

TRUST

aWARE



Dr Javier Gutiérrez Meana
TREE TECHNOLOGY SA

ENHANCING DIGITAL SECURITY, PRIVACY AND TRUST IN SOFTWARE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

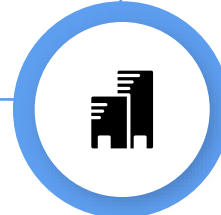
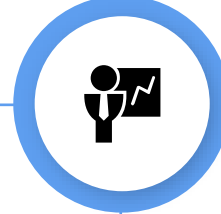
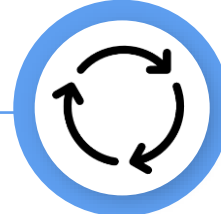

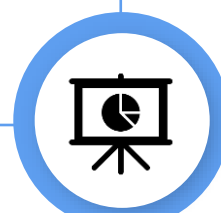
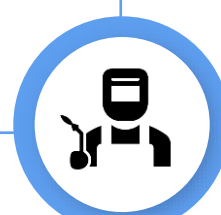
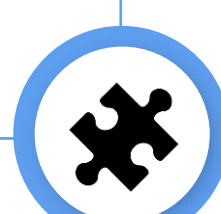




Factsheet

Programme	Horizon 2020
Grant Agreement	101021377
Topic	SU-DS03-2019-2020 - Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Funding scheme	IA – Innovation Action
Budget	€ 5, 244, 997.50
EU-Contribution	€ 4, 645, 031.25
Start date	1 June 2021
End date	31 May 2024
Website	www.trustaware.eu
Social media	@Trustaware  

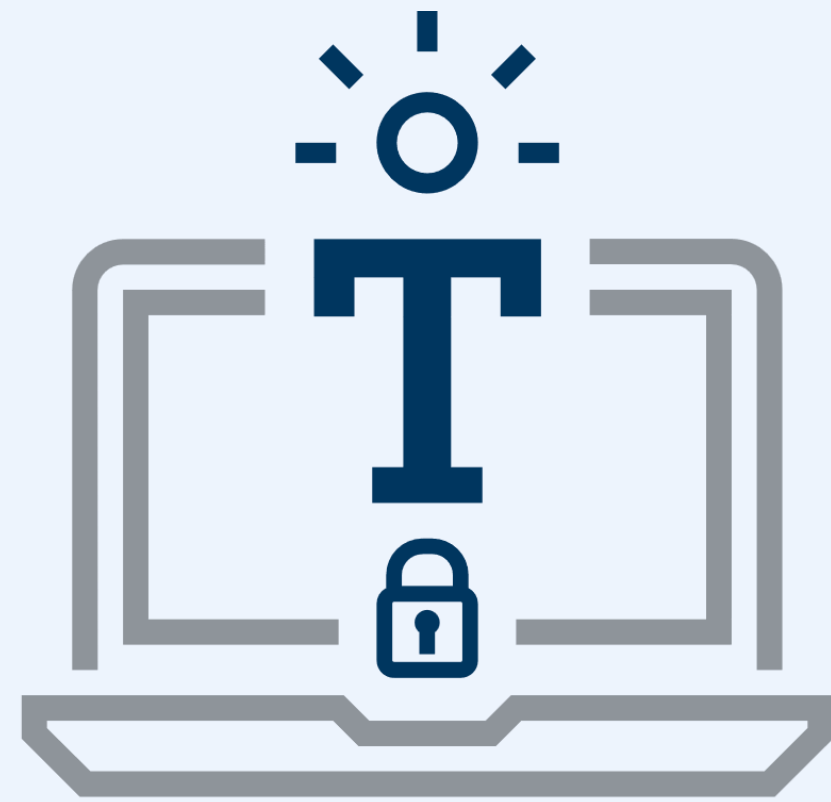


Index

- 01  Who we are
- Motivation  02
- 03  S&P vicious vs virtuous cycle
- Overall mission  04
- 05  Outcomes
- Technical challenges  06
- 07  Socio-technical challenges
- Community engagement  08
- 09  Contact



Who we are

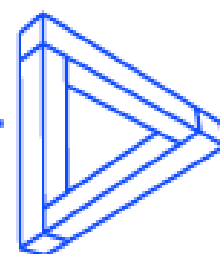


TRUST
aWARE

- 04 | User associations
- 03 | Industrial companies
- 03 | Research organisations
- 01 | CERT body
- 01 | International platform



Who we are



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377



Motivation



01

Users are not always aware of their exposure to Security & Privacy (S&P) risks when they use software. This results in bad usage habits and lack of risk prevention mechanisms.

