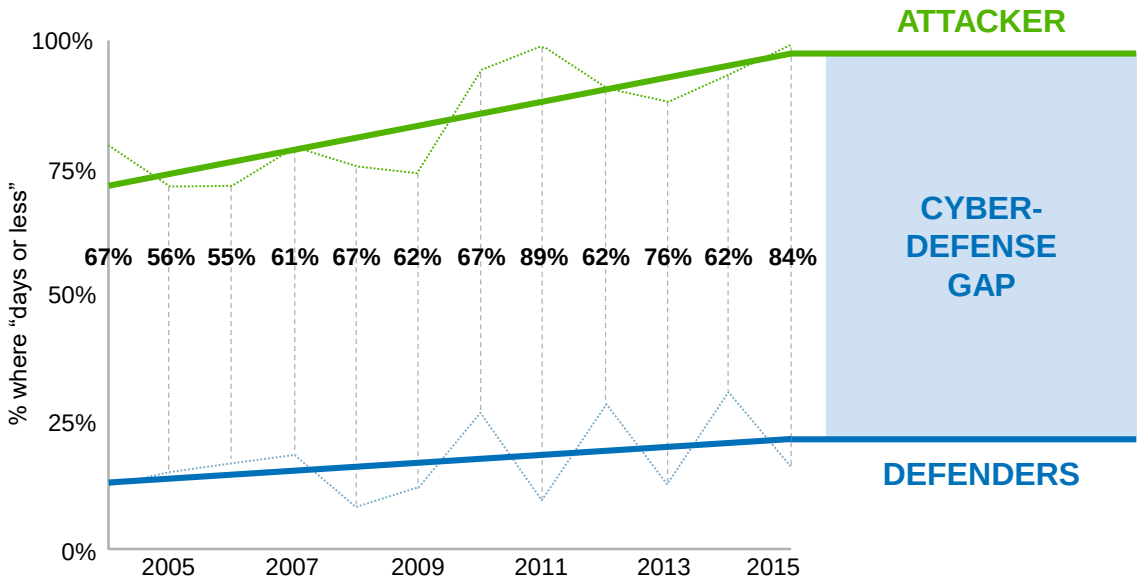
Status Quo: Threat Detection and Response

COST AND TIME FOR REMEDIATION IS HIGH AND RISING [2]



2016: On average, it took respondents 242 days to spot a breach caused by a malicious attacker, and further **99 days to contain** it.

DEFENDERS LOSING THE INNOVATION BATTLE[1]



Average total cost of a data breach	Average cost per stolen record	Cost increase per record
$4,31 Mio.	**$225**	**25%**

[1] Verizon DBIR 2016 | [2] Ponemon Institute 2015

TÜVRheinland®
Precisely Right.

Reducing time to detect and contain incidents

Opportunities for improvement

Big Data Analytics

Real-time security insights across the large and growing data of the modern enterprise

Emerging Technologies

Machine learning and behavior anomaly detection beyond traditional event correlation

