



Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D7.7 Report on Information and Presentation Materials (M12)

Published by the SAPPAN Consortium

Dissemination Level: Public



H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file: D7.7 Report on Information and Presentation Materials - M12
Document version: 1.0
Document owner: Mehdi Akbari Gurabi (FIT)

Work package: WP7
Task: T7.3
Deliverable type: Report
Delivery month: M12
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), Lasse Nitz (FIT)	2020-04-15	Preliminary document outline
0.2	Mehdi Akbari Gurabi (FIT)	2020-04-22	Initial draft
0.3	Mehdi Akbari Gurabi (FIT)	2020-04-23	Applying FIT internal feedback, the first complete version to collect feedback from partners
1.0	Mehdi Akbari Gurabi (FIT)	2020-04-28	Applying reviewers' feedback, ready for submission

Internal review history:

Reviewed by	Date	Summary of comments
Lasse Nitz (FIT)	2020-04-22	check-reading content (except for dates, slides and pictures), grammar corrections
Sarka Pekarova (DL)	2020-04-27	Grammar, spelling and structure, except presentations themselves.
Arthur Drichel (RWTH)	2020-04-28	Grammar and spelling

Executive Summary

The purpose of the report on information and presentation materials is to help to present the project's results to all interested stakeholders.

This deliverable lists all the SAPPAN presentation materials such as the deliverable template, logo, website and social media accounts, as well as the presentation of concepts, vision, goals, and results of the project and spreading of information to the target audience in the events by any of SAPPAN consortium members. The last part of the deliverable describes planned information and presentation materials during the lifetime of SAPPAN project.

This is the first iteration of the document. Future iterations will be delivered at M24 and M36.

Table of Contents

EXECUTIVE SUMMARY	3
1 INTRODUCTION	5
2 CREATED INFORMATION AND PRESENTATION MATERIALS.....	5
2.1 SAPPAN DELIVERABLES TEMPLATE	5
2.2 SAPPAN LOGO.....	5
2.3 PROJECT WEBSITE	5
2.4 TWITTER ACCOUNT.....	6
2.5 LINKEDIN GROUP	7
2.6 AVAILABILITY ON CYBERWATCHING PROJECT HUB	8
2.7 INTRODUCTION PRESENTATION SLIDES	8
2.8 MENTIONS OF SAPPAN ON PARTNERS' WEBSITES.....	8
3 SHORT SUMMARY OF PRESENTATION IN THIRD PARTY EVENTS	9
3.1 58TH TF-CSIRT MEETING.....	9
3.2 SUMMER SCHOOL MACHINE LEARNING AND SECURITY	14
3.3 FRAUNHOFER FIT SCIENTIFIC END OF THE YEAR EVENT 2019.....	16
3.4 SAPPAN-SOCCRATES NETWORKING EVENT	24
4 PLANNED INFORMATION AND PRESENTATION MATERIALS.....	28
5 CONCLUSION	29

1 Introduction

The aim of this report is to summarize the current information and presentation materials of SAPPAN, which lists both the general presentations of the consortium, as well as the individual presentations of the partners in events for dissemination of SAPPAN goals and results.

The information and presentation materials are and will be used to bring the project's vision, components, and results, as well as experiences obtained throughout the project to the public in scientific and commercial events. These activities are focused on raising awareness, showing and explaining the result of the partner's research to reach target audience entities and experts, and increasing the synergy in the research area of cybersecurity with 3rd parties, especially other EU funded projects.

The rest of this document is organized as follows: Section 2 describes the general created information and presentation materials. Then, Section 3 includes short summaries of presentations in third party events and Section 4 lists the plan of information and presentation materials for the next stages.

During the lifetime of the SAPPAN project, the report on information and presentation materials will be updated at M24 and M36.

2 Created Information and Presentation Materials

2.1 SAPPAN Deliverables Template

A word template for deliverables was created following the EU H2020 guideline. It is available internally in the online collaboration workspace of the consortium. Each submitted deliverable of type "report" used the mentioned template. It is planned to also provide a LATEX template for scientific deliverables in the near future.

