



Risk monitoring of a pseudonymisation service based on TRICK Service

21/09/2015

Speaker: Ben Fetler

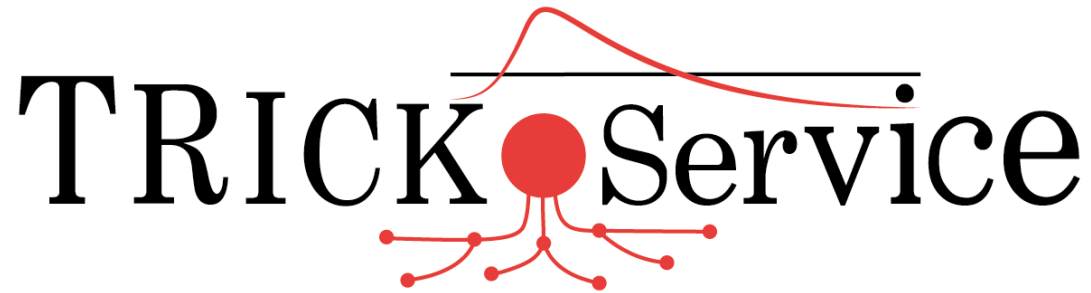
Authors: Ben Fetler, Steve Muller

Agenda

Introduction to TRICK Service & ÉpStan project

Real-time risk assessment

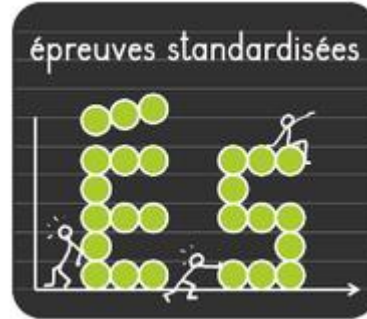
Conclusion and outlook

The logo for TRICK Service. The word "TRICK" is in a large, black, serif font. The letter "I" is replaced by a red circle. A red line starts from the top of the circle, curves upwards and to the right, then downwards and to the right, ending above the letter "S". Below the circle, several red lines branch out downwards and to the left and right, ending in small red dots, resembling a network or a stylized figure.

Tool for **R**isk management of an **I**SMS based on a **C**entral **K**nowledge base

Core principles

- Risk management following ISO/IEC 27005;
- Quantitative assessment of likelihood and impact of different risk scenarios;
- “Risk Reduction Factor” (RRF) determination which enables to quantify the influence of security measures on the losses caused by threats to assets;
- Cost-effectiveness of security controls; TRICK Service considers the Return On Security Investment (ROSI) and derives a prioritised action plan.



Luxembourg's national school monitoring programme

Requirement:

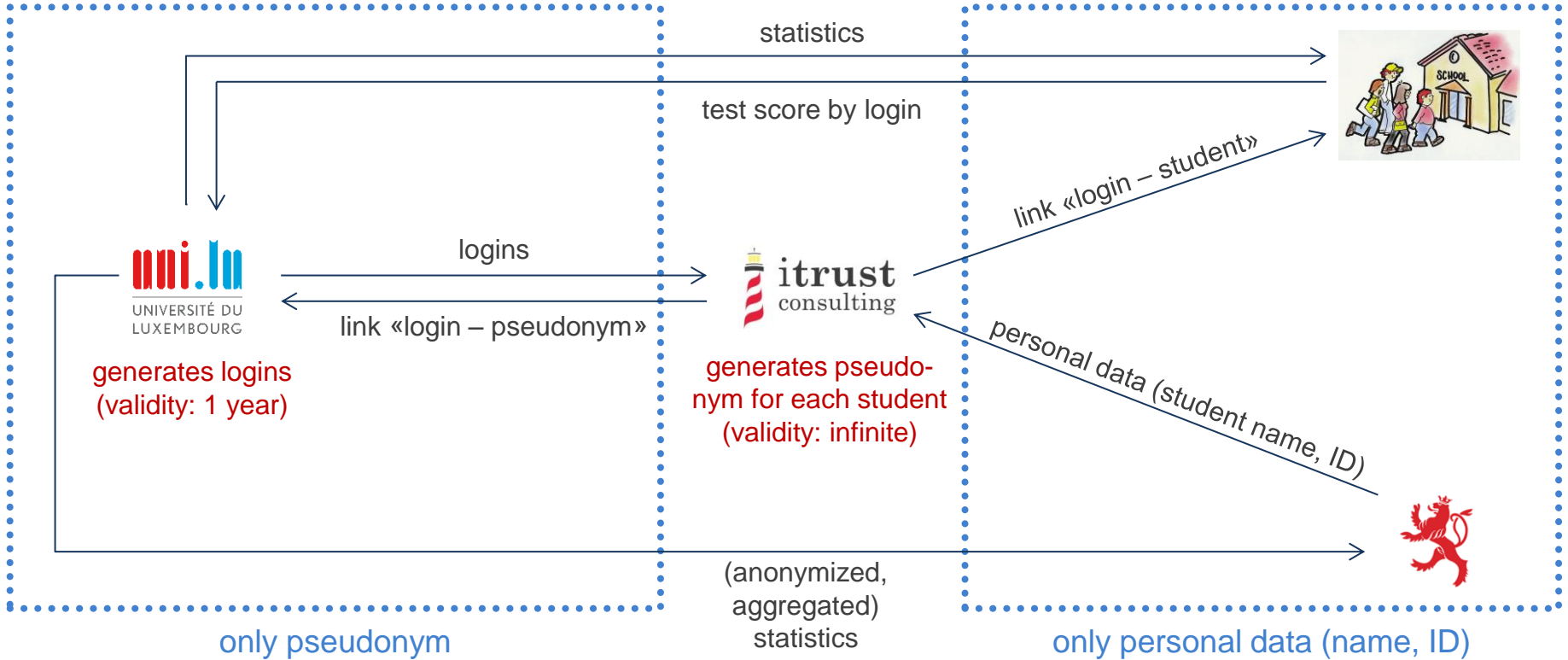
University and Ministry shall not make link between results and student.

