Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D7.14 Dissemination Plan and Reports (M36)

Published by the SAPPAN Consortium

Dissemination Level: Public

H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file: D7.14 Dissemination Plan and Reports – M36
Document version: 1.0
Document owner: Mehdi Akbari Gurabi (FIT)

Work package: WP7
Task: T7.3
Deliverable type: Report
Delivery month: M36
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	Mehdi Akbari Gurabi (FIT)	2022-04-07	Preliminary document outline
0.2	Mehdi Akbari Gurabi (FIT)	2022-04-22	Incorporation of partners' input
0.3	Mehdi Akbari Gurabi (FIT)	2022-04-27	Ready-to-review version
0.4	Mehdi Akbari Gurabi (FIT)	2022-04-29	Application of the reviewers feedback
1.0	Mehdi Akbari Gurabi (FIT)	2022-04-30	Ready for submission

Internal review history:

Reviewed by	Date	Summary of comments
Milan Cermak (MU)	2022-04-28	Content enhancement suggestions, partially grammar and spelling check
Avikarsha Mandal (FIT)	2022-04-29	Structure improvement and content enhancement suggestions

Executive Summary

This report is the follow-up version of previous the dissemination plan and reports D7.12 and D7.13. This report not only focuses on the dissemination and communication report on the third year of the project but also mentions the future plans for activities after the project ends. These include, for example, further publications and communication via social media and the project website to gain the attention of the target audience about the final results of the project, without going deep into scientific or technical details.
In the previous reports the following points are covered:

- Target groups of dissemination and communication actions of SAPPAN
- Individual plans of the project partners include:
  - Conferences
  - Fairs
  - Internet presence
  - Meetings and events
  - Publications
  - Teaching and theses supervision
  - Workshops
- Summary of dissemination and communication goals
- Report on finished and planned dissemination activities per project partner for the first year of the project
- Update the dissemination plan influenced by COVID-19 and address mid-term review feedback
- Refinement of dissemination and communication KPIs

The dissemination and communication plan of SAPPAN includes the availability of project concepts, results, news, and deliverables on the project website, publication of research results in related journals and conferences, visibility in the general press and technical fairs, participation and presentation of SAPPAN results in related events, organization of workshops, as well as spreading information to target audiences via social media channels such as Twitter and YouTube. The current iteration of the deliverable is a report on updates of progress on dissemination and communication activities during the third year of the project. It also includes an overview of the achieved KPIs to monitor the project achievements with regard to dissemination and communication objectives.

Table of Contents

1 Introduction

Dissemination of the results is a key point to show the progress of a project. SAPPAN consortium members are committed to enabling it. The goal of a regular dissemination plan and report during the project lifetime is to ensure that the project's vision, activities, and outcomes are widely recognized and realised from a scientific, technological, and commercial point of view, as well as among potential end-users. Some of the main objectives of the dissemination and communication tasks are presentations at special events such as national or international conferences, dissemination of digital marketing materials, the establishment of communication channels such as social media, maintenance and refinement of the project website as the key dissemination and communication channel to show the objectives and results of SAPPAN to increase the impact of the project.

This document lists the dissemination and communication plan of SAPPAN and reports on the dissemination tasks carried out until the end of the project, both for the general approach of the consortium and for each partner, separately. This report not only focuses on dissemination but also presents communication activities. Dissemination and communication are horizontal activities of the SAPPAN project to spread the concepts, vision, objectives and results of the project. This document is the third follow-up to the original dissemination plan from M3 (deliverable D7.11) and the third annual report on dissemination and communication activities after deliverables D7.12 and D7.13.

As follows, section 2 describes the changes to the dissemination plan in general, section 3 lists the completed, ongoing, and planned activities by each partner in the third year of the project. Further, section 4 focuses on the project's general approach to dissemination and communication, plus a report on third-year dissemination activities, and section 5 overview the dissemination and communication activities and KPIs for the entire project lifetime.

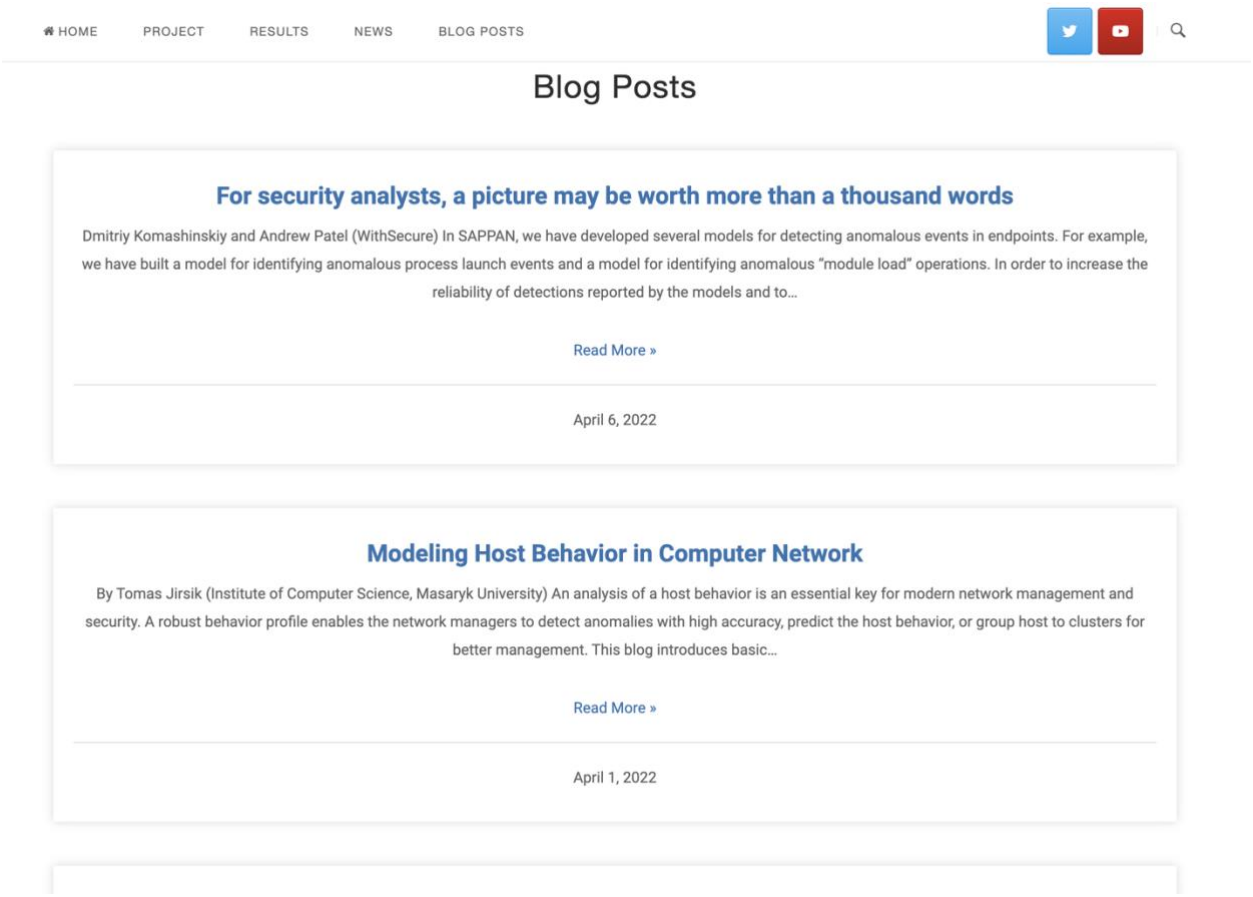
2 Updates on the Dissemination Plan

2.1 Influence of the pandemic on dissemination

We planned to disseminate the results through the symposiums, meetings, conferences, workshops and fair trades where the partners often participated in different dissemination forms such as demos. As in the second year of the project, the situation has continued due to COVID-19 restrictions in the third year. Many of the events were cancelled or only were organized remotely. Therefore, we increase our effort to disseminate results through publishing the results in scientific and promotional publications with the relevant audience (such as ARES, PST, IEEE TNSM journal, ERCIM news, and blog posts) and organizing and participating in virtual events such as webinars and online workshops. The COVID-19 restrictions also resulted in lower spending from the dissemination-related budgets and shifted our planned physical events, such as the final stakeholder event, to virtual events. However, the COVID-19 restrictions were slowly reduced at the end of the project. Therefore, we again participated in on-site events.