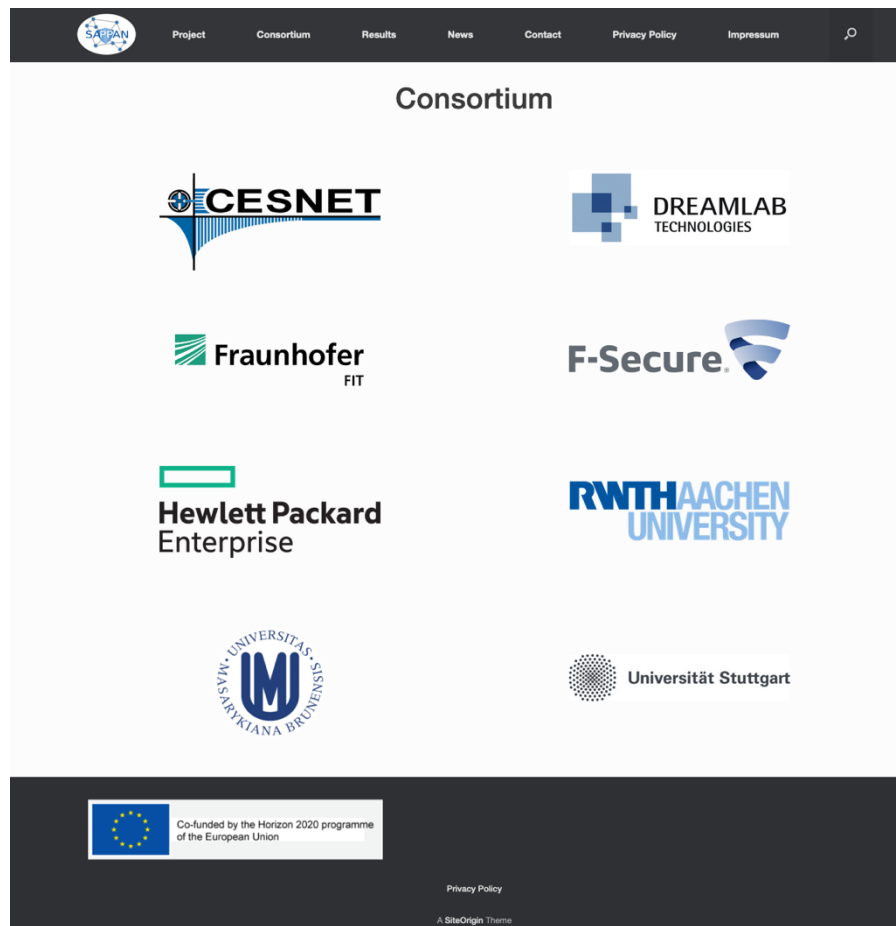
2.2 SAPPAN Logo

The SAPPAN logo is designed for the dissemination and presentation of the project on different platforms. The logo is used in deliverables, the project website, social media accounts and channels, as well as in the presentation slides introducing the project or disseminating the project concepts and results. An instance of the logo is shown in the following picture.



2.3 Project Website

The project website has been available since month 4 of the project life cycle (link: <https://sappan-project.eu/>).



The website was created with the intent to provide a platform for public documentation of the progress and achievements of SAPPAN. It is planned to provide updates on project progress in more detail on the website than on other dissemination channels. Public deliverables will be uploaded to the website as soon as they were reviewed and confirmed by the European Committee. Other project results such as publications and dissemination materials will be available on the website as well. Updates on events (such as meetings, workshops, and conferences) and other project related news will also be continuously presented on the website.

Currently, a new, more lightweight, and modern design of the project website is under construction and will be available soon.

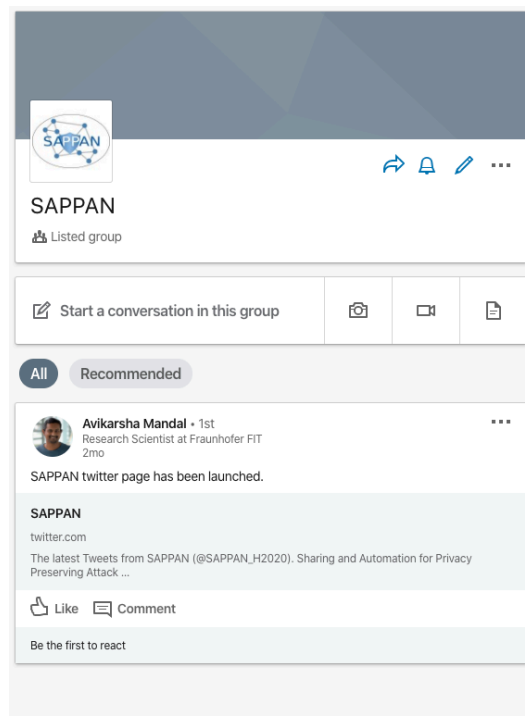
2.4 Twitter Account

In order to show presence on social media, a twitter account (link: https://twitter.com/SAPPAN_H2020) has been created to provide public updates about the project progress of SAPPAN. Enabling communication with other cybersecurity projects and increasing the visibility of SAPPAN to the domain experts and potential stakeholders is one of the goals of having social media accounts.



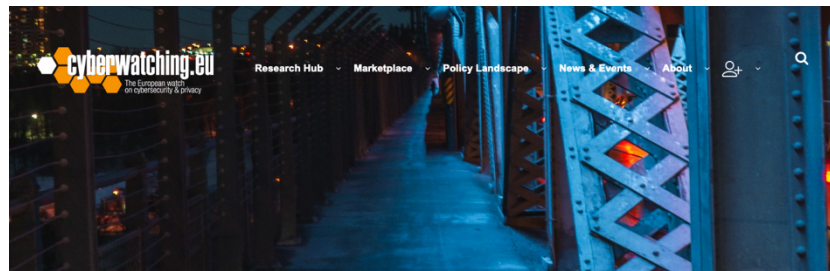
2.5 LinkedIn Group

As part of the dissemination plan for SAPPAN, a LinkedIn group has been created. The LinkedIn group is available for those consortium members and stakeholders who might have interest in accessing the project's progress and results. The group is ready for starting discussions around the SAPPAN concepts and goals by members.



2.6 Availability on Cyberwatching Project Hub

Cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy and is funded under the EU H2020 program. It aims to contribute to a safer digital marketplace by promoting and understanding of European cutting-edge cybersecurity and privacy services which emerge from research and innovation initiatives. SAPPAN is promoted by project hub of Cyberwatching: <https://cyberwatching.eu/projects/1807/sappan>



SAPPAN

Sharing and Automation for Privacy-Preserving Attack Neutralization

[Home](#) » [Projects](#) » SAPPAN

Contact Avikarsha Mandal	Start Project 01 May 2019	End Project 30 April 2022	Project type EC funded project
------------------------------------	-------------------------------------	-------------------------------------	--

SAPPAN project aims to enable efficient protection of modern ICT infrastructures via advanced data acquisition, threat analysis, and privacy-aware sharing and distribution of threat intelligence aimed to dynamically support human operators in response and recovery actions. The SAPPAN project will develop a collaborative, federated, and scalable attack detection to support response activities and allow for timely responses to newly emerging threats supporting different privacy-levels. We plan to identify a standard for the interoperable and machine-readable description of incident response reports and recovery solutions. The risk assessment, privacy, and security will be addressed in the standard design. Results of both attack detection and recovery and response processes will be shared on a global level to achieve an advanced response and recovery via knowledge sharing and federated learning. We develop a mechanism for sharing information on threat intelligence, which implements a combination of encryption and anonymization to achieve GDPR compliance. Novel visualization techniques will be developed to assist security and IT personnel and provide an enhanced content of context of the response and recovery, and improved visual presentation of the process.