Solution:

Involve a third party (itrust consulting) offering a pseudonymisation service.

Introduction

ÉpStan



Real-time risk assessment

Risk computation

Dynamically



$$Risk(asset) = \sum_{scenario} Impact \cdot Probability \cdot RiskReduction$$

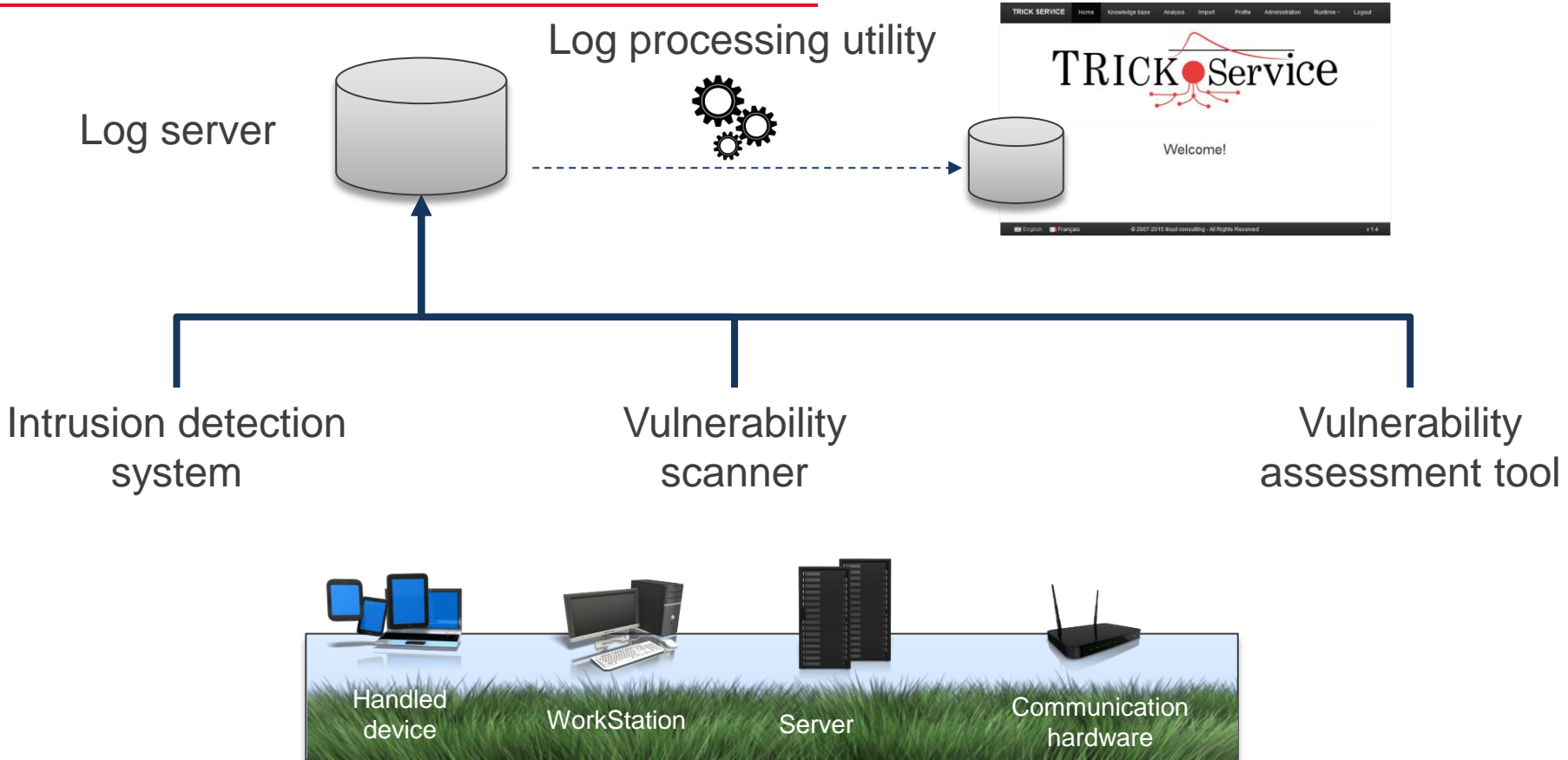
Damage caused to asset in scenario

Probability that scenario occurs

Reduction of risk caused by implementation of security measures (factor between 0 and 1)