2.2 Blog posts and webinars

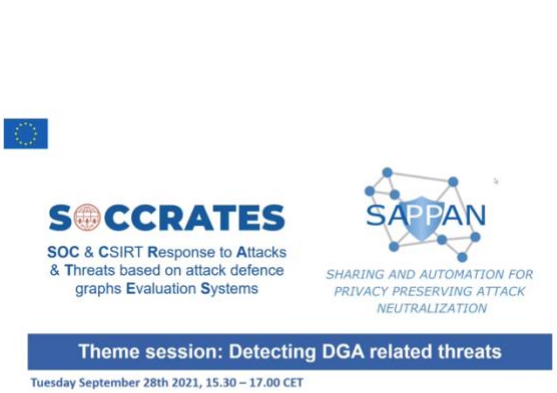
As we revisited the formulation of the dissemination strategy of the SAPPAN project in the previous iteration of the report to address the project mid-term review and advisory board feedback and increase the visibility of the project via more publications and remote events, we decided to push for regular blog posts based on our deliverables and project results. These blog posts aimed to target more general audiences than the technical deliverables. The goal of having eight blog posts until the end of the SAPPAN project has been achieved. It includes seven blog posts in the SAPPAN blog post series, plus two blog posts by F-secure and one blog post by Dreamlab in their communication channels. Additionally, we plan to publish two more blog posts in May.



Organising joint webinars with other EU projects was another target that we wanted to fulfil in the third year of the project. We had a joint webinar with the SOCCRATES EU project on the innovations in DGA detection. Also, the SAPPAN project was presented in a roundtable on the cluster topic Threat Intelligence in Cyberwatching webinar: Shaping the future of cybersecurity. Moreover, we participated in a promotional event with a talk in the HPE WiS group (Women in Security) webinar. A detailed description of the events is reported in D7.9 Report on Information and Presentation Materials - M36 deliverable. Also, the information about the events is available on the SAPPAN website via the following links:

- https://sappan-project.eu/?p=1226
- https://sappan-project.eu/?p=2060
- https://sappan-project.eu/?p=2115

The following pictures represent the webinar events.



2.3 Addressing midterm review feedback

After the project midterm review, we focus on the incorporation of the dissemination- and communication-related feedback into our dissemination plan. We revisited the dissemination KPIs and refined them in the previous version of this report (D7.13) to address feedback and pandemic-related restrictions. We list the KPI evaluations in the last section of this report. In the following table, the feedback points in the M18 review and a highlight of the corresponding actions are shown:

Review feedback	Actions taken
More effort should be devoted to dissemination, especially in the form of journal papers. Also, it would be good to have more data about the planned publications, apart from the specific topics.	• The planned publications have been addressed in D7.13 and the current document. • We have 18 scientific peer-reviewed publications in journals or the proceedings of peer-reviewed conferences or workshops. • We plan to publish a joint journal paper regarding SAPPAN innovations (currently work in progress). • We listed our different forms of non-scientific publications such as blog posts.

The project website should become one of the main tools for dissemination. The aggregated statistics about the website, including the number of visitors should be provided.	• Public deliverables have been made accessible on the project website after they were approved as part of the M18 midterm review. • Further public deliverables will be uploaded on the website after EC approval. • The website has been constantly updated to distribute information about the project, consortium members, objectives, events, datasets, and publications. • Monthly blog posts are published on the website. • The website has been promoted on various occasions. • The website's aggregated statistics are available via the Matomo web analytics tool.
Apart from the reports on the current progress and contributions of each consortium member, it is worthwhile to have more data on collaboration among partners.	• Dissemination and communication-related collaborations are mentioned in this document. (E.g., joint publications, NG-SOC workshops, standardisation workshop, SOCCRATES-SAPPAN webinar)
To meet the objectives defined in the EU Commission's gender equality strategy, some specific actions should be defined to promote gender equality in research and innovation in cybersecurity.	• A "Girls' Day" has been hosted at the University of Stuttgart to introduce the next generation of female computer science researchers to topics related to cyber security. • An interview with a SAPPAN member for International Women's Day 2021 has been promoted. • We promote gender equality information from EC and other projects through the SAPPAN Twitter account (E.g., International women's day 2022). • HPE prepare a talk for the Women in Cyber webinar (for junior high school girls in Ireland).
More engagement with the wider community of stakeholders (end-users, business, innovators/SMEs, policy-makers, ...) would be convenient.	• A SAPPAN End-User Committee has been assembled, consulted and involved in the KPI evaluation. • A final SAPPAN stakeholder event has been organised. • Publication of two articles in ERCIM News, which featured special themes relevant to the SAPPAN target group (No. 126: Privacy-Preserving Computation, No. 129: Fighting Cybercrime). • We participated and presented SAPPAN results in the events such as TF-CSIRT, Slush and Swiss Cyber Security Days with relevant target groups.
Despite the good results, there is a risk that little impact will be made outside of the industrial partners of the consortium. As opposed to many other research projects, SAPPAN actually has a very compact target group, (European) analysts working in SOCs. Such a well-defined group with an even smaller number of Enterprises employing them could be efficiently and effectively reached by even simple measures like newsletters or social media.	• Various dissemination and communication events have been hosted. This also includes a final SAPPAN event. • The NG-SOC workshop was hosted in 2020 and 2021 as a joint effort of the SAPPAN and SOCCRATES consortia. • The NG-SOC workshop will be hosted in 2022 after the project. • Monthly blog posts have been published on the SAPPAN project website to further disseminate SAPPAN results. • Continuous activity on social media (especially Twitter). • Participation in industrial-focused events such as TF-CSIRT, Slush and Swiss Cyber Security Days.

3 Organization-specific Report of Dissemination Activities (M25-M36)

In the following subsections, the list of finished activities in the third year of the project by each partner is provided via bullet points, followed by a list of ongoing or planned activities after the end of the project.

3.1 CESNET

Dissemination activities

- Publishing and presentation of R&D results at ARES conference 2021
- Publishing 2 SAPPAN blog posts
- Presenting SAPPAN standardization effort regarding playbooks at 2nd Joint Workshop – Dynamic Countering of Cyber-attacks
- Presentation at the Final SAPPAN event
- Publishing three conference papers in the reporting period
- A joint publication (with Fraunhofer and CESNET) in ERCIM news 129
- Presenting the results in person at NOMS 2022 conference

Plans for dissemination activities after the project

With lowering COVID-19, we plan to participate more in the community workshops as before COVID such as CESNET days, TF-CSIRT, and GEANT symposiums. Also, a joint paper will be published with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal). Moreover, CESNET will submit and present papers summarising project results at relevant conferences:

- ACM Internet Measurement Conference 2023,
- Passive Active Measurement Conference 2023,
- Network Operations and Management Symposium 2023.

3.2 Dreamlab Technologies

Dissemination activities

- Participation in the MITRE Africa / EMEA conference detailing the utilization of MITRE in SAPPAN and introducing SAPPAN to a wider audience of security professionals in Africa: https://www.youtube.com/watch?v=f-SQptd5O4w
- Participation at the NG-SOC 2021 with a specific talk "Taking a look at the *.ch zone with a DGA detector", detailing some results of the effort to adapt general DGA detection models for language-specific domains.
- A blog post disseminated on Dreamlab's website: https://dreamlab.net/en/blog/post/detecting-suspicious-ch-domains-using-deep-neural-networks/
- An introduction to SAPPAN to a larger audience of vendors, security professionals and customers, by presenting SAPPAN at the Swiss Cyber Security Days 2022 - the largest cyber security event in Switzerland: https://scsd365.app.swapcard.com/widget/event/scsd-2022/planning/UGxhbm5pbmdfODcxMDE4
- Publishing a blog post for SAPPAN
- A joint publication (with Fraunhofer and CESNET) in ERCIM news 129

Plans for dissemination activities after the project

A joint paper will be published with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal).