Enhanced Use of Threat Intelligence

Integration of threat intelligence correlation across data sources

Visibility into IoT & OT

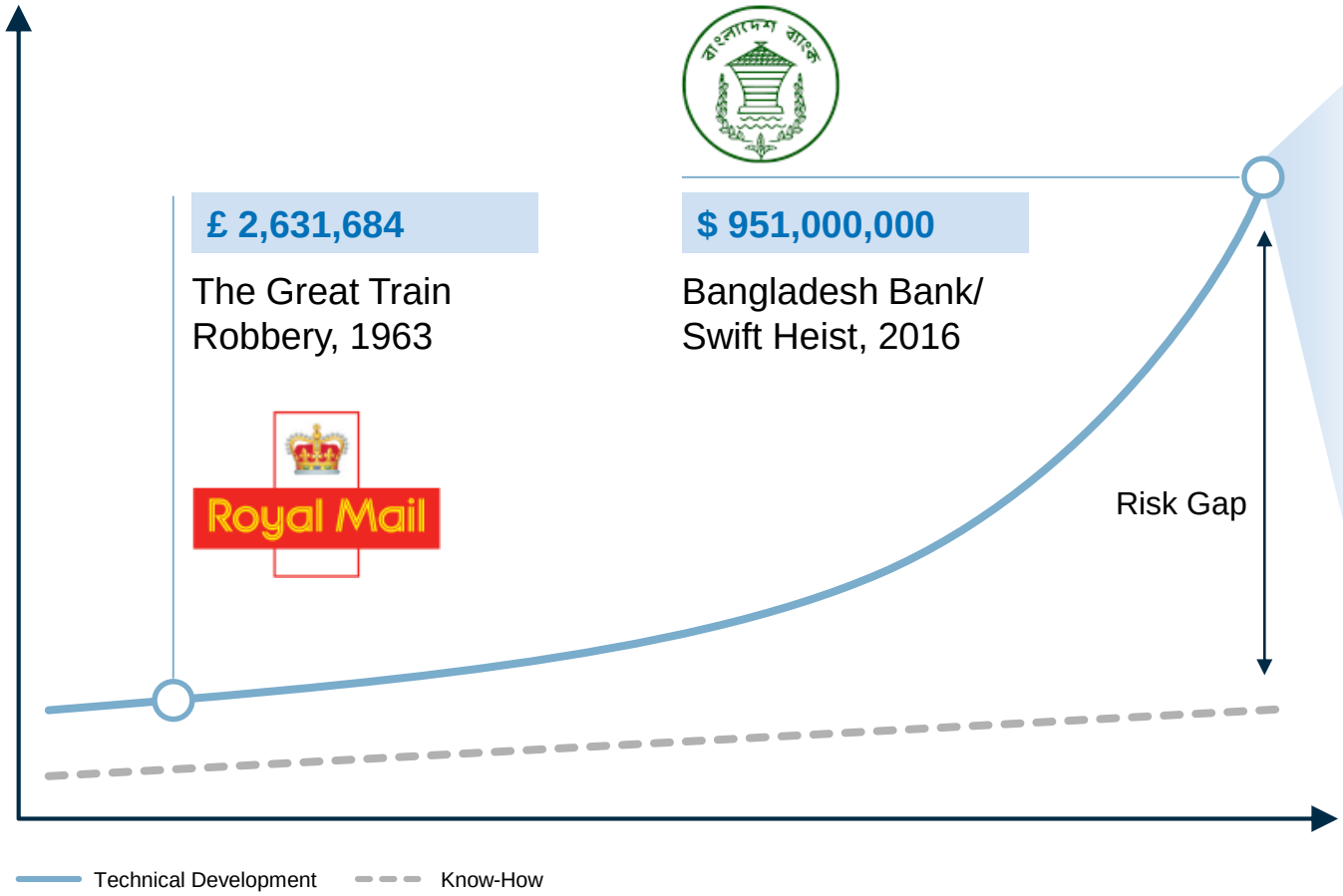
Behavior based analytics for Internet-of-Things and Operational Technology

Risk-Aligned Threat Detection

Focus detection on top risks, accelerate investigation and response, and report on capabilities and operational metrics

Digitalisation is Progressing. Unstoppable.

Risks develop exponential as well.



INDUSTRY 4.0

- Automation
- Scalability and Interconnectivity
- AI and Machine Learning
- Agility

CYBER RISK 4.0

- Attack automation
- AI and Machine Learning
- Attackers are agile
- Complexity increases attack surface
- Vulnerabilities are hardly to avoid

Cyber Risk = Business Risk

TÜVRheinland®
Precisely Right.

