CYBERSECURITY CHALLENGES
CELTIC Online Proposer's Day

Heiko Lehmann, Telekom Innovation Laboratories, September 2020

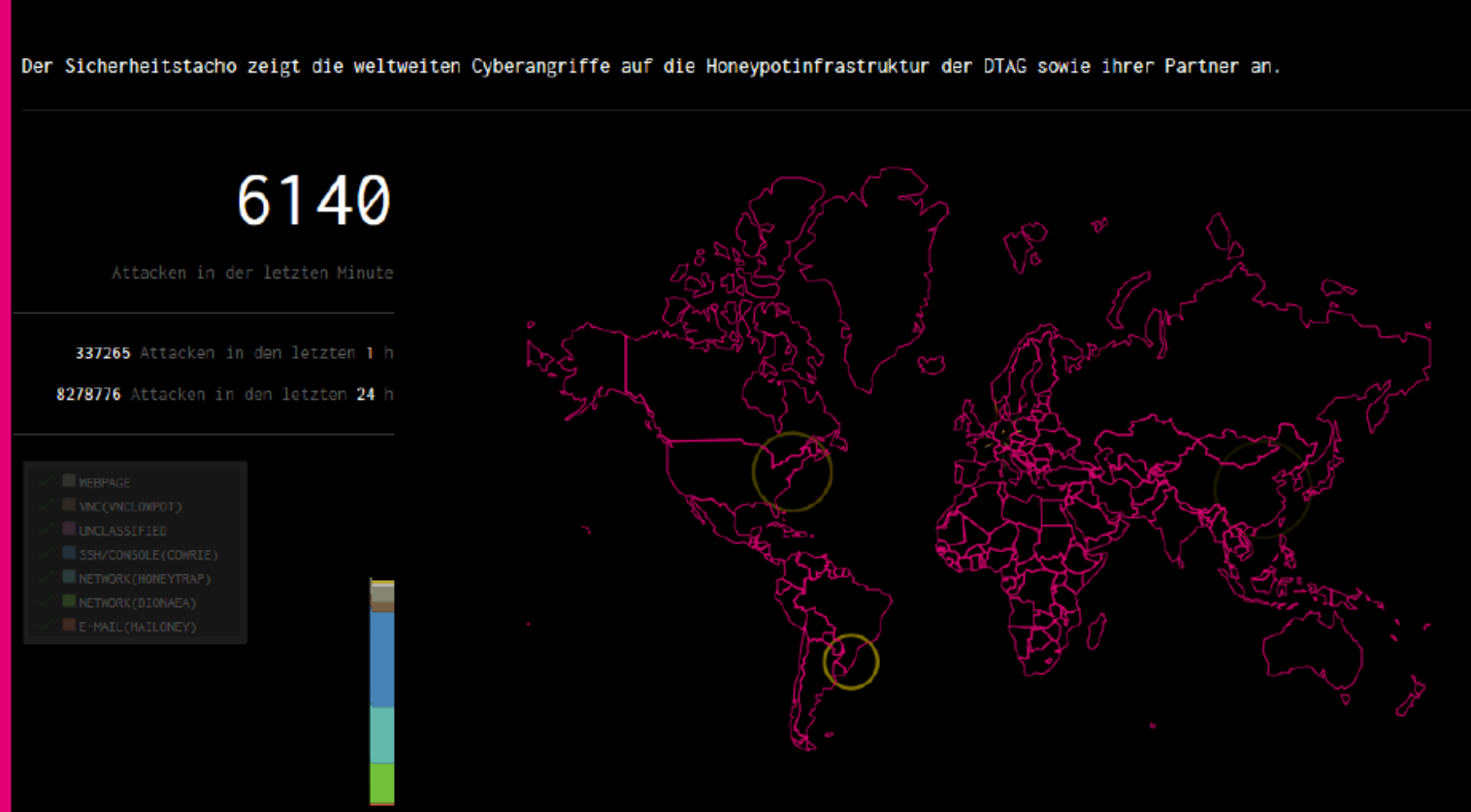
T . .

VERBINDET.

