



Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D7.9 Report on Information and Presentation Materials (M36)

Published by the SAPPAN Consortium

Dissemination Level: Public



H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file: D7.9 Report on Information and Presentation Materials – 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)	2022-11-03	Preliminary document outline
0.2	Mehdi Akbari Gurabi (FIT)	2022-04-22	Initial draft with partners' input
0.3	Mehdi Akbari Gurabi (FIT)	2022-04-27	First complete version, ready for review
1.0	Mehdi Akbari Gurabi (FIT)	2022-04-30	Application of reviewer feedback, ready for submission

Internal review history:

Reviewed by	Date	Summary of comments
Avikarsha Mandal (FIT)	2022-04-29	Content enhancement suggestions, grammar and spelling check

Executive Summary

The report on information and presentation materials aims to present the project's public results to all interested target groups. This is the follow-up iteration of the deliverables D7.7 and D7.8 which were submitted at M12 and M24, respectively. This deliverable includes presentation materials that have been created and used in the third year of the project. This is the last iteration of the report.

This report lists all the SAPPAN presentation materials and activities in the third 12-month cycle of the project such as the website updates and social media presence, as well as any project related motivational, promotional or technical presentations. The last part of the deliverable describes planned information and presentation materials after the end of the SAPPAN project.

Table of Contents

EXECUTIVE SUMMARY	3
1 INTRODUCTION	5
2 CREATED INFORMATION AND PRESENTATION MATERIALS M25 – M36	5
2.1 UPDATES ON PROJECT WEBSITE	5
2.2 TWITTER ACCOUNT	8
2.3 YOUTUBE CHANNEL	9
2.4 SAPPAN BLOG POST SERIES	10
2.5 SAPPAN BLOG POSTS IN PARTNERS' CHANNELS	11
2.6 ERCIM NEWS ARTICLES	12
2.7 THE ORGANISATION OF NG-SOC 2021 WORKSHOP	12
2.8 PREPARATION OF NG-SOC 2022 WORKSHOP	18
2.9 JOINT SOCCRATES-SAPPAN WEBINAR: DETECTING DGA RELATED THREATS	18
2.10 2ND JOINT WORKSHOP - DYNAMIC COUNTERING OF CYBER-ATTACKS	21
2.11 SAPPAN FINAL EVENT	24
3 SHORT SUMMARY OF SAPPAN PRESENTATIONS IN THE EVENTS	30
3.1 SWISS CYBER SECURITY DAYS 2022	30
3.2 MITRE AFRICA / EMEA CONFERENCE	31
3.3 2021+2022 TF-CSIRT MEETINGS & FIRST REGIONAL SYMPOSIUM EUROPE	33
3.4 SECRIPT 2021	35
3.5 PST 2021 CONFERENCE	39
3.6 DFRWS EU 2022	41
3.7 SLUSH 2021	43
3.8 HPE SECURITY SUMMIT 2021	43
3.9 HPE WIS GROUP (WOMEN IN SECURITY) WEBINAR	45
3.10 GRASEC WORKSHOP (AT NOMS 2022 CONFERENCE)	46
4 FUTURE PLANS FOR INFORMATION AND PRESENTATION MATERIALS	47
5 CONCLUSION	47

1 Introduction

This report aims to summarize the current information and presentation materials of SAPPAN. It lists general presentations of the consortium and individual presentations of the partners in events to disseminate SAPPAN goals and results.

The information and presentation materials are used to bring the project's vision, components, results, and experiences obtained throughout the project to the public in scientific and non-scientific events. These activities are focused on raising awareness, showing and explaining SAPPAN results to reach experts and other target audiences, and increasing the synergy in the cybersecurity research area with other parties.

The rest of this document is organised as follows. Section 2 describes the general created information and presentation materials. Section 3 includes short summaries of presentations at events. Lastly, Section 4 lists the future plans for information and presentation materials after the end of the project.

This is the third and last iteration of the report on information and presentation materials after D7.7 and D7.8. This report focuses on the third year of the project (M25-M36) as the reporting period.

2 Created Information and Presentation Materials M25 – M36

In this section, we briefly report the information and presentation materials that are generated or updated in the third year of the project's lifetime.

2.1 Updates on Project Website

During the third year of the project (M25 – M36), the project website received several upgrades and provided more information about the project's progress and objectives. Thus, new visitors are more likely to learn more about the project and already interested people are more likely to revisit the website to view the continuously updated content. The project website is the key dissemination and communication channel. Information about the consortium, each consortium members, project objectives and advisory board members are available on the website. The home page and the page showing the project partners are presented in the following pictures. The project website is accessible via <https://sappan-project.eu/>





We continued updates on partners' information including F-Secure rebranding, which is announced on the 22nd of March 2022 with a press release (Link: <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™. 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). We also announced it by a post on the website news section (Link: <https://sappan-project.eu/?p=2067>). However, in our deliverables, we constantly use F-secure (in abbreviation FSC) for the sake of consistency.



HOME PROJECT RESULTS NEWS BLOG POSTS

WithSecure

Logo:

Website:

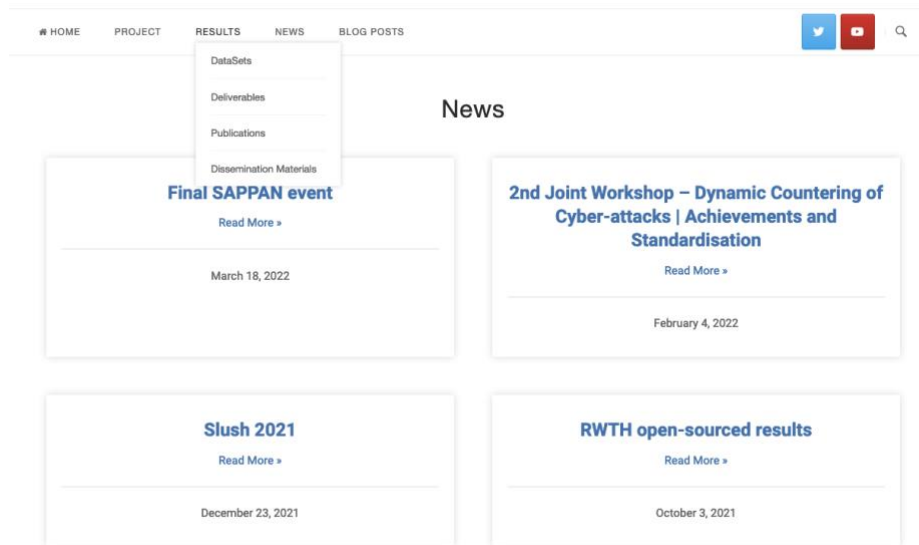
<https://www.withsecure.com>

Country:

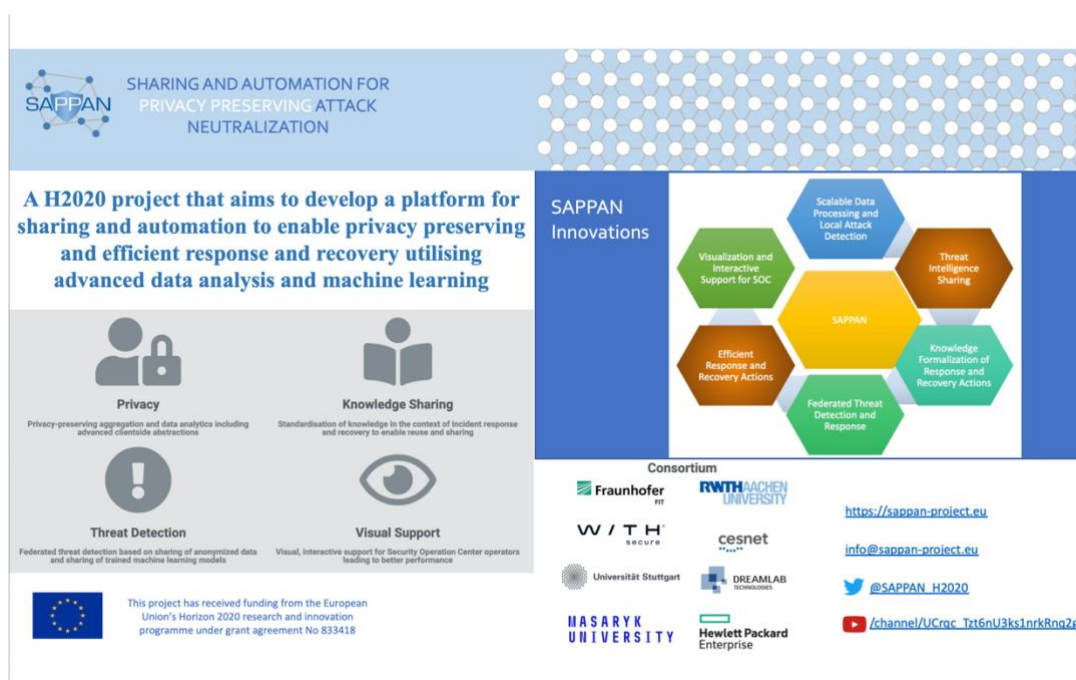
WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd. We are a founding member of the European Cyber Security Organization (ECSO).

