

MetricStream

GRC

SUMMIT 2017

November 6 - 7, 2017

L O N D O N

Present and upcoming security threats

Thomas Tschersich

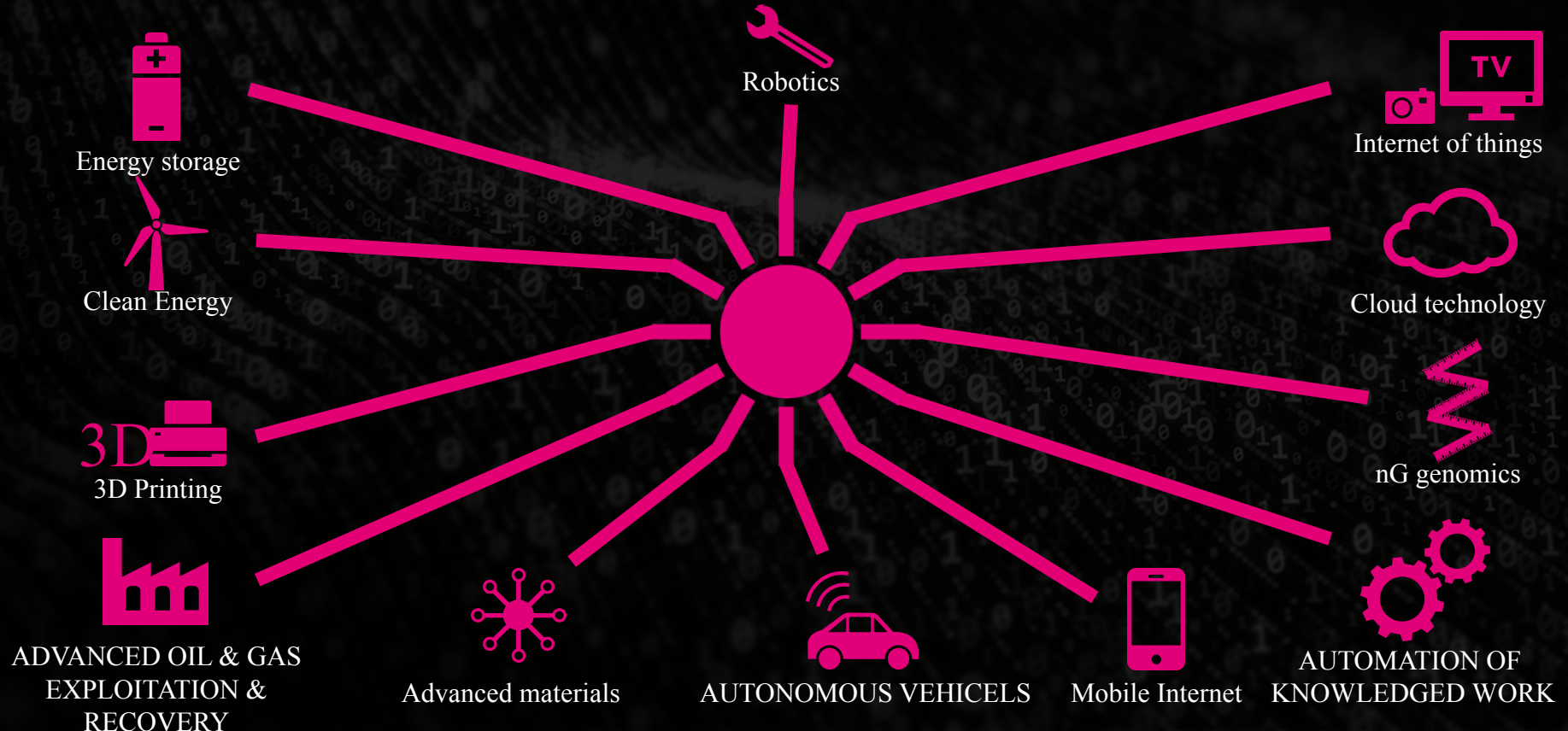
Presenter Details



Thomas Tschersich
SVP of Internal Security & Cyber Defense
Deutsche Telekom Group



The 12 most important innovation fields: without cyber security no innovation



It is not arguable whether digitalization is taking place, it's just a question of when, where & How?

understanding of
customers



Digital Processes /
eCompany



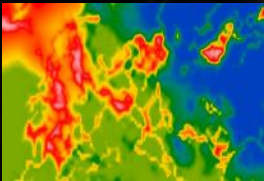
Digital
identity



SimpliciTy delights



Anticipate customer
needs



consistent SERVICE
experience



secure Network



Security and privacy



ALL IS
MOBILE

ALL IS
CLOUD

ALL IS
IP

ALL IS
SECURE



... HOW DOES
REALITY
LOOK LIKE?

