



# CYBERSECURITY CHALLENGES CELTIC Online Proposer's Day

Heiko Lehmann, Telekom Innovation Laboratories, September 2020



VERBUNDEN.

# CONTENT/AGENDA

---

01 It's bad... (and getting worse)

---

02 Time and Complexity

---

03 DT approach: ML & Automation

---

04 Closing

---

DATA, TRAFFIC  
AND ATTACK  
VECTORS  
EXPLODE

EVERY  
MILLISECOND  
COUNTS

Der Sicherheitstacho zeigt die weltweiten Cyberangriffe auf die Honeypotinfrastruktur der DTAG sowie ihrer Partner an.

6140

Attacken in der letzten Minute

337265 Attacken in den letzten 1 h

8278776 Attacken in den letzten 24 h

- WEBPAGE
- VNC/VND.OUTPUT
- UNCLASSIFIED
- SSH/CONSOLE (COWRIE)
- NETWORK (HONEYTRAP)
- NETWORK (DIONAEA)
- E-MAIL (MAILONEY)



#### LIVE TICKER

DOMÄIN	DATUM	QUELLE	ZIEL	ANGRIFFSTYP	PARAMETER
COHN	17:05:14	BR	DE	Webpage	/db.php?path_local-&#x27;0-A
COHN	17:05:13	US	US	Network (honeytrap)	Attack on port 993/tcp
COHN	17:05:12	FR	FR	SSH/Console (cowrie)	user:root, password:root
COHN	17:05:11	US	US	Network (honeytrap)	Attack on port 5000/tcp
COHN	17:05:11	-	IN	Webpage	POST: /wp-admin/

#### TOP ATTACKER 2

11

LAND AT

Data traffic in our networks is growing to fuel the digital economy. But they are vulnerable to a variety of different attack types



**WE ARE CONSTANTLY UNDER ATTACK!**

**75 MILLION**

**YEARLY MALWARE ATTACKS**

MALWARE INFECTED MACHINES CAUSE SEVERE DAMAGES IN CORPORATE NETWORKS

**\$2.6 MILLION**

IS THE AVERAGE COST OF A MALWARE ATTACK ON A COMPANY

**\$20-40K**

IS THE AVERAGE COST PER HOUR FROM A DDOS ATTACK BY BOTNETS

**3.4 BILLION**

**DAILY PHISHING MAILS**

CYBER CRIMINALS PRODUCE HUGE LOSSES TO ONLINE ECONOMY BY PHISHING

**€10 MILLION**

IS THE ANNUAL LOSS FOR DEUTSCHE TELEKOM BY INTERNATIONAL VOICE FRAUD

**\$3.86 MILLION**

IS THE AVERAGE COST OF A DATA BREACH



# RAPID THREAT EVOLUTION CREATES A GROWING MARKET

## THE THREAT IS EVER-EVOLVING

**Telcos struggling to mitigate the threats of cyber attacks**

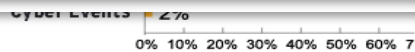
EfficientIP's 2018 DNS Threat Report took an average of 18 hours to mitigate

REUTERS World Business Markets  
CYBER RISK MAY 12, 2017 / 4:25 PM / 2 YEARS AGO

**Telefonica, other Spanish companies hit by "ransomware" attack**

MADRID (Reuters) - Spain said on Friday a large number of companies, including telecommunications giant Telefonica (TEF.MC), had been infected with malicious software known as "ransomware" which locks up computers and demands ransoms.

highlighted that it took three days or more to apply a critical security patch after notification.



**Automation becoming the new norm for cybersecurity**

By Anthony Spadafora August 28, 2018 Security

Organisations look to AI and machine learning to better secure their businesses.



## THE MARKET OPPORTUNITY IS GROWING

**2016 Cybersecurity Skills Gap**

**Few Cybersecurity Professionals**

Innovation Leadership

**Job With A Cyber Security**

UPDATED AS CAREER. FOR MEN, IT IS 67%. HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.

but the talent pool of defenders is not keeping pace.

cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study, September 2015. 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. SACA 2015 IT Risk/Reward Barometer/Member Study, 2015. 6. ISACA 2015 IT Risk/Reward Barometer/Member Study, 2015. 7. UK House of Lords Digital Skills Committee. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015. 9. State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015. 12. 2015 ISACA Risk/Reward Barometer/Member Study, September 2015.