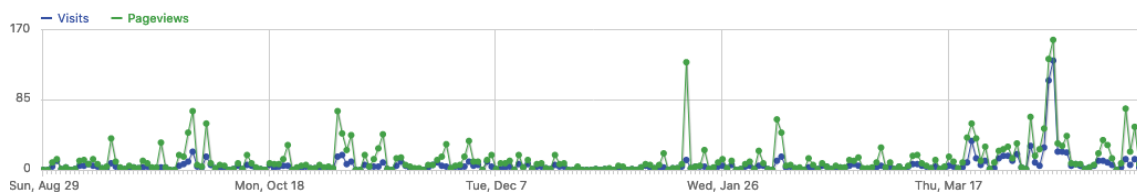
We have been continuously adding important news, which is related to the SAPPAN project on the website and have been uploading any dissemination material arising in a timely manner. These materials include the public deliverables as soon as we receive EU confirmation, public datasets, the project's scientific publications, and other dissemination materials such as partners' blog posts and presentations. Furthermore, we established a blog post series aimed to present the project results to more general audiences. The following picture shows the news page in addition to the menu bar for public datasets, EC confirmed public deliverables, scientific publications, and other dissemination materials.



Additionally, we prepared a new flyer for the project, as it is shown in the following picture. It is available on the dissemination materials page on the website. The direct link to the flyer is: https://sappan-project.eu/wp-content/uploads/2022/04/SAPPAN_flyer.pdf



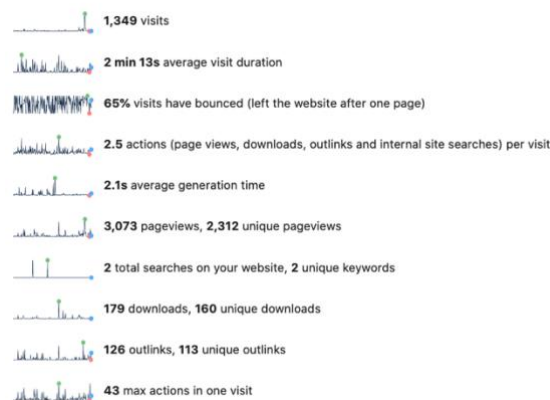
Further, we have collected the traffic and visit statistics of the project to address EC feedback from the mid-term review. To determine the popularity of the website and the number of visits from different categories, we collect anonymized data. For this reason, we use Matomo (<https://matomo.org/>). Matomo is a free and open-source web analytics tool that we operate securely through the Fraunhofer host. The only purpose of the collected data is to create aggregated graphs to display the traffic load and the data is not used for any other purposes. Moreover, we update our privacy policy to include the purpose of data collection and provide an opt-out option to disable it. We only have enabled the web analytics tool since the end of August 2021. Therefore, we only collect the website visits for the last eight months of the project. We had over 1300 unique visitors with more than 3000 page views. The general statistics about the website in the last 8 months period of the project are illustrated in the pictures below.



Channel Types

CHANNEL TYPE	VISITS	ACTIONS	ACTIONS PER VISIT	AVG. TIME ON WEBSITE	BOUNCE RATE
Direct Entry	740	2,157	2.9	2 min 36s	60%
Social Networks	264	490	1.9	1 min 53s	79%
Search Engines	246	545	2.2	1 min 41s	65%
Websites	69	154	2.2	1 min 57s	62%
Campaigns	30	34	1.1	52s	90%

Visits Overview



2.2 Twitter Account

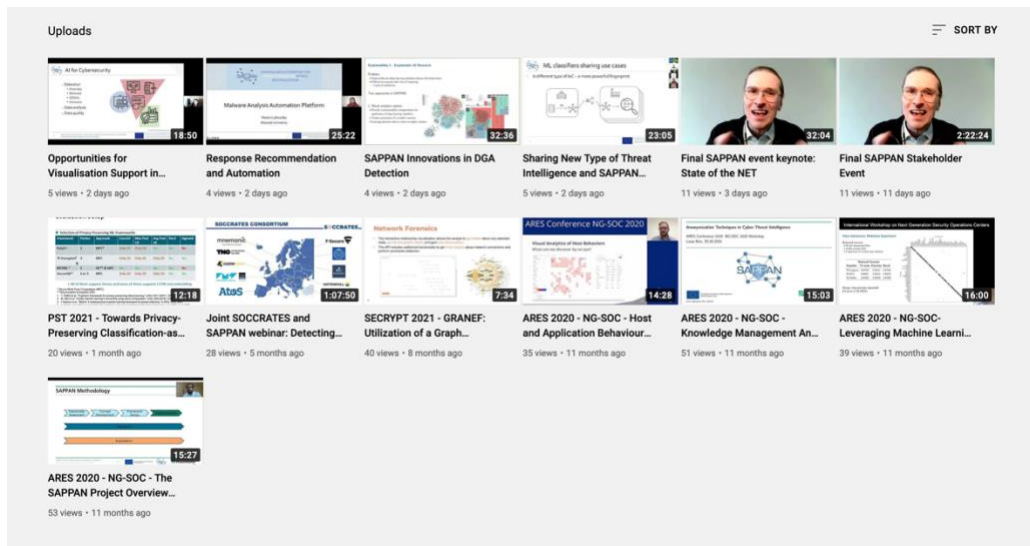
We actively present on social media by our Twitter account to enable communication with other cybersecurity projects and increase the visibility of SAPPAN to the domain experts, potential stakeholders, and other target groups. We continuously report our progress, results and events in our account. So far, we have around 400 followers on Twitter and more than 100 tweets about the progress of the project and other project-related news. We also had over 38000 impressions on our account based on the Twitter analytics report. The following figures show the Twitter profile (https://twitter.com/SAPPAN_H2020) of the project and the statistics of the account from the beginning to the 28th of April.



2.3 YouTube Channel

SAPPAN YouTube channel has been created in January 2020. Currently, 13 presentation videos have been uploaded to the channel. These videos include four SAPPAN public videos of the NG-SOC 2020 workshop, six recordings from the SAPPAN final event, one webinar, and two presentations at the conferences. Also, we have a public playlist of the SAPPAN talks in the other events. At the time of writing this report, the videos uploaded to our channel cumulatively reached around 400 views. The following picture shows the uploaded videos on the channel so far.

Link: https://www.youtube.com/channel/UCrqc_Tzt6nU3ks1nrkRnq2g




2.4 SAPPAN Blog Post Series

As we revisited the dissemination strategy of the SAPPAN project 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 target general audiences in contrast to the technical deliverables and scientific publications. We establish a blog post series from October 2021 with monthly updates. We also create a blog post template and guidelines about the level of details and structure of the blog posts. We distribute the news via our social media channels, as well as partners' communication channels. As an example, FSC's blog post is presented as follows in the ECSO awareness calendar in April 2022.

Link: <https://www.ecs-org.eu/documents/publications/6256822ca926c.pdf>

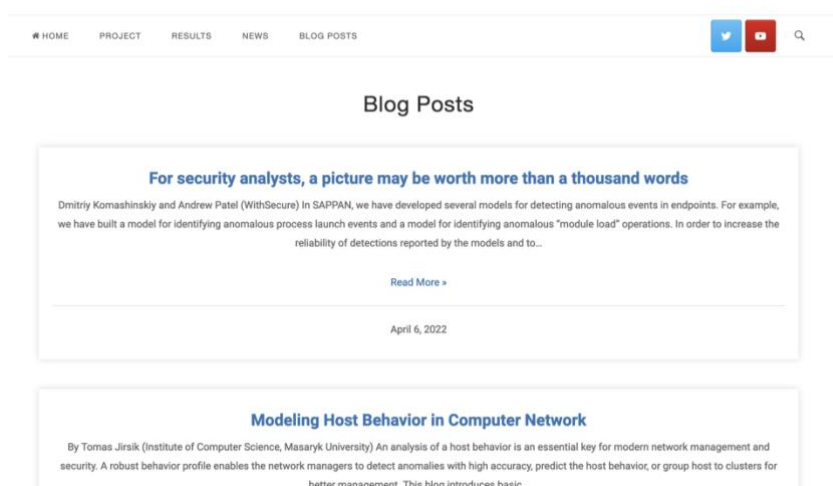
Cybersecurity and Machine Learning Supporting Each Other

WithSecure™, formerly known as F-Secure Business, continues its research efforts in topics connecting cybersecurity and machine learning. In SAPPAN (has received grant agreement No 833418 under the EU's H2020 research and innovation programme), we have developed several models for detecting anomalous events in endpoints. To increase the reliability of detections reported by the models and to support security analysts in handling those detections, we have experimented with combining detected anomalies in so-called provenance graphs. Our initial approach is presented [here](#). WithSecure has been building its expertise and capabilities in the security of the machine learning domain. As part of our activities in SPATIAL (grant agreement No 101021808 under the EU's H2020 programme), we designed a security [self-assessment questionnaire](#) for machine learning-based systems. The questionnaire aims to help organisations assess their posture in security of machine learning and to let WithSecure better understand real-world machine learning security challenges.