Cyber security development from the past into the future

PREVIOUS

- To come to fame
- Try & error
- ...

TODAY

- Cyber crime
- Cyber intelligence
- Cyber sabotage

UPCOMING

- Cyber war
- Controlling connected cities
- ...

CYBER Defence FACTS and figures

886 system vulnerabilities have been detected in July within the corporate network

4.236.296 attacks against telekom.de from the internet

131.508 blocked internal requests for malicious URLs

24.909 viruses have been detected on office workplaces

24 malicious websites have been identified by sandboxing and thereupon blocked companywide at the proxies

651 vulnerabilities were reachable from the internet

in July **158** issues have been reported to CERT

552 critical attacks against mobile platforms have been detected on office devices

32,8 Bn. botnet packets have been detected at the fixed and mobile network's backbone

CYBER
ATTACKS ARE
REAL
AND
INCREASING

53%

Of all German companies are victims of cyber attacks

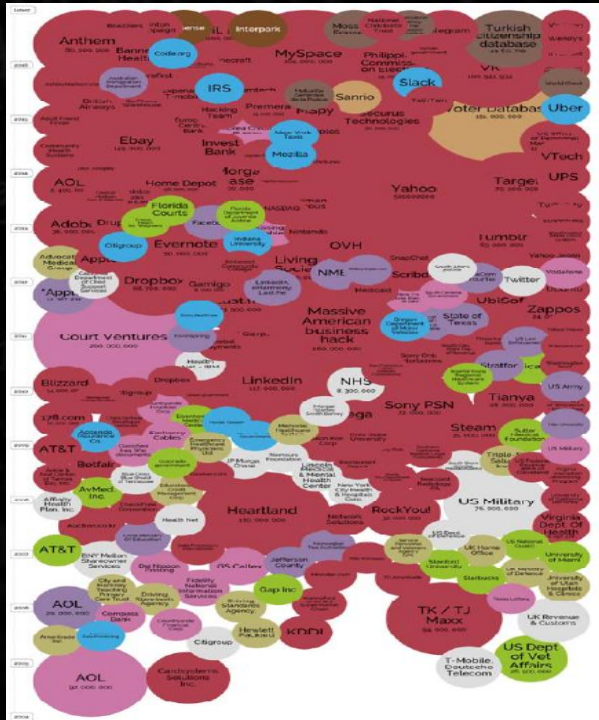
65%

Of the affected companies are medium-sized enterprises

ALMOST
55 BN. €

Damage of the German economy PER YEAR

Examples of worldwide successful cyber attacks: each company is a possible victim



<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

	Details on more than 3 billion user accounts stolen
	Hackers say they have information on file for 6 million users
	Iranian hackers have compromised more than a dozen accounts and identified the phone numbers of 15 million Iranian users
	Indian hacker group leaks data of 1.7 million Snapchat users
	300 million € negative financial impact caused by WannaCry
	An attack on Dyn-server with millions of IP addresses was responsible that online services along the USA west coast were not up any more

Cyber security development

www.sicherheitstacho.eu



The T-Sec Radar shows cyber attacks happening worldwide on our and our partners honeypot infrastructure.

437

attacks during the last minute

56256 attacks in 1 h

1559549 attacks in 24 h



LIVE TICKER				
DATE	SOURCE	TARGET	ATTACK TYPE	PARAMETER
11:37:44	CN	PIR	Network(Dionaea)	
11:37:43	NL	Network(honeytrap)	Attack on port 5900	
11:37:42	NL	Network(honeytrap)	Attack on port 5900	
11:37:41	RU	JP	Webpage	//inc/inc/textpattern/suse/servelet/.rD_vtl.cnf/10p/3ee/examples/software

TOP ATTACKER 2017-10	
COUNTRY	ATTACKS
RU	10988934
DE	2851093
US	2738821
PIR	2092204
NL	1956614



Current situation




- More than 180 sensors (Honeypots) in action
- DETAILED LOGS OF ATTACKS AND ASSAULTING VECTORS
- GEOGRAPHICAL ALLOCATION OF ATTACK SOURCES
- Attacks per day