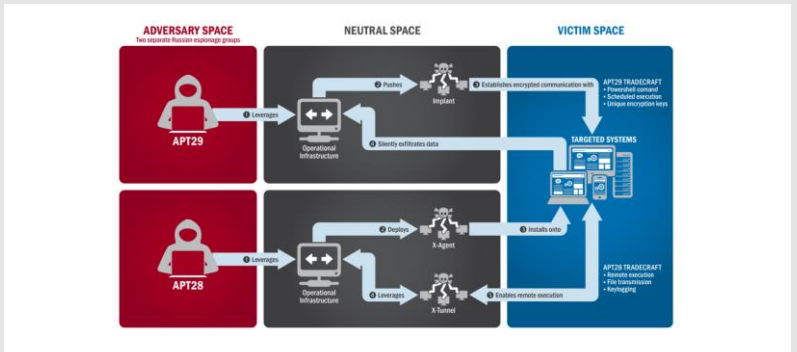
Risk-aligned threat detection approach

1 Identify top risks

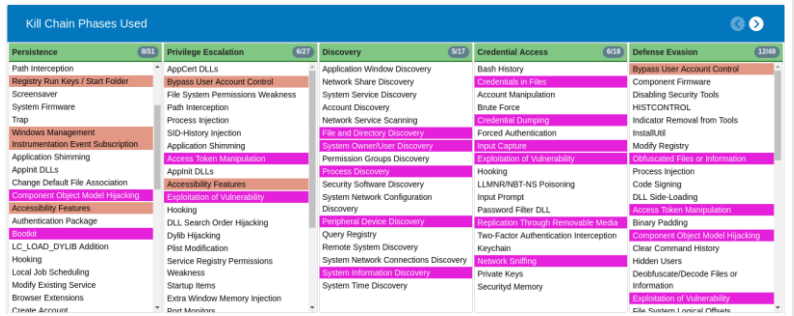
Top Cyber Risks

- Industry Risk Profiles
- Enterprise Risk Register

2 Define related attack scenarios



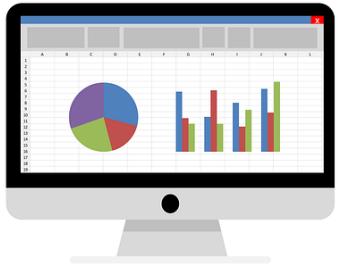
3 Map threat activities



4 Develop Analytics

5 Monitor, Investigate & Respond

6 Capture Metrics & Inform GRC



TÜVRheinland®
Precisely Right.

What are the most likely attack scenarios for the risk statement?

Example Risk Statement:

Critical data is encrypted in a ransomware attack, disrupting healthcare delivery operations, resulting in permanent injury or death, or significant financial loss

RANSOMWARE ATTACK SCENARIOS

- Phishing attack: malicious email attachment
- Phishing attack: malicious email link
- Vulnerability: internet facing system
- Vulnerability: laptop on untrusted network
- Compromised vendor/partner: software update
- Compromised vendor/partner: network trust relationship
- Malicious insider: intentional
- Etc.

TÜVRheinland®
Precisely Right.

Risk Prioritization

Many ways to prioritize risk – this example uses a scoring method and considers controls and residual risk

	Impact				Likelihood				Inherent Risk		Controls Reduction		Residual Risk
Risk Statement	Confidentiality	1	2.5	×	Treat Means	4	3.0	=	7.5	−	4.7	=	2.8
	Integrity	4			Treat Motive	1							
	Availability	1			Threat Opportunity	4							
	Safety	4											
Risk Statement	Confidentiality	4	1.8	×	Treat Means	4	4.0	=	7.2	−	5.1	=	2.1
	Integrity	1			Treat Motive	4							
	Availability	1			Threat Opportunity	4							
	Safety	1											

TÜVRheinland®
Precisely Right.

Define threat activities by attack phase for the selected attack scenario

Models available to assist

Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- **Installation**
- **Command & Control**
- **Actions on Objectives**

CIS Community Attack Model

- Initial Recon
- Acquire/Develop Tools
- Delivery
- Initial Compromise
- **Misuse/Escalate Privileges**
- **Internal Recon**
- **Lateral Movement**
- **Establish Persistence**
- **Execute Mission Objectives**

MITRE ATT&CK

- **Persistence**
- **Privilege Escalation**
- **Defense Evasion**
- **Credential Access**
- **Discovery**
- **Lateral Movement**
- **Execution**
- **Collection**
- **Exfiltration**
- **Command & Control**

Cyber Threat Framework

- Preparation
- Engagement
- **Presence**
- **Effect/Consequence**

Unfetter – NSA tool that utilizes ATT&CK

UNFETTER

Assessments | Intrusion Set Dashboard | Threat Dashboard | Analytic Hub | Link Explorer | View API | STIX