The blog post series helped us to increase the project's online visibility. All the blog posts are publicly accessible via a separate section of the SAPPAN website.

Link: https://sappan-project.eu/?page_id=1243



The following table lists the current blog posts available on the website, as well as their authors and direct links.

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

2.5 SAPPAN Blog Posts in Partners' Channels

The following table lists the blog posts related to SAPPAN on our partners' websites in the period of this report (M25-M36).

Beneficiary	Type	Title	Link of SAPPAN-related blog posts and news
DreamLab	Blog post	Detecting suspicious *.ch-domains using deep neural networks	https://dreamlab.net/en/blog/post/detecting-suspicious-ch-domains-using-deep-neural-networks/

2.6 ERCIM News Articles

ERCIM News is the magazine of the European Research Consortium for Informatics and Mathematics (ERCIM). The main objective of the magazine is to reflect the contribution made by ERCIM to the European Community in Information Technology through short articles and news items. It provides a pool for the exchange of information between the institutes and also with the wider scientific community and experts. ERCIM News enables an opportunity to present the high-level research items to a broad audience inside and outside of the usual research community. The magazine is published in the physical and online format and reaches about 10,000 audiences in the field widely distributed in the European Commission. More information about the magazine is available here: <https://ercim-news.ercim.eu/about-ercim-news>

Two ERCIM articles by SAPPAN have been published in the magazine two editions of the magazine related to SAPPAN research on July 2021 and April 2022:

- "Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery" in ERCIM news 126 in the special theme track "Privacy preserving computation". Direct link to the online version (2291 hits): <https://ercim-news.ercim.eu/en126/special/towards-privacy-preserving-sharing-of-cyber-threat-intelligence-for-effective-response-and-recovery>
- "From Collaboration to Automation: A Proof of Concept for Improved Incident Response" in ERCIM News 129 in the special theme track "Fighting Cybercrime". Direct link to the online version of the article (471 hits): <https://ercim-news.ercim.eu/en129/special/from-collaboration-to-automation-a-proof-of-concept-for-improved-incident-response>



2.7 The Organisation of NG-SOC 2021 Workshop

Together with the consortium of the EU project SOCCRATES, SAPPAN organised the 3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) for the second time alongside ARES 2021 (<https://2021.ares-conference.eu/conference-2021/detailed-program/>). The NG-SOC 2021 workshop aimed to create a forum for researchers and experts to discuss the challenges associated with SOC operations and focused on research contributions to address

these challenges. In contrast to the previous year, we organised a Call for Papers for the workshop and requested contributions for peer review. The call for peer-reviewed publications has been a step towards establishing the workshop as a respected forum for research contributions on SOC operations and has helped to gain visibility within the community. The workshop details and CfP are available at: <https://2021.ares-conference.eu/workshops-eu-symposium/ng-soc-2021/index.html>

Moreover, selected members of the projects' consortia presented their research activities. The workshop includes a keynote speech with the title "Scaling or Failing Cybersecurity?". This workshop took place online on Tuesday, 17th of August 2021, 13:45 – 18:45. The full agenda of the event is as follows.

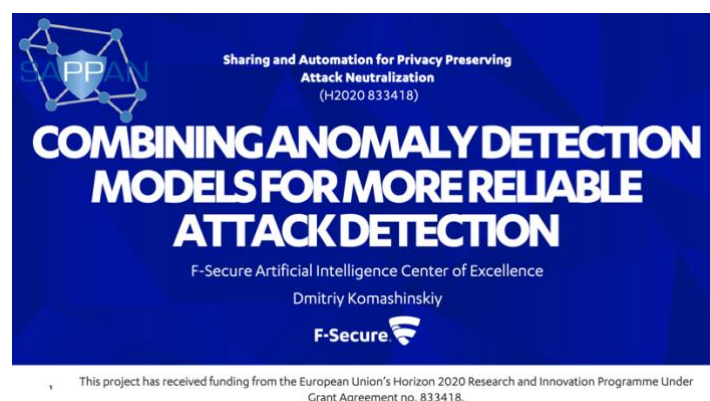
Event Agenda:

Time	Talks
13:45 - 14:00	Welcome and Workshop Overview Ewa Piatkowska (AIT Austrian Institute of Technology, Austria)
NG - SOC I	
Session Chair: Irina Chiscop, TNO, The Netherlands	
14:00 - 14:20	System for Continuous Collection of Contextual Information for Network Security Management and Incident Handling Martin Husák, Martin Laštovička, Daniel Tovarňák (Masaryk University, Czech Republic)
14:20 - 14:40	On the Evaluation of Sequential Machine Learning for Network Intrusion Detection Andrea Corsini (University of Modena and Reggio Emilia, Italy), Shanchieh Jay Yang (Rochester Institute of Technology, USA), Giovanni Apruzzese (University of Liechtenstein, Liechtenstein)
14:40 - 15:00	A Recommender System for Tracking Vulnerabilities Philip Huff, (Kylie McClanahan University of Arkansas, USA), Thao Le (Bastazo Inc., USA) and Qinghua Li (University of Arkansas, USA)
NG - SOC II	
Session Chair: Tomáš Jirsík, Masaryk University, Czech Republic	
15:30 - 16:10	Keynote: Scaling or Failing Cybersecurity? Frode Hommedal, Chief Technology Officer and head of Cyber Threat Operations (Defendable, Norway)
16:10 - 16:30	Combining anomaly detection models for more reliable attack detection Dmitriy Komashinskiy (F-Secure, Finland)
16:30 - 16:50	Quantitative Impact Analysis Christophe Kiennert (Télécom SudParis, France)

NG - SOC III	
Session Chair: Avikarsha Mandal, Fraunhofer FIT, Germany	
17:15 - 17:35	Adversary Emulation Planner: Generating MITRE ATT&CK Technique Sequences Martin Eian (mnemonic, Norway)
17:35 - 17:55	Graph-based Network Traffic Analysis for Incident Investigation Milan Cermak (Masaryk University, Czech Republic)
17:55 - 18:15	Automated Infrastructure Modelling – Foundation for Security Operations Ville Alkkiomäki (F-Secure, Finland)
18:15 - 18:35	Taking a look at the *.ch zone with a DGA detector Mischa Obrecht (DreamLab Technologies AG, Switzerland)
18:35 - 18:45	Wrap Up Ewa Piatkowska (AIT Austrian Institute of Technology, Austria)

SAPPAN colleagues chaired two sessions and prepared three talks about the SAPPAN results highlighted in the table above.

The first talk, "Combining Anomaly Detection Models for More Reliable Attack Detection" presented by Dmitriy Komashinskiy focused on models for detecting security-related anomalies in endpoints and on approaches to combining observations of such models via provenance graphs. Here you can see some sample slides. The full slides are available on the SAPPAN website: https://sappan-project.eu/wp-content/uploads/2022/04/ARES_Workshop_slides_2021_final.pdf



THRESHOLD: 40



16

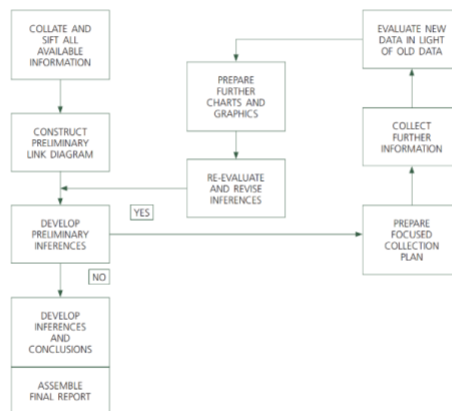


The second talk was presented by Milan Cermak presenting "Graph-based Network Traffic Analysis for Incident Investigation". Although network traffic is typically encrypted, and it is almost impossible to look into the content of transmitted data, the analysis of metadata and characteristics of each connection still plays an important role in an incident or criminal investigation. Significant development of various approaches for storing and analysing large-scale data offers great potential for expert analysts performing digital forensics and network traffic investigation, as it corresponds to their natural perception of the data. In the following, some sample slides are presented. The full slides are available on the SAPPAN website: <https://sappan-project.eu/wp-content/uploads/2022/04/2021-ARES-graph-based-network-traffic-analysis-for-incident-investigation-presentation.pdf>

The image shows the top section of a presentation slide. On the left is the SAPPAN logo, which consists of a blue shield with the word 'SAPPAN' in white, surrounded by a network of blue nodes and orange lines. To the right of the logo, the text 'SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION' is displayed in blue, uppercase letters. The background of this section is light blue with a pattern of small white stars on the left and right sides.



