Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D7.1 Exploitation Plan and Report (M12)

Published by the SAPPAN Consortium

Dissemination Level: Public

H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file: D7.1 Exploitation Plan and Report (M12)
Document version: 1.0
Document owner: Mehdi Akbari Gurabi (FIT)

Work package: WP7
Task: T7.1
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	Lasse Nitz (FIT)	2020-03-23	Preliminary document outline
0.2	Mehdi Akbari Gurabi (FIT)	2020-04-24	Initial draft
0.3	Mehdi Akbari Gurabi (FIT)	2020-04-25	Filling out partners' inputs
1.0	Mehdi Akbari Gurabi (FIT)	2020-04-28	Corrections according to feedback, ready for submission

Internal review history:

Reviewed by	Date	Summary of comments
Alexey Kirichenko (FSC)	2020-04-25	Grammar and spelling check for the executive summary, introduction, and F-secure parts.
Sarka Pekarova (DL)	2020-04-27	Grammar and spelling
Arthur Drichel (RWTH)	2020-04-27	Grammar, spelling and structure

Executive Summary

This is the first exploitation plan for the SAPPAN project. The exploitation plans cover exploitation approaches such as business scenarios and models, knowledge and intellectual property usage, and high impact publications which are assessed as a scientific outcome for research-based institutes and R&D departments of organizations. Individual exploitation plans from each partner focus on innovation aspects, adopting SAPPAN results in the products, gaining experience in the area, and how to support third parties that adopt the SAPPAN results. This report is the first iteration of the exploitation plan and report including the first-year activities of the project. This report will be followed up by deliverables D7.2 and D7.3 throughout the remaining project life cycle.

TABLE OF CONTENTS

1 Introduction

The SAPPAN project works on several components that can be exploited by the partners. Each partner is interested in working on specific SAPPAN components and exploiting the results of their research and activities based on their experiences, requirements, research focus, and market sector. Examples include data sets, anomaly detection algorithms, large-scale data processing set-ups, privacy-preserving techniques. Another exploitation example is the use of SAPPAN experience to improve internal processes, provide training, sell related services, or use it as an input to lectures. Finally, most partners also regard high impact publications as an exploitable asset because either they are research institutes which are directly evaluated and funded based on their scientific output or as it can be used to position an organization in their markets as a thought leader and a high profile provider of services. In the following chapters of this document, the Exploitation plan for each project partner, the amendments of the exploitation plan, and the progress of the exploitation activities per organization in the first 12-months period of the project are reported. The current report is the first iteration of the exploitation plan and report and will be updated yearly by deliverables D7.2 and D7.3 as future iterations.

2 Individual Exploitation Plans of the Project Partners

2.1 **CESNET**

CESNET will utilize SAPPAN results to improve cybersecurity response and recovery tools and procedures in its national and research educational network with more than 300 organizations and 400,000 users. The large backbone network offers a possibility to evaluate the results in comparison with already existing and deployed tools. In particular, SAPPAN will be fed with real online reports on network security events such as reports from honeypots, IDS, and monitoring points observing backbone links at the perimeter of the CESNET network. The amount of data collected every day is more than 2 million reports per day and by exploiting SAPPAN results we envision to aggregate, correlate, filter, and prioritize only the relevant information that will allow to reveal unknown attacks, purpose, and motivation of the attackers, work out the impacts, the damage and causality.

The response actions suggested by SAPPAN will be simulated on real traffic, in particular, suspicious traffic will be diverted to a dedicated box capable of performing response heuristics designed in the SAPPAN project. CESNET-CERT will verify the outputs and will identify any functional issues and scope for improvement.

CESNET will also exploit SAPPAN results to further support the exchange of network security operational as well as forensic data. Since at the end of the project the expected results will be of TRL 6, CESNET will deploy SAPPAN in parallel to its existing tools rather than to replace the existing system directly. However, CESNET is convinced of the need for a complex approach to respond and recover from the cybersecurity threats as well as of a need to address privacy issues of monitoring which are not properly addressed in current tools. Therefore, CESNET will proceed with the development of SAPPAN or its particular parts after the project end to achieve TRL 7. Productional level SAPPAN will then be fully integrated into the incident handling process as the main tool for the CESNET-CERT team to be aware and capable of responding to the cybersecurity issues in CESNET e-infrastructure.

During the project itself, CESNET will utilize its tools developed in other projects to simulate various attacks and inject data on those attacks into the monitoring and response pipeline as well as to utilize tools developed in previous projects to support demonstrate and integrate the SAPPAN results.