\*\*\* Employees refers to data security professionals at organizations that potentially have access to survey respondent's personal information.



https://cybersecurity.isaca.org January 2016

# THE CURSE OF HAVING TO REACT

Cybersecurity is a bit like  
*The Hare and the Hedgehog,*

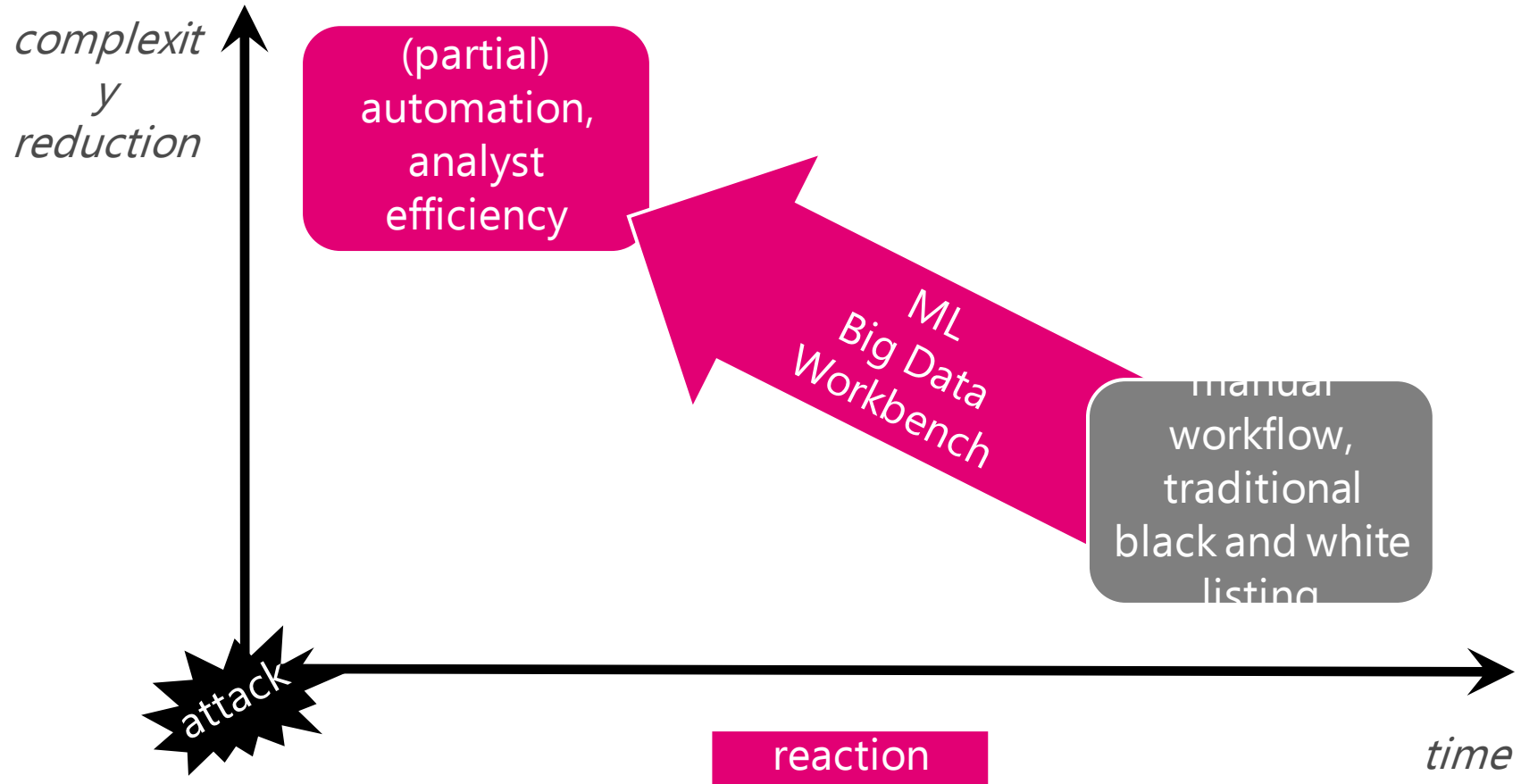
(or doping and the ):