Criminal Investigation and Link Analysis



United Nations Office on Drugs and Crime (UNODC) – [Criminal Intelligence: Manual for Analysts](#)

7



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

The third talk presented by Mischa Obrecht was about the result of the Dreamlab investigation on DGA detection: "Taking a look at the *.ch zone with a DGA detector". They utilise SAPPAN results for the investigation of DGA detection in domains from Switzerland. Sample slides are shown as follows. The full slides are available on the SAPPAN website:

https://sappan-project.eu/wp-content/uploads/2022/04/ARES_SAPPAN_2021_DGA-CH-TLD.pdf



Dreamlab Technologies

Taking a look at the *.ch zone with a DGA detector

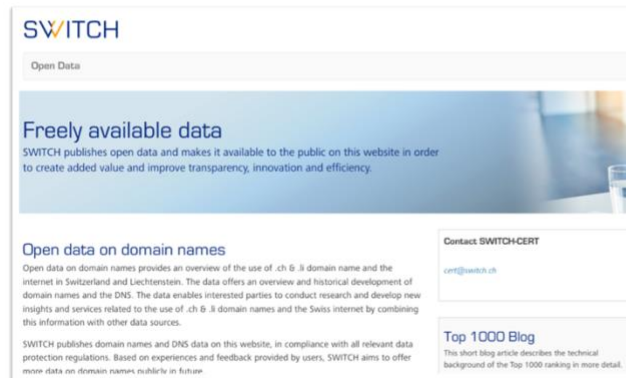


2021



Introduction

switch.ch publishes *.ch and *.li zonefiles



2260606
Entries for .ch

Dreamlab Technologies AG

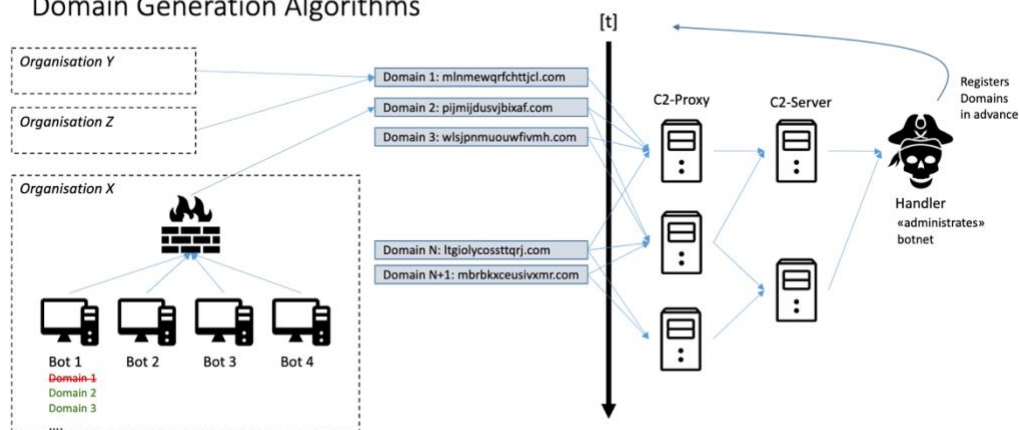
www.dreamlab.net

5



Introduction

Domain Generation Algorithms



Dreamlab Technologies AG

www.dreamlab.net

6



Methodology

Model 1 (B-NYU)

Model 2 (B-ResNet)

Training Iteration 1

- Benign Training-Set: Cisco¹ Popularity List Top 1m
- Malicious Training-Set: Netlab OpenData Project's DGA Domain List²

Analysis Iteration 1

- Test Dataset: *.ch-Zonefile

Training Iteration 2

- Benign Training-Set: Cisco Popularity List Top 1m + Part of *.ch Zonefile with existing MX-record
- Malicious Training-Set: Netlab OpenData Project's DGA Domain List

Analysis Iteration 2

- Test Dataset: *.ch-Zonefile
- Manual verification of results

¹Cisco Umbrella Project - <https://s3-us-west-1.amazonaws.com/umbrella-static/index.html>
²<https://data.netlab.360.com/dga>

Dreamlab Technologies AG

www.dreamlab.net

10

2.8 Preparation of NG-SOC 2022 Workshop

We plan to hold the 4th International Workshop on Next Generation Security Operations Centers (NG-SOC 2022) in collaboration with SOCCRATES and CyberSEAS H2020 EU projects after the end of the SAPPAN project. All members of SOCCRATES, SAPPAN and CyberSEAS consortia, all members of the advisory boards of the projects, all projects funded in the same topic or same EU call, and individual networks of workshop chairs will be invited to the event. The event will take place on the 23rd of August, 2022 in conjunction with the 17th International Conference on Availability, Reliability and Security (ARES 2022). The draft programme is now available as follows.

DRAFT Programme:

Project	Speaker	Affiliation	Topic
SOCCRATES	Mathias Ekstedt, Giuseppe Nebbione	Foreseeti, KTH	Reinforcement learning-based Courses of Action
	Zsolt Kucsavan	UTwente	Automating playbook generation
	Irina Chiscop, Francesca Soro	TNO, AIT	Detection of automatically generated domains
SAPPAN	Dmitriy Komashinskiy	WithSecure	An approach to analysis of detected anomalies in endpoints
CyberSEAS	Luigi Coppolino	CINI	Prevention of cyber threats in supply chains
	Paolo Rocchetti	ENG	CyberSEAS presentation and its technical ambition

In addition to these presentations, we expect to have a keynote. The speaker and the topic are yet to be confirmed. More information about the event is available here: <https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2022/>

2.9 Joint SOCCRATES-SAPPAN Webinar: Detecting DGA Related Threats

To disseminate our research results to a more general audience, we decided to co-organise a webinar session with the SOCCRATES H2020 project. As the results of these two projects converge in some use cases and research areas, we find Domain Generation Algorithms (DGAs) detection an interesting mutual theme. DGAs are often operated by botnets to sustain their criminal activity by rotating Command and Control (C2) domains at a great pace. Blocking or seizing such dynamic and random-looking C2 domains is a major challenge for defenders and law enforcement. In this joint theme session, two projects explained the nature and magnitude of the DGA problem and present some of the novel techniques that they have pursued to combat DGAs more effectively. The session included a short overview of both projects followed by a demonstration of the “DGA Detective” solution that was developed by the SOCCRATES and an overview of both academic and operational real-life impact that SAPPAN and SOCCRATES have achieved to date. We decided to use the SOCCRATES website as the main communication channel also for the registration

(Link: <https://www.socrates.eu/webinars/novel-approaches-to-detecting-dga-related-threats/>) However, we distribute the event information on the SAPPAN website and social media. The webinar was held on September 28, 2021. Also, the recorded video of the event is available on the SAPPAN YouTube channel (Link: <https://www.youtube.com/watch?v=FwLSQpPUH0M>) Also, SAPPAN presentations are available on the SAPPAN website via the following links:

- SAPPAN overview: <https://sappan-project.eu/wp-content/uploads/2022/04/SAPPAN-project-introduction.pdf>
- SAPPAN innovations in DGA detection: <https://sappan-project.eu/wp-content/uploads/2022/04/socrates-sappan-webinar-dga-1.pdf>



SOCRATES
SOC & CSIRT Response to Attacks
& Threats based on attack defence
graphs Evaluation Systems



SAPPAN
SHARING AND AUTOMATION FOR
PRIVACY PRESERVING ATTACK
NEUTRALIZATION

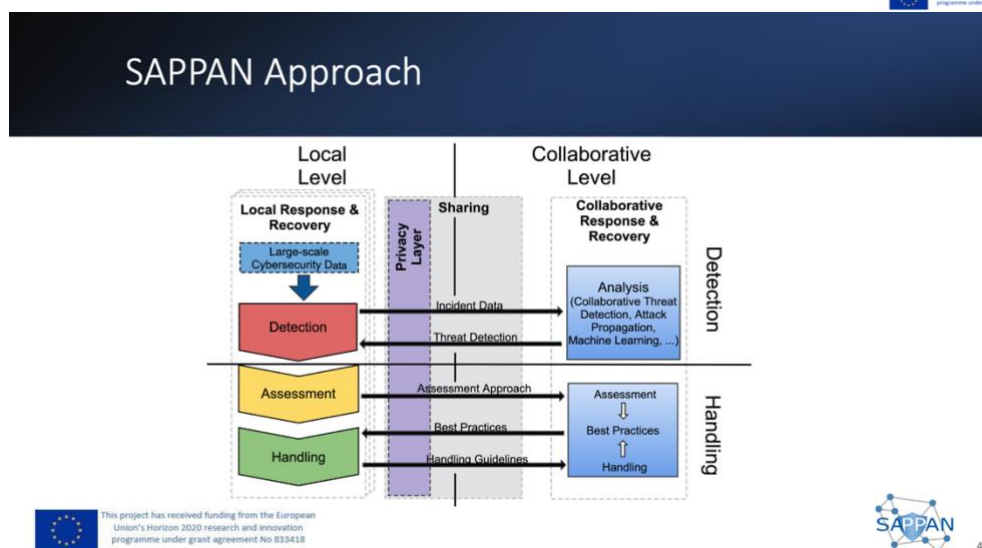


SAPPAN Project Presentation

Theme session: Detecting DGA related threats

Avikarsha Mandal
Fraunhofer FIT, Germany

Tuesday September 28th 2021, 15.30 – 17.00 CET





SAPPAN Innovation in DGA Detection

Arthur Drichel
RWTH Aachen University
Research Group IT-Security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418.