Search

Results (2) Intrusion Sets — Clear Fliters

- [ ] APT1
- [ ] APT16
- [ ] APT18
- [x] APT29
- [ ] APT30
- [ ] APT34
- [ ] BRONZE BUTLER
- [ ] Charming Kitten
- [ ] CopyKittens
- [ ] Deep Panda
- [ ] Dragonfly
- [ ] Equation
- [ ] FIN5
- [ ] FIN7
- [ ] Gamaredon Group
- [ ] Ke3chang
- [ ] Lotus Blossom
- [ ] Magic Hound
- [ ] Molerats
- [ ] Naikon
- [ ] OilRig
- [ ] APT12
- [ ] APT17
- [x] APT28
- [ ] APT3
- [ ] APT32
- [ ] Axiom
- [ ] Carbanak
- [ ] Cleaver
- [ ] Darkhotel
- [ ] DragonOK
- [ ] Dust Storm
- [ ] FIN10
- [ ] FIN6
- [ ] GCMAN
- [ ] Group5
- [ ] Lazarus Group
- [ ] MONSOON
- [ ] Moafee
- [ ] NEODYMIUM
- [ ] Night Dragon
- [ ] PROMETHIUM

Intrusion Sets

Attack Patterns Used | Critical Security Controls (CSC)

Attack Patterns Used Per Intrusion Set

APT29 13 / 188

APT28 31 / 188

Kill Chain Phases Used

Persistence 8/51	Privilege Escalation 6/27	Discovery 5/17	Credential Access 6/18	Defense Evasion 12/49
.bash_profile and .bashrc	AppCert DLLs	Application Window Discovery	Bash History	Bypass User Account Control
AppCert DLLs	Bypass User Account Control	Network Share Discovery	Credentials in Files	Component Firmware
Component Firmware	File System Permissions Weakness	System Service Discovery	Account Manipulation	Disabling Security Tools
External Remote Services	Path Interception	Account Discovery	Brute Force	HISTCONTROL
File System Permissions Weakness	Process Injection	Network Service Scanning	Credential Dumping	Indicator Removal from Tools
Hypervisor	SID-History Injection	File and Directory Discovery	Forced Authentication	InstallUtil
LSASS Driver	Application Shimming	System Owner/User Discovery	Input Capture	Modify Registry
Login Item	Access Token Manipulation	Permission Groups Discovery	Exploitation of Vulnerability	Obfuscated Files or Information
Path Interception	AppInit DLLs	Process Discovery	Hooking	Process Injection
Registry Run Keys / Start Folder	Accessibility Features	Security Software Discovery	LLMNR/NBT-NS Poisoning	Code Signing
Screensaver	Exploitation of Vulnerability	System Network Configuration Discovery	Input Prompt	DLL Side-Loading
System Firmware	Hooking	Peripheral Device Discovery	Password Filter DLL	Access Token Manipulation
Trap	DLL Search Order Hijacking	Query Registry	Replication Through Removable Media	Binary Padding
Windows Management Instrumentation Event Subscription	Dylib Hijacking	Remote System Discovery	Two-Factor Authentication Interception	Component Object Model Hijacking
Application Shimming	Plist Modification	System Network Connections Discovery	Keychain	Clear Command History
AppInit DLLs	Service Registry Permissions Weakness	System Information Discovery	Network Sniffing	Hidden Users
Change Default File Association	Startup Items	System Time Discovery	Private Keys	Deobfuscate/Decode Files or Information
			Securityd Memory	

Made by NSA Information Assurance — Partners | View API

TÜVRheinland® Precisely Right.

Process to map and review threat activities

1. Document key activities by attack phase for attack scenario
2. Document all assets involved in attack scenario
3. Review and document existing detection capabilities for each activity
4. Identify and prioritize opportunities to improve detection