03

Standards and certifications are key enablers for assessing and assuring the level of S&P protection provided by modern software and their risks. **However, developers and operators lack S&P certification methods and standards.**

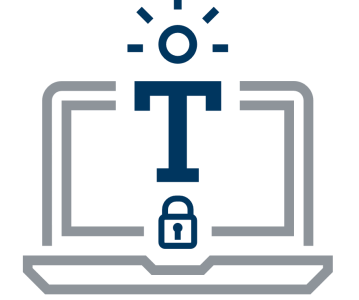
02

Developers are lacking best-practices for S&P-by-design in software engineering.

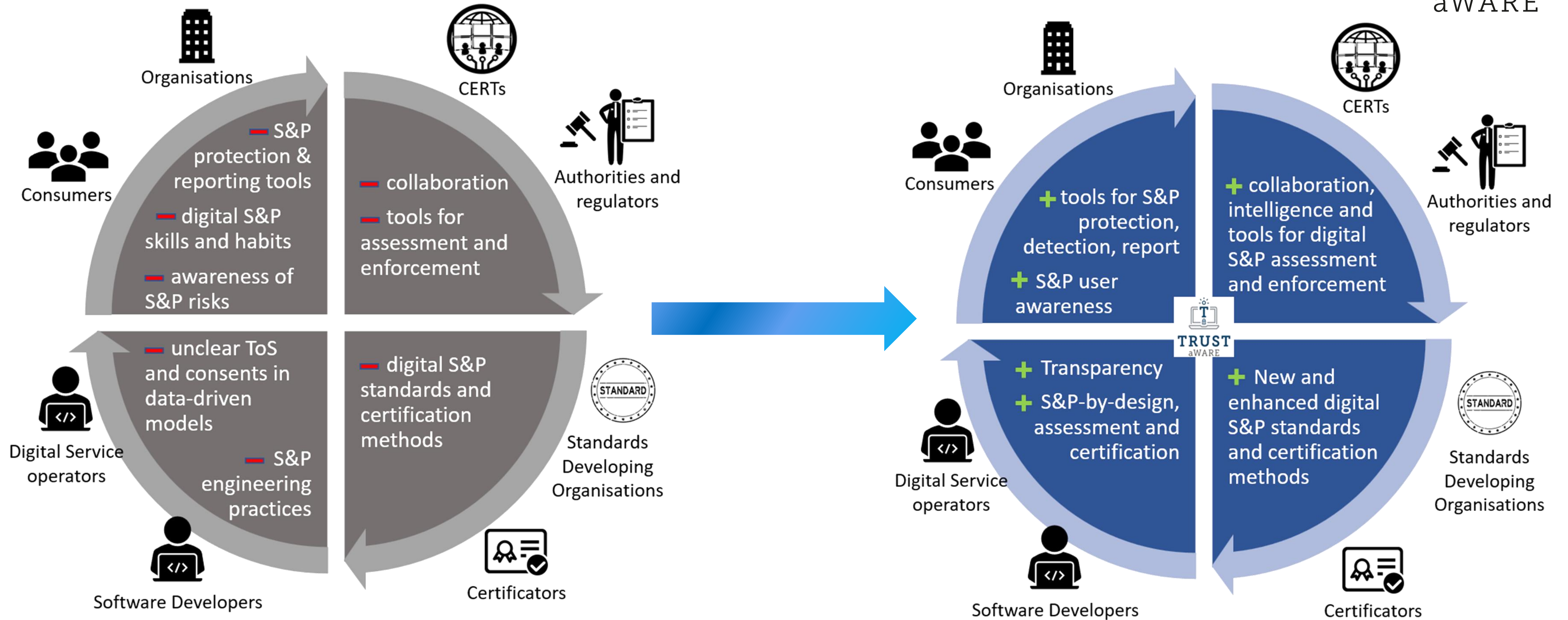
04

Regulators and national agencies all over the world **are defining and implementing new legal frameworks** for protecting citizens against online S&P threats. But it is **unclear whether the penalties are sufficient** deterrent against S&P mispractices.

S&P Vicious VS Virtuous cycle



TRUST
aWARE



Overall mission



TRUST aWARE's mission is to provide a **holistic and effective digital Security & Privacy (S&P) framework** comprising a set of novel and integrated tools and services co-created by citizens and stakeholders. This framework will help to **identify, audit, analyse, prevent, and mitigate the impact of the various S&P threats** associated with citizen's digital activities in a timely manner, while enhancing software trust and regulatory compliance.