Use-case DGA Detection in SAPPAN

- Research driven approach
- 6 peer-reviewed accepted papers on DGA detection
 - 1 paper currently under review

- Real-world application of research results
- Classifiers are real-time capable & scalable
 - Integration of research into existing Security Information and Event Management (SIEM) solutions



Explainability I - Explainable AI Research

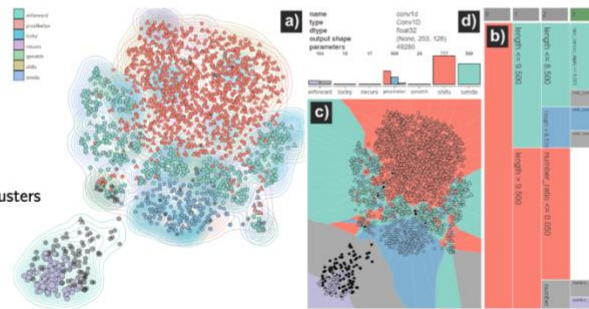
Problem:

- State-of-the-art deep learning classifiers behave like black boxes
- Difficult to evaluate their line of reasoning
 - Lack of confidence

Two approaches in SAPPAN:

1. Visual analytics system:

- Provide understandable interpretations for predictions of deep learning classifiers
- Cluster activations of a model's neurons
- Leverage decision trees in order to explain clusters



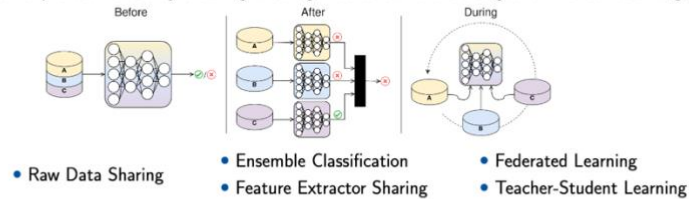
6

Collaborative Machine Learning - Privacy-Preserving Intelligence Sharing

Problem:

- How to improve detection by collaboration?
- Decision models are directly influenced by sensitive training data
- Models are susceptible to leak such sensitive information

Improve generalization and performance by sharing intelligence at different stages of model training:



Our empirical study shows Feature Extractor Sharing and Federated Learning perform best:

- Significant reduction of false positive rate (FPR), up to 50% compared to single-party
- Reduction rate of FPR correlates with increasing number of parties
- Preliminary privacy-utility trade-off study

8

Privacy-Preserving Classification as a Service (CaaS)

Problem:

- Real-world training data is mandatory for well performing classifiers
- What about resource constrained devices?
- Domain names / trained models may contain privacy-critical information



Naive application of privacy-preserving ML frameworks to existing DGA detection classifiers

→ Single inference can cost additional: 13 min inference latency, 234 GB communication

Comprehensive study & proposed model simplifications:

- Reduction in inference latency of up to 95%
- Reduction in communication complexity of up to 97%
- Accuracy penalty of less than 0.17%

→ Still, future work is required to make privacy-preserving CaaS feasible!

10

DGA Detection - Current Research & Future Work

Robustness

- NX-classifiers more robust against adversarial attacks
- Usage of adversarial machine learning to improve robustness

New DGA detection

- Real-world experiment: 6 unknown DGAs, 1 unknown Bamital seed
- Adaptive new DGA detection system

manipulation-want-date.pw
refers-spare-criticism.pp.ua
fashioned-achieve-disable.pro

(a) Unknown DGA 1

dv4850fc.co.ir
thrsssk05.co.ir
thr10pg13.co.ir

(c) Unknown DGA 3

2b4b1d67-b38a-40c1-ba3e-af73245d7b14.com
86a94dd8-5724-4b9a-8a7a-bea8733f7e60.com
adcb3f60-d260-478a-99f2-ac24eea1de16.com

(e) Unknown DGA 5

egbvalb5pgh7fb.jmrboqa6i67zd1rwhj.com
27422j8tqot.8chcu-tza86fxaz-df70y9-t8o.com
bt-7hb7k0aqqyr-61d8o5d.dg88rz6qobme421f.com

(f) Unknown DGA 6

02836ae5435c57300fc95bf13e9ba7bb.info
073fcd0286615c7a5ac348f9a1ab0250.info
08211a534fad3885624a92573cc2af44.info

(g) Unknown seed of Bamital

go2mysuite.eu
citrixgo2mypc.co.uk
gotomobileaccess.com

(b) Unknown DGA 2

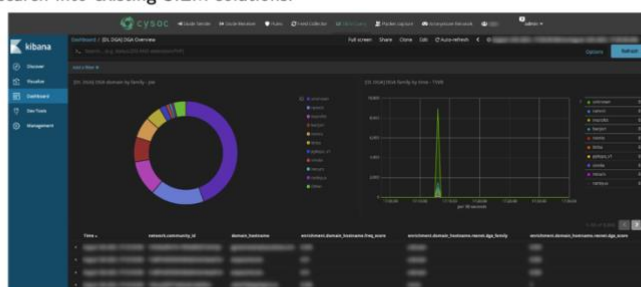
www.c75ff6bd.com
www.94e47d25.com
www.41019163.com

(d) Unknown DGA 4

11

Impact of SAPPAN Innovations II

Integration of research into existing SIEM solutions:



Facilitating the work of Security Operation Center (SOC) analysts

- Improvement of detection performance
- Reduction of false positives
- Providing explanations for predictions

14

2.10 2nd Joint Workshop - Dynamic Countering of Cyber-attacks

On the 8th of February 2022 the 2nd Joint Workshop of Dynamic Countering of Cyber-Attacks Projects, Achievements and Standardisation, took place online between 9:00 and 16:00 CET on February 8th 2022. This workshop was organised as the follow up to the first edition back in 2021. The workshop aimed at gathering the projects from the SU-ICT-01-2018 H2020 call, whose main topic is Dynamic countering of cyber-attacks, to share the main progress of the project, create synergies and set a common ground for standardisation activities, with guest speakers from Concordia project, ENISA, and StandICT. Moreover, experts representing each project discussed the different approaches to the common problem of attack detection and situational awareness in different environments. The workshop is organised by the CyberSANE EU project and supported by Fiware Foundation with the collaboration of SAPPAN, C4IoT, CAMEL, GUARD, SIMARGL, and SOCCRATES. This workshop was a public event and advertised via the Eventbrite platform. More information about the event is available here: <https://www.cybersane-project.eu/standardisation-workshop-2022/>



We distribute the information about the event on our website and Twitter account to reach a broader range of audiences.

Further, SAPPAN was mainly responsible for involving ENISA and inviting the keynote speaker to this event. The workshop Keynote was "From Security Operations Centres (SOCs) to securing machine learning: opportunities to enhance cybersecurity in Europe" by Dr Ioannis Agrafiotis from European Union Agency for Cybersecurity (ENISA).

SAPPAN consortium presented one project introduction and four technical presentations at the event.

Avikarsha Mandal from Fraunhofer FIT presented "An Overview of SAPPAN project", then Martin Zadnik from CESNET presented "Sharing Cybersecurity playbooks". After that, Martin Laštovička from Masaryk University presented "Malware Analysis Automation Platform". The presentation provided information about the development of the prototype by the CSIRT-MU team in course of SAPPAN for automation of response to malware detection. At the end of the session, Willie Victor from F-Secure presented "Response Recommendation Datasets". The slide set of the presentation is available on the SAPPAN website: <https://sappan-project.eu/wp-content/uploads/2022/04/SAPPAN-jointworkshop.pdf>



SAPPAN Innovations

5

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Sharing cybersecurity playbooks

- Multiple playbook formats
 - Workflows
 - SAPPAN
 - CACAO
- Uniform sharing format needed
 - CACAO covers it all
- MISP integration
- Table with metadata and playbook

Playbook standard
Playbook type
Description
Label
Abstraction
Validity
Playbook

9

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Platform Architecture

12

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Response Action Data

- Response workflows are generally well recorded
 - Needed for accountability, since response actions tend to be invasive
 - Also useful for personnel training purposes
- Specific actions can often be linked to elements of an incident at a *high level*
- Fine-grained *causal* relationships tend to be missing
 - "Response action X was directly related to observations A, B, and C in data"
- To enable effective and accurate assistive technologies for tactical incident response scenarios, strong "action -> cause" links are needed

26

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

In another session, Martin Zadnik presented "SAPPAN: Standardisation of cybersecurity playbooks". The presentation provided an overview of the SAPPAN effort to standardise the response and recovery steps and cooperation with the OASIS TC CACAO on the integration of the standard into the MISP ecosystem. The slide set of this presentation is available on the SAPPAN website as well: <https://sappan-project.eu/wp-content/uploads/2022/04/sappan-standardisation-playbooks.pdf>

SAPPAN: Standardization of cybersecurity playbooks

Martin Zadnik
CESNET

1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Playbooks intro

- The response handling information captures guidelines for the particular phase in incident handling life cycle (preparation, analysis, containment, post-incident) and the particular threat/attack/incident. The guidelines are often documented as playbooks that are high-level human-readable, written in plain text without structure.
- One of the SAPPAN goals was to give structure to playbooks to make them machine-readable and actionable.