Category:
Secure systems and technology

Vertical Category:
ICT

[🔗](#)
[✉️](#)
[🐦](#)
[in](#)

2.7 Introduction Presentation Slides

For the purpose of presenting the basic concept of the project in events, a set of PowerPoint slides has been created. The introduction slides include general aim, key contributions, consortium members, an overview of cyber incident response and recovery, SAPPAN concept, and a brief description of work packages. Introduction slides will be available on the website of the project.

2.8 Mentions of SAPPAN on Partners' Websites

Consortium members announced the start of the project and important events on their official websites and social media channels. In the following table, samples of project-related links are provided:

Beneficiary	Link of SAPPAN-related news
DreamLab	<ul style="list-style-type: none"> https://dreamlab.net/en/news/article/eu-research-project-horizon-2020-sappan/
Masaryk University	<ul style="list-style-type: none"> https://www.muni.cz/en/research/projects/46829 Czech CyberCrime Centre of Excellence C4e: https://c4e.cz/projects/sappan Cybersecurity Team of Masaryk University: https://csirt.muni.cz/about-us

RWTH Aachen	<ul style="list-style-type: none"> • https://www.rwth-aachen.de/go/id/elwbb?lidx=1 • Research group IT-Security: https://www.itsec.rwth-aachen.de/cms/ITSEC/Forschung/Projekte/~fnwlp/SAPPAN/lidx/1/
University of Stuttgart	<ul style="list-style-type: none"> • https://www.vis.uni-stuttgart.de/en/projects/eu-sappan/

3 Short Summary of Presentation in Third Party Events

3.1 58th TF-CSIRT Meeting

Short description of the event:

The 58th TF-CSIRT Meeting hosted by CSIRT-CY took place from 16th to 17th of September 2019 at the Annabelle Hotel, Paphos, Cyprus. TF-CSIRT is a task force that promotes collaboration and coordination between CSIRTs in Europe and neighboring regions, whilst liaising with relevant organizations at the global level and in other regions. The members are from the TF-CSIRT community, consisting of experts of various CSIRT/CERT teams from all over Europe. The participants were from government/institutional (national CSIRTs) or industry (company's CSIRTs). These facts make the TF-CSIRT's community potential target users of the SAPPAN platform. During this event, an introduction to SAPPAN was presented to an audience of about 30 people.

Link: <https://tf-csirt.org/tf-csirt/meetings/58th/>

Presentation:

The main ideas and concepts of SAPPAN were introduced at the 58th TF-CSIRT Meeting. The goal was to spread the knowledge about SAPPAN and its ideas to the relevant community, getting feedback from the discussion, and disseminating the project. The presentation received feedback from several members of the domain expert audience, which helped us to steer the project in the right way. In addition, SAPPAN's website was promoted to stay in contact with the community members to gain more useful insights from them.



The following slides set was presented in the meeting:

Sharing and Automation for Privacy Preserving Attack Neutralization

58th TF-CSIRT Meeting – Paphos, Cyprus

September 17th, 2019

Tomáš Jirsík

CSIRT-MU, Masaryk University, Brno



Co-funded by the Horizon 2020 programme of the European Union



CSIRT-MU

SAPPAN – Sharing and Automation for Privacy Preserving Attack Neutralization

▪ H2020 – Call: Dynamic countering of cyber-attacks

- **Scope:** Cyber-attacks management – advanced response and recovery



▪ Highlights from the Call:

- dynamic support of human operators, CSIRTs
- controlling **response and recovery** actions, including information **visualization**.
- best **measures** are to withstand and recover from a threat/attack (beyond cyber)
- utilization of both **structured** (e.g. logs) and **unstructured** data
- handling (e.g. classification, anomaly detection) of **encrypted** network traffic
- dynamic, evidence based security and privacy risk **assessment methodologies and management** tools targeting emerging/advanced technologies

2

SAPPAN Concept

▪ General Aim:

- develop a platform for sharing and automation ...
- ... to enable privacy preserving and efficient response and recovery ...
- ... utilizing advanced data analysis and machine learning.

▪ Key Contributions

- **privacy-preserving** aggregation and data analytics including advanced client-side abstractions
- **federated threat detection** based on sharing of anonymised data and sharing of trained machine learning models
- **standardisation of knowledge** in the context of incident response and recovery to enable **reuse and sharing**
- **visual, interactive support** for Security Operation Center operators.