takes time and effort

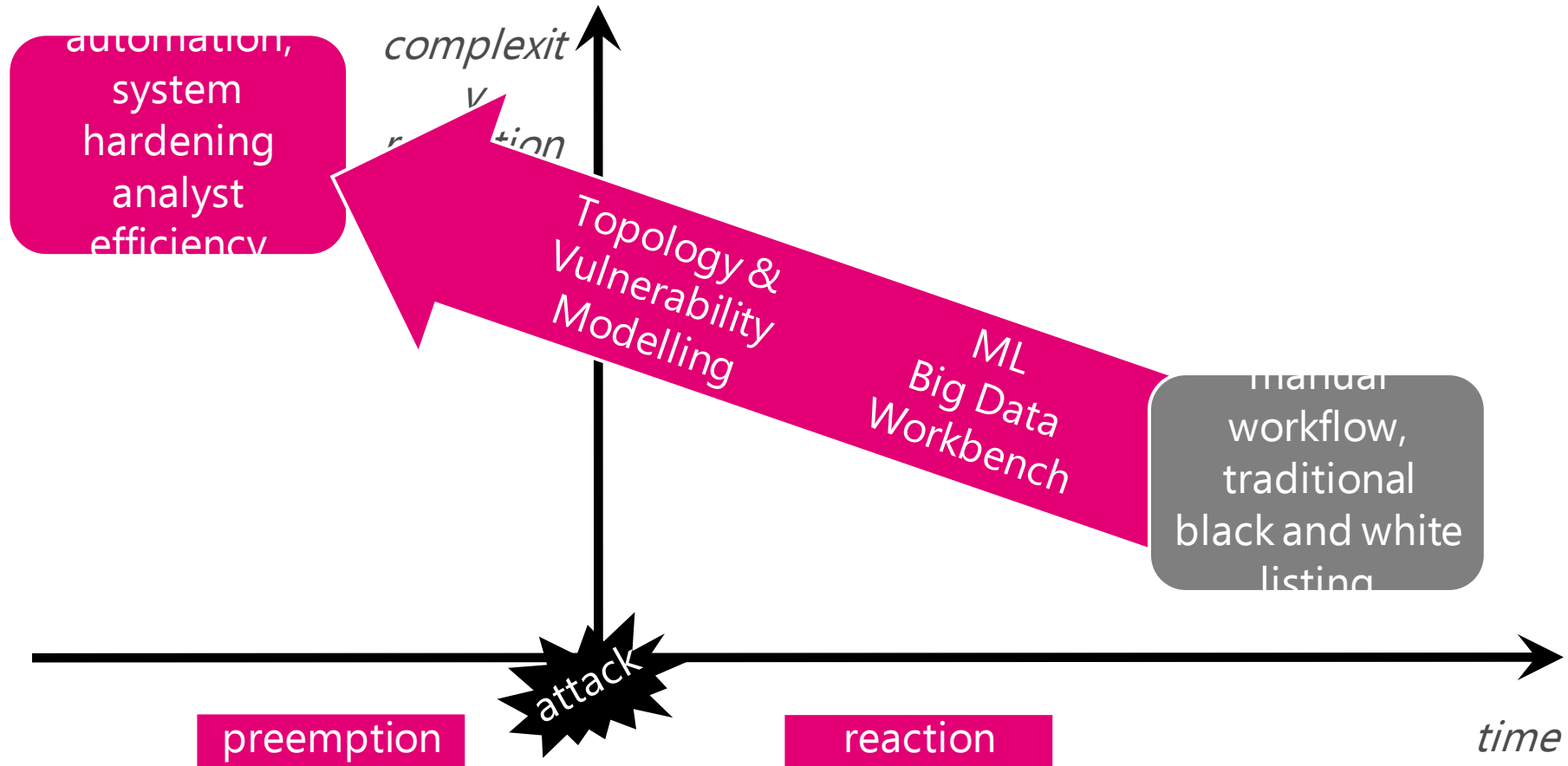
# TIME AND COMPLEXITY

# THE DIMENSIONS OF THE PROBLEM





# THE DIMENSIONS OF THE PROBLEM



# DT APPROACH: THE PREEMPT PROJECT

# FUNDAMENTALS

- Eat your own lunch: Solutions first for the DT intranet.

- Strictly adhere to data protection and privacy laws.

- Ease of Transfer: Generalized and adaptable solutions.