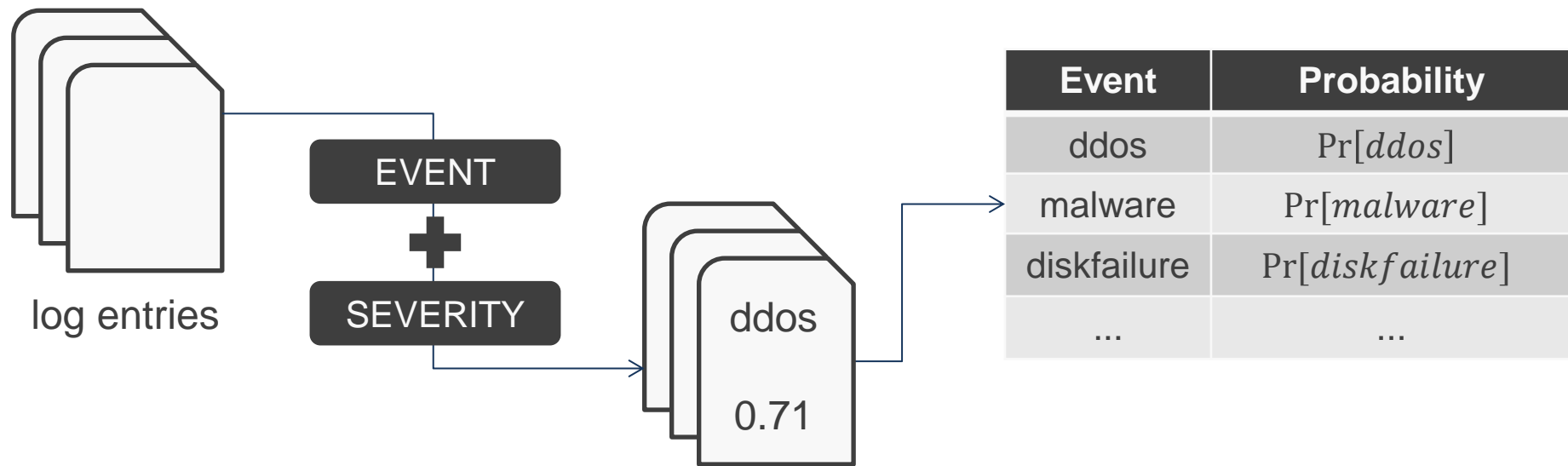
Real-time risk assessment

Strategy



Real-time risk assessment

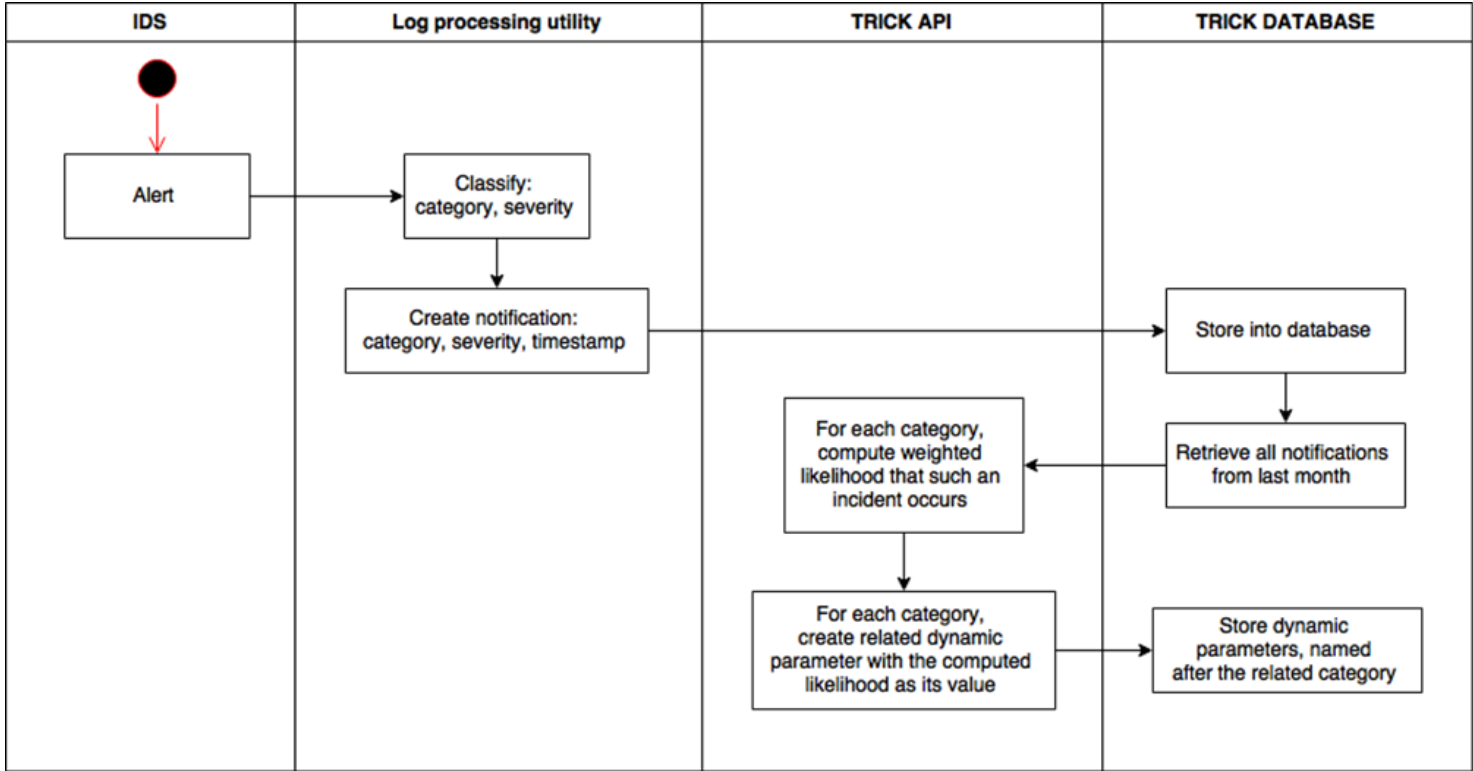
Log processing utility



- $\Pr[event]$ increases with each log entry (the higher the severity, the higher the increase)
- $\Pr[event]$ decreases with time

Real-time risk assessment

PoC - Intrusion detection system



Real-time risk assessment

TRICK Service: dynamic likelihood

+ Add Edit Select Unselect Estimation

<input type="checkbox"/>	#	Name	Type	Value (k€)	ALE (k€)
<input type="checkbox"/>	1	ÉpStan application	SW	65	34,2
<input type="checkbox"/>	2	ÉpStan data	Info	40	47,6
<input type="checkbox"/>	3	ÉpStan service	Busi	10	13,9
<input type="checkbox"/>	4	ÉpStan server	HW	2	2,4
Total				117	98.1

- Definition of all ÉpStan-related assets
- Automatic real-time estimation of Annual Loss Expectancy (ALE)
ALE = impact · likelihood