3

SAPPAN Consortium

- **Coordinator:**



- **Industrial Partners:**

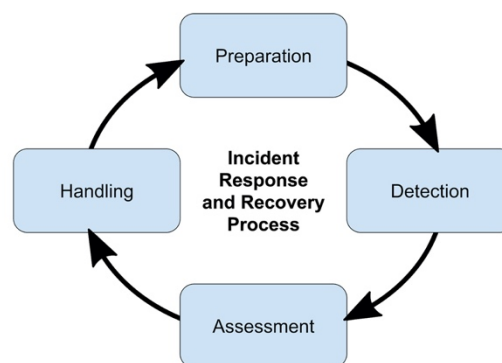


- **Academia:**



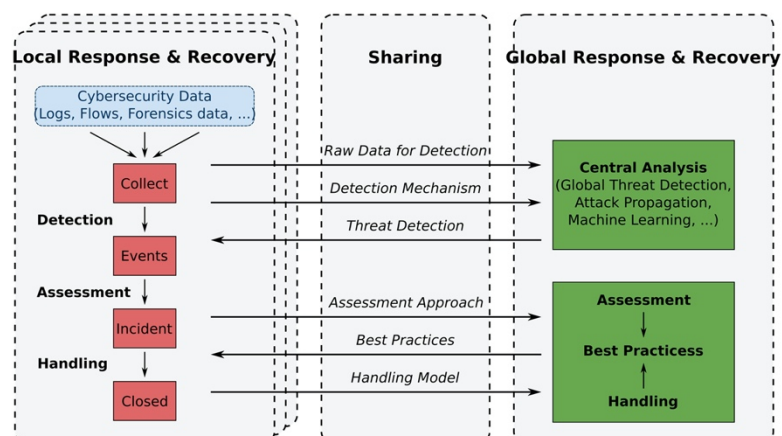
4

SAPPAN Concept - Cyber Incident Response and Recovery



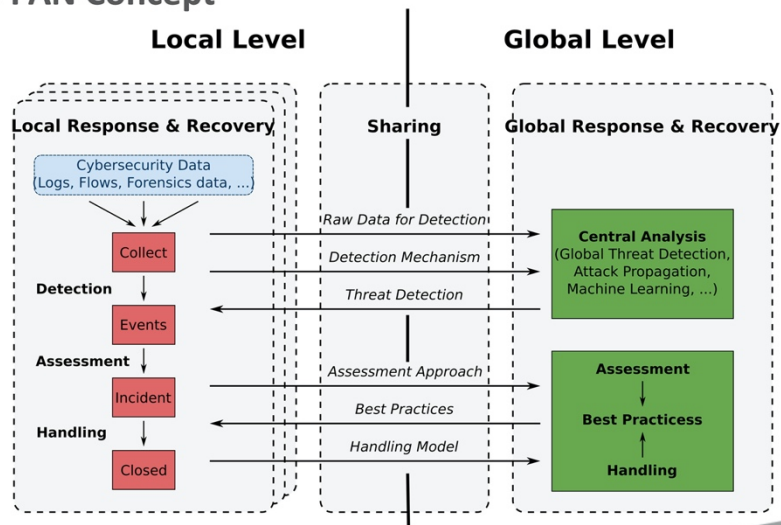
5

SAPPAN Concept



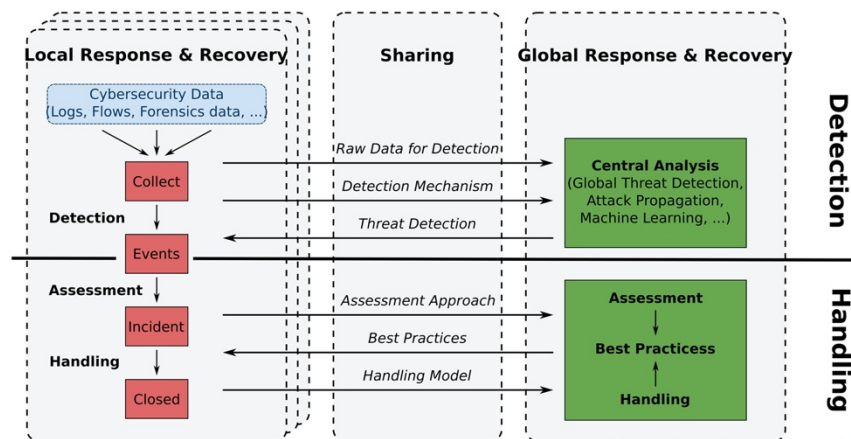
6

SAPPAN Concept



7

SAPPAN Concept



8

WP: Use Cases and Requirements Analysis

- Analysis and specification of response and recovery use-cases
- Privacy requirements
- Presentation requirements
- Functional specification and architecture definition
- Evaluation methodology

WP: Massive Data Acquisition and Local Attack Detection

- Data selection and data processing design
- Fast and scalable processing of cybersecurity data
- Analysis of encrypted and anonymised cybersecurity data
- Development of cybersecurity data abstractions that allow for anonymous data transit
- Visualisation support for the design of attack and anomaly detection models

9

WP: Managing and Automating Threat Intelligence

- Develop a methodology for formalising and modeling response and recovery actions and their triggers
- Develop approach for capturing and expressing incident response and recovery steps with involvement of human operators
- Develop approach for automatically recommending response and recovery actions to human operators
- Develop approach to automate response and recovery actions without human operators
- Tracking of analytical provenance

WP: Sharing and Federation for Cyber Threat Detection and Response

- Distributed Learning of a global model based on shared anonymized data
- Federated learning of a global model based on shared locally trained models
- Federated learning of a global model without sharing local models
- Sharing response handling information
- Visualisation support for distributed and federated learning of models

10

WP: Integration, Validation, and Visualization

- Dashboard for response and recovery awareness
- SAPPAN demonstrator
- Validation of response and recovery capabilities

11

Your comments are welcome

Advisory board member wanted

 <https://sappan-project.eu>

Tomas Jirsik

jirsik@ics.muni.cz



CSIRT-MU

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme, under the Grant Agreement number 833418.

3.2 Summer School Machine Learning and Security

Short description of the event:

2019 International Summer School on Machine Learning and Security (MLS) took place at the University of Padova, Italy from September 9th to September 13th, 2019. The goal of the school is to bring together security research community members to discuss recent issues and developments in the area of machine learning and security. SAPPAN members attending the school aimed to improve their knowledge about advanced topics related to machine learning that can be applied to SAPPAN. The event lectures were held by professors of different universities teaching topics in Machine Learning and security. Approximately 45 participants attended the summer school, mainly Ph.D. students whose research lies in the area of machine learning and security. Also, as an industry speaker, Facebook was present.

Link: <https://spritz.math.unipd.it/events/2019/PIU2019/PagesOutput/MLS/index.html>

Presentation:

Due to the main concepts and planned features of SAPPAN, it was helpful to have a discussion and presentation of SAPPAN ideas and vision to other participants and organizers of the school interested in machine learning and security. At the event, the main ideas of SAPPAN were discussed. The discussion included the sharing of intelligence to improve intrusion detection and to reduce response times, different types of machine learning related intelligence which could be shared, the impact on the privacy of a sharing party, as well as possible privacy-enhancing technologies which could be applied in SAPPAN.