Trend

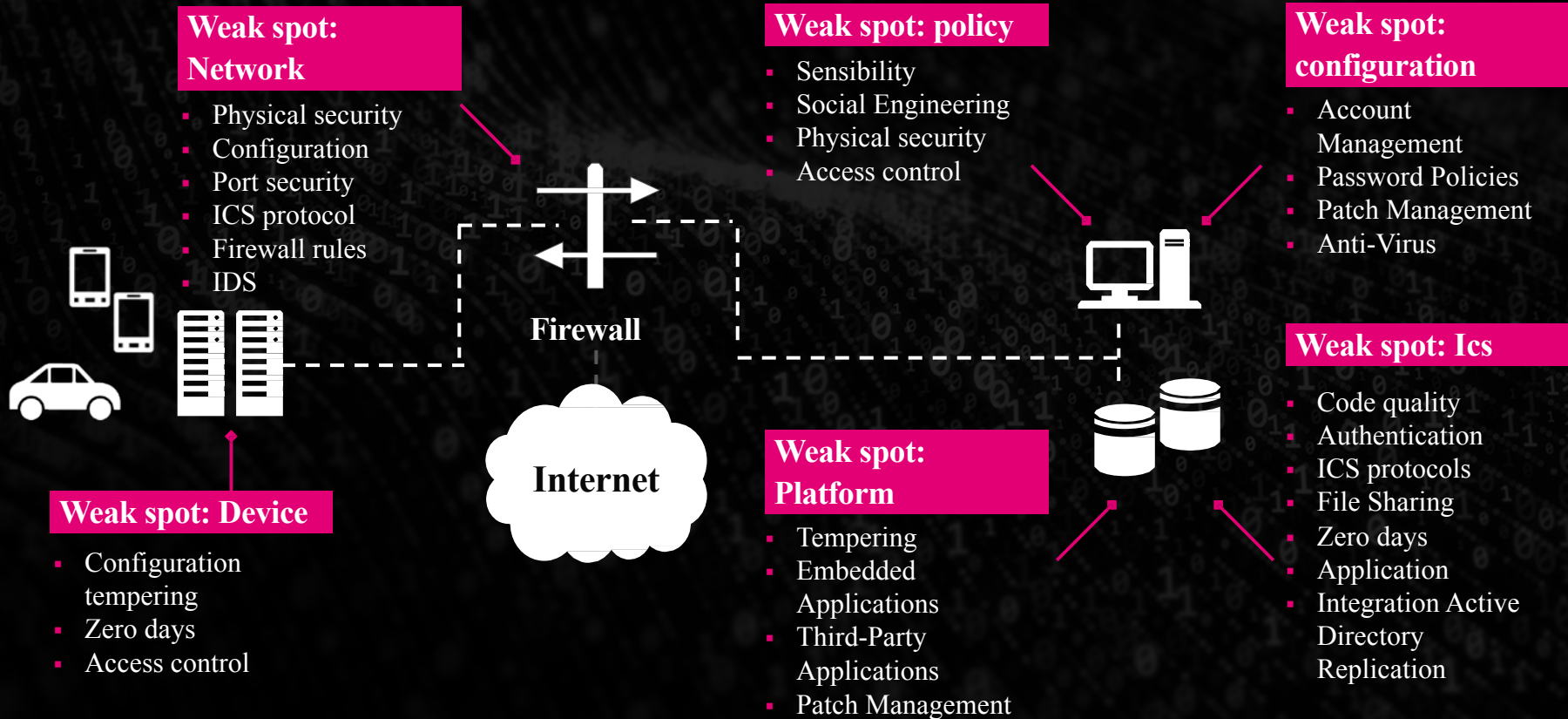
SEPTEMBER 2017:
APPROX. 200 MILL.

September 2016:
APPROX. 150 Mill.

various types of attackers, but same methods with divergent objectives

	Classical hackers	Organised Crime	Hacktivists	Intelligence services
Motivation 	Fame and honor Show what you can do Fun and games	Fraud Blackmail Money laundering	Expressing political opinions	Espionage Sabotage
Resources 	Usually individuals	Well-organized groups High division of labor Worldwide distribution Vast funding available	Well-organized groups High division of labor Worldwide distribution	State-controlled Virtually unlimited funding available
Examples 	Defacing websites Reporting vulnerabilities in websites to the press ...	Phishing mails DDoS against online shops/online betting SPAM ...	DDoS against banks that blocked Wikileaks accounts Anonymous attacks on businesses ...	Stuxnet (Iranian nuclear program) Red October (governments in the Eastern Block) ...

Different assaulting vectors



Attacks on smartphones is the new trend

Changing the attack focus

- Until 2008/2009 concentration of cyber attacks on PC
- Since 2009 increasing attacks on smartphones
 - Concentration of finance and access data
 - Eavesdropping of phone calls
 - Convert camera
 - (new) Dialer
 - Access to contacts
 - Access to pictures
 -

Examples of new targets

- July/August 2015: Stagefright
 - 950 million Android smartphones affected
 - Attack via MMS
- September 2017: BlueBorn
 - Billions of smartphones of all fabricators affected
 - Attack via Bluetooth protocol



How effective is the update policy of all smartphone fabricants?