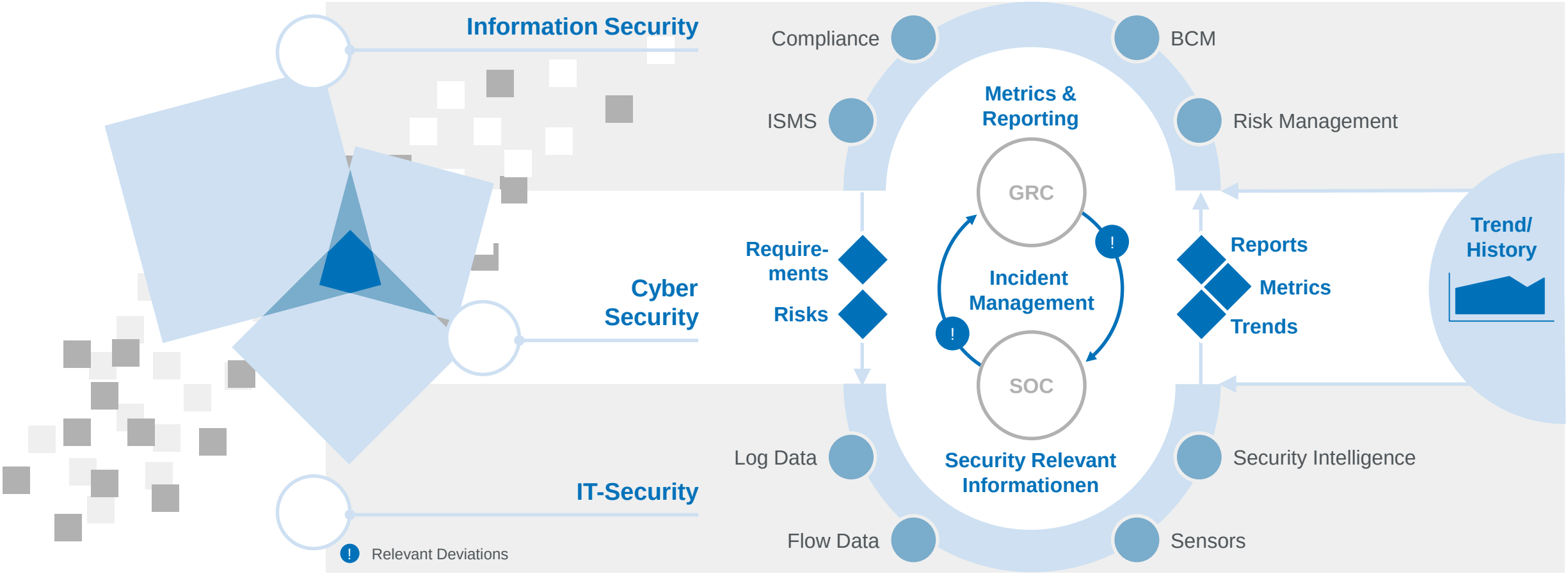
Develop and documenting threat analytics

- Threat activity
- Analytic name
- Analytic description
- Key risk indicator
- Data sources
- Required data
- Analytics (platform specific)
- Threat detection guidance
- Notes
- Map to risk statements
- Author
- Date

EXAMPLE: THREAT ACTIVITY – LOGIN WITH COMPROMISED CREDENTIALS (EXPLOIT PHASE)

Threat Activity	Analytic Name	Analytic Description	Key Risk Indicator	Data Sources	Required Data
Azure AD login	Login from unusual location	GeoIP lookup for successful login from unusual location	Login outside of geographic area of business that does not correspond with authorized work travel	Azure Active Directory	1. Login success 2. Source IP 3. GeoIP 4. Authorized travel
Azure AD login	Concurrent logins from separate locations	GeoIP lookup for successful login concurrently from separate locations	Concurrent logins from geographically separate areas	Azure Active Directory	1. Login success 2. Source IP 3. GeoIP
Azure AD login	Logins from separate locations within unreasonable timeframe	GeoIP lookup for successful logins from separate locations where travel time is unreasonable between logins	Logins from separate locations within unreasonable travel time	Azure Active Directory	1. Login success 2. Source IP 3. GeoIP
Azure AD login	Login from anonymous IP address	Login IP correlated against threat intelligence for known anonymous proxy IP address	Login from an IP address that has been identified as an anonymous proxy IP address	Azure Active Directory Threat Intel	1. Login success (AD) 2. Source IP (AD) 3. Anonymous IPs (TI)
Azure AD login	Login from known malicious IP address	Login IP correlated against threat intelligence for known malicious IP address	Login from an IP address that has been identified as a known malicious IP address	Azure Active Directory Threat Intel	1. Login success (AD) 2. Source IP (AD) 3. Malicious IPs (TI)

Risk-Aligned Threat Detection



TÜVRheinland®
Precisely Right.