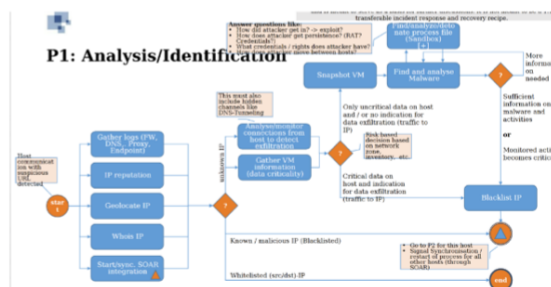
2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418



SAPPAN playbook

- SAPPAN created its standard to capture cybersecurity response and recovery actions 1/2021
- Approximately at the same time we discovered there is Technical Committee CACAO under OASIS introducing its standard for cybersecurity playbooks



3



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418



Sharing playbooks

- We got in touch with the CACAO TC
- Discussed our next goal to share the playbooks
- Proposed an implementation of playbook representation in MISP
- After fine-tuning details we pushed the cybersecurity playbook object data model in MISP repository with positive reaction from A. Dulanoy (CIRCL.LU)
- Joint paper describing our effort
 - Mavroedis, V. et al: On the Integration of Course of Action Playbooks into Shareable Cyber Threat Intelligence.

4



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

2.11 SAPPAN Final Event

The final stakeholder event has been held online for the public audience. The event aimed to present advanced data acquisition, threat analysis, visualisation, and privacy-aware sharing and distribution of threat intelligence to dynamically support human operators in incident management. The event started with a keynote speech by Mikko Hyppönen from WithSecure (<https://mikko.com/>), who gave a talk on "STATE OF THE NET", followed by presentations about selected key results of SAPPAN.

We provided a flyer for the event available on the SAPPAN website: https://sappan-project.eu/wp-content/uploads/2022/03/Stakeholder_Event-1.pdf



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 Hronis (HPE Ireland)
15:25-15:35	Coffee Break	--
15:35 - 16:00	Response Recommendation and Automation	David Karpuk (F-Secure), Martin Laštovička (Masaryk University), Mircha 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	--

Technical speakers:



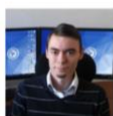
Franziska Becker, Researcher

Franziska studied cognitive science and computer science at the University of Osnabrück before joining the visualization institute (VIS) at the University of Stuttgart as a PhD. Her main research topics include visualization for explainable artificial intelligence as well as sensemaking and decision making with visualization.



Arthur Drichel, Researcher

Arthur Drichel received the B.Sc. and M.Sc. degrees in Computer Science from RWTH Aachen University. He is a researcher at the Research Group IT-Security at RWTH Aachen University. His research interests lie primarily in the areas of intrusion detection systems, machine learning, and privacy enhancing technologies.



Martin Laštovička, Head of the cybersecurity operations group

Martin Laštovička obtained his Ph.D. in Informatics at the Faculty of Informatics, Masaryk University, Czech Republic, and currently works as the head of the cybersecurity operations group in CSIRT-MU. His research topic lies in network traffic analysis and practical applications of machine learning to build Cyber Situational Awareness through the identification of network entities and their relationships. His focus is to apply research outputs to real-world data and enhance operations of the CSIRT-MU team.



Robert Rapp, Researcher

Robert Rapp is a PhD Student at the Visualisation and Interactive Systems Institute (VIS) at the University of Stuttgart. After graduating with a degree in business informatics, he started his research in visual cyber analytics. As part of the Horizon 2020 project EU: SAPPAN his current work focuses on visual analysis of endpoint sensor data and analytical provenance in web interfaces.



Martin Zadnik, Network cybersecurity researcher

Martin Zadnik is a deputy leader at the department of tools for network security and administration at CESNET a.s. He has been a project leader in many national and contributor to many European projects related to network security, cyber threat intelligence, and network monitoring at high speeds. He cooperates with both public and commercial sectors in research and innovation of network cybersecurity concepts and their implementation into open-source tools or products.

Meeting Details:

Meeting link: <https://cesnet.zoom.us/j/98176996869>

Topic: Final SAPPAN event
Time: Apr 4, 2022 02:00 PM Prague Bratislava

Join Zoom Meeting
<https://cesnet.zoom.us/j/98176996869>

Meeting ID: 981 7699 6869
One tap mobile
+420228882388,,98176996869# Czech Republic
+420239018272,,98176996869# Czech Republic

Dial by your location
+420 2 2888 2388 Czech Republic
+420 2 3901 8272 Czech Republic
+420 5 3889 0161 Czech Republic
Meeting ID: 981 7699 6869
Find your local number: <https://cesnet.zoom.us/j/98176996869>

About Speakers:

Keynote speaker:



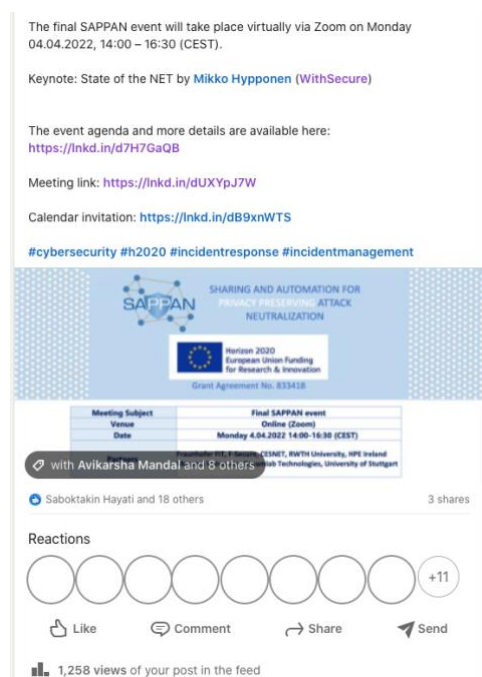
Mikko Hyppönen is a global security expert. He has worked at F-Secure since 1991. Mr. Hyppönen has written on his research for the New York Times, Wired and Scientific American and he appears frequently on international TV. He has lectured at the universities of Stanford, Oxford and Cambridge. He was selected among the 50 most important people on the web by the PC World magazine and was included in the FP Global 100 Thinkers list. Mr. Hyppönen sits in the advisory boards of t2 and Social Safeguard.



David Karpuk, Senior Data Scientist

Dr. David Karpuk is Senior Data Scientist at F-Secure, focusing on applications of machine learning and artificial intelligence to the construction of algorithms for cyberattack detection and response systems. He received his Ph.D. in Mathematics from the University of Maryland, College Park in 2012, and was previously a Postdoctoral Researcher at Aalto University in the Algebra, Number Theory, and Applications research group in the Department of Mathematics and Systems Analysis. After his postdoctoral work, he subsequently served as Assistant Professor in the Department of Mathematics at Universidad de los Andes, Colombia. David was previously the recipient of an Academy of Finland Postdoctoral Researcher grant, as well as a Postdoctoral Researcher grant from the Magnus Ehrnrooth Foundation.

We distribute our event via our website and social media channels, as well as the communication channels of the partners. As an example, the distribution of the event details reached 1258 hits on LinkedIn.

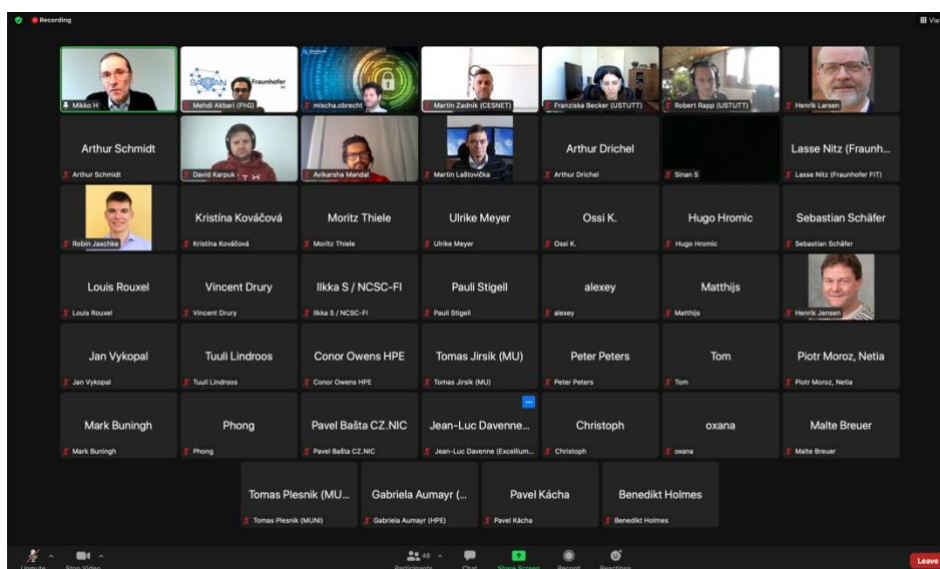


Additionally, we advertised our event via the Eventbrite platform, which reached 279 views.