Exploitation Plan:

The planned results to be exploited by CESNET will be SAPPAN as a whole component, SAPPAN tools, data sets, and knowledge.

Channels or actions:

CESNET as an NREN, will disseminate SAPPAN and its results to the European NREN community during dedicated meetings such as TNC conference, TF-CSIRT meetings, and GÉANT symposiums. These meetings have high impact on other NRENs which tend to try and adopt best practices of presenting NRENs. CESNET will also advertise SAPPAN at the national level through its own dedicated workshops as well as local conference and meetings for example with the Czech national CSIRT team.

Last but not least, CESNET is a research organization and plans to further undertake research into the topics of collaborative and distributed systems for cybersecurity.

2.2 Dreamlab Technologies

Dreamlab Technologies has more than 20 years of experience in providing consultancy services in a highly confidential environment. Since 1998, Dreamlab has supported military, commercial, governmental, and educational institutions and organizations. The company's main activities are cyber defense, cyber forensics, audits, strategic consulting, and education, as well as the conception, realization, integration, operation, and maintenance of IT solutions based on open standards.

As part of the audit services, Dreamlab provides red-teaming and adversary simulation, which will provide SAPPAN with insights about the attacker's perspective while designing intrusion detection models, and visualizations for incident responders. We expect to develop novel and more accurate adversary simulation tools that allow us to perform experiments on cyber and physical space to gain knowledge about the dynamics of IT and human interaction under cyberattacks. On the defensive side, we would like to increment our capabilities on IDS and SOC solutions with SAPPAN's federated IDS approach.

Exploitation Plan:

Dreamlab plans to exploit the results of novel incident response techniques which include automated or assisted privacy-preserving forensic acquisition, processing and sharing of data, and anomaly detection algorithms in network data and filesystems.

Channels or actions:

- Direct sales of related services in our partner network
- Transferring research into privacy aware LI/SOC solutions
- Conference and workshop presentations

2.3 Fraunhofer FIT

Fraunhofer FIT has been very successful in transferring the latest research results into ready-to-use solutions. The SAPPAN project will provide commercialization opportunities for new algorithms for federated threat detection. FIT will exploit developed tools within other research activities to enhance its capability to deal with new challenges in the intrusion detection area (e.g., integrate it into our Knowledge Pipeline). Besides, the knowledge will be used to provide research and implementation services to our large partner network.

Further, Fraunhofer FIT is active in providing training to organizations in several IT-related areas. Our goal is to also sell training on privacy-preserving intrusion detection and sharing of response and recovery actions and SAPPAN technology in particular.

One of the metrics used to evaluate the Fraunhofer Institute is the publication of scientific work in high level forums.

Hence, we also want to contribute to this activity during the project and use the knowledge gained to continue doing that afterwards.

Exploitation Plan:

Fraunhofer FIT will use formalization of knowledge about incidents response and recovery actions, algorithms for federated threat detection, and cybersecurity data abstractions that allow for anonymous data transit as the results of the project for exploitation.

Channels or actions:

- Direct sales of related services in our partner network
- Training
- High level publication

2.4 F-Secure

F-Secure Corporation provides security technology to defend against both common attacks, such as botnets and ransomware, and advanced attacks, including cyber espionage, and also runs such cybersecurity services as incident response, digital forensics, red teaming, and security consulting activities. While historically F-Secure's focus was on protecting endpoints, the company has been recently investigating options for augmenting endpoint protection mechanisms with network-based ones. The main driver behind this is our new Rapid Detection & Response (RDR) technology, which combines AI methods with top-class security expertise of F-Secure's Rapid Detection Center personnel for guarding organizations against advanced cyberattacks. RDR includes state-of-the-art endpoint behavioral sensors, but we know very well that a holistic view of customer environments is required for detecting sophisticated attacks at early stages.

Through the participation in SAPPAN, we expect to significantly improve our expertise in the network side of security, design and prototype technologies for detecting attack indicators and traces in network traffic, and investigate approaches to combine endpoint- and network-based detection methods. Besides, we see a great opportunity of learning advanced network security techniques from the SAPPAN partners to improve the competitiveness of RDR and other coming F-Secure's solutions.