Overall mission

01



TO PROTECT CONSUMERS
AGAINST S&P
CYBERTHREATS

02



TO ENSURE TRANSPARENT,
SECURE AND REGULATORY
COMPLIANT DIGITAL
PRODUCTS

03



TO FOSTER S&P-BY-
DESIGN SOFTWARE BY
SUPPORTING STANDARDS
AND CERTIFICATION
METHODS

Collective intelligence for Computer Emergency Response Teams (CERTs) and Authorities in collaboration with citizens, Chief Information Security Officers (CISOs) and Data Protection Officers (DPOs) to ensure and audit that digital products and their S&P practices are transparent, secure and in compliance with regulation.

User-friendly tools to protect consumers against S&P cyberthreats (attacks, abusive practices and inappropriate behaviours of digital services) to enable them to better **understand, control, detect and respond to S&P threats and attacks** in a timely manner, as well as configuring their own S&P protection settings.



Knowledge to foster S&P-by-design in software engineering by supporting developers and digital service operators with standards and certification methods for compliance with the European S&P regulation..

Outcomes – The TRUST aWARE dashboard



Privacy Adviser

The Privacy Adviser helps you understand information about your privacy from Android applications, so you can make more informed decisions about your privacy. It simplifies privacy-related documents and allows you to find the most important information within these documents. The tool also provides some recommendations to avoid any potential privacy implication and risk.

[Check it out](#)



Security Analysis

The Security Analysis helps you check the security of files and websites. For files you will be informed if they are malicious or potentially unwanted. For websites you will be informed whether it is clean, used for malicious purposes, or not suitable for specific categories of the users.

[Check it out](#)



Ad Analysis

The Ad Analysis gives you information about the advertisement that you receive on Facebook and YouTube. It shows you why advertisers target you with their ads. It also lets you block advertisers on Facebook when you do not want to see their ads.

[Check it out](#)



Resources

The Resources section gives you access to both basic as well as in-depth information about how to protect your security and privacy online.

[Check it out](#)



Outcomes – The TRUST aWARE MISP



/login

TRUSTaWARE: Enhancing Digital Security, Privacy and TRUST in software.



MISP
Threat Sharing

Login

Email

Password

Login

Potential privacy and security issues in the Android app Calculator version 8.0 (387657499)