CONTENT/AGENDA

DATA, TRAFFIC AND ATTACK VECTORS EXPLODE

EVERY MILLISECOND COUNTS



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

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

$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

$3.86 MILLION

IS THE AVERAGE COST OF A DATA BREACH

RAPID THREAT EVOLUTION CREATES A GROWING MARKET

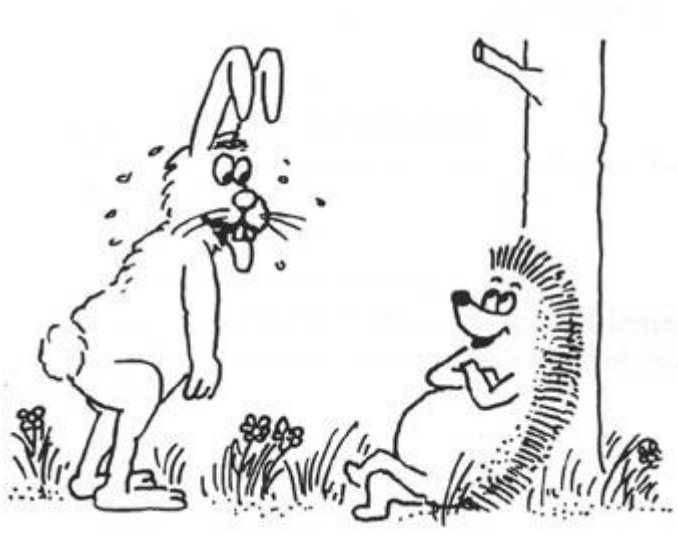
THE THREAT IS EVER-EVOLVING

THE MARKET OPPORTUNITY IS GROWING

THE CURSE OF HAVING TO REACT

Cybersecurity is a bit like
The Hare and the Hedgehog,

(or doping and th WORLD ANTI-DOPING AGENCY play true):