The following slides were presented in the summer school as a brief introduction:



Previous Work

DNS-based network fingerprinting

- Fingerprinting of devices and applications based on DNS traffic
- Developing of a tool for e.g. pentesters/administrators to get an overview over a network
- Using rule-based approaches as well as machine learning (Neural Networks)
- NAT detection and de-NATing based on DNS traffic

Future Research

- Improve labeling of machine learning data sets
 - Hard to find data sets including ground truth
- Find ways to evaluate approaches without (or partial) ground truth data

1 of 3

Machine Learning and Security School
Research Group IT-Security | RWTH Aachen University
12.09.2019

IT | SEC Research Group
IT-Security

RWTH AACHEN
UNIVERSITY

Collaborative learning in the field of intrusion detection

EU funded project: Sharing and automation for privacy preserving attack neutralization)

- Improve local detection mechanisms with new machine learning approaches
 - Building a privacy preserving platform for sharing data, intelligence, playbooks, intrusion detection (local and collaborative)
- Share local models/knowledge, compute global models for improved detection rates

Challenges with shared detection

- Train global models by sharing local data
 - How to share data in an efficient and privacy preserving way?
- Train global models by sharing local models
 - How to combine models to increase detection rates?
- Train global models without sharing local data or models
 - Use e.g. teacher-student models

2 of 3

Machine Learning and Security School
Research Group IT-Security | RWTH Aachen University
12.09.2019

IT | SEC Research Group
IT-Security

RWTH AACHEN
UNIVERSITY

Concerns with collaborative training of models

- Either trust all sharing parties or make the process robust to poisoning
 - Link to adversarial machine learning
- Even learning a global model without sharing local models or data might not be privacy preserving
 - When using teacher-student models, it might be possible to reconstruct the (private) local models to some extend
 - Or to even reconstruct the private local training data

3 of 3

Machine Learning and Security School
Research Group IT-Security | RWTH Aachen University
12.09.2019

IT | SEC Research Group
IT-Security

RWTH AACHEN
UNIVERSITY

3.3 Fraunhofer FIT Scientific End of the Year Event 2019

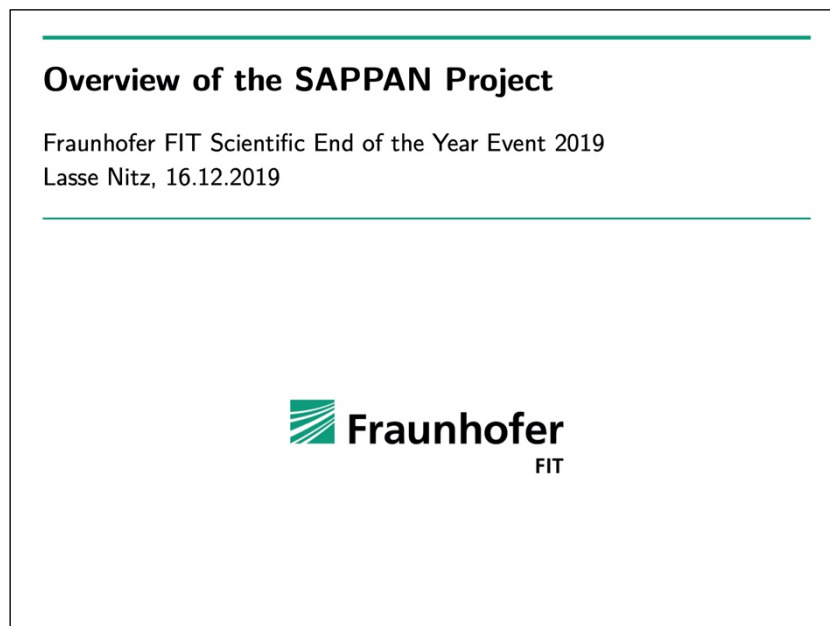
Short description of the event:

The Fraunhofer FIT Scientific End of the Year Event 2019 took place on the 16th of December 2019 at Birlinghoven, Sankt Augustin. It is an inter-department colloquium within the Fraunhofer Institute for Applied Information Technology FIT in which the insights, objectives, current stage of Ph.D. theses, and some research projects are presented by Ph.D. students, several post-doctoral research fellows, and heads of research groups and departments. Even though the event was an internal FIT event, most of the organizers and participants are jointly affiliated with various universities. This provided the opportunity to share SAPPAN ideas, concepts, and research topics with researchers from different domains and locations.

Presentation:

In this event, two presentations were related to SAPPAN. The first presentation was an overview of the SAPPAN project and the second one was about data sharing in SAPPAN. The slides that were presented in the event are given in the following:

Overview of the SAPPAN Project:



Overview of the SAPPAN Project

General Information

Motivation: Intrusion Detection Systems

General Idea of SAPPAN

Key Topics of SAPPAN

Interesting Research Topics








Overview of the SAPPAN Project | Lasse Nitz | 16.12.2019 | 1
© Fraunhofer-Institut für Angewandte Informationstechnik FIT



SAPPAN - General Information

SAPPAN

Sharing and Automation for Privacy Preserving Attack Neutralization

- H2020 project, running from May 2019 until May 2022
- Coordinator: FIT
- Participants:
 - CESNET 
 - Dreamlab 
 - F-Secure 
 - Hewlett-Packard Enterprise 
 - Masaryk University 
 - RWTH Aachen University 
 - University of Stuttgart 

Overview of the SAPPAN Project | Lasse Nitz | 16.12.2019 | 2
© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Motivation: Intrusion Detection Systems

Basic scenario:

- Networks are monitored
- Suspicious patterns can trigger alerts
- Alerts can be resolved by response&recovery actions ("playbooks")
- New cybersecurity threats might cause new patterns

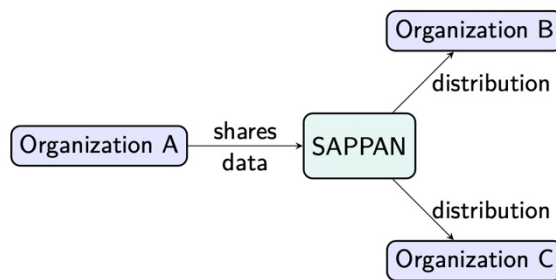
Main Challenges:

- Fast detection of new patterns
- Low rate of false positive alerts
- Automation of response&recovery actions

Overview of the SAPPAN Project | Lasse Nitz | 16.12.2019 | 3
© Fraunhofer-Institut für Angewandte Informationstechnik FIT



General Idea of SAPPAN



Problems:

- The shared data contains confidential information
- Which format should be used?