# INNOVATION WORK AT DEUTSCHE TELEKOM



- Serves as our development environment for quick development of individual use cases
- Combines pre-configured methods and standardized access to data platforms and other assets
- Incorporates previous work done and platforms established

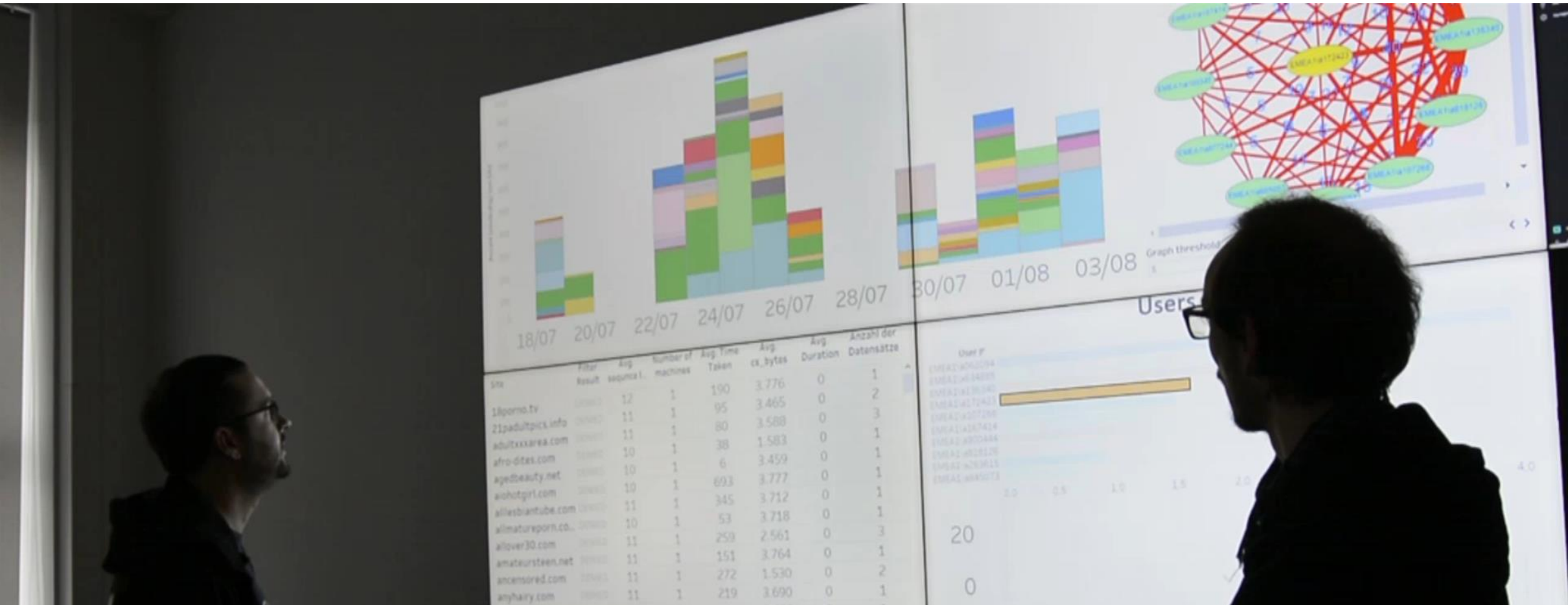
# use case details

	Infected Machines Detection	Privilege Misuse Detection	Phishing Detection	Data Leakage Detection	International Voice Fraud Detection
Threat TYPE	<ul style="list-style-type: none"> <li>Malware infection causes severe damages in corporate networks</li> </ul>	<ul style="list-style-type: none"> <li>Compromised privileged accounts can lead to abuse and unauthorized access</li> </ul>	<ul style="list-style-type: none"> <li>Cyber criminals produce huge losses to online economy by Phishing</li> </ul>	<ul style="list-style-type: none"> <li>Illegal or unwanted transfer of data over covert channels</li> </ul>	<ul style="list-style-type: none"> <li>By Int'l Revenue Share Fraud criminals obtain phone revenue illegally.</li> </ul>
Example Customer Risks	May 2017: Wannacry Ransomware causes chaos in hospitals and med. centers	July 2017: Anthem Hit with Data Breach of 18.580 Medicare Members	Campaigns targeted to specific customers groups (e.g. financial insitutions)	"DNS tunneling": transfer payload data fraudulently over DNS at Vodafone in 2015	FRITZ!Box hack in 2014 with 1,000 hacked subscribers
PREEMPT INNOVATION	detect unknown unknowns	detect abnormal behavior	automate detection and detect sophisticated attacks	prevent data leakages and resulting financial losses	make DT an unattractive target for fraudsters





