Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D7.11 / D65 Dissemination Plan (M3)

Published by the SAPPAN Consortium

Dissemination Level: Public

H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file:	D7.3.3 – Dissemination Plan
Document version:	1.0
Document owner:	Benjamin Heitmann (Fraunhofer FIT)
Work package:	WP7
Task:	
Deliverable type:	Report
Delivery month:	M3
Document status:	☒ approved by the document owner for internal review ☒ approved for submission to the EC

Document History:

Version	Author(s)	Date	Summary of changes made
0.1	Benjamin Heitmann (FIT)	23.07.2019	Outline and first draft
0.5	Benjamin Heitmann (FIT)	13.08.2019	First complete version to collect feedback.
0.6	Benjamin Heitmann (FIT)	15.08.2019	Incorporated feedback
1.0	Benjamin Heitmann (FIT)	19.08.2019	Finished version with all feedback and updates

Internal review history:

Reviewed by	Date	Summary of comments
Tanja Blascheck (USTUTT)	13.08.2019	Additions to USTUTT dissemination activities and small corrections.
Tomas Jirsik (MU)	14.08.2019	Additions to MU dissemination activities and small corrections.
Arthur Drichel (RWTH)	15.08.2019	Additions to RWTH dissemination activities and small corrections.
Josef Niedermeier (HPE)	15.08.2019	Update of HPE dissemination activities.
Alexey Kirichenko (FSC)	16.08.2019	Update of FSC dissemination activities.
Martin Zadnik (CESNET)	16.08.2019	Confirmation of CESNET dissemination activities.
Jacek Jonczy (DL)	19.08.2019	Update of DL dissemination activities.

Executive Summary

The dissemination and communication actions of SAPPAN will target at the following groups:

- Network operators and managers, in order to help them understand the additional capabilities offered by SAPPAN with respect to standard cybersecurity intrusion detection solutions.
- The research and development (R&D) community in academic, governmental and industry organizations, in order to make them aware of the different kinds of results from SAPPAN.
- Small and midsize businesses (SMEs), who might be interested in privacy-preserving outsourcing of cyber threat handling, as they lack the expertise and capacity to face modern cyber threats.
- The general public, in order to inform them of the improvements of network security which is enabled by the contributions of the SAPPAN project and how these contributions can be transferred to cybersecurity in general.

The foreseen channels include quick availability of the project deliverables on the web, publishing the project results on major journals and magazines, information spreading via various social media channels (such as LinkedIn and Twitter), participation at industrial fairs and holding workshops with interested stakeholders.

Table of Contents

1 Introduction

This document outlines the dissemination and communication plan of SAPPAN, and lists both the general approach of the consortium, as well as the individual plans of the partners.
Dissemination and communication is a horizontal activity of the SAPPAN project, in order to disseminate the concepts, vision, and results of the project. The dissemination activities will be organized with the aim of bringing the projects results to a broad public, transferring the methodology defined and experiences obtained throughout the project, informing society, and also promoting the commercial exploitation of the project's results and components.

The rest of this document is organized as follows: Section 2 describes the general approach of the project regarding the dissemination and communication. Then Section 3 lists the plans of each partner.

During the lifetime of the SAPPAN project, the dissemination plan will be updated at M12, M24 and M36.

2 General dissemination and communication plan

In this section we list the target groups, the communication channels and the metrics for evaluating our dissemination plan.

2.1 Target groups

The dissemination and communication actions of SAPPAN will target to the following groups:

Network operators and managers, in order to help them understand the additional capabilities offered by SAPPAN with respect to a standard cybersecurity intrusion detection solutions. This includes roles such as:

- Computer security incident response team (CSIRT) members.
- Security Operation Centre (SOC) members.
- Network Operation Centre (NOC) members.
- Administrators of National research and education networks (NREN).

The research and development (R&D) community in academic, governmental and industry organizations, who might be interested in or dealing with cybersecurity, intrusion detection, and specifically response and recovery actions. The aim will be to make them aware of the different kinds of results from SAPPAN, which can be conceptual or theoretical contributions, as well contributions implemented in software. This includes roles and interests such as:

- Academic or governmental institutions.
- Cybersecurity and privacy practitioners and researchers.
- Visualization practitioners and researchers.
- ICT professionals.
- Students interested in theory and applications of public SAPPAN results.