3.3 Fraunhofer FIT

Dissemination activities

- Maintenance and continuous updates of the SAPPAN website
- Continues updates about the project on social media (Twitter, YouTube, LinkedIn)
- Promoting important events such as the final stakeholder event via Fraunhofer FIT communication channels
- Establishing the SAPPAN blog post series
- Co-organising and chairing the NG-SOC 2021
- Presenting SAPPAN in a roundtable on cluster topic Threat Intelligence, cyberwatching webinar: Shaping the future of cybersecurity
- Publishing a conference paper in collaboration with RWTH
- Presenting a conference paper results in PST 2021 (Available on SAPPAN YouTube Channel: https://www.youtube.com/watch?v=5NUywNi1nzQ)
- Publishing an article in ERCIM news 126 with the special theme "Privacy Preserving Computation": Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery
- Publishing an article in ERCIM news 129 with the special theme "Fighting Cybercrime" (In cooperation with CESNET and Dreamlab): From Collaboration to Automation: A Proof of Concept for Improved Incident Response
- A SAPPAN introduction talk in a joint SOCCRATES-SAPPAN webinar session
- A SAPPAN project presentation on the 2nd Joint Workshop - Dynamic Countering of Cyber-attacks
- Co-organising and chairing the final SAPPAN event

Plans for dissemination activities after the project

- Co-organisation of NG-SOC 2022 with SOCCRATES and CyberSEAS projects in conjunction with ARES 2022 conference: https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2022/
- Further publications are planned for:
  - Short string encoding and hardening approaches for bloom filters
  - A joint paper with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal)
  - A paper on Semantic modelling and formalization of cyber security incident response and Incident response vocabulary
  - A paper on the SAPPAN playbook capturing tool
- Publish an article in regards to SAPPAN results in the Fraunhofer yearly report 2022

3.4 WithSecure™ (Formerly F-Secure)

Dissemination activities

- A talk on NG-SOC 2021 (at ARES 2021): Combining Anomaly Detection Models for More Reliable Attack Detection, by Dmitriy Komashinskiy (slides: ARES_Workshop_slides_2021_final.pdf)
- Presentation on ECSO CYBER INVESTOR DAYS (SLUSH 2021 SIDE EVENT, 1-2 December 2021): CYBERSECURITY INNOVATION IN THE NORDICS, by Janne Pirttilahti
- Final SAPPAN event:
  - Keynote by Mikko Hyppönen
  - Response Recommendation and Automation, David Karpuk as a co-presenter
- Publishing a blog post for SAPPAN ("For security analysts, a picture may be worth more than a thousand words", https://sappan-project.eu/?p=1699)
- Promoting the SAPPAN blog post by presenting it in the ECSO Awareness Calendar: https://www.ecs-org.eu/documents/publications/6256822ca926c.pdf

Plans for dissemination activities after the project

- NG-SOC 2022 (at ARES 2022): a talk on the use of provenance graphs for presenting detected security-related anomalies of various types and connections among those
- A joint paper with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal)

3.5 Hewlett Packard Enterprise

Dissemination activities

- Presentation on HPE Security Summit (8-10 November 2021): Big Data Processing for Cybersecurity: How we Aggregate and Enrich Fortinet Syslog Events
- Presentation on HPE TechX Forum (29th July 2021): Data Staging Platform: How we Aggregate and Enrich Fortinet Syslog Events
- Talk in the final SAPPAN event: SAPPAN DGA innovations
- Presentation on HPE WiS group (Women in Security) webinar organised by the CodePlus project: professional paths towards Computer Science careers, including involvement in the SAPPAN project

Plans for dissemination activities after the project

There are no future plans for dissemination at this time.

3.6 Masaryk University

Dissemination activities

- Creation of several tweets on activities on SAPPAN at the CSIRT-MU Twitter (https://twitter.com/csirtmu). These tweets were then redistributed by the SAPPAN Twitter account as soon as it was created.
- Participation (serving as TPC members) in the preparation of the proposal of the joint workshop with the SOCCRATES project - NG-SOC 2021, which was

accepted and was conducted in association with the 16th International Conference on Availability, Reliability, and Security (ARES 2021)
- Publishing a scientific paper in IEEE Transactions on Network and Service Management journal and a poster paper at the SECRTYPT conference (GRANEF: Utilization of a Graph Database for Network Forensics)
- Participation in International Workshop on Next Generation Security Operations Centers (NG-SOC 2021):
  - Chairing a session
  - Having a talk on Graph-based Network Traffic Analysis for Incident Investigation
- Presenting the SAPPAN results at several events:
  - 2022 TF-CSIRT Meeting & FIRST Regional Symposium Europe
  - 2nd Joint Workshop - Dynamic Countering of Cyber-attacks
  - Digital Forensic Research Workshop (DFRWS EU 2022) (28.3.-6.4.2022)
  - Graph-based network Security (GraSec) in conjunction with IEEE/IFIP Network Operations and Management Symposium NOMS 2022
  - Final SAPPAN event
- Publishing two blog posts on SAPPAN's website
- Networking activities and passive presenting of SAPPAN results: CyberSec&AI (4.-5.11.2021)

Plans for dissemination activities after the project

- Publish a blog post about datasets (network and host data) in the SAPPAN blog post series
- A joint paper with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal)

3.7 RWTH Aachen University

Dissemination activities

- Supervision of 2 finished bachelor theses
- Supervision of 3 finished master theses
- Five accepted scientific peer-reviewed conference papers:
  - First Step Towards EXPLAINable DGA Multiclass Classification (ARES 2021)
  - Finding Phish in a Haystack: A Pipeline for Phishing Classification on Certificate Transparency Logs (IWCC 2021)
  - Towards Privacy-Preserving Classification-as-a-Service for DGA Detection (PST 2021)
  - The More, the Better? A Study on Collaborative Machine Learning for DGA Detection (CYSARM 2021)
  - Sharing FANCI Features: A Privacy Analysis of Feature Extraction for DGA Detection (CYBER 2021)
- Three submitted conference papers currently under peer-review
- Talk in Joint SOCCRATES-SAPPAN webinar on detecting DGA related threats
- Talk in the final SAPPAN event

Plans for dissemination activities after the project

- Continuation of the supervision of bachelor and master theses
- Publish further articles in scientific peer-reviewed conferences based on knowledge gained over the course of SAPPAN
- Publish a blog post about application profiling in the SAPPAN blog post series
- A joint paper with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal).

3.8 University of Stuttgart

Dissemination activities

- Publishing two blog posts on the SAPPAN webpage to raise awareness about our project and the results in visualization for AI and analytic provenance for SOCs
- Preparation of several presentations for the end-user committee and the final stakeholder event
- One submitted conference paper currently under peer review: at ACM TiiS 2022 with the title Understanding Sensemaking for XAI Visualizations with Interaction Logs: An Online Study

Plans for dissemination activities after the project

- A joint paper will be published with SAPPAN consortium partners (Currently work in progress and to be submitted in a Journal)
- Further publication of SAPPAN results is planned for:
    - process tree visualisation
    - visual analytics system for analysis of similar incidents

4 General Dissemination and Communication Activities (M25-M36)

To improve our communication strategy, we came up with a plan described in the D7.13 deliverable. We regularly discussed these subjects at the consortium level to monitor the progress of the communication strategy and refined it whenever it was necessary during the project lifecycle.

4.1 Overview of general dissemination activities

We documented strategies regarding dissemination and communication activities in the previous iterations of the report. In addition to this, we have already carried out dissemination activities in the last year of the project, such as various in-house and public presentations about the SAPPAN project, which are listed above in the partner-specific section. Two joint workshops (NG-SOC 2021 with the H2020 project SOCCRATES, and 2nd Joint Workshop - Dynamic Countering of Cyber-attacks with several H2020 projects from the same call) were organised, for which various partners contributed to the events. At the end of the project, we organised a final SAPPAN event to share our interesting results with the stakeholders such as researchers, industrial stakeholders, policymakers, etc. We have continuously updated the project website, Twitter account, YouTube channel, and LinkedIn group to reach the interested public.