Exploitation Plan:

The SAPPAN work and outcomes will contribute primarily to F-Secure Rapid Detection & Response (RDR) technology and service and to incident response capabilities of the F-Secure Cybersecurity Services division. We are investing heavily in RDR, which combines automatic attack detection methods with top-class security expertise of F-Secure's Rapid Detection Center personnel for guarding organizations against advanced cyberattacks. Brought by the SAPPAN work, better analytical methods for detecting attacks in network traffic will complement our strong detection capabilities in endpoints, making our service more competitive and, via the use of federated learning-based methods, more scalable, cost-efficient, and non-intrusive. Recommender tools to support response and recovery activities of over 200 of F-Secure's Cybersecurity Services professionals will significantly reduce the amount of manual work, help avoid mistakes and improve their efficiency and customer satisfaction.

On a more concrete level, we expect technical first implementations of several novel methods, including algorithms for modeling network traffic at the endpoint and sending the data to the backend, algorithms for utilizing modeled network traffic information for attack detection and algorithms and processes for combining (modeled) network data with host-based information for attack/threat detection. Furthermore, we expect great value from the evaluation of results of the methods for more detailed decision making on multiple topics: evaluation of the detection performance difference between utilization of raw network data vs. anonymized vs. abstracted, evaluation of the benefit of adding network data (raw/anonymized/abstracted) to host-based data and evaluation of the computational cost of network data modeling/abstraction and required resources.

Channels or actions:

F-Secure will promote the SAPPAN results and technologies based on those to a number of its key customers and partners, including members of its network of more than 200 Internet Service Providers and Mobile Network Operator partners in more than 40 countries around the world. We hope that the work in SAPPAN will lead to strong publications on-network data analytics for security and we will talk about the project advances in public and conference presentations. In the long run, we anticipate using the SAPPAN results as a part of our RDR offering.

2.5 Hewlett Packard Enterprise

Hewlett Packard Enterprise is a multinational company that highly regards the Cybersecurity of its business. The results of SAPPAN are of significant relevance for HPE. The HPE Cyber Defence Centre (CDC) is a dedicated operational department that is responsible for the Cybersecurity of the company. From the early stages of the project, we will collaborate with the CDC. First, during the use-case collection and gap analysis, we will incorporate feedback from the operational perspective on the use-cases specification. Then, the TRL6 results of SAPPAN will be evaluated (in parallel with current tools) in the CDC from the functional and operational point of view. An iterative approach then will aim to onboard SAPPAN results (APIs, algorithms, platform, etc.) in the production routine of the CDC.

Exploitation Plan:

HPE plans to use the results of anomaly detection algorithms, large-scale data processing, privacy-preserving techniques, and SAPPAN-related knowledge as their exploitation strategy.

Channels or actions:

A strong collaboration with the CDC will allow us to productize parts of SAPPAN results in the CDC's daily work in order to increase the security measures.

2.6 **Masaryk University**

SAPPAN will be deployed in the MU network and leveraged in the day-to-day operations of the local Cyber Incident Response Team CSIRT-MU. The deployment fully meets the long-term goals of MU for 2020, strategic priority Information systems, and IT support. The SAPPAN project naturally complements other national research projects of CSIRT-MU, such as "Complex analysis and visualization of large-scale heterogeneous data" (VI20172020096).

The privacy-preserving techniques will be exploited in the GÉANT TF-CSIRT community. The techniques will support the motivation for data sharing inside the community.

The results of the SAPPAN project will be exploited via cooperation with the National Cybersecurity Center of the Czech Republic (NCSC) and Government CERT. We will cooperate on facilitating cybersecurity data and observables to be able to effectively use project concepts within the current architecture for security monitoring of national institutions and critical information infrastructure of the Czech Republic. The creation of advanced security anomalies patterns and best practices for response and recovery created at the global level will contribute to better protection of individual institutional networks and elements of nationally critical information infrastructure.

MU works closely with industry partners through different national projects funded by the Technology Agency of the Czech Republic (e.g., Research and Development of Tools for IT Operations Analytics TH02010185/2016). The SAPPAN outputs will be utilized in further cybersecurity research and industry collaboration opportunities.

Exploitation Plan:

Masaryk University plans to exploit the results of the project such as SAPPAN as a whole component, data selection, preparation, and annotation techniques, anomaly/Intrusion detection algorithms, privacy-preserving techniques, incident handling models, as well as knowledge and visualizations results.

Channels or actions:

MU will promote SAPPAN results and techniques to national authorities (NCSC, Government CSIRT). The results of SAPPAN will further be distributed on the European level among the Trusted introducer TF-CSIRT community, e.g., via presentations on regular community meetings and sharing of knowledge and code.