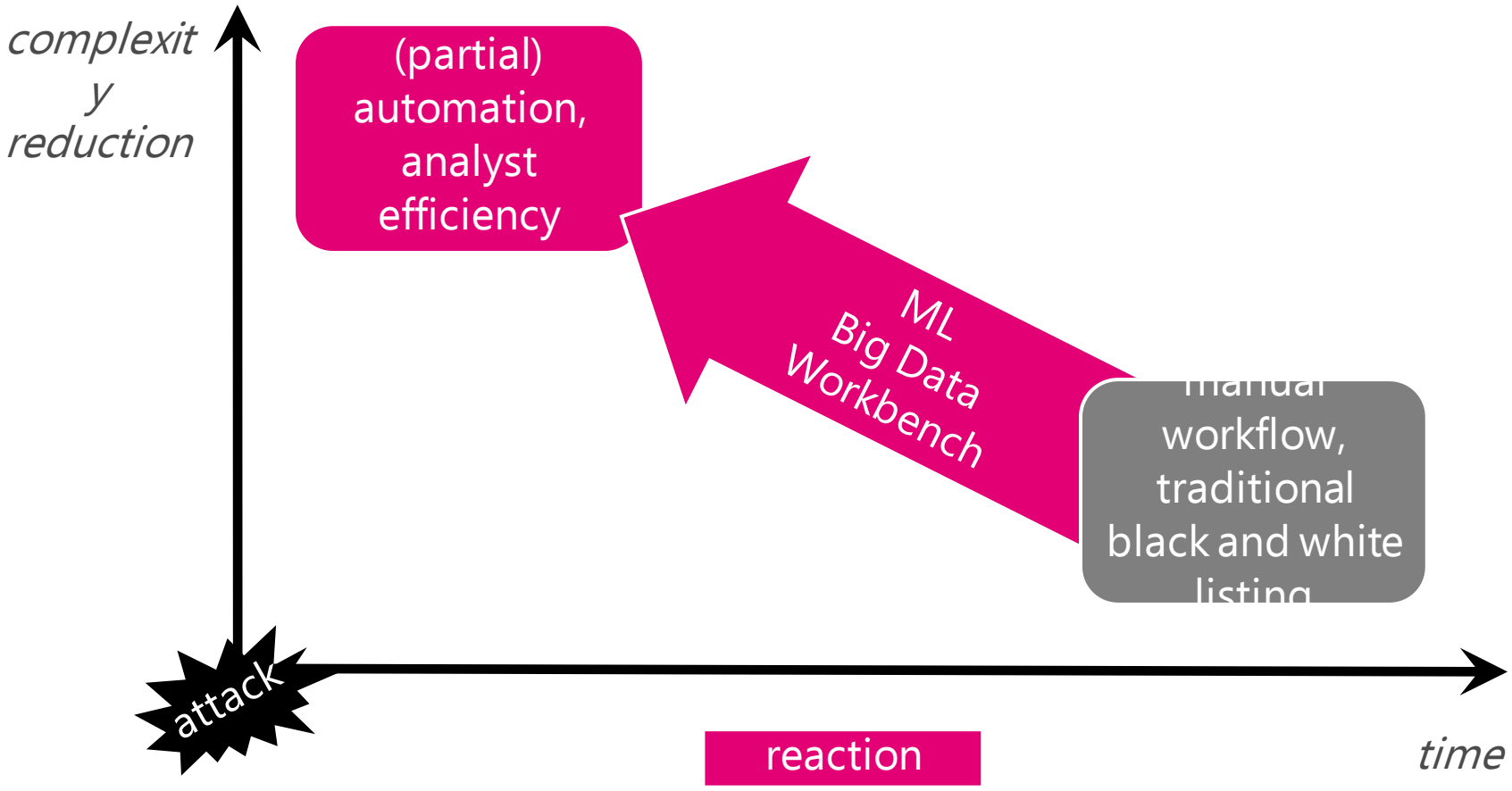


Attack → Detection → Analysis → Counter-measure

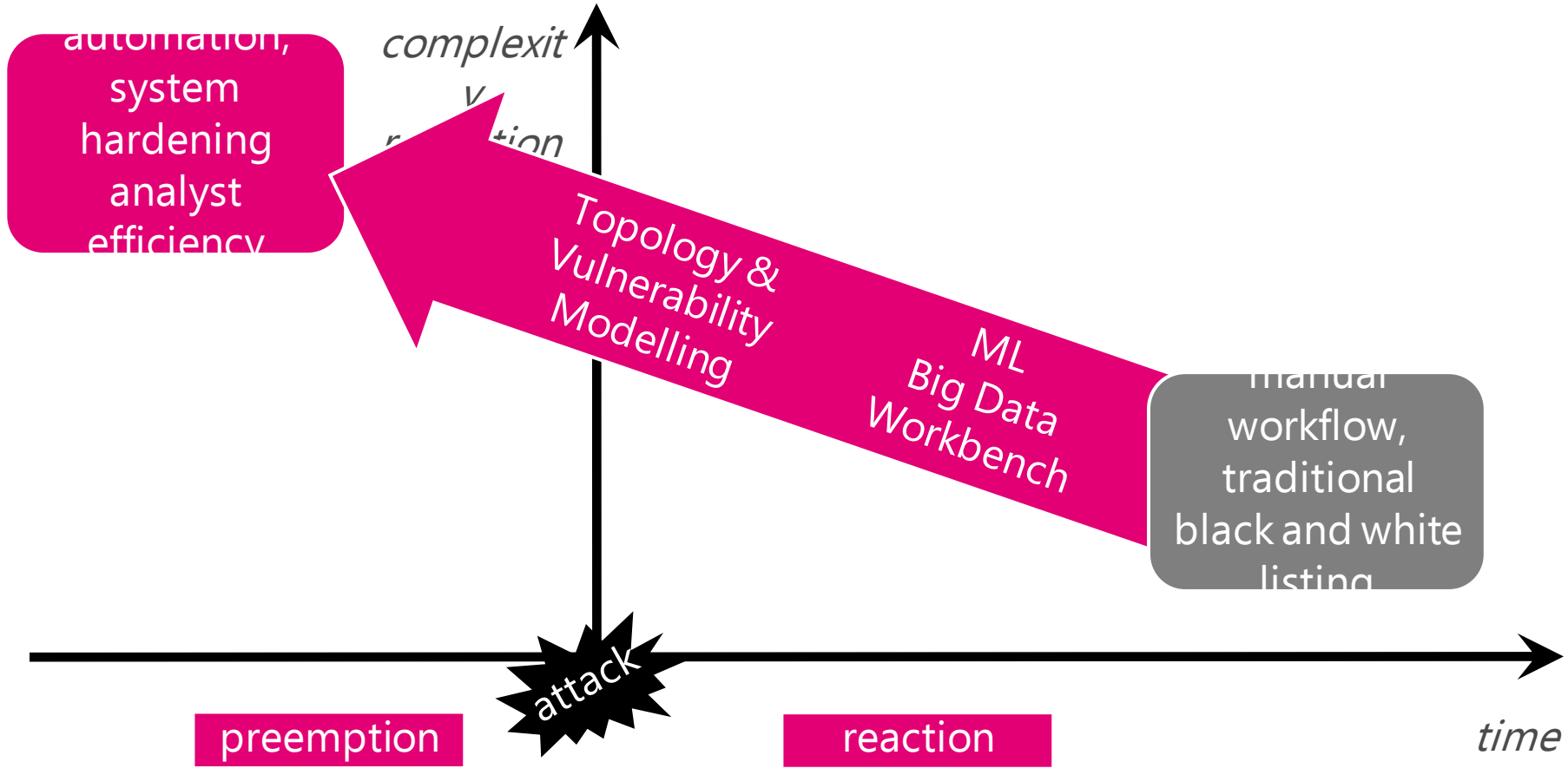
takes time and effort

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 adaptible solutions.