Also, publishing blog posts and presenting SAPPAN results in workshops and webinars are further dissemination and communication plans to increase the visibility of the project and reach identified target groups. We established a SAPPAN blog posts series intending to monthly publish our results on the website for more general audiences. We promote the blog posts via our Twitter and LinkedIn accounts. We also published two peer-reviewed news-style articles (ERCIM news) to reach a wider community of stakeholders such as scientific audiences, end-users, businesses, innovators, SMEs, and policymakers. ERCIM News is widely distributed in the European Commission and reaches about 10,000 readers. Moreover, the results have been published in 12 peer-reviewed scientific publications during the last year, which increase the number of our peer-reviewed scientific publications to 18 from the beginning of the project. Further works are currently under review or planned to be published later.

4.2 Communication activities

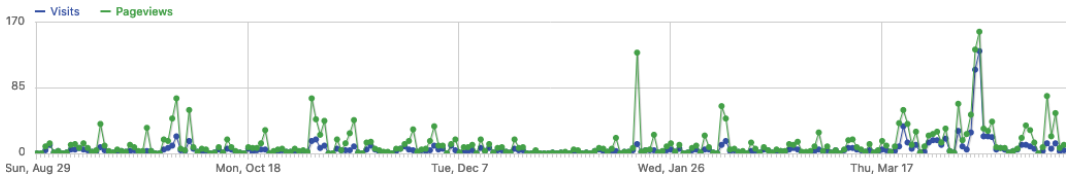
Communication activities, their goals and current progress are provided as follows. More details about presentation and dissemination materials are given in deliverable D7.9 which is the third year iteration of the *Report on Information and Presentation Materials*. Also, the progress on dissemination and communication KPIs are given in the following.

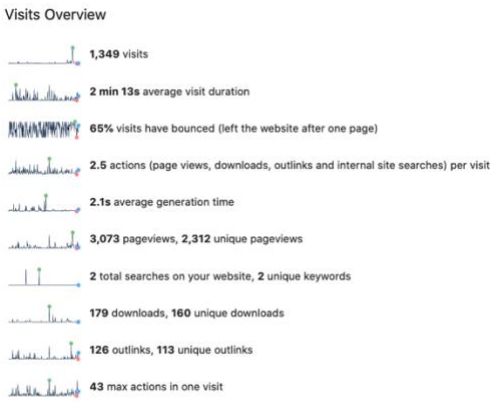
Project website

The website of the project gives a dissemination platform on which all relevant project information is presented, along with the objectives of the project, public deliverables after EC approval, publications and promotional material, as well as news and events associated with the project. We also established a blog post series with monthly updates available on the website.

The website is designed and has been online since the fourth month after the project started. The website is the key dissemination and communication channel of the project. It has been maintained continuously and updated with information on project progress, news, events, flyers, and results. The website will also be updated with the future results after the project's lifetime. All public deliverables with a due date until M18 have been approved by EC and are available on the website. Further public deliverables will be available online after the EC confirmation. Detailed information about the website updates is available in the D7.9 deliverable.

We also select a web analytics tool to monitor the visits to the website from the end of August 2021. It is available to address the EC mid-term review feedback by asking for aggregated statistics about the website, including the number of visitors. We have received over 3000 page views by 1300 visitors in the last eight months. It also leads to more than 175 downloads of the dissemination materials. The following figures show some aggregated statistics about website views. More information about the web analytic tool is available in the D7.9 deliverable.





Reflection of F-Secure rebranding

F-Secure confirmed the process of rebranding on the 22nd of March 2022 (Press release: https://www.withsecure.com/en/whats-new/pressroom/f-secure-corporate-security-relaunches-as-withsecure). From that time, the corporate security business of F-Secure has relaunched as a new brand that shares the company's new name WithSecure™. The launch of WithSecure™ follows plans announced in February 2022

to separate into two companies. WithSecure utilises a new logo, website, and communication channels. We reflect the changes such as the brand name, logo, and description of the partner on the SAPPAN website (E.g., https://sappan-project.eu/?page_id=763). However, in our reports, we constantly use F-secure (in abbreviation FSC) for the sake of consistency.

Events and presentations

By participating in the events we aimed to present SAPPAN results in research and industry forums and other events. SAPPAN overview, objectives and motivations have been presented at many in-house and external events such as three TF-CSIRT meetings, SAPPAN-SOCCRATES webinar, Swiss cybersecurity days, Cyberwatching webinar, the Slush event, and MITRE Africa/EMEA conference, as well as scientific presentation of conference papers in various conferences and workshops.

Further, for the second time, the 3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) was jointly organised by SAPPAN and SOCCRATES H2020 projects. It is held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021). NG-SOC 2022 also will take place after the end of the project. This time another H2020 project CyberSEAS will join SAPPAN and SOCCRATES in course of organising the event. The workshops' goal is to bring experts and researchers together in the field of Security Operation Centres (SOC) to identify and address major challenges and research-based solutions. NG-SOC 2021 also had a peer-review publication section with publication results in the proceeding of the ARES conference. SAPPAN members chaired two sessions and prepared three talks about the SAPPAN results. The following pictures represent the event's CfP. Detailed information about the event, its agenda, and SAPPAN presentations is provided in the deliverable D7.9.

ARES Conference
International Conference on Availability, Reliability and Security

SOCCRATES

SAPPAN

Call for Papers

3rd International Workshop on
Next Generation Security Operations Centers
(NG-SOC 2021)

to be held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021 – http://www.ares-conference.eu)

August 17 – August 20, 2021
All-digital Conference

Workshop Description

Organisations in Europe face the difficult task of detecting and responding to increasing numbers of cyber-attacks and threats, given that their own ICT infrastructures are complex, constantly changing (e.g. by the introduction of new technologies) and there is a shortage of qualified cybersecurity experts. There is a great need to drastically reduce the time to detect and respond to cyber-attacks. A key means for organizations to stay ahead of the threat is through the establishment of a Security Operations Center (SOC). The primary purpose of a SOC is to monitor, assess and defend the information assets of an enterprise, both on a technical and organizational level.

The aim of this workshop is to create a forum for researchers and practitioners to discuss the challenges associated with SOC operations and focus on research contributions that can be applied to address these challenges. Through cooperation among H2020 European projects, the workshop intends to provide a more comprehensive overview of the promising research-based solutions that enable timely response to emerging threats and support different aspects of the security analysis and recovery process.

The workshop is jointly organized by two H2020 projects: SOCCRATES (https://www.soccrates.eu/) and SAPPAN (https://sappan-project.eu/).

Moreover, the consortium co-organised and participated in the second joint standardisation workshop initiated by the CyberSANE H2020 project after the first workshop participation last year. The workshop is titled 2nd Joint Workshop - Dynamic Countering of Cyber-attacksProjects, Achievements and Standardisation. It aimed to gather the projects from the SU-ICT-01-2018 H2020 call, whose main topic is the Dynamic countering of cyber-attacks. SAPPAN was mainly responsible for involving ENISA and inviting the keynote speaker (Dr Ioannis Agrafiotis, Keynote: From Security Operations Centres (SOCs) to securing machine learning: opportunities to enhance cybersecurity in Europe) to the event in addition to five project-related talks. The following picture presents the event banner. In the deliverable D7.9, we provide more information about the event and SAPPAN presentations.

Additionally, at the end of the project, we prepared a final event to present the results of the project to the stakeholders. We invited representatives from both public and private organisations mainly from the EU. Also, we prepare a Flyer for the event and distribute the news about the event via Eventbrite, our website and organisation specific and project communication channels.