Traffic from Promotional Tools

Category	Page Views
Direct Traffic	279
Direct Traffic	279
TOTAL	279

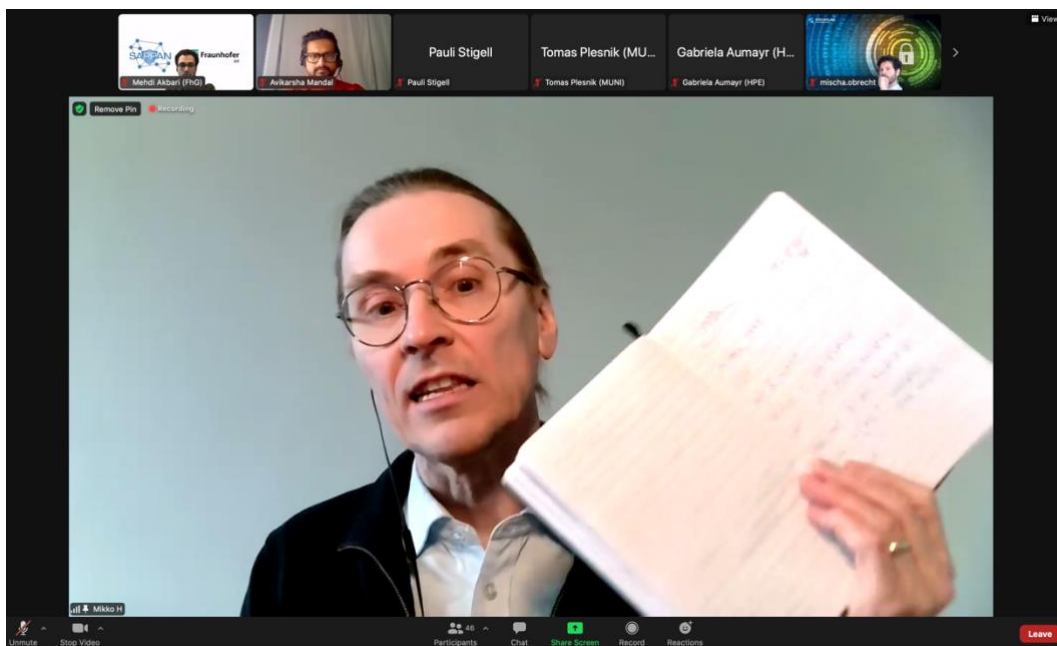
We invited all technical, end-user committee, and advisory board members of SAPPAN consortia, all EU projects from the same domain, and individual networks of the partners to reach a wide community of stakeholders such as researchers, end-users, business entities, innovators, SMEs, and policymakers. We had around 50 participants in the final event as shown in the following picture. The event agenda was as follows.



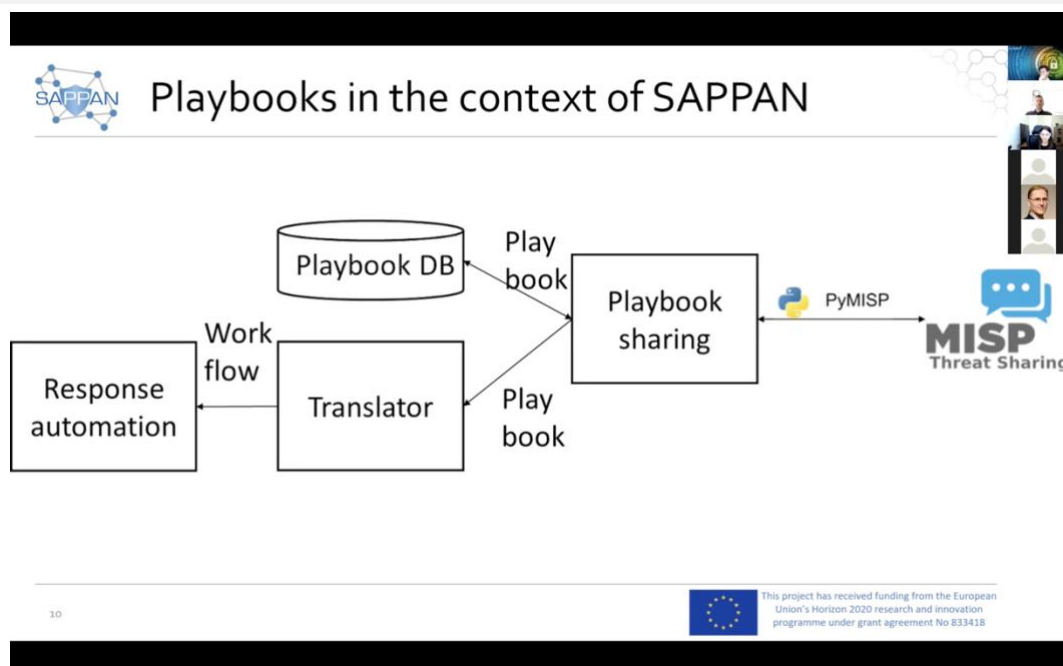
Event Agenda:

Time	Subject	Speaker
14:00-14:05	Welcome	Fraunhofer FIT
14:05-14:35	Keynote: State of the NET	Mikko Hyppönen (WithSecure)
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 (WithSecure), 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	—

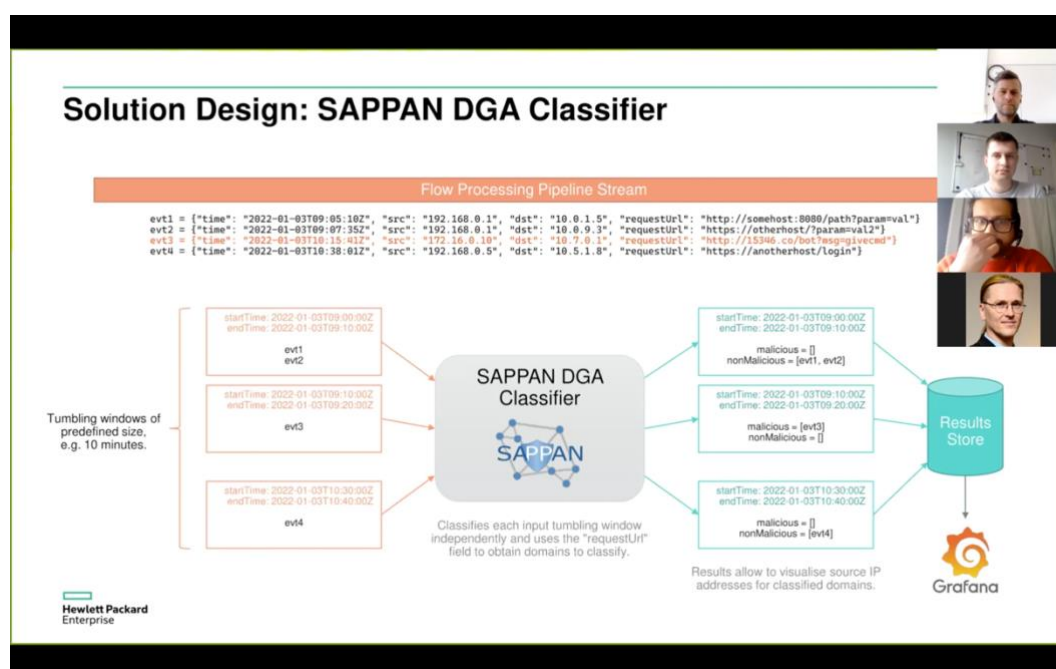
After the welcome and introduction, Mikko Hyppönen from WithSecure started his keynote talk about the state of the net.



The event continued with the presentation by Martin Zadnik from CESNET about sharing new types of threat intelligence and SAPPAN standardisation efforts. The talk introduced our innovative result in privacy-preserving sharing of new types of Indicators of Compromise in the form of the machine learning models and cybersecurity playbooks to the audience.



The next talk was SAPPAN innovations in DGA detection by RWTH and HPE Ireland presented by Arthur Drichel and Hugo Hromic.