The novel methods and techniques of SAPPAN will be leveraged in academic research and teaching at the Faculty of Informatics of MU through graduate courses & seminars as well as dissemination of results in other related projects in cooperation with industry partners.

The project will contribute to fulfilling international cooperation key performance indicator of CyberSecurity, CyberCrime, and Critical Information Infrastructures Center of Excellence (C4e) (CZ.02.1.01/0.0/0.0/16_019/0000822) that MU participates in.

We further anticipate that work on SAPPAN will result in strong scientific publications consequently presented in relevant scientific forums that improve the scientific renomé of the MU team in the cybersecurity community.

2.7 **RWTH Aachen University**

RWTH Aachen is a large, research-focused university with a long history of groundbreaking inventions. In this project, the Research Group IT-Security at this university will have the opportunity to use its experience in designing privacy-preserving protocols for various contexts including reconciliation, e-commerce, and medical applications, and leverage their experience with machine-learning-based intrusion detection. We expect to contribute to the field of privacy-preserving data processing by providing efficient building blocks allowing to operate on large-scale data. New insights about the synergy of different privacy notions will be of general interest beyond the scope of intrusion detection and will allow controlling the trade-off between performance and the provided degree of privacy. In addition, we will contribute to privacy-preserving machine learning in the context of the response and recovery life-cycle. It is expected that ongoing as well as upcoming research projects dealing with privacy-preserving in intrusion detection or more generally in machine learning will be able to build on the privacy-preserving techniques devised in this project.

Exploitation Plan:

Novel techniques for privacy-preserving data sharing related to response and recovery as well as intrusion detection will be interesting results for RWTH Aachen University to be exploited. In addition, the exploitation of new mechanisms to enable privacy-preserving federated detection and response handling, and new insights about the compatibility of different privacy notions are in their plan.

Channels or actions:

- High level publications
- Conference and workshop presentations
- Public research talks
- Transferring research results to the classroom
- Involving students via theses, projects, and seminars
- Build on privacy-preserving building blocks and machine-learning-based detection modules in prior projects

2.8 **University of Stuttgart**

The University of Stuttgart has established research institutes in the fields of information visualization, visual analytics, and human-computer interaction. In this environment, USTUTT continues to explore new application areas complementing its strong standing in visual analytics for geo-located and social-media data and visual support for training machine learning algorithms.

As advances in visualization and visual analytics nowadays are mostly domain-driven, SAPPAN will establish a new, exciting application area for USTUTT, thus broadening

the scope of the already existing research on visual analytics for security applications. We expect the work on visualization for SAPPAN to create synergies with existing basic research work in the fields of visual analytics and information visualization for machine learning. Further, the provided input from security practitioners as well as access to real-world big data will be valuable assets for our field of research.

Exploitation Plan:

University of Stuttgart has the plan to exploit the results of novel visualization techniques for situational awareness in the cybersecurity area and for machine learning models, as well as novel techniques for the visualization of uncertainty from different sources. Also, a visual analytics system for cybersecurity including novel techniques of tracking analytical provenance is part of their exploitation plan.

Channels or actions:

- High-level publications, e.g. in “IEEE Transactions on Visualization and Computer Graphics” or “Computer Graphics Forum”
- Conference and workshop presentations, e.g. IEEE VIS (InfoVis, VAST, VizSec), PacificVis and EuroVis
- Public research talks
- Involving students via theses, projects, and seminars

3 Updates on Exploitation Plan

In this section, all changes to the exploitation plan since its most recent iteration are listed with a brief justification of why the change has been done.

The following table will be extended in future iterations of the report.

Organization	Change	Reason
Changes for the initial deliverable at M12		
FSC	The original plan items are valid, this is to add two more items that have grown in priority since the project kick-off and one remark on the exploitation channels: ▪ Results of the work on response recommenders and automation and on methods of visualization are of high value for the FSC Rapid Detection Center (FSC's SOC) personnel, in addition to cybersecurity consultants. ▪ ML models for local attack detection in endpoints and methods of distributed/federated learning for attack detection are of high value for the competitiveness of F-Secure RDR. On the channels side, our growing ecosystem of MSSPs, delivering their services based on the RDR technology, is an important target for exploiting SAPPAN results.	With the core RDR technology, processes, and business operations maturing, we see new opportunities for utilizing SAPPAN results.