Meeting Subject	Final SAPPAN event
Venue	Online (Zoom)
Date	Monday 4.04.2022 14:00-16:30 (CEST)
Partners	Fraunhofer FIT, F-Secure, CESNET, RWTH University, HPE Ireland Masaryk University, Dreamlab Technologies, University of Stuttgart

It is our utmost pleasure to invite you to the **"Final SAPPAN event"**. SAPPAN is a Horizon 2020 project funded by the European Commission to enable efficient protection of modern ICT infrastructures via advanced data acquisition, threat analysis, visualisation, and privacy-aware sharing and distribution of threat intelligence aimed to dynamically support human operators in incident management. We are also very happy to introduce our keynote speaker Mikko Hyppönen (https://mikko.com/), who will give a talk on "STATE OF THE NET", followed by presentations about selected key results of SAPPAN.

The event will take place **virtually (Zoom)** on **Monday 4.04.2022, 14:00 - 16:30 (CEST).** We are looking forward to your participation.

Event Agenda:

Time	Subject	Speaker
14:00-14:05	Welcome	Fraunhofer FIT
14:05-14:35	Keynote: State of the NET	Mikko Hyppönen (F-Secure)
14:35- 15:00	Sharing New Type of Threat Intelligence and SAPPAN Standardisation Efforts	Martin Zadnik (CESNET)
15:00-15:25	SAPPAN Innovations in DGA Detection	Arthur Drichel (RWTH University), Hugo Hromic (HPE Ireland)
15:25-15:35	Coffee Break	--
15:35 - 16:00	Response Recommendation and Automation	David Karpuk (F-Secure), Martin Laštovička (Masaryk University), Mischa Obrecht (Dreamlab Technologies)
16:00 - 16:25	Opportunities for Visualisation Support in CyberSecurity	Robert Rapp, Franziska Becker (University of Stuttgart)
16:25- 16:30	Wrap Up	--

Our event on the Eventbrite has been reached around 279 times.

Traffic from Promotional Tools

Category	Page Views
Direct Traffic	279
Direct Traffic	279
TOTAL	279

The list of presentations is given in the *Presentations and Other Dissemination Materials* sub-section in the following, and the event agenda and more information about the presentations are available in D7.9.

Publications

The publication of articles and newsletters in specialized and general press about the objectives and the results of SAPPAN is one of the main communication and dissemination goals of the project. We present the results in relevant business and technological events and produce scientific papers in relevant peer-reviewed journals, conferences, and workshops. We currently have 18 peer-reviewed publications published in journals, high-rank conferences and workshop proceedings, and two peer-reviewed articles in the ERCIM news journal. We currently have four publications under peer review. Project partners have further plans for publications, mentioned in the partners-specific dissemination reports. All mentioned published papers are peer-reviewed and listed in the *Publication* section. They are also available on the project website. We also plan to collaboratively publish a journal paper about the general innovations in the SAPPAN project. This will have contributions from all partners. The effort regarding this publication is still ongoing. Moreover, a poster has also been presented in VizSec 2021. Also, technical blog posts and general press are and will be published regarding the project results on our website and relevant communication channels. Moreover, academic partners in the project successfully supervised 26 bachelor's and master's theses listed in the section *publications.* There are also four theses which are still ongoing.

Social media

Information about the project has been distributed through the social network accounts of the project members as well as our project-specific accounts on Twitter, YouTube and LinkedIn. The information shared is about objectives, progress, dissemination materials (E.g., SAPPAN blog post series), and information about events, and activities of the advisory board or end-users committee. We have an active Twitter account as the main social media communication channel, a closed group on LinkedIn, and a YouTube channel to publish our videos and presentations. So far, we have had more than 100 tweets and reached around 400 followers on Twitter.

4.3 Scientific publications

In this section, all the scientific peer-reviewed publications of SAPPAN results from this reporting period (M25-M36). Also, ongoing publications are listed in the *submitted and preprint papers* and finished and ongoing bachelor's and master's theses are recorded as follows in the *Bachelor's and Master's Theses* table.

Published papers

The following table represents all the scientific peer-reviewed publications of the project results in the third year of the project (M25-M36). In the current reporting period, we published 12 peer-reviewed papers, which increased the total number of our publications in the project lifetime to 18 peer-reviewed publications. We also published two peer-reviewed news-style articles in ERCIM news and one poster that we indicate as "other" types of scientific publications in the table.

Type of scientific publication	Title of the scientific publication	DOI/ ISSN/ eSSN	Authors	Title of the journal or equivalent	Publisher	Year of publication	Peer-review	Open access?
Scientific paper	On the Integration of Course of Action Playbooks into Shareable Cyber Threat Intelligence	10.1109/BigData52589.2021.9671893	V. Mavroeidis, P. Eis, M. Zadnik, M. Caselli and B. Jordan	IEEE International Conference on Big Data (Big Data)	IEEE	2021	Yes	Yes
Scientific journal paper	Predictive methods in cyber defense: Current experience and research challenges	10.1016/j.future.2020.10.006 ISSN: 0167-739X	M. Husák, V. Bartoš, P. Sokol and A. Gajdoš	Future Generation Computer Systems	Elsevier	2021	Yes	Yes
Scientific paper	Towards Evaluating Quality of Datasets for Network Traffic Domain	10.23919/CNSM52442.2021.9615601	D. Soukup, P. Tisovčík, K. Hynek and T. Čejka	17th International Conference on Network and Service Management (CNSM)	IEEE	2021	Yes	Yes
Scientific paper	Detection of https brute-force attacks with packet-level feature set	10.1109/CCWC51732.2021.9375998	LUXEMBURK, Jan; HYNEK, Karel; ČEJKA, Tomáš	2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)	IEEE	2021	Yes	Yes
Scientific paper	First Step Towards EXPLAINable DGA Multiclass Classification	10.1145/3465481.3465749	Arthur Drichel, Nils Faerber, Ulrike Meyer	The 16th International Conference on Availability, Reliability and Security (ARES 2021)	ACM	2021	Yes	Yes
Poster	Interactive process tree analysis Poster	-	Robert Rapp, Christoph Müller, Franziska Becker (USTUTT), Paolo Palumbo (F-Secure), Thomas Ertl (USTUTT)	2021 IEEE Symposium on Visualization for Cyber Security (VizSec 2021)	IEEE	2021	Yes	Yes
Scientific paper	Finding Phish in a Haystack: A Pipeline for Phishing Classification on Certificate Transparency Logs	10.1145/3465481.3470111	Arthur Drichel, Vincent Drury, Justus von Brandt, Ulrike Meyer	The 16th International Conference on Availability, Reliability and Security (ARES 2021)	ACM	2021	Yes	Yes

Type of scientific publication	Title of the scientific publication	DOI/ ISSN/ eSSN	Authors	Title of the journal or equivalent	Publisher	Year of publication	Peer-review	Open access?
Article	Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery	ISSN: 0926-4981	Lasse Nitz, Mehdi Akbari Gurabi, Avikarsha Mandal, Benjamin Heitmann	ERCIM News 126	ERCIM	2021	Yes	Yes
Scientific paper	The More, the Better? A Study on Collaborative Machine Learning for DGA Detection	10.1145/3474374.3486915	Arthur Drichel, Benedikt Holmes, Justus von Brandt, Ulrike Meyer	The 3rd Workshop on Cyber-Security Arms Race (CYSARM 2021)	ACM	2021	Yes	Yes
Scientific paper	Sharing FANCI Features : A Privacy Analysis of Feature Extraction for DGA Detection	10.48550/arXiv.2110.05849	Benedikt Holmes (RWTH), Arthur Drichel (RWTH), Ulrike Meyer (RWTH)	The Sixth International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2021)	IARIA XPS Press	2021	Yes	Yes
Scientific paper	Towards Privacy-Preserving Classification-as-a-Service for DGA Detection	10.1109/PST52912.2021.9647755	Arthur Drichel, Mehdi Akbari Gurabi, Tim Amelung, Ulrike Meyer	18th International Conference on Privacy, Security and Trust (PST 2021)	IEEE	2021	Yes	Yes
Scientific paper	GRANEF: Utilization of a Graph Database for Network Forensics	10.5220/0010581807850790 Electronic ISSN: 2184-7711	Milan Cermak and Denisa Sramkova	18th International Conference on Security and Cryptography	SCITEPRESS	2021	Yes	Yes (after registration)
Article	From Collaboration to Automation: A Proof of Concept for Improved Incident Response	ISSN: 0926-4981	Lasse Nitz, Martin Zadnik, Mehdi Akbari Gurabi, Mischa Obrecht, Avikarsha Mandal	ERCIM News 129	ERCIM	2022	Yes	Yes
Scientific paper	Towards Inference of DDoS Mitigation Rules	Not available yet	Martin Žádník	IEEE/IFIP Network Operations and Management Symposium	IEEE	2022	Yes	Yes

Type of scientific publication	Title of the scientific publication	DOI/ ISSN/ eSSN	Authors	Title of the journal or equivalent	Publisher	Year of publication	Peer-review	Open access?
Scientific paper	VITALflow: Visual Interactive Traffic Analysis with NetFlow	Not available yet	Tina Tremel, Jochen Kögel, Florian Jauernig, Sebastian Meier, Dennis Thom, Franziska Becker, Christoph Müller, Steffen Koch	International Workshop on Analytics for Network and Service Management (ANNET 2022)	IEEE	2022	Yes	Yes

Submitted and preprint papers

The table below lists the publications that are already submitted to high-ranked conferences with peer-reviewed proceedings which are are still under review, or preprint publications.