Real-time risk assessment

TRICK Service: dynamic likelihood

Scenario	Imp. (k€)	Pro. (/y)	ALE (k€)
A_all - Complete loss, including backup	i6	ids_malware*0.05+ ids_disk_failure_db	15,2
C3 - Accidental disclosure	i7	p3	11,5
A_1 - Partial loss or temporary	i4	ids_ddos*0.1	5,1
I3 - Accidental manipulation	i5	p4	5
C1 - Partial theft coming from external	i6	ids_login_bruteforce_db*0.1	4,4

i0	2 k€	p0	1/100y
i1	4 k€	p1	1/50y
i2	10 k€	p2	1/30y
i3	16 k€	p3	1/16y
i4	25 k€	p4	1/10y
i5	50 k€	p5	1/5y
i6	100 k€	p6	1/3y
i7	200 k€	p7	1/2y
i8	400 k€	p8	1/y
i9	800 k€	p9	2/y
i10	1 600 k€	p10	3/y

- Support for expressions in 'likelihood' field involving variables resulting from log processing utility
- ALE is updated in real-time

Real-time risk assessment

TRICK Service: dynamic risk reduction

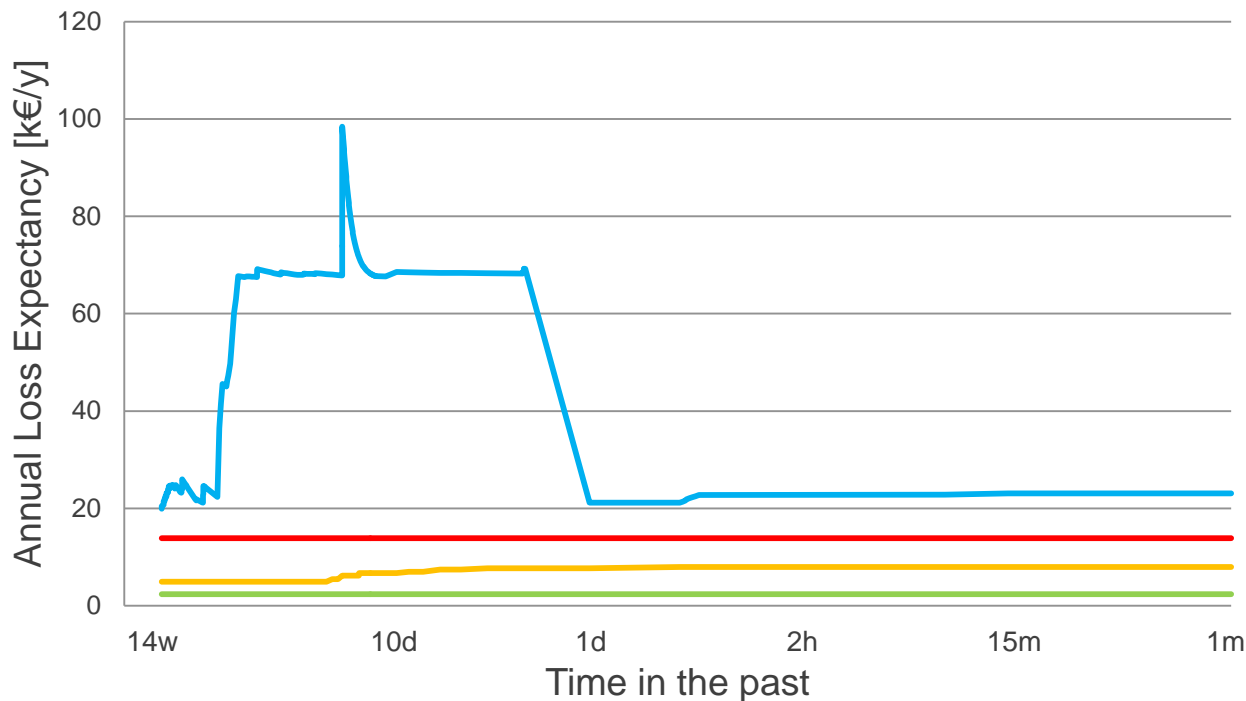
IR = Implementation Rate

Ref	Domain	Status	IR (%)	IW (md)	EW (md)	INV (k€)	LT (y)	IM (md)	EM (md)	RM (k€)
12.5	Control of operational software									
12.5.1	Installation of software on operational systems	AP	ids_patch_mgmt	2	0	0	5	0,2	0	0
12.6	Technical vulnerability management									
12.6.1	Management of technical vulnerabilities	AP	50	1	0	0	1	0,1	0	0
12.6.2	Restrictions on software installation	AP	50	0	0	0	5	1	0	0
12.7	Information systems audit considerations									
12.7.1	Information systems audit	AP	70	0	0	0	5	1	0	0