Conclusion

Benefits of risk-aligned threat detection

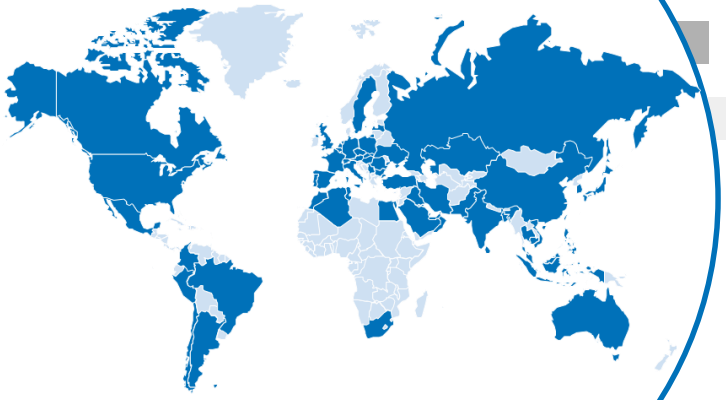
- Better focus on threat activity that matters most to the organization
- More context and clarity about detected threat events
- Opportunities to automate investigation and response activities
- Improved risk management program
- Reduced time to detect and contain incidents

TÜV Rheinland. Who are we?

TÜVRheinland®

Precisely Right.

- $2.3 Billion
- Privately Held
- 144 Years Old
- 500 Locations
- 69 Countries
- 19,320 people