Name	Authors	Submitted to	Status
A Pipeline for DNS-based Software Fingerprinting	Sebastian Schäfer (RWTH), Ulrike Meyer (RWTH)	Networking 2022	under review
Accurate Real-Time Labeling of Application Traffic	Sebastian Schäfer (RWTH), Alexander Loebel (RWTH), Ulrike Meyer (RWTH)	LCN 2022	under review
Detecting Unknown DGAs without Context Information	Arthur Drichel (RWTH), Justus von Brandt (RWTH), Ulrike Meyer (RWTH)	ARES 2022	under review
Understanding Sensemaking for XAI Visualizations with Interaction Logs: An Online Study	Franziska Becker (USTUTT), Thomas Ertl (USTUTT)	ACM TiiS 2022	under review
Large Scale Measurement on the Adoption of Encrypted DNS	Sebastián García (Czech Technical University in Prague), Karel Hynek (Czech Technical University in Prague & CESNET), Dmtrii Vekshin (Avast), Tomáš Čejka (CESNET), Armin Wasicek (Avast)	*arXiv preprint* *arXiv:2107.04436*	*arXiv preprint* DOI: 0.48550/arXiv.2107.04436

Bachelor's and master's theses

The table below lists all the finished and ongoing bachelor and master theses related to the SAPPAN project supervised by academic partners in the period of this report (M25-M36). We supervised successfully nine more theses which increased the finished thesis to 26 in total. We also have four ongoing theses related to the project.

Name	Author	Type	Institute	Supervisor/ Advisor	Status (Ongoing/ Finished)
Process for Automated Threat Response to Phishing	Michal Čech	Master thesis	MU	Daniel Tovarňák	Finished
Adversarial Attacks and Defenses on DGA classifiers	Konstantin Kaulen	Bachelor thesis	RWTH	Ulrike Meyer, Arthur Drichel	Finished
Detection of new DGAs in the Multiclass DGA classification setting	Justus von Brandt	Master thesis	RWTH	Ulrike Meyer, Arthur Drichel	Finished
Distributed and Automated Network Traffic Generation of Applications with a Graphical User Interface	Paul Suetterlin	Bachelor thesis	RWTH	Ulrike Meyer, Sebastian Schäfer	Finished
Application Fingerprinting using Deep Learning based on Network Traffic	Raoul Offizier	Master thesis	RWTH	Ulrike Meyer, Sebastian Schäfer	Finished
Anonymization and Sharing of application-labeled Network Traces	Alexander Loebel	Master thesis	RWTH	Ulrike Meyer, Sebastian Schäfer	Finished
Detecting Obfuscated Scripts With Machine Learning Techniques	Mariam Pogosova	Master thesis	FSC	Dmitriy Komashinskiy	Finished
Graph-based Anomaly Detection in Network Traffic	Denisa Sramkova	Master thesis	MU	Milan Cermak	Finished
Graph-Based Analysis of IP Flows	Aneta Jablunkova	Bachelor thesis	MU	Milan Cermak	Finished
Visualization for Graph-based Analysis of Network Traffic	Tatiana Fritzova	Master thesis	MU	Milan Cermak	Ongoing
Graph-Based Analysis of Network Traffic and EDR Logs	Matus Jarkovic	Master thesis	MU	Milan Cermak	Ongoing
Development and Implementation of a Process Mining-Based Tool for Software Fingerprinting	Josef Ruffer	Master Thesis	RWTH	Ulrike Meyer, Sebastian Schäfer	Ongoing
Web-based Pipeline for Rule-based Application Fingerprinting	Johannes Reinartz	Bachelor Thesis	RWTH	Ulrike Meyer, Sebastian Schäfer	Ongoing

4.4 Presentations and other dissemination materials

In this section, we list all the presentations and technical posts regarding the SAPPAN dissemination in the third year of the project (M25-M36). This includes events such as the introduction and motivational talks about SAPPAN, presenting project results in NG-SOC 2021 workshops and 2nd joint workshop on dynamic countering of cyber-attacks, a joint SAPPAN-SOCCRATES webinar, a talk in a motivational webinar for gender equality in Ireland, a talk in cyberwatching webinar, and SAPPAN related technical blog posts on our partners' websites. It also includes a technical presentation

of our results in different scientific and industrial events, as well as, our final stakeholder event.

Name	Presenter	Event
Final SAPPAN Stakeholder Event (full video)	-	Final SAPPAN event, Monday 04.04.2022, 14:00 – 16:30 CEST
Opportunities for Visualisation Support in CyberSecurity	Franziska Becker, Robert Rapp (USTUTT)	Final SAPPAN event, Monday 04.04.2022, 14:00 – 16:30 CEST
Response Recommendation and Automation	David Karpuk (FSC), Martin Laštovička (MU), Mischa Obrecht (DL)	Final SAPPAN event, Monday 04.04.2022, 14:00 – 16:30 CEST
SAPPAN Innovations in DGA Detection	Arthur Drichel (RWTH), Hugo Hromic (HPE)	Final SAPPAN event, Monday 04.04.2022, 14:00 – 16:30 CEST
Sharing New Type of Threat Intelligence and SAPPAN Standardisation Efforts	Martin Zadnik (CESNET)	Final SAPPAN event, Monday 04.04.2022, 14:00 – 16:30 CEST
Final SAPPAN event keynote: State of the NET	Mikko Hyppönen (FSC)	Final SAPPAN event, Monday 04.04.2022, 14:00 – 16:30 CEST
Sharing and Automation for Privacy Preserving Attack Neutralization (SAPPAN) - Introduction, HIghlights, Results	Mischa Obrecht (DL)	Swiss Cyber Security Days 2022, 6-7 April, 2022
Toward Graph-Based Network Traffic Analysis and Incident Investigation	Milan Cermak (MU)	DFRWS EU 2022, 29th March - 1st April 2022
Malware Analysis Automation Platform	Martin Laštovička (MU)	2022 TF-CSIRT Meeting & FIRST Regional Symposium Europe, 2-3 March, 2022
SAPPAN Project Presentation: Standardization of cybersecurity playbooks	Martin Žádník (CESNET)	2nd Joint Workshop - Dynamic Countering of Cyber-attacks, 8th February 2022
SAPPAN Project Presentation: Response Recommendation Datasets	Willie Victor (FSC)	2nd Joint Workshop - Dynamic Countering of Cyber-attacks, 8th February 2022
SAPPAN Project Presentation: Automation of Malware Analysis Workflow	Martin Laštovička (MU)	2nd Joint Workshop - Dynamic Countering of Cyber-attacks, 8th February 2022
SAPPAN Project Presentation: Project Overview	Avikarsha Mandal (FIT)	2nd Joint Workshop - Dynamic Countering of Cyber-attacks, 8th February 2022
Towards Privacy-Preserving Classification-as-a-Service for DGA Detection	Mehdi Akbari Gurabi (FIT)	PST 2021, 13-15 December 2021
Professional paths towards Computer Science careers, including involvement with the SAPPAN project	Gabriela Aumayr (HPE)	HPE WiS group (Women in Security) Webinar, 9 December 2021
CYBERSECURITY INNOVATION IN THE NORDICS (SAPPAN was the	Janne Pirttilahti (FSC)	ECSO CYBER INVESTOR DAYS (SLUSH 2021 SIDE EVENT), 1-2 December 2021