Small and midsize businesses (SMEs), who might be interested in privacy-preserving outsourcing of cyber threat handling, as they lack the expertise and capacity to face modern cyber threats. The aim will be to make them aware of the SAPPAN results and to involve them in potentially incorporating those results as part of existing or newly emerging solutions or products. This includes the following types of companies:

- Cybersecurity industry.
- Small and midsize companies (SMEs).

The general public, in order to inform them of the progress of SAPPAN, regarding the improvement of network security which is enabled by the contributions of the project and how the contributions can be transferred to cybersecurity in general. This includes roles and interests such as:

- Broader public with technical background.
- Developers as well as non-technical stakeholders.

2.2 Communication channels

The project aims to achieve its dissemination and communication objectives by appropriately using a mixture of channels.

- **Project web site:** A web site will be available to collect and make public all the information related to the project. The web site will allow subscribing to a newsletter which will be used to inform interested persons of new developments with regards to the project. The web site will be described in a separate deliverable. Each partner will use its own web site to include updated information about the SAPPAN project and provide a link to the SAPPAN web site.
- **Workshops, conferences, publications:** The SAPPAN project and its results will be presented in conferences or events related to topics such as cybersecurity, privacy, data mining, machine learning, visual analytics, visualisation and general ICT. The events can be at a national, European or world-wide level.
- **Dedicated SAPPAN workshops**: SAPPAN will organize several dedicated workshops addressing various CSIRT teams from governmental, commercial and academic environments. In addition, a final event will be organized for presenting the final results of the project and state the future opportunities for upscaling to the community.
- **Commercial fairs:** We are targeting the dissemination of the project results in commercial fairs, where industrial partners with an interest in using the project results are reachable.
- **Social media:** We expect that our presence on social networks will be mainly targeted to professional networks, such as LinkedIn and Twitter, as our target audience is rather specialized.

The following key performance indicators (KPIs), related to the dissemination/communication campaign, will be targeted by the SAPPAN consortium:

Communication activities	Measurement of results
Web site of the project The web site of the project where all relevant information will be presented, including the goals of the project, public deliverables, promotional material, links to events related to the project. The web site will be available for at least ten years after completion of the project.	Project web site is publicly available after month 4.
Events and presentations Presentation of results in research and business forums and other corporate events.	At least 5 events to foster new requirements from stakeholders and to inform them about the results of the project. The consortium will prepare a final event to present the results of the project. We will invite representatives of

	both public and private organizations as well as EU Commission representatives.
Publications The publication of articles and newsletters in specialized and general press about the objectives and the results of SAPPAN. We will present the results in relevant business and technological development fairs and produce journal papers in relevant peer reviewed journals, conferences and workshops.	At least 6 publications in specialized scientific publication channels, 2 publications in more general press, and 4 technological fairs.
Active presence in Social networks Information about the project will be diffused through the principal social network accounts of the members of the consortium and other specific accounts of the project e.g. in LinkedIn and Twitter. The information shared will be about objectives, progress and information about events, advisory board activities or participation of end-users. There will also be a GitHub organization to maintain artefacts which will be made publicly available.	Creation of specific accounts for the SAPPAN project on social media outlets. We aim at getting a following on Twitter of over 500 users and over 200 members on our LinkedIn Group. The GitHub organization must have all source code which is made publicly available.

3 Individual plans of the project partners

This section describes the initial dissemination and communication plans of each partner.

3.1 CESNET

3.1.1 Meetings and events

Objective:

To spread knowledge about SAPPAN and its results to European network security community from governmental and academic sector, for example, GÉANT TF-CSIRT meeting and GÉANT Symposium.

Target audience:

Network operators and managers, such as CSIRT teams, network administrators of NRENs and academic institutions.

3.1.2 Workshops

Objective:

To provide hands on experience or at least a demo of SAPPAN. CESNET organizes its own network security workshops which are attended by academic as well as industry members. CESNET plans to hold at least 2 dedicated SAPPAN workshops.

Target audience:

Network operators and managers, such as CSIRT members, members of Security Operation Centre (SOC), members of Network Operation Centre, administrators.

3.1.3 Conferences

Objective:

To publish results of research and development activities, for example, at TNC conference, IMC, QuBit.

Target audience:

Research and development community and network operators from the NREN community.