# Use Case at work: Infected Machines Detection



# translating generic ML advances into cyber security application

## CUTTING EDGE ML Technologies

Deep Learning embedding

Automatic feature extraction

Transfer learning

Element/set comparison (sensitivity hashing, Siamese NN)

Auto adaptation of detection thresholds

Auto-configuration of neural networks (hyper-parameters)

## NEW Cyber security capabilities

**Multi-source big data  
analysis and  
correlation**

(ready for the Data  
Avalanche)

**Detect low-amplitude  
(stealth) anomalies**

(ready for Smart Attacking)

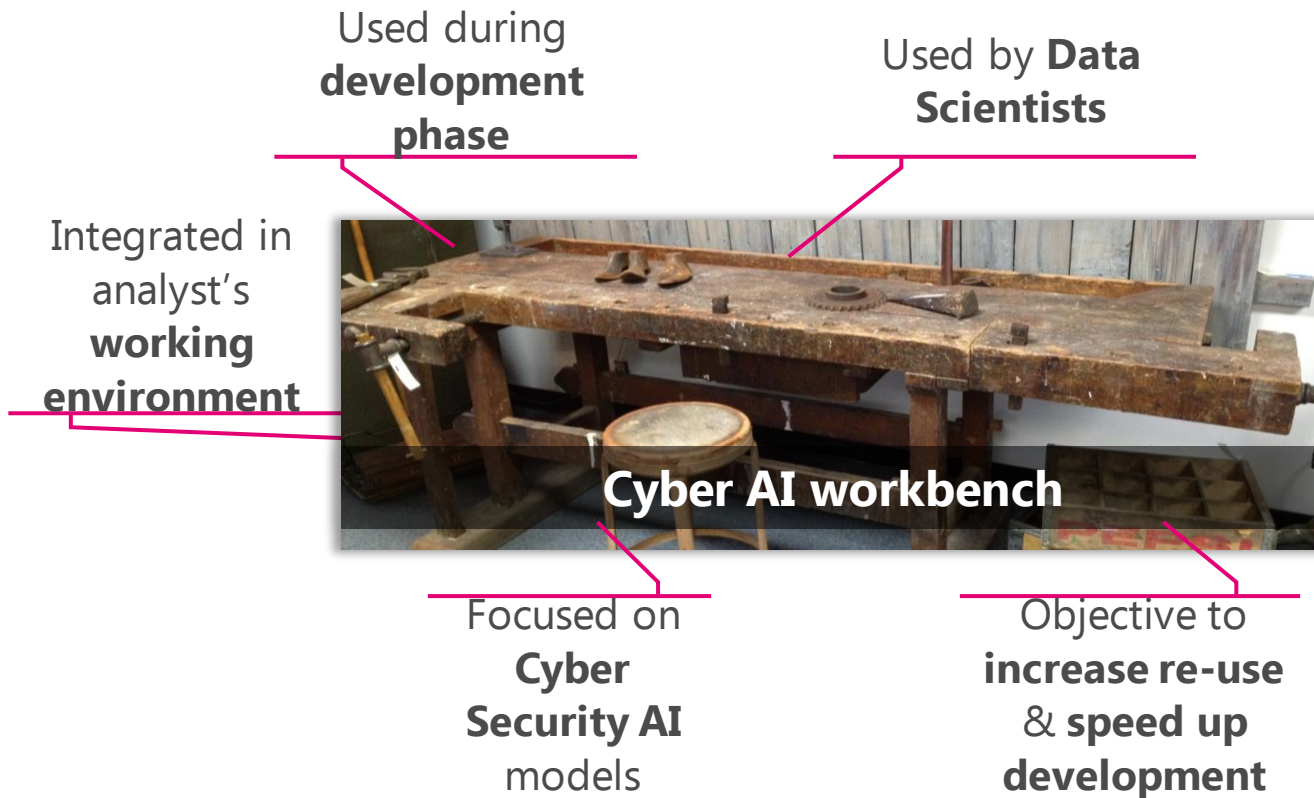
**Concept-drift  
readiness: constant  
adaptation to new  
circumstances**

(ready for Agile Attacking)

**Transfer learning  
experiences between  
use cases and clients**

(ready for Swiftess)

# CYBER AI Workbench speeds up development and re-use of Cyber Security use cases



- User interface to access data sets, algorithms, use cases etc.
- Content includes code repository, data descriptions, pipeline stages, deployment, configuration notes.