Overview of the SAPPAN Project | Lasse Nitz | 16.12.2019 | 4
© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Key Topics of SAPPAN

What is SAPPAN about?

- Formalization of knowledge about response&recovery actions
- Automated response&recovery actions for cybersecurity incidents
- Anonymization of shared data
- Distributed machine learning across company borders
- Visualization in the cybersecurity domain

Overview of the SAPPAN Project | Lasse Nitz | 16.12.2019 | 5
© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Interesting Research Topics

- Anonymization in a distributed environment while preserving utility
 - of cybersecurity data (e.g. logs, flow data)
 - of machine learning updates and models
- Knowledge formalization for automated cybersecurity response&recovery actions
 - Playbooks are usually human-readable
 - Formats depend on the organization
 - Level of detail: How to formalize playbooks without leaking confidential information?
- Automation of cybersecurity response&recovery actions
 - Rankings of response&recovery actions for certain alerts/patterns
 - Trust/quality metric for provided playbooks
 - Threshold for certainty to avoid false positives

Overview of the SAPPAN Project | Lasse Nitz | 16.12.2019 | 6
© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Data Sharing in SAPPAN:

Data Sharing in SAPPAN

Fraunhofer FIT Scientific End of the Year Event 2019

Mehdi Akbari Gurabi

16.12.2019

**Sharing and Automation for Privacy Preserving
Attack Neutralization**



Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Agenda

- Cyber Threat Information Sharing
- Overview of Available Sharing Systems
- Open Questions for the SAPPAN Sharing System

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Cyber Threat Information Sharing

Motivation:

- Share knowledge about cyber threats
- Speed up the recovery and response process

Challenge:

- Establishing policy about sharing
- Consistency
- Compatibility (different input types)

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Overview of Available Sharing Systems



Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Overview of Available Sharing Systems (Cont.)



Malware Information Sharing Platform (MISP)

- Can be used to share technical and non-technical information about malware samples, incidents, attacks and general intelligence
- Can be used without contributing
- Flexible data model that can express complex objects and links between object
- Adjustable Taxonomy described in JSON that uses machine tags
- Integration of encryption and signing for notifications via PGP and/or S/MIME

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Overview of Available Sharing Systems (Cont.)



Structured Threat Information Expression (STIX)

A language and serialization format for exchanging cyber threat intelligence

- Machine-readable
- Collaborative threat analysis
- Uses 12 different *STIX Domain Objects (SDOs)* as templates for different actors, events, etc. (E.g., Malware, Attack Pattern, Indicator, Tool)

Trusted Automated Exchange of Intelligence Information (TAXII)

A simple and scalable application layer protocol for communication of cyber threat information over HTTPS

- Primarily intended to be used with STIX, but can be used separately for other sharing systems
- RESTful design approach

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Overview of Available Sharing Systems (Cont.)



Open Threat Exchange (OTX)

- Free-to-use, not open source
- Cloud-hosted
- Shared data is automatically cleansed, aggregated, validated and published
- Allows to create private communities and discussions
- DirectConnect API using Java, Python, or Golang SDKs
- Has a social network style component that allows users to share, discuss and research security threats as „Pulses“

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Overview of Available Sharing Systems (Cont.)

	MISP	STIX/TAXII	OTX
Open Source	Yes	Yes	No
Real-time	Yes	Yes	Yes
Data Model	Flexible	Semi Fixed	Fixed
API	PyMISP	Python STIX 2	DirectConnect (Java, Python, or Golang SDKs)
Cloud based	No	No	Yes
Documentation	Very Good	Good	Poor

Missed:

- Automated threat response
- Focus on privacy preserving approaches

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Open Questions for the SAPPAN Sharing System

■ Central vs. distributed

■ Central:

- Easier to implement
- Single point of failure
- Requires a trusted third party
- Distributed might be more interesting from a research perspective

→ Still open

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Open Questions for the SAPPAN Sharing System (Cont.)

■ Use of (parts of) existing sharing platforms

vs. implementation from scratch

- Reusing existing sharing platforms might save a lot of effort
- Existing sharing platforms might not be applicable to all SAPPAN goals
- Implementation from scratch is not depending on licenses from third parties

→ Adopt from other Incident Sharing Platforms (E.g., MISP)

→ Find a general-purpose sharing platform (It is not fit to threat intelligence sharing)

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Open Questions for the SAPPAN Sharing System (Cont.)

■ Push model vs. pull model

■ Push model:

- Provides new data as fast as possible
- Might allow for faster detection of new threats

■ Pull model:

- Allows the SOC Agent to request data when necessary
- Avoids information overload

→ Sharing (push) link to the data, then consumers can pull it based on their needs and regulations

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Open Questions for the SAPPAN Sharing System (Cont.)

■ Data types which are shared via the SAPPAN Sharing System

- Cyber threat intelligence
- Feedback
- Machine learning updates/models

→ Examples: Endpoint data from appliances/ Logs from proxy and firewalls/ DNS traffic/ Non-existent domain responses (NXDs)/ Netflow/ Network segmentation/ Phishing data

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



Thank you for your attention!