main example of the EU-wide R&I collaboration benefits)		
Big Data Processing for Cybersecurity: How we Aggregate and Enrich Fortinet Syslog Events	Gabriela Aumayr, Hugo Hromic (HPE)	HPE Security Summit, 8-10 November 2021
Interactive process tree analysis Poster	Robert Rapp, Christoph Müller, Franziska Becker (USTUTT), Paolo Palumbo (FSC), Thomas Ertl (USTUTT)	VizSec 2021, 27 October 2021
SAPPAN Project Presentation	Avikarsha Mandal (FIT)	Joint SOCCRATES and SAPPAN webinar - Detecting DGA related threats 28/09/2021 15.30-17.00 CET
SAPPAN Innovation in DGA Detection	Arthur Drichel (RWTH)	Joint SOCCRATES and SAPPAN webinar - Detecting DGA related threats 28/09/2021 15.30-17.00 CET
Graph-based Network Traffic Analysis for Incident Investigation	Milan Cermak (MU)	3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) held in conjunction with the 16th International Conference on Availability, Reliability and Security
Taking a look at the *.ch zone with a DGA detector	Mischa Obrecht (DL)	3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) held in conjunction with the 16th International Conference on Availability, Reliability and Security
Combining Anomaly Detection Models for More Reliable Attack Detection	Dmitriy Komashinskiy (FSC)	3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) held in conjunction with the 16th International Conference on Availability, Reliability and Security
The SAPPAN-project (Sharing And Automation for Privacy Preserving Attack Neutralization) and utilization of MITRE for attack emulation	Mischa Obrecht (DL)	Africa & ME ATT&CK Community Workshop, July 2021
Roundtable on cluster topic Threat Intelligence: SAPPAN project	Avikarsha Mandal (FIT)	Cyberwatching webinar: Shaping the future of cybersecurity, 13 July 2021
Data Staging Platform: How we Aggregate and Enrich Fortinet Syslog Events	Gabriela Aumayr, Hugo Hromic (HPE)	HPE TechX Forum, 29th July 2021

GRANEF: Utilization of a Graph Database for Network Forensics	Milan Cermak and Denisa Sramkova(MU)	SECRYPT 2021, 6-8 July 2021
Project SAPPAN at CSIRT-MU	Tomas Jirsik (MU)	63rd TF-CSIRT Meetin, 28 May 2021

SAPPAN blog post series

The following table lists the available blog posts published on the SAPPAN website so far.

Title	Author	Link
Sharing of incident response playbooks	Martin Žádník (CESNET)	https://sappan-project.eu/?p=1269
Detecting suspicious *.ch-domains using deep neural network	Mischa Obrecht (DL)	https://sappan-project.eu/?p=1321
Datasets Quality Assessment For Machine Learning	Dominik Soukup (CESNET)	https://sappan-project.eu/?p=1428
Challenges in Visualization for AI	Franziska Becker (USTUTT)	https://sappan-project.eu/?p=1435
Analytic provenance for security operation centres	Robert Rapp (USTUTT)	https://sappan-project.eu/?p=1594
Modeling Host Behavior in Computer Network	Tomas Jirsik (MU)	https://sappan-project.eu/?p=1683
For security analysts, a picture may be worth more than a thousand words	Dmitriy Komashinskiy and Andrew Patel (WithSecure)	https://sappan-project.eu/?p=1699

4.5 Collaboration between partners regarding dissemination and communication

As mentioned in several places in the report, partners have cooperated in different dissemination activities. As an example, this included the organization of the NG-SOC 2020 and 2021 workshops, which involved various partners as workshop chairs or as part of the technical committee. Other activities include joint publications and thesis supervision which are listed in detail in previous sections. It also includes joint presentations at different events, such as the second workshop on Dynamic Countering of Cyber-attacks and the final SAPPAN event. Most consortium partners are further collaborating on writing a journal paper regarding project innovations. This joint effort is still ongoing. In addition, we plan to hold the NG-SOC 2022 workshop in collaboration with SOCCRATES and CyberSEAS H2020 projects after the end of the SAPPAN project.

5 Overview of Dissemination and Communication Activities

5.1 Categorising dissemination and communication activities

In the table below, we categorise our dissemination and communication activities during the project lifetime, into different types. Also, we give an estimation of the number of target audiences reached by those activities in the next table.

Type of dissemination and communication activities	Number	List
Organisation of a Workshop / Conference	4	• NG-SOC 2020 • Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects • NG-SOC 2021 (with peer-review call-for-papers published in ARES proceedings) • 2nd Joint Workshop – Dynamic Countering of Cyber-attacks | Achievements and Standardisation
Press release	3	• SAPPAN presence at cyberwatching.eu: https://cyberwatching.eu/projects/1807/sappan/news-events/sappan-european-approach-enable-privacy-preserving-federation-cybersecurity-incident-detection-and-handling • ERCIM news 216: Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery (FIT) • ERCIM news 219: From Collaboration to Automation: A Proof of Concept for Improved Incident Response (FIT/ CESNET/ DL)
Non-scientific and non-peer-reviewed publication (popularised publication)	11	• A whitepaper on the Blackfin project (FSC) • Blog post in F-Secure's Security Blog: Phishing is here to stay • Blog post in F-Secure's Security Blog: Project Blackfin has launched • Blog post in Dreamlab's Research Blog: Detecting suspicious *.ch-domains using deep neural networks • SAPPAN blog post series (7 blog posts so far)
Exhibition	2	• Slush 2021 (FSC) • Slush 2019 (FSC)
Flyer	2	• Final SAPPAN Event Flyer: https://sappan-project.eu/wp-content/uploads/2022/03/Stakeholder_Event-1.pdf • SAPPAN project Flyer: https://sappan-project.eu/wp-content/uploads/2022/04/SAPPAN_flyer.pdf
Training	1	NOMS 2022 (https://noms2022.ieee-noms.org/program/workshops) tutorial preparation and performing at GRASEC workshop (https://grasec.uni.lu/)

Social Media	3	• Twitter: https://twitter.com/SAPPAN_H2020 • Linkedin: https://www.linkedin.com/groups/12363174/ • YouTube: https://www.youtube.com/channel/UCrqc_Tzt6nU3ks1nrkRnq2g
Website	1	Project website: https://sappan-project.eu/
Participation to a Conference	17	• CyberTIM 2020 (RWTH) • ARES 2020 (RWTH) • CyberTIM 2020(CESNET) • IEMCON 2020 (CESNET) • VizSec 2020 (USTUTT/RWTH) • Leuven AI Law & Ethics Conference (F-Secure) • SECRYPT 2021 (MU) • IWCC 2021 (RWTH) • ARES 2021 (RWTH) • CYBER 2021 (RWTH) • CYSARM 2021 (RWTH) • PST 2021 (RWTH/FIT) • Big Data 2021 (CESNET) • CNSM 2021 (CESNET) • CCWC 2021 (CESNET) • VizSec 2021 (USTUTT) • DFRWS EU 2022 (MU)
Participation to a Workshop	7	• NG-SOC 2020 • Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects • NG-SOC 2021 • 2nd Joint Workshop – Dynamic Countering of Cyber-attacks | Achievements and Standardisation • NOMS 2022 Workshops - GraSec 2022 (MU) • NOMS 2022 Workshops - AnNet 2022 (USTUTT) • Africa & ME ATT&CK Community Workshop July 2021 (DL)
Participation to an Event other than a Conference or a Workshop	15	• Joint SOCCRATES-SAPPAN webinar: Detecting DGA related threats • HPE Women in Security (WiS) group Webinar • Swiss Cyber Security Days 2021 (DL) • Swiss Cyber Security Days 2022 (DL) • Slush 2021 (FSC) • 63rd TF-CSIRT Meeting (MU) • Cyberwatching webinar: Shaping the future of cybersecurity (FIT) • HPE TechX Forum 2021 • HPE Security Summit • Girls Day 2021 at USTUTT • ISC2 chapter Switzerland, 2021 (DL) • The talk at Slush 2019 by Mikko Hyppönen (FSC) • 58th TF-CSIRT Meeting (MU) • Machine learning Summer school (RWTH) • Fraunhofer FIT Scientific End of the Year Event 2019