4 First Year Overview of Exploitation Activities per Organization

4.1 CESNET

Finished exploitation activities (M12)	No exploitation activities finished in the current reporting period.
Progress towards future exploitation activities until M12	CESNET extended its monitoring infrastructure with capabilities supporting DGA and phishing SAPPAN showcase. The monitoring infrastructure consists of network probes that report statistics on network traffic in the form of NetFlow and IPFIX records. These records are collected by a central collector. The collector is responsible for normalization, storage, resolving queries, and automated analysis. The probes, as well as the collector and all the collector software, were extended with the capability to work with flow records containing DNS and HTTP fields included in the headers of these protocols. Such a capability will be important not only to collect relevant data and demonstrate the showcases but also to deploy the SAPPAN results directly in the infrastructure after the project end.

4.2 Dreamlab Technologies

Finished exploitation activities (M12)	No exploitation activity has been finished in the current reporting period.
Progress towards future exploitation activities until M12	Not applicable yet.

4.3 Fraunhofer FIT

Finished exploitation activities (M12)	No exploitation activity has been finished in the current reporting period.
Progress towards future exploitation activities until M12	Scientific results carried out from the deliverables on the knowledge formalization of response and recovery actions and their triggers (D4.1, D4.2, and D4.3) might be the basis for future publications.

4.4 F-Secure

Finished exploitation activities (M12)	Two models (one local and one global) for detecting anomalous activities in endpoints have been integrated into the F-Secure Detection and Response (RDR) line of products and are being validated in actual security monitoring.

Progress towards future exploitation activities until M12	• One model supporting decision-making for response is introduced to the F-Secure Detection and Response team, integration and internal testing are ongoing. • One model supporting decision-making for response is being integrated as a prototype for testing. • Work started on a model for collaborative filtering of events in endpoints to reduce data transmission and processing costs and reduce the volume of potentially sensitive data that endpoints submit to the security backend.

4.5 Hewlett Packard Enterprise

Finished exploitation activities (M12)	No exploitation activity has been finished in the current reporting period.
Progress towards future exploitation activities until M12	Not applicable yet.

4.6 Masaryk University

Finished exploitation activities (M12)	SAPPAN project contributed to fulfilling international cooperation key performance indicator of CyberSecurity, CyberCrime, and Critical Information Infrastructures Center of Excellence (C4e) (CZ.02.1.01/0.0/0.0/16_019/0000822) that MU participates in.
Progress towards future exploitation activities until M12	Preparation of the host profile visualization for presentation to the CSIRT-MU team. Proposal of the experiment for application monitoring using host- and network-based data that is planned to be published in relevant scientific forums.

4.7 RWTH Aachen University

Finished exploitation activities (M12)	No exploitation activity has been finished in the current reporting period.
Progress towards future exploitation activities until M12	Performed research on DGA detection classifiers, enhancing their detection capabilities and analyzing their real-world applicability including explainability, robustness against adversarial attacks, generalization capability, and real-time capability. Additionally, the class imbalance problem is under analysis for this showcase. This work will as well as the work on phishing certificate detection serve as the basis for future publications. Preliminary planning was done towards a scientific publication regarding endpoint profiling and anomalous behavior detection (cooperation between RWTH and MU).

4.8 University of Stuttgart

Finished exploitation activities (M12)	The current activities with regards to the prototypical process tree visualization and the visualization for DGA detection models are the basis for future publications. Security visualization as a new application area for the institute's activities in the areas of information visualization and Visual Analytics has been established by a first dedicated staff member and two ongoing student theses.
Progress towards future exploitation activities until M12	The main exploitation goal for USTUTT is establishing visualization for cybersecurity as an additional research area at the institute while fostering exchange with other application areas for information visualization and visual analytics. The activities for prototypical visualizations for F-Secure's host-based data and the machine-learning models from RWTH lead to application-driven novel visualization approaches while SAPPAN staff benefits from experience in other application areas available at the institute.

5 Conclusion

The current document is the first iteration of the exploitation plan and report and covers the exploitation activities in the first 12-month period of the project. It revisits the exploitation plan for each organization in the consortium, followed by a list of updates on the exploitation plan during the first year. In this iteration, changes were only applied by F-secure. Subsequently, the exploitation activities that have been done and the progress of ongoing activities per partner are listed. As the SAPPAN project and results are still in the early stage, it is expected that the number of exploitation activities will increase in the future periods of the project. This report will be followed up yearly by deliverables D7.2 and D7.3.