Generic concepts (ML!) allow easy solution transfer into different environments

Groundwork delivered in DT intranet solutions

Phishing detection in mobiles

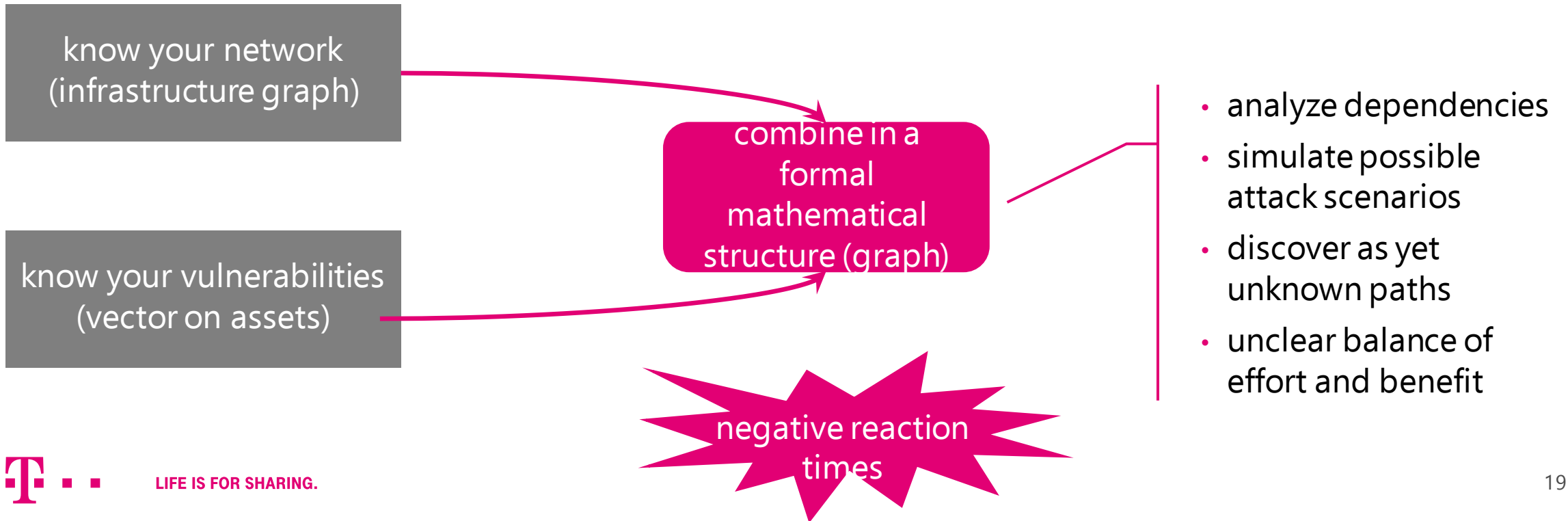
blue-printable SME solution

# Closing and Outlook



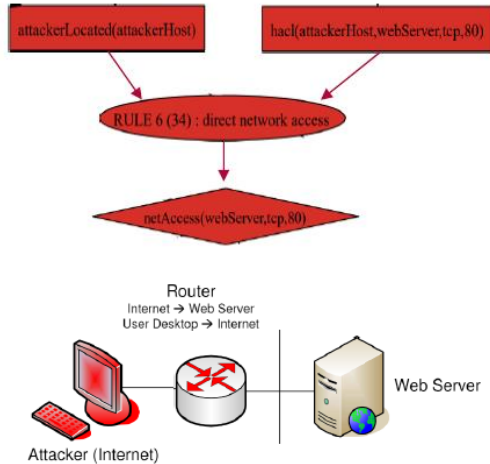
# TRUE PREEMPTION: ATTACK GRAPH MODELLING

with clear definitions and terminology absent, the principal idea is:



# TRUE PREEMPTION: ATTACK GRAPH MODELLING

was



- logical model
- rigid rules
- relies on information completeness
- highly complex
- difficult to maintain
- error-prone