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



References:

- MISP features general information, last visited on 15 Dec 2019: <https://www.misp-project.org/features.html>
- MISP user guide, last visited on 15 Dec 2019: <https://github.com/MISP/misp-book>
- Introduction to STIX, last visited on 15 Dec 2019: <https://oasis-open.github.io/cti-documentation/stix/intro>
- Introduction to TAXII, last visited on 15 Dec 2019: <https://oasis-open.github.io/cti-documentation/taxii/intro>
- OTX user guide, last visited on 15 Dec 2019: <https://www.alienvault.com/documentation/otx.htm?tocpath=Documentation%7CAlienVault@%20Open%2%A0Threat%20Exchange@%7C0>

Data Sharing in SAPPAN

© Fraunhofer-Institut für Angewandte Informationstechnik FIT



3.4 SAPPAN-SOCCRATES Networking Event

Short description of the event:

A networking event between the consortia of SAPPAN and SOCCRATES was held on the 21st of January at F-Secure's headquarter in Helsinki. SOCCRATES is another EU H2020 funded project which has a close synergy with SAPPAN. F-Secure is a consortium member of both projects. The event was held during the SAPPAN internal ML-Focused Workshop which was held from 20th to 21st of January 2020. Around 35 members of SAPPAN and SOCCRATES participated in this event, coming from different research institutes and industry partners.

Presentation:

At this event, the following introductions were presented.

- Introduction of SOCCRATES: insight, roadmap, and goals
- Introduction of SAPPAN: insight, roadmap, and goals
- Brief introduction of each (SAPPAN / SOCCRATES) project partner

The meeting continued by a discussion on the assessment of cooperation and collaboration between these two EU H2020 projects with strong synergy. These discussions lead to an agreement on having a joint workshop. The proposal of the joint workshop was prepared and accepted to be held in association with the 15th International Conference on Availability, Reliability and Security (ARES 2020). The International Workshop on Next Generation Security Operations Centers (NG-SOC 2020) will be held on 25th to 28th of August 2020 at the University College Dublin if the program will not be affected by SARS-CoV-2 situation.

The SAPPAN introduction slides which were presented in the meeting are given in the following:



SAPPAN Concept

General Aim

- develop a platform **for sharing and automation** to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and **machine learning**.
- develop **ML and visualization methods** and a **platform for sharing data, threat intelligence and ML models** to enable privacy preserving and efficient attack detection and response.

Key Contributions

- **privacy-preserving** aggregation and data analytics including advanced client-side abstractions
- **federated threat detection** based on sharing of anonymised data and sharing of trained machine learning models
- **standardisation of knowledge** in the context of incident response and recovery to enable **reuse and sharing**
- **visual, interactive support** for Security Operation Center operators with support for conveying uncertainty induced by anonymization.

2

SAPPAN Consortium

Coordinator:



Industrial Partners:



Academia:



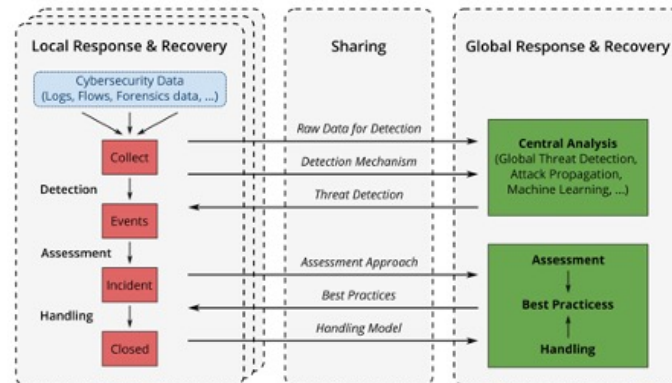
3

SAPPAN Concept - Cyber Incident Response and Recovery



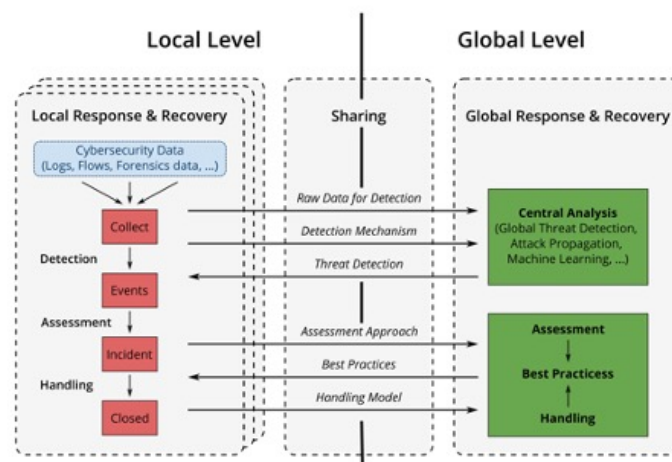
4

SAPPAN Concept



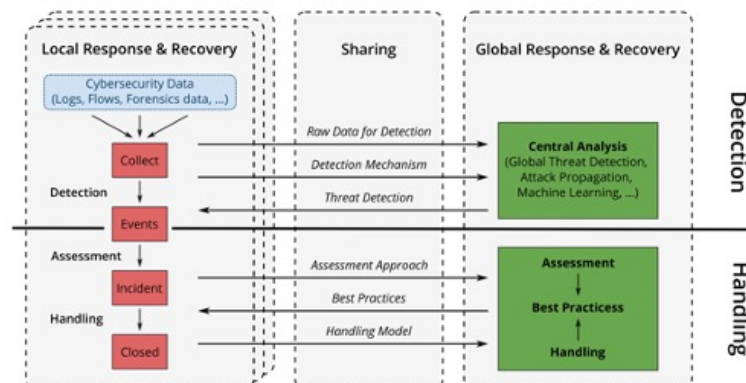
5

SAPPAN Concept



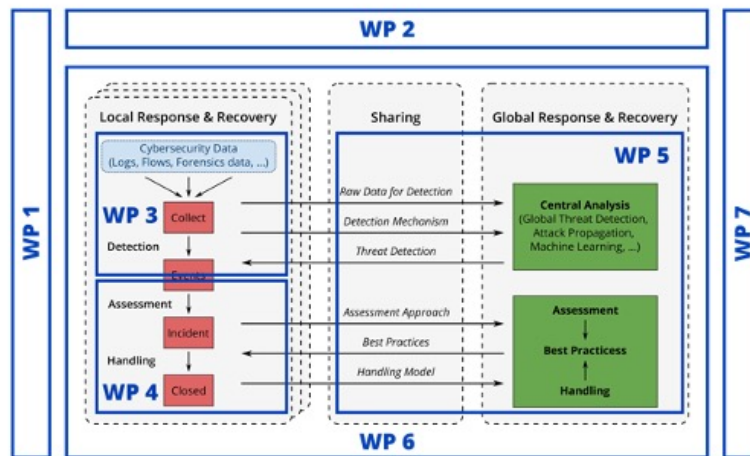
6

SAPPAN Concept



7

SAPPAN Concept



WP2: Use Cases and Requirements Analysis



- Analysis and specification of response and recovery use cases
- Privacy requirements
- Presentation requirements
- Functional specification and architecture definition
- Evaluation methodology

WP3: Massive Data Acquisition and Local Attack Detection

- Data selection and data processing design
- Fast and scalable processing of cybersecurity data
- Analysis of encrypted and anonymised cybersecurity data
- Development of cybersecurity data abstractions that allow for anonymous data transit
- Visualisation support for the design of attack and anomaly detection models

WP4: Managing and Automating Threat Intelligence

- Develop a methodology for formalising and modelling response and recovery actions and their triggers
- Develop approach for capturing and expressing incident response and recovery steps with involvement of human operators
- Develop approach for automatically recommending response and recovery actions to human operators
- Develop approach to automate response and recovery actions without human operators
- Tracking of analytical provenance

WP5: Sharing and Federation for Cyber Threat Detection and Response

- Distributed learning of a global model based on shared anonymized data
- Federated learning of a global model based on shared locally trained models
- Federated learning of a global model without sharing local models
- Sharing response handling information
- Visualisation support for distributed and federated learning of models

WP6: Integration, Validation, and Visualization

- Dashboard for response and recovery awareness
- SAPPAN demonstrator
- Validation of response and recovery capabilities

11

*If we knew what it was we were doing, it would not be called
research, would it?*

 <https://sappan-project.eu>



Tomas Jirsik

jirsik@ics.muni.cz

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme, under the Grant Agreement number 833418.

4 Planned Information and Presentation Materials

In this section the planned activities for the next part of the project life cycle are summarized in a table:

Type of presentation activities	Planned Activities
Organization of a conference or workshop	<ul style="list-style-type: none"> • International Workshop on Next Generation Security Operations Centers (NG-SOC 2020): Joint workshop with the SOCCRATES project. To be held in conjunction with the 15th International Conference on Availability, Reliability and Security (ARES 2020 – http://www.ares-conference.eu) August 25 – August 28, 2020, University College Dublin, Dublin, Ireland Workshop Link: https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2020/

Participation in activities organized jointly with other H2020 projects	<ul style="list-style-type: none"> • International Workshop on Next Generation Security Operations Centers (NG-SOC 2020) (details mentioned in the above row)
Non-scientific and non-peer reviewed publications (popularized publications)	<ul style="list-style-type: none"> • Blog posts regarding the project' initiatives on partners' blogs
Training	<ul style="list-style-type: none"> • Training activities as part of the dissemination plan of several academic partners of the project • Use of project knowledge and experiences in security and privacy courses and proposing bachelor and master theses related to project topics
Website	<ul style="list-style-type: none"> • New design will be available soon • Continuous updates on the project progress, events, and materials
Participation in conferences and workshops	<ul style="list-style-type: none"> • Participation in conferences and workshops is a SAPPAN dissemination KPI and has been promised and planned by most of the consortium members • Presenting the progress of the project, spreading the knowledge about SAPPAN, and receiving feedback supposed to be done in each event
Participation in an event other than a conference or workshop	<ul style="list-style-type: none"> • Participating in ICT exhibitions and trade fairs such as Hannover Messe • SAPPAN-related presentations in third party meetings and events
Social media	<ul style="list-style-type: none"> • Continuous updates on Twitter and LinkedIn • YouTube account has been created, but no videos have been produced and uploaded yet
Videos	<ul style="list-style-type: none"> • Uploading at least 5 videos to the SAPPAN YouTube channel as it is promised in GA
Flyers/brochures	<ul style="list-style-type: none"> • General project flyers will be prepared and available for the next events such as NG-SOC 2020 workshop
Pitch event	<ul style="list-style-type: none"> • Presenting the progress of the project and its advantages and features in the next events including workshops, conferences, and talks in exhibitions • Finding potential stakeholders for the project
Other	<ul style="list-style-type: none"> • Providing a poster of the architecture design once it is amended and updated

5 Conclusion

Currently provided information and presentation materials are the template for SAPPAN deliverables, the SAPPAN logo, introductory presentation slides, the project website and its contents, and social media accounts. Further, SAPPAN is listed in the hub of the research-based European cutting-edge cybersecurity and privacy services, and also SAPPAN-related content is mentioned in partners' websites and other dissemination channels to increase the visibility of the project.

SAPPAN objectives, initiatives, and results were presented in two third party events (58th TF-CSIRT Meeting and 2019 International Summer School on Machine Learning and Security), a FIT inter-department scientific meeting and a joint networking event

with the EU H2020 funded project SOCCRATES. The slides that were presented in the mentioned events are given in the report.

In the last part of the document, planned activities regarding information and presentation are listed in a table. The most important ongoing presentation activity is preparing for the accepted joint workshop with SOCCRATES project (NG-SOC 2020) which will be held in August 2020 in association with ARES 2020.