3.1.4 Internet multimedia

Objective:

To spread knowledge about SAPPAN to broader public interested in computer science, for example, via root.cz, lupa.cz.

Target audience:

Broader public with technical background

3.2 F-Secure

3.2.1 Conferences and fairs

Objective:

Presenting SAPPAN work at conferences on practical security, such as Virus Bulletin Conference and AVAR International Anti-Virus Security Conference.

Target audience:

Research and development community and interested businesses from the cybersecurity domain.

3.2.2 Internet blog

Objective:

Operating a security weblog regularly (https://labsblog.f-secure.com/).

Target audience:

Research and development community, such as ICT professionals and the general public with an interest in cybersecurity

3.3 FIT

3.3.1 ICT Scientific Publications and ICT Conferences

Objective:

Publications in venues like the Association for Computing Machinery (ACM), one of the largest international associations related to the field.

Target audience:

Research and development community, in the domains of security and privacy.

3.3.2 Commercial Fair

Objective:

Commercial fairs such as the Hannover Messe, an important commercial fair in Europe in the area of ICT (Hannover, Germany).

Target audience:

Security practitioners and businesses interested in training in the scope of the project.

3.4 HPE

3.4.1 Conferences and fairs

Objective:

Presentations on: QuBit - cybersecurity conference in Prague, Atlantech - Ireland ICT conference.

Target audience:

Cybersecurity community, Industry security practitioners in HPE and Ireland

3.4.2 Meetings and events

Objective:

Meetings with academic and industry in Ireland to spread knowledge about the SAPPAN project and its principles.

Target audience:

Academic (Insight, NUIG,GMIT, AIT, LYIT) and industry sector in Ireland.

3.4.3 Teaching and training activities

Objective:

Trainings for Advanced thread and Cyber Defence Center teams about SAPPAN principles and architecture, capabilities and use.

Target audience:

HPE cybersecurity practitioners

3.5 MU

3.5.1 Scientific publications and conferences

Objective:

Publication on IEEE or ACM Conferences focused on network and cybersecurity, and data analysis.

Target audience:

Security practitioners, CSIRT teams, and researchers

3.5.2 Teaching and training activities

Objective:

Knowledge transfer by supervision of BSc and MSc students, as well as new educational content for a practical course on IT Security.

Target audience:

Students interested in theory and applications of public SAPPAN results.

3.5.3 Meetings and events

Objective:

To spread knowledge about SAPPAN and its results to European security community, governmental and academic sector, and CSIRT community, for example at TF-CSIRT meetings.

Target audience:

CSIRT teams, governmental institutions, academic institutions

3.6 RWTH

3.6.1 Scientific publications

Objective:

Publication in security and privacy related conferences/journals such as Proceedings on USENIX Security or IEEE Symposium on Privacy Enhancing Technologies.

Target audience:

Security and privacy researchers

3.6.2 Teaching and training activities

Objective:

Knowledge transfer by supervision of BSc and MSc thesis students, as well as new educational content for a practical course on IT Security.

Target audience:

Students interested in theory and applications of public SAPPAN results

3.7 USTUTT

3.7.1 Scientific publications

Objective:
Publication in visualization or visual analytics related conferences/journals like IEEE VIS, EuroVis, PacificVis, VizSec, "IEEE Transactions on Visualization and Computer Graphics" and "Computer Graphics Forum".

Target audience:

Visualization researchers

3.7.2 Teaching and training activities

Objective:
Knowledge transfer by supervision of B.Sc. and M.Sc. theses.

Target audience:

Students interested in visualization, visual analytics and/or cybersecurity as an application field

3.8 DL

3.8.1 Conferences

Objective:
To spread knowledge about the theory behind privacy preserving attack neutralization and practical examples of the problems solved by SAPPAN at technical information security conferences across Europe and worldwide.

Suitable platforms for this purpose include but are not limited to:

- Dreamlab's South American Conference 8dot8, see https://www.8dot8.org/.
- OWASP Security Conference, https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference.

Target audience:

ICT Customers, Information Security Researchers, Cyber Security Professionals

3.8.2 Sharing with Product partners

Objective:

Knowledge Sharing with Product partners, and thereby leveraging a larger network of customers and end users.

Target Audience:

Cyber Security Professionals, ICT Customers.