Protecting society since 1872

Industry 1.0
Mechanical Production

Industry 2.0
Mass Production & Electricity

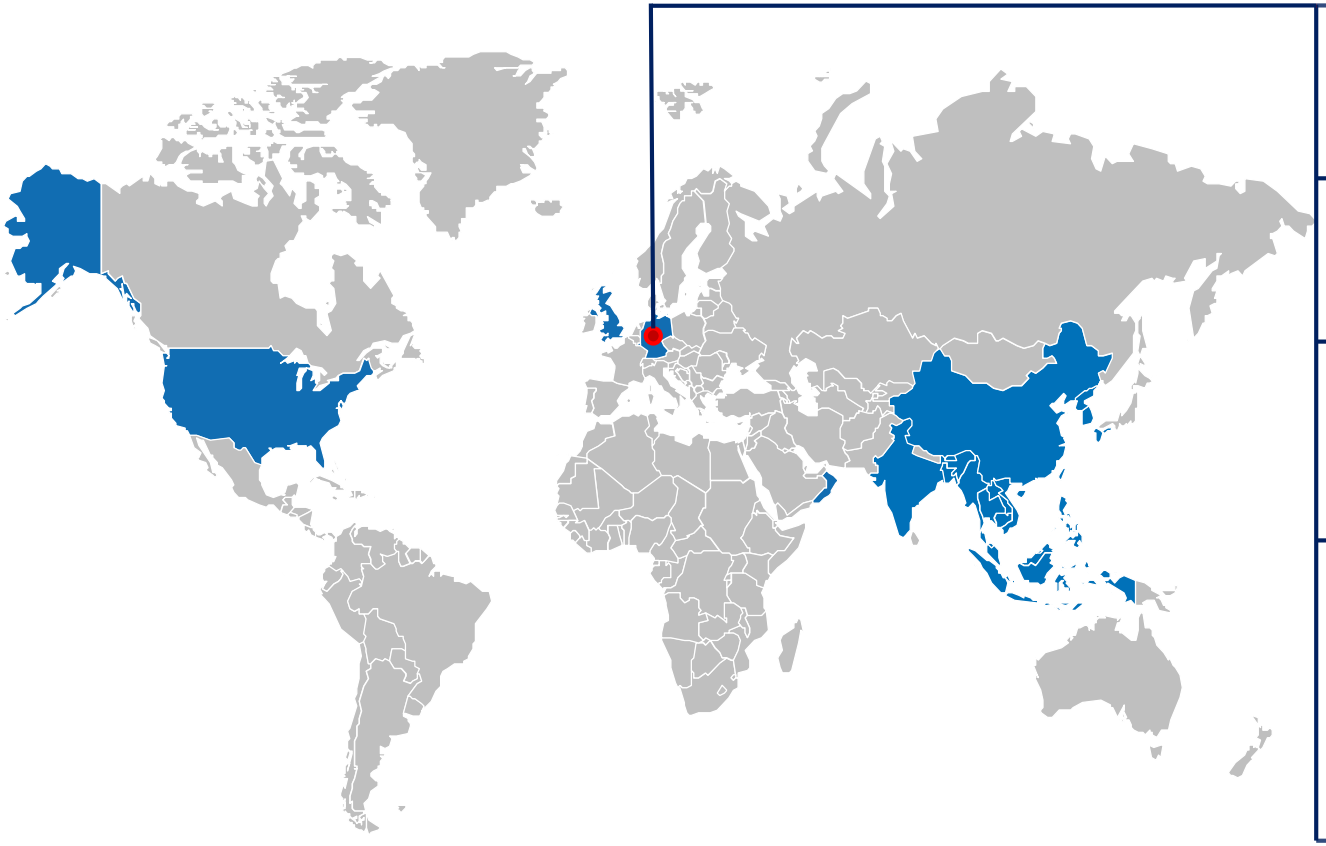
Industry 3.0
Electronic & IT Systems

Industry 4.0
Cyber-physical Systems, Social, Mobile, Analytics, Cloud

! The digital transformation will be defined by the use of “cyber-physical” systems.

TÜVRheinland®
Precisely Right.

TÜV Rheinland ICT & Business Solutions. Cybersecurity.



HQ´s
Cologne / Boston / London

68 Mio. € Revenue 2016

400 Security Experts

Core Industries
Finance, Automotive
Chemie & Pharma, Energy, Telecommunication

Regions
Germany, USA, UK, Golf Region, APAC as Growth Case

TÜVRheinland®
Precisely Right.

Thank you.

Wolfgang Kiener

Business Development Manager – Cybersecurity

https://tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Visit our TÜV Rheinland Experts at CEBIT 2018!

Hall 12, Japan Pavilion

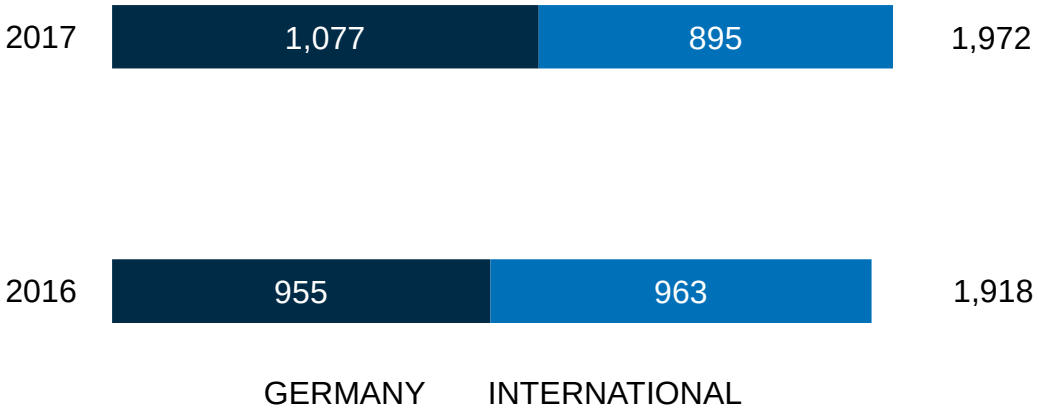
Stand D123, (11)

TÜVRheinland®
Precisely Right.