Video/Film	20	Available on our YouTube channel: • NG-SOC videos (4 public videos available on YouTube) • Final SAPPAN event (1 full video + 5 topic videos) • PST 2021 conference presentations • Joint DGA workshop video (SAPPAN + SOCCRATES) • SECRYPT 2021 conference presentations Not available on our YouTube channel: • NG-SOC videos (4 private videos not available on YouTube) • VizSec 2020 conference short paper presentation video • Cyberwatching webinar: Shaping the future of cybersecurity • Africa & ME ATT&CK Community Workshop (July 2021) presentation
Pitch Event	11	• Swiss Cyber Security Days 2022 (DL) • TF-CSIRT meetings 2022 event (MU) • Swiss Cyber Security Days 2021 (DL) • Slush 2021 (FSC) • TF-CSIRT meetings 63 (MU) • NG-SOC 2020 • TF-CSIRT meetings 58 (MU) • SAPPAN-SOCCRATES networking event • ML Summer School (RWTH) • Fraunhofer FIT end of the year event • ISC2 Chapter Switzerland Workshop, March 2021 (DL)
Trade Fair	4	• Slush 2021 (FSC) • Slush 2019 (FSC) • Swiss Cyber Security Days 2021 (DL) • Swiss Cyber Security Days 2022 (DL)
Participation in activities organised jointly with other EU project(s)	8	• NG-SOC 2020 • NG-SOC 2021 • SAPPAN-SOCCRATES event in Helsinki • Project SPARTA - cooperation between SPARTA TSHARK and SAPPAN • Joint SOCCRATES-SAPPAN webinar: Detecting DGA related threats • Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects • 2nd Joint Workshop – Dynamic Countering of Cyber-attacks | Achievements and Standardisation • Cyberwatching webinar: Shaping the future of cybersecurity (FIT)

Other	9	• Cyberwatching Project Hub • SAPPAN as Project of the week from Cyberwatching Project Hub • Submitting IPFIXcol Kafka plugin with policer as docker images into git • Interview with a SAPPAN member for the International Women's Day 2021 (MU) • promoting SAPPAN project through CSIRT-MU Twitter and LinkedIn, CESNET Twitter, FIT Twitter and LinkedIn, DreamLab LinkedIn, and WithSecure (formerly F-secure) Twitter accounts • Supervision of finished bachelor/master theses • Promoting gender equality information from EC and other projects through SAPPAN Twitter account (E.g., International women's day 2022) • Promoting SAPPAN via the ECSO Awareness Calendar (FSC)

5.2 Target groups that were reached

For this section, we aggregate the estimated number of audiences in the events we participated. The number here is just a lower bound estimation. For instance, we only count direct conference participants for scientific reach and skip the number of views on each paper in different scientific mediums. Also, for the media audience, we follow the same method and only count the number of followers and skip the number of views and interactions.

Type of audience reached (In the context of all dissemination & communication activities)	**Estimated number of persons reached**
Scientific Community (Higher Education, Research)	5000+
Industry	2500+
Civil Society	400+
General Public	1000+
Policy Makers	50+
Media	500+
Investors	30+
Customers	250+
Other	-

5.3 Dissemination and communication KPIs results

We revisited and extended the communication and dissemination KPIs in the previous iteration of this report, deliverable D7.13, to address the EC midterm review and the restrictions caused by COVID-19. It resulted in the refinement and extension of dissemination goals by adding particular indicators for remote events and online presence to have more clear measures for monitoring the progress of the activities. Currently, we stick with the KPIs we represented in D7.13, which was the extension of dissemination and communication KPIs from the Grant agreement and the first iteration of the dissemination plan D7.11. We have no further updates regarding the KPIs in this report.

We have successfully fulfilled almost all of the target dissemination and communication KPIs. Eighteen peer-reviewed scientific publications of SAPPAN results in journals and proceedings of high-level conferences and workshops were a significant achievement (target KPI was 8+) and will definitely impact the scientific community. Some of the publications of SAPPAN results are currently under review or work in progress, so we expect to have more peer-reviewed publications of SAPPAN results after M36. Another highlight was disseminating SAPPAN results in various venues and events to raise community interest. We have made a remarkable effort of 39 SAPPAN presentations at different events (target KPI was 7+). We tried our best to make our active presence on social media. It was not possible to achieve the KPI of LinkedIn group members as consortium members preferred the group as "closed" to consortium members and the key stakeholders. We have given more effort to our presence on Twitter as our primary public social media channel, and we gained around 400 followers (at M24 it was 125). We had over 38000 impressions on our account based on the Twitter analytics report. Consortium partners also open-sourced their codes and results individually via their public repositories. The overview of evaluated KPIs is presented in the following table.

Activities	**key performance indicators (KPIs) for measurement of results**	**Current Progress**
Availability of the SAPPAN web site	Online Since M4 (Yes/No)	Yes
	Present the goal of the project (Fully/Partially/Not available)	Fully available
	Information about project partners, advisory board, other consortium bodies (Fully/Partially/Not available)	Fully available
	Disseminate public deliverables after EC confirmation (Fully/Partially/Not available)	Fully available
	Availability of promotional materials (Fully/Partially/Not available)	Fully available
	Links to related events (Fully/Partially/Not available)	Fully available
	Website traffic statistics (Yes/No)	Yes, the last 8 month of the project
Events and presentations	7+ presentations in events (including remote events)	39
	2+ webinar sessions	3
	Organizing a final event	Yes, held online
Publications	8+ scientific peer-reviewed publications	18
	2+ general press	3
	4+ technical fairs	4
	8+ blog posts	10
Active presence in Social networks	500+ Twitter followers	400+
	100+ tweets	110
	200+ LinkedIn Group members	~20
	8+ YouTube videos	13

	Availability of GitHub repository to maintain open source developments (Yes/ No)	Yes, • Consortium private GitLab repository hosted by FIT • Partner-specific GitHub repositories for open-sourcing

6 Conclusion

This report is a follow-up to D7.13 at M24, and it includes dissemination activities completed during the project's third (last) 12-month cycle.

Communication activities are also included, and the progress of the general dissemination and communication activities is presented in this report.

The communication activities based on the plan are categorized into four groups: project website, events and presentations, publications, and social media activities. The main communication activities done in the third year of the project are:

- The establishment of the SAPPAN blog post series
- The organisation of NG-SOC 2021
- SAPPAN-related presentations at NG-SOC 2021, ECSO CYBER INVESTOR DAYS (SLUSH 2021 SIDE EVENT), MITRE Africa/EMEA conference, TF-CSIRT events, Cyberwatching webinar, SWISS Cyber Security Days 2022 and several scientific conferences and events
- The organisation of and participation in events such as the 2nd Joint Standardization Workshop - Dynamic countering of cyber-attacks with other EU projects, and SOCCRATES-SAPPAN joint webinar
- The organisation of the final SAPPAN event

Moreover, the project website, Twitter account, YouTube channel, and LinkedIn group have been updated continuously due to the dissemination of project concepts, objectives, news, and results. Besides, research works lead to 18 published and 4 submitted (under peer-review) scientific publications, as well as, 26 successfully supervised bachelor and master theses so far.

Furthermore, an overview of the dissemination and communication KPIs which were revisited and extended in the previous iteration of the document (D7.13) and any changes in the dissemination plan and its reasons are listed in this dissemination report. There were changes regarding the dissemination strategy due to the influence of the COVID-19 pandemic and also to address midterm review feedback of the project.