Transport sector gets into attackers' focus

automotive IT is no longer only a subject of researchers



Automotive Multimedia-Terminal

Operating system Windows CE / Linux

Connectivity inside car

- CANBus net
- Ethernet
- High speed media bus

Wireless access

- Bluetooth
- Wi-Fi
- Mobile communication
- GPS
- IR remote
- XM satellite

Physical access

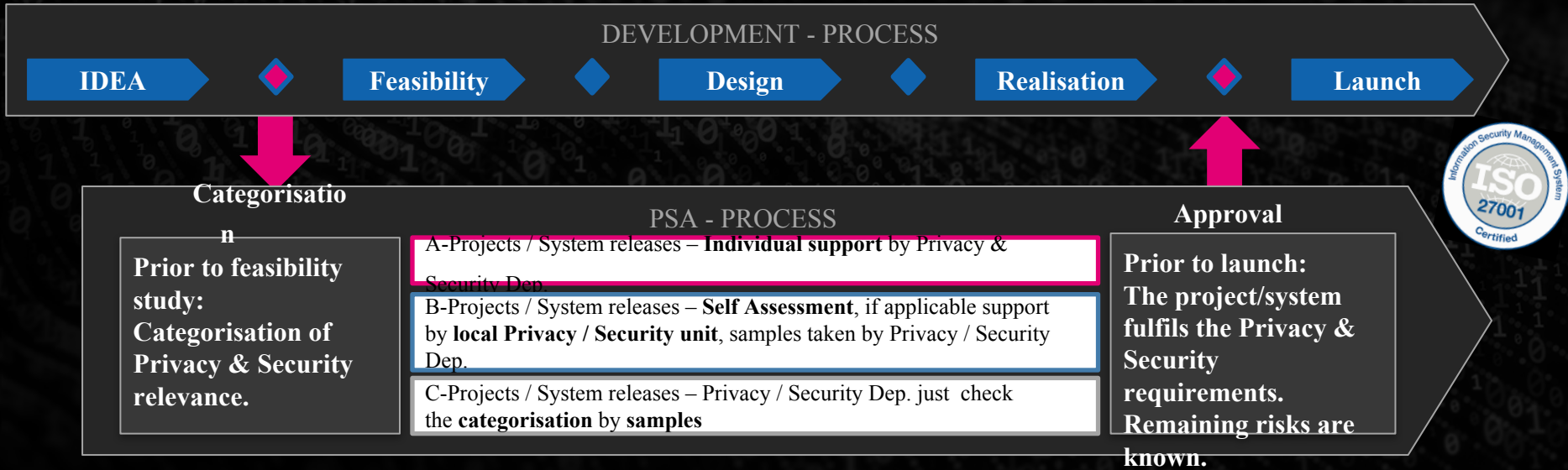
- USB-Port
- AUX port
- CD-ROM
- DVD
- Touchscreen

... WHAT SHALL
WE DO?

... IMPLEMENT
SECURITY EXPLICITLY
IN DEVELOPMENT
PROCESSES!

Privacy and Security by Design

The Privacy and Security Assessment (PSA process) is the core element in safeguarding security and data privacy at Deutsche Telekom. Each year we manage more than 4.000 projects through the PSA process.



Developing cyber security: how does psa WORK in the agile world?

- Agile model
 - Ad hoc communication
 - Simplification
 - Security Champion
 - Multistage support intensity
- Security- & Attack-Resilience-by-design
 - „learning“ self-monitoring
 - Threat analysis
 - Recognizing attack pattern





CYBER DEFENCE AS A SERVICE

Our Cyber defence as a Service Approach

Monitoring of your critical infrastructure



24/7 Event Monitoring & Analysis



Telekom Security Threat Intelligence



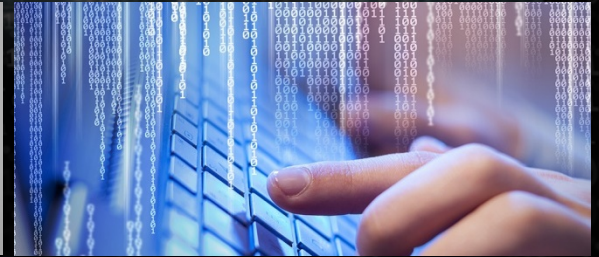
Telekom Security Content Engineering



Incident Response Retainer Services



Telekom Security Use Case Library



Europe's most modern CYBER DEFENCE CENTER Opening in October 2017



Zero Impact Operations: Our Approach to beat the attackerS

Exemplary
Daily Cyber
Attacks

Denial-of-service

Software-
Vulnerabilities

Advanced Persistent
threats (APT)