INNOVATION WORK AT DEUTSCHE TELEKOM

Preempt

Cyber security
Developed and run
by Deutsche
Telekom

5 Cyber Security use cases for deployment

Addressing specific threat types in productive environment, leveraging the methods and assets from the workbench

1. Detect Infected Machines
2. Botnet Detection
3. Phishing Detection
4. Data Leakage Prevention
5. International Voice Fraud Detection

- 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	▪ Malware infection causes severe damages in corporate networks	▪ Compromised privileged accounts can lead to abuse and unauthorized access	▪ Cyber criminals produce huge losses to online economy by Phishing	▪ Illegal or unwanted transfer of data over covert channels	▪ By Int'l Revenue Share Fraud criminals obtain phone revenue illegally.
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 INNO-VATION	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)

Concept-drift readiness: constant adaptation to new circumstances

(ready for Agile Attacking)

Detect low-amplitude (stealth) anomalies

(ready for Smart Attacking)

Transfer learning experiences between use cases and clients

(ready for Swiftness)

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

Used during **development phase**

Used by **Data Scientists**

Integrated in analyst's **working environment**

Focused on **Cyber Security AI** models

Objective to **increase re-use** & **speed up development**

- 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

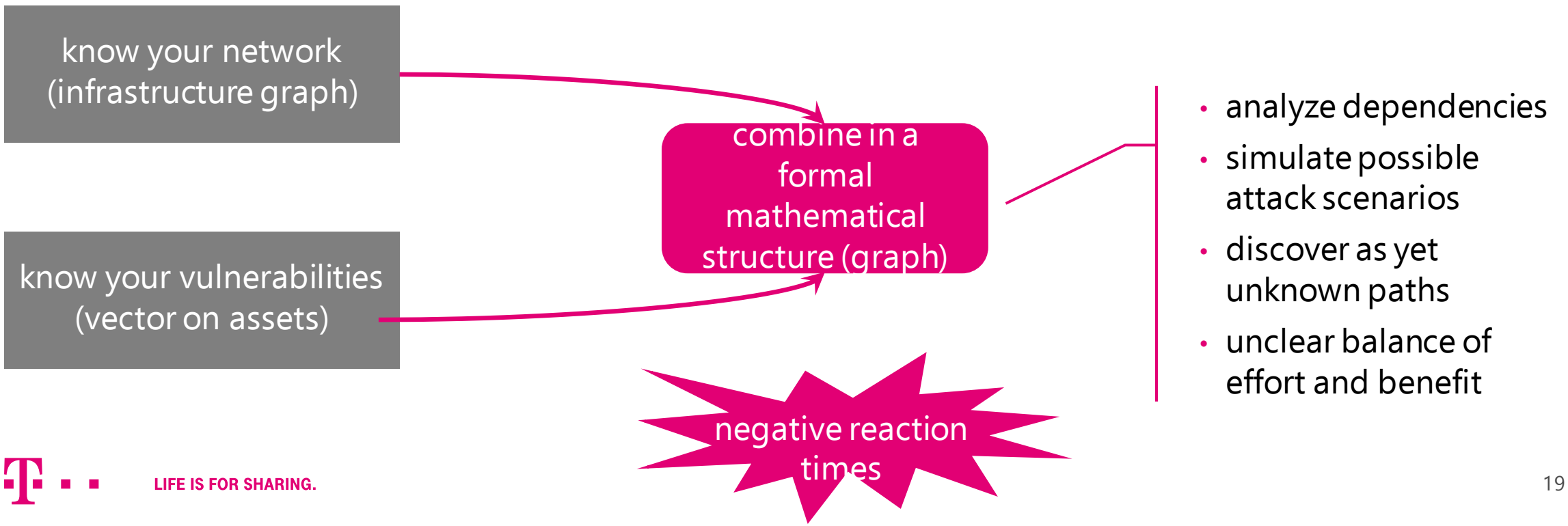
Phishing detection in mobiles

blue-printable SME solution

Closing and Outlook

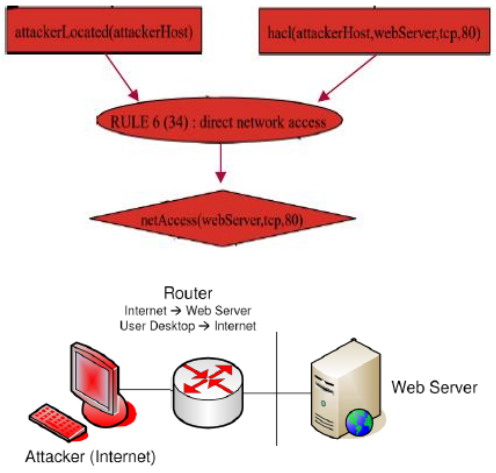
TRUE PREEMPTION: ATTACK GRAPH MODELLING

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



TRUE PREEMPTION: ATTACK GRAPH MODELLING

was

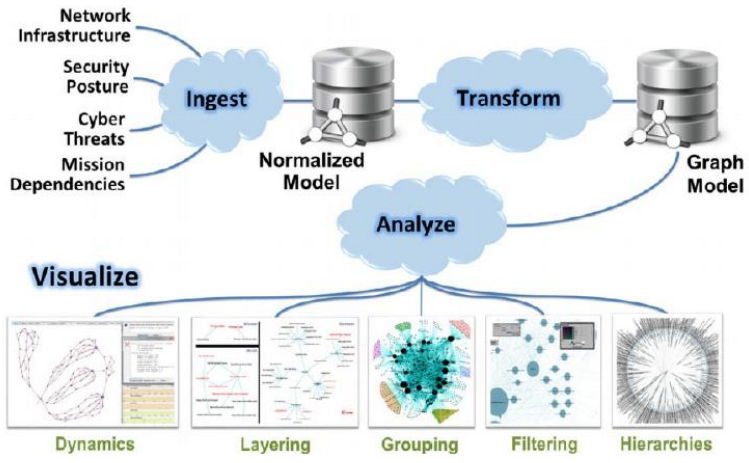


- logical model
- rigid rules
- relies on information completeness
- highly complex
- difficult to maintain
- error-prone

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.

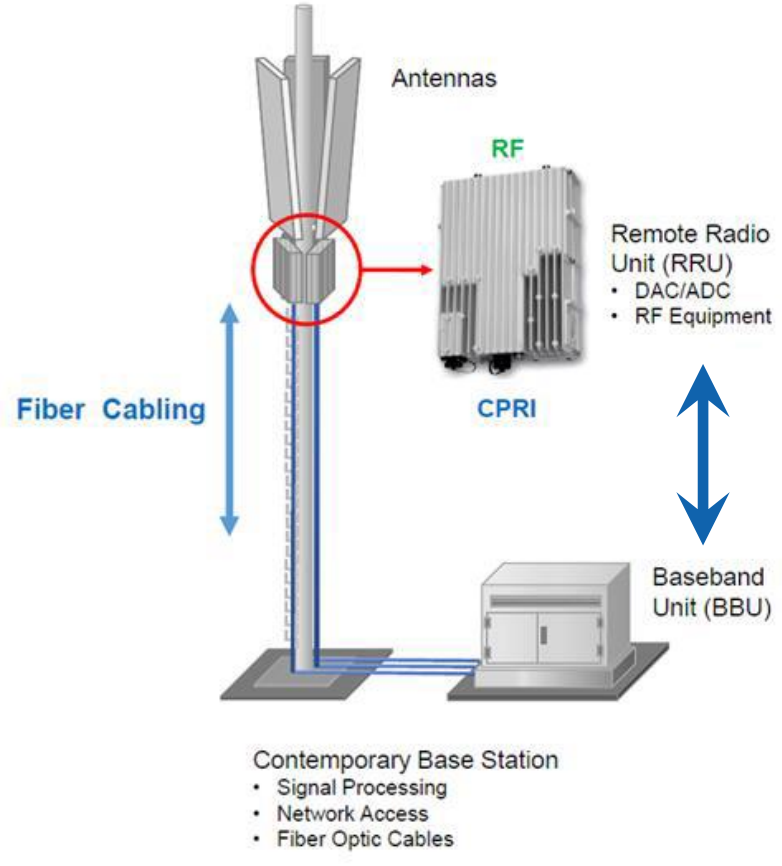
evolves into

- 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

ENCOURAGE THE HARE!

THX!