- Implementation rate with support for expressions
- Real-time update of implementation rate

Real-time risk assessment

TRICK Service: Cockpit

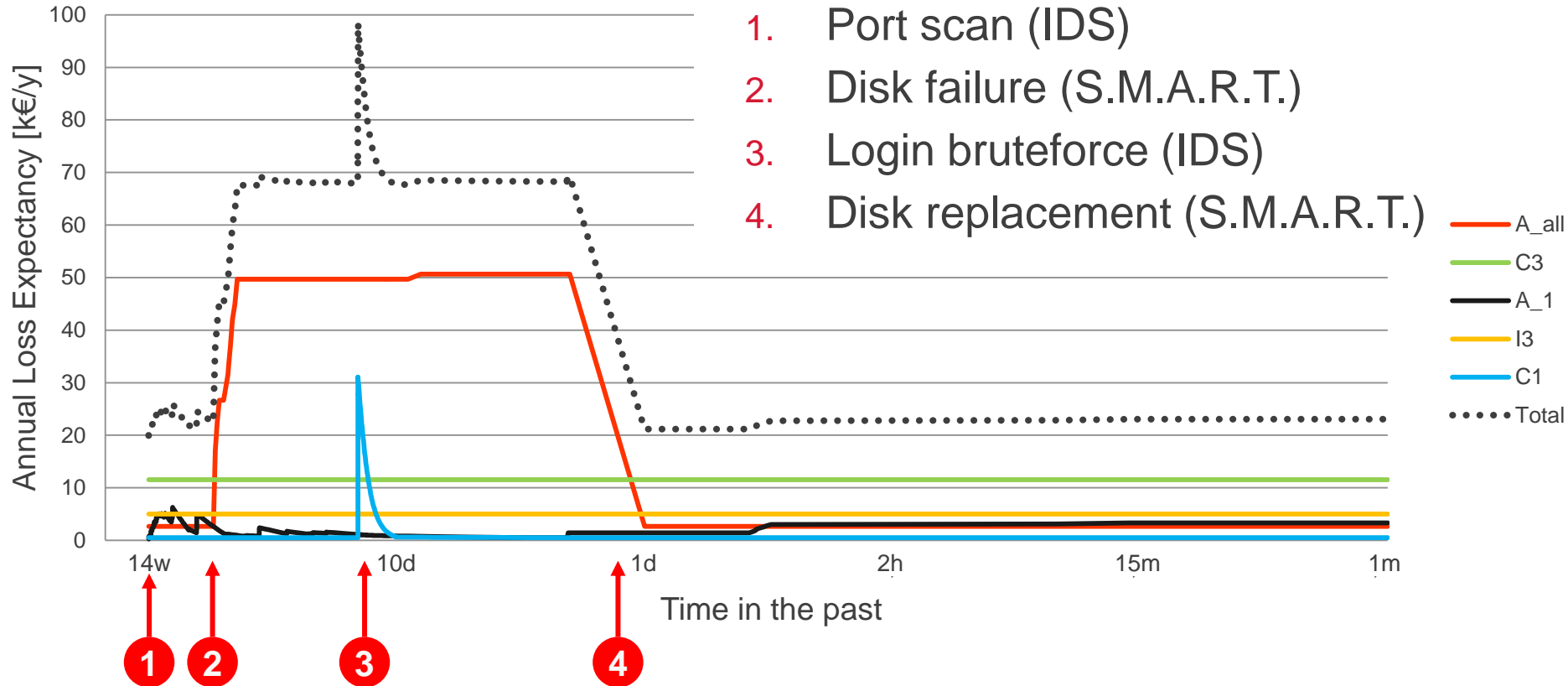


- Information (ÉpStan data)
- Software (ÉpStan Application)
- Service (ÉpStan Service)
- Hardware (ÉpStan Server)

- Real-time graph displaying ALE per asset type
- Logarithmic time scale to put focus on recent past
- Click on asset type opens up detailed view (see next slide)

Real-time risk assessment

TRICK Service: ALE evolution of «Information» assets



- Real added value: Having view on current risk situation & its impacts;
- Use logs of several information security tools;
- Apply real-time risk assessment to Industrial Control System environment;
- Define generic expressions for dynamic likelihood and risk reduction computation;
- Add asset dependency functionality.