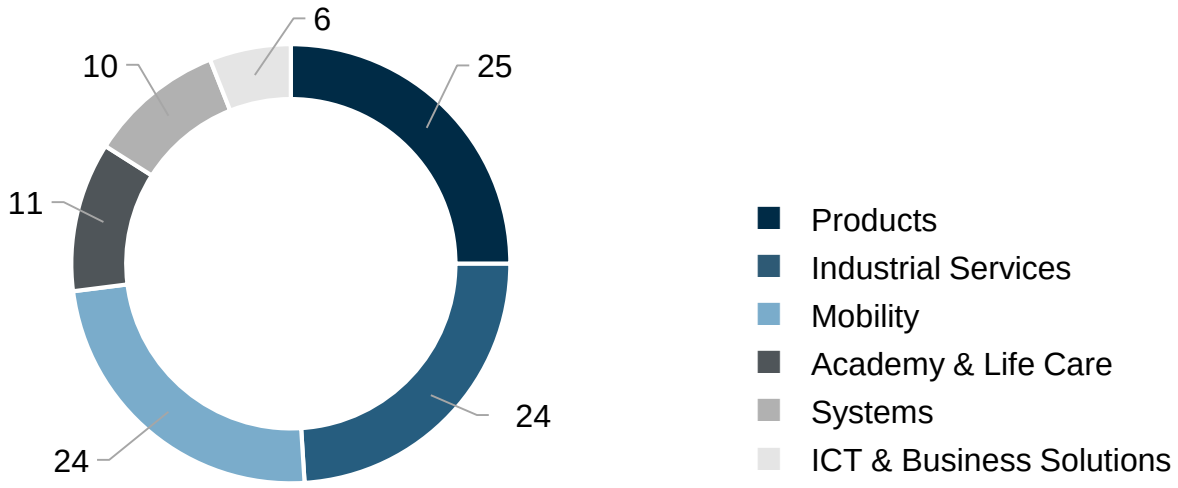
Figures 2017

1,972 Revenue in € millions

Revenue Germany/International (in € millions)



Revenue per Business Stream (in %)



Consolidated data (according to IFRS)

Statistics in 2017: consolidated data

TÜVRheinland®
Precisely Right.

ICT & Business Solutions

From strategic consulting, design, and process optimization to implementation, operation, and certification of systems

TÜVRheinland®
Precisely Right.

ICT & Business Solutions

Key facts

139 Sales in € m.

6% of total sales

600 Auditors/specialists

BUSINESS FIELDS

- IT-Services & Cyber Security
- Telco Solutions & Consulting

FOCUS INDUSTRIES

- In-depth experience in key industries
  - aerospace and aviation
  - energy
  - financial services
  - health care
  - manufacturing
  - mobility, logistics, automotive
  - telecommunications
  - trade

GOOD TO KNOW

- As of 2014, we are the leading independent provider of IT & cyber security in the German market and are a relevant key player worldwide.
- We advise network operators to plan, build and maintain their telecommunication infrastructure with high-quality, in a technology-driven and cost-effective way.

Statistics in 2017: unconsolidated data

TÜV Rheinland i-sec. Information and IT security.

- Leading independent service provider for information security in Germany
- Consulting and solution expertise in integrated information security – from the steering level to the data center, including operational support services
- Excellent technological expertise, comprehensive industry know-how, partnerships with market leaders
- Internationally, in the network with our sister companies OpenSky and 2MC, we number among the most important independent suppliers
- ISO 27001 and ISO 9001 certified

TÜVRheinland®
Precisely Right.

TÜV Rheinland i-sec GmbH. Facts and Figures.

Locations in Germany

- Cologne (HQ)
- Munich
- Gelnhausen
- Saarbrücken
- Hanover
- Hamburg

Technical Specialist Team

- 15 × Sales
- 20 × Security Engineering
- 60 × Management Consulting
- 45 × Professional Service and Operations

Industries and headquarters of our customers

- Finances
- Automotive
- Energy sector
- Chemistry/ pharmaceuticals
- Telecommunications
- Intl. conglomerates
- Transport/logistics
- Public service
- Trade

! Project work on 25,000 days in 2016

TÜVRheinland®
Precisely Right.

Digital Enterprise. Protected.

A complete, global services portfolio designed to protect the digital enterprise.

Portfolio Categories:

Service Types:

Portfolio Categories			Consulting Services	Testing Services	Managed Services
Mastering Risk & Compliance	Governance & Strategy	Business Continuity Management			
	Risk & Compliance Management	Data Privacy			
	Information Security Management Systems				
Advanced Cyber Defenses	Identity & Access Management	IoT Security			
	Network Security	OT Security			
	Application Security	Security Analytics & Detection			
	Endpoint Security	Incident Response			
	Data Protection				
Secure Cloud Adoption	Cloud Security				
	Enterprise Cloud Adoption				
	Hybrid Infrastructure				

TÜVRheinland®
Precisely Right.