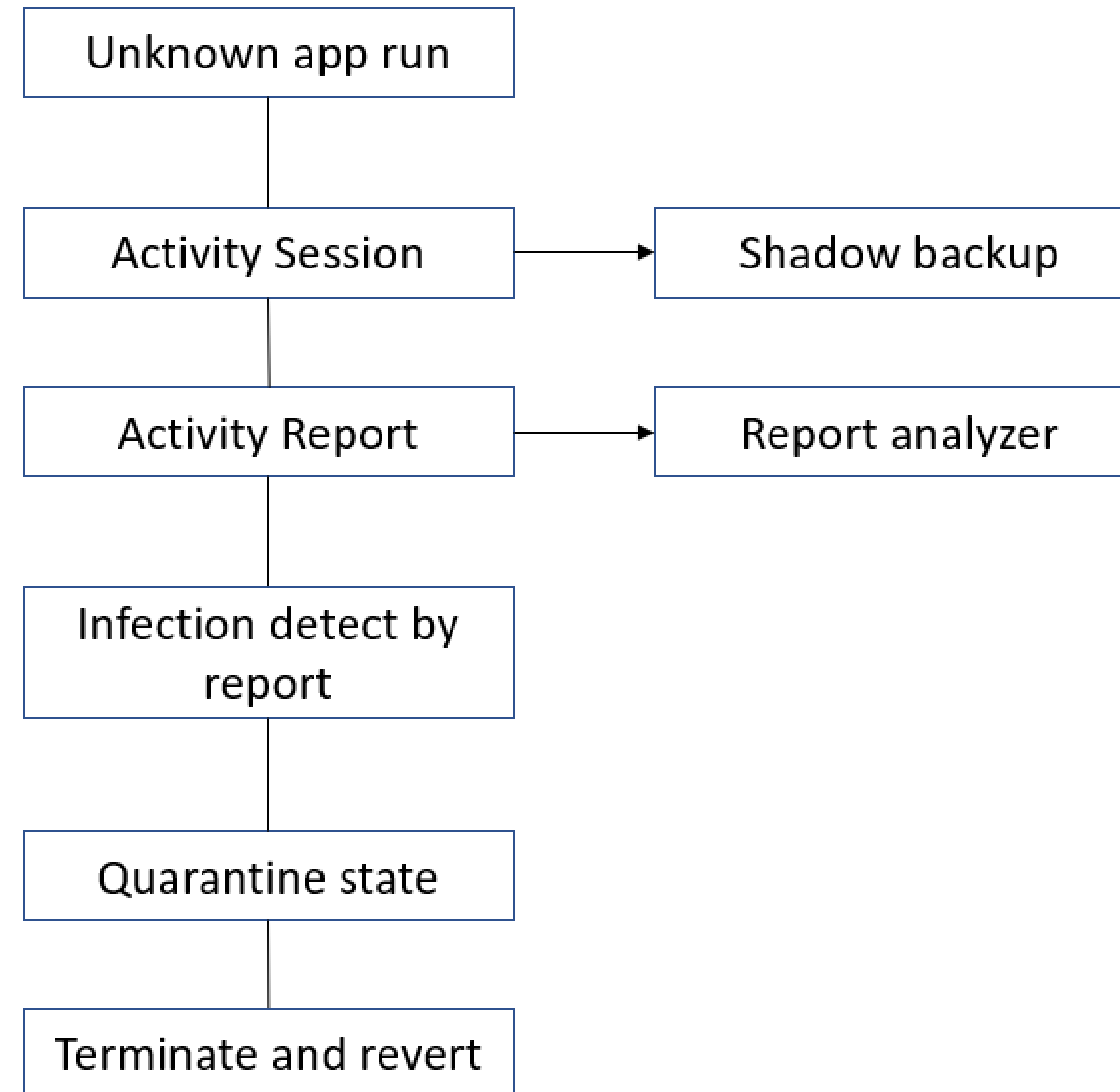
Event ID	111935
UUID	b136796b-15b6-4a1a-a17d-9bb1f1787fef
Creator org	TRUST aWARE
Creator user	api@api.test
Protected Event (experimental)	Event is in unprotected mode.
Tags	Malware analysis, Privacy analysis, Static analysis, Dynamic analysis, MALWARE, privacy, Android, Security Risk, app, Privacy issue, Data leak, PII, Data breach, Personally Identifiable Information, s_p-threats:info-dissemination="breach-of-confidentiality", s_p-threats:info-processing="exclusion", s_p-threats:info-processing="identification", s_p-threats:info-processing="insecurity", s_p-threats:info-processing="secondary-use", s_p-threats:info-collection="external-surveillance", s_p-threats:compliance="not-complying-with-individual-rights"
Date	2023-08-09
Threat Level	High
Analysis	Initial
Distribution	All communities
Published	No
#Attributes	206 (0 Objects)
First recorded change	2023-08-09 10:17:29
Last change	2023-08-09 10:17:29
Modification map	
Sightings	0 (0) - restricted to own organisation only.

—Pivots —Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports —Attributes —Discussion

x 111935: Potential p...



Outcomes – The TRUST Activity Monitor



Technical challenges



- 1 A **Digital S&P Analysis Lab** (DS&PA Lab) will provide digital S&P assessment capabilities longitudinally and at scale to gain **behavioural intelligence on S&P risks in digital products** used by regular users (applications, websites, and browser extensions).
- 2 **Digital S&P Enhancing Tools (S&PETs) for end users** augmented with the intelligence generated in the **DS&PA Lab** to identify a wider spectrum of risks
- 3 **Collective S&P Cyber Threat Intelligence (S&PCTI) for stakeholders**, building bridges between **citizens, organisations, CERTs, DPAs, and developers.**



Socio-technical challenges



1

Build on a multidisciplinary analysis of the framework conditions that determine the various S&P risks faced by EU citizens, addressing **technical, social, economic, ethical, standardisation, regulatory** and **legal aspects**. These are critical for informing the different software engineering stages (from design to production) towards the assurance of impact and adoption of TRUST aWARE's solutions. Additionally, this process will allow us to obtain evidence and insights for informing the cyberthreat, standardisation, and regulatory debates and efforts.

2

Develop a user-centric co-creation and evaluation process, with users and stakeholders involved for assuring the impacts of TRUST aWARE in **operational environment** (Technology Readiness Level: **TRL-7**). User-driven pilots will enable a continuous feedback loop. As TRUST aWARE will provide **tools for all citizens**, including vulnerable groups, our pilots will consider gender balance and diverse population groups, with specific focus on **minors** (<18 y/o), where special S&P protection is required; and **elderly** (>65 y/o), who often lack digital skills.

3

Perform cross-disciplinary actions in a holistic manner for assuring **impacts, sustainability and adoption**, fostering: **training** programs for citizens and stakeholders; **certification** methods (building on [Europrivacy](#)); liaison and contributions to relevant **standardisation** initiatives; and **exploitation** and **communication** actions.

Community engagement



Follow Us



www.trustaware.eu



@trustaware