Hacker Objectives



Secure Operations
Objectives



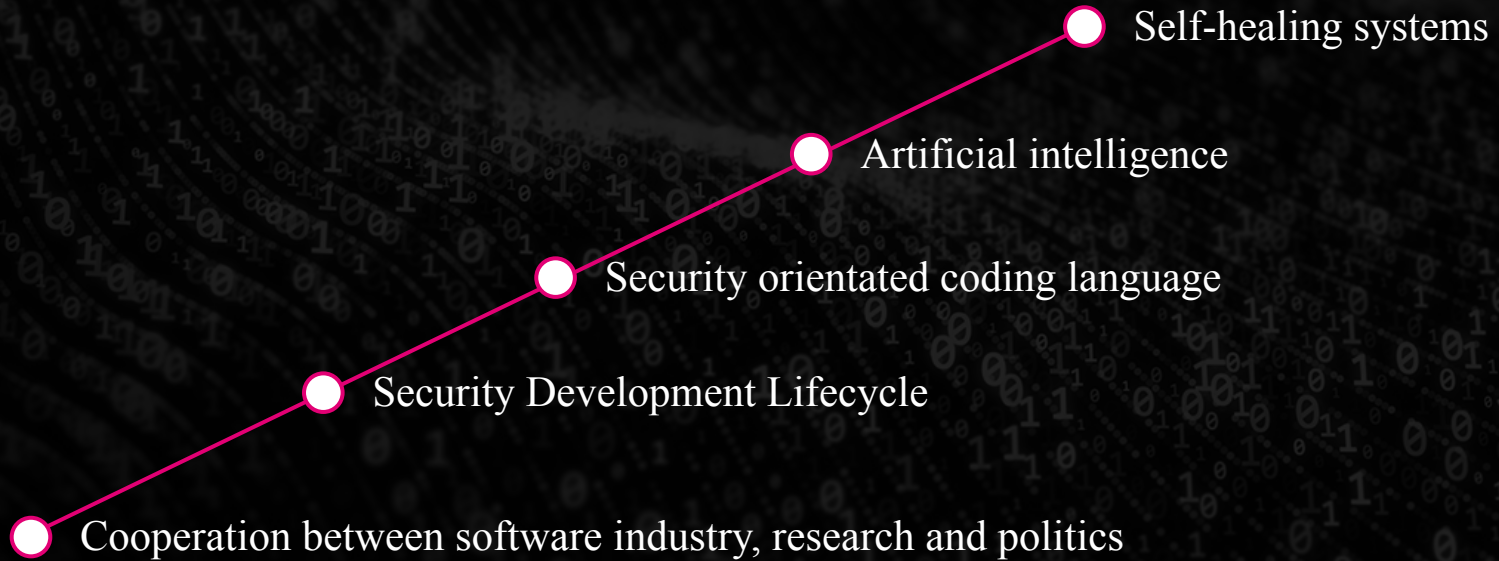
CAPABILITIES of Zero Impact

Zero Impact – 18 capabilities are defining the foundation of a Secure Operations Model

ZERO IMPACT CAPABILITIES

<p>Vulnerability Mgmt. & Assessment (incl. Security Patch Mgmt.)</p> 	<p>Asset & Config. Mgmt. of HW and SW</p> 	<p>Incident & Problem Mgmt.</p> 	<p>Change Mgmt.</p> 	<p>Security Services</p> 
<p>Security Testing</p> 	<p>Threat Intelligence</p> 	<p>Threat Defense Solutions</p> 	<p>Logging and Monitoring, Event Mgmt. and Alarming</p> 	<p>Partner Mgmt.</p> 
<p>Secure Development</p> 	<p>Back-up & Restore</p> 	<p>Risk Mgmt.</p> 	<p>Lifecycle Mgmt.</p> 	
<p>Privileged Access Mgmt.</p> 	<p>Physical Security</p> 	<p>Security Trainings & Skill Assessment</p> 	<p>Customer Interaction</p> 	

Future challenges for security operations: security by design



“With regard to the future, it is not our job to predict it, but instead to make it possible.”

Antoine de saint-exupery



Q&A

MetricStream

GRC

SUMMIT 2017

November 6 - 7, 2017

L O N D O N

Continue the conversation online

#GRCSummit

Thank You!



GRC for High Performers