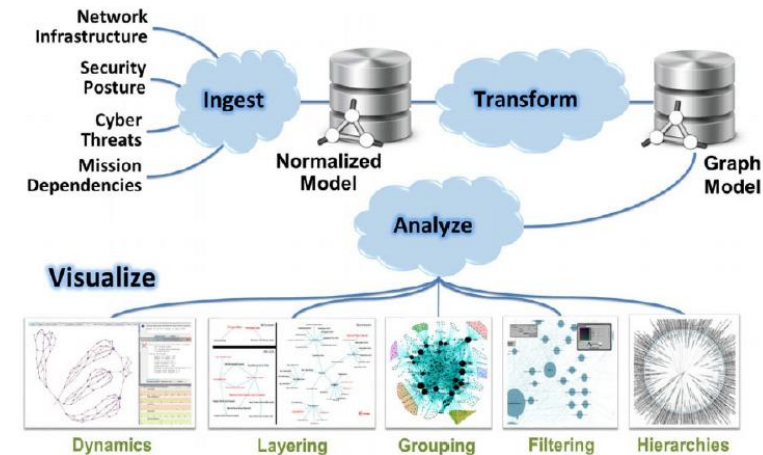
**Definition 1** An *attack graph* or *AG* is a tuple  $G = (S, \tau, S_0, S_s)$ , where  $S$  is a set of states,  $\tau \subseteq S \times S$  is a transition relation,  $S_0 \subseteq S$  is a set of initial states, and  $S_s \subseteq S$  is a set of success states.



LIFE IS FOR SHARING.

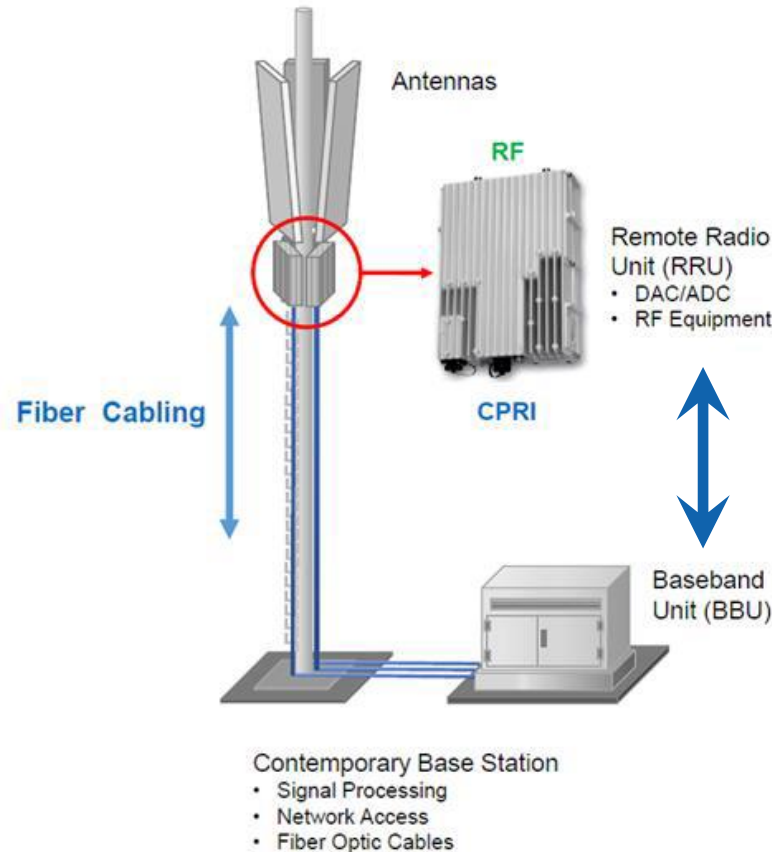
evolves into

- relate to knowledge graphs
- replace  $[0, 1]$  of logical model by probabilities
- use ML to assess critical assets and evaluate correlation
- (e.g. CyGraph)



# ... THE RACE NEVER ENDS; NEW INFRASTRUCTURAL VULNERABILITIES: OPEN RAN

Open System of  
HW and SW must  
be protected  
against attackers.



SW defined radio

open interface

proprietary SW with  
virtualized functions on  
COTS servers



LIFE IS FOR SHARING.

ENCOURAGE THE HARE!



THX!