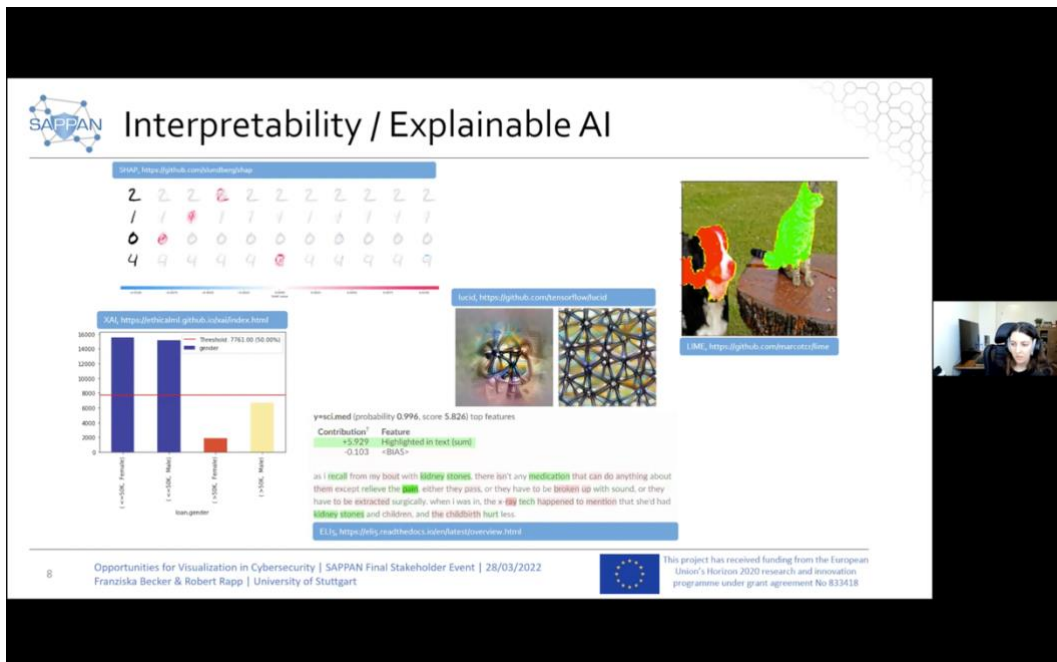
The event continued after a short break with a talk about SAPPAN results in response recommendation and automation presented by the colleagues from F-Secure, Masaryk University and DreamLab technologies.

The F-Secure section focused on the incident similarity and clustering work and the outlook for its exploitation. Then the Masaryk University and DreamLab sections focused on proof-of-concept prototypes for malware analysis automation and DGA response automation, respectively.



The slide features the SAPPAN logo at the top left, which consists of a blue shield with a network of nodes and lines. To the right of the logo, the text reads: "SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION". Below this, the main title "Response Recommendation and Automation" is displayed in a large, bold, blue font. Underneath the title, the authors are listed: "David Karpuk – F-Secure | Martin Laštovička – Masaryk University | Mischa Obrecht - Dreamlab Technologies AG". At the bottom left, there is a small number "5". At the bottom right, there is a European Union flag logo and a text box stating: "This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418". A small video feed of a man with a beard and headphones is visible on the right side of the slide.

The final presentation was about the visualisation support and SAPPAN visualisation results and innovations in the domain of cybersecurity presented by Franziska Becker and Robert Rapp from the University of Stuttgart.



The slide features the SAPPAN logo at the top left. The title "Interpretability / Explainable AI" is displayed in a large, bold, black font. Below the title, there are several visualizations and links. On the left, there is a bar chart showing the distribution of "Non-incident" and "Incident" cases across different "Non-incident" categories. In the center, there is a grid of handwritten digits (2, 1, 0, 4) with some digits highlighted in red. To the right of the grid, there are two images: a cow and a cat. Below the images, there are two links: "LUCID, https://github.com/kensho-technologies" and "LIME, https://github.com/jarvisruoz/". At the bottom left, there is a small number "8". At the bottom right, there is a European Union flag logo and a text box stating: "This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418". A small video feed of a woman with dark hair is visible on the right side of the slide.

All the presentation materials are available on the SAPPAN website and YouTube channel:

<https://www.youtube.com/playlist?list=PLjOJOMqIFPRXFqOhhuWEM4O7cWB6z2oC>

3 Short Summary of SAPPAN Presentations in the Events

SAPPAN results were presented in 24 events in the third year of the project (M25-M36), including scientific conference presentations and promotional and pitch events. It increases the overall number of SAPPAN presentations to 39 in total. We present some highlights of our presentations in the last year of the project as follows.

3.1 Swiss Cyber Security Days 2022

Short description of the event:

Switzerland's leading cybersecurity event, Swiss Cyber Security Days (SCSD), brought together key decision-makers and experts on domestic and international cybersecurity for two days on Wednesday 6 and Thursday 7 April 2022. The first day focused on core issues of overall security for Switzerland, while the second explored specific and innovative preventive solutions for businesses, particularly SMEs. The program comprised more than 60 lectures, keynote speeches, panel discussions, best practice presentations and round tables. The full program can be viewed here: <https://swisscybersecuritydays.ch/agenda/>


The fourth edition of the Swiss Cyber Security Days offered a high-level knowledge input for the audience and Switzerland with the American Cyber Security Director and advisor to President Joe Biden. He emphasized the importance of good cooperation, as cyberspace knows no national borders, and praised Switzerland's potential for innovation. The conclusion from the more than 130 presentations and discussions: Switzerland has caught up in cybersecurity, created more necessary awareness and wants to intensify international cooperation.

Presentation:

Dreamlab has participated in SAPPAN for the last three years. In this talk, they explored some highlights of three years worth of research to provide a glimpse behind the curtains of SAPPAN and showed some possible applications and upcoming projects to watch. They talked about the project's aim to explore ways how sharing information and models, automation and machine learning combined with privacy-enhancing techniques can be leveraged to improve cyber defence with respect to reaction time and accuracy.

Link to the event: <https://scsd365.app.swapcard.com/widget/event/scsd-2022/planning/UGxhbm5pbmdfODcxMDE4>

Here are examples of the presentation slides. Full presentation slides are available on the SAPPAN website: https://sappan-project.eu/wp-content/uploads/2022/04/sappan-scsd_v1.pdf



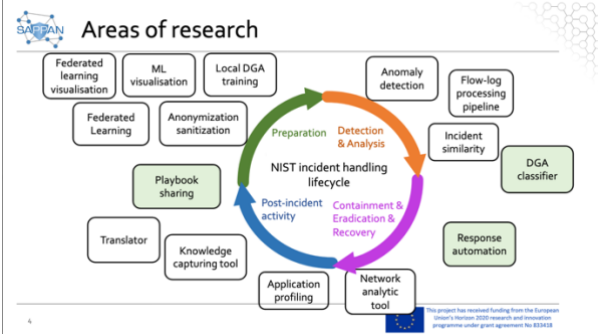
Introduction, Highlights and Results

Mischa Obrecht
Dreamlab Technologies AG

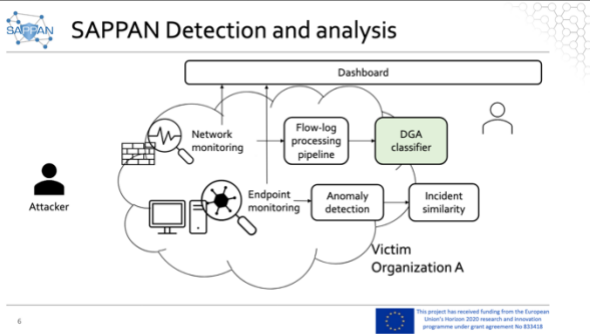
Outline

- Project overview
- Research areas
- Spotlights:
 - Neural Nets for Domain Generation Algorithm Detection
 - Response automation
 - Sharing of playbooks
- Conclusion

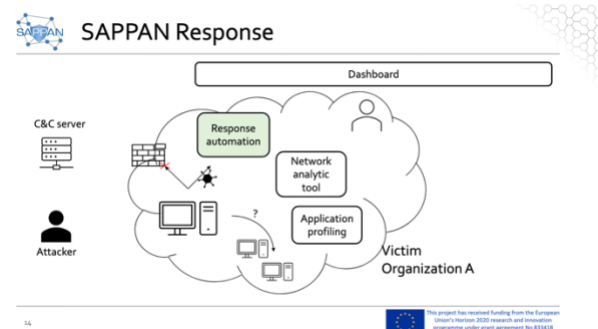
Areas of research




SAPPAN Detection and analysis



SAPPAN Response



Playbook sharing



3.2 MITRE Africa / EMEA Conference

Short description of the event:

It was a conference on the utilization of MITRE Att&ck by security professionals in Africa and the Middle East. The AME ATT&CK community is a vendor-agnostic community where end-users, decision-makers, and researchers discuss and exchange their use and experience of the MITRE Framework in practical cases during day-to-day activities. The AME ATT&CK Community is a community of cybersecurity professionals who actively use MITRE ATT&CK to improve cyber operations inside or outside organisations regionally.

Information about the event is available here: <https://attackcommunity.org/events>

Presentation:

Overview of SAPPAN and the utilization of MITRE Att&ck throughout the Red Team Exercises conducted to generate cyber security data. Additionally, our colleague distributed the news about establishing our End User Committee and requested interested participants.

The video of the presentation is available on the host's YouTube Channel:

https://www.youtube.com/watch?v=f-SQptd5O4w&ab_channel=AMEATT%26CKCommunity

Also, the presentation slide set is available on the SAPPAN website (Link: https://sappan-project.eu/wp-content/uploads/2022/04/MITRE_SAPPAN_Overview.pdf), and the following pictures are examples of slides.

Dreamlab Technologies

The SAPPAN-project (Sharing And Automation for Privacy Preserving Attack Neutralization) and utilization of MITRE for attack emulation



2021



SAPPAN – Current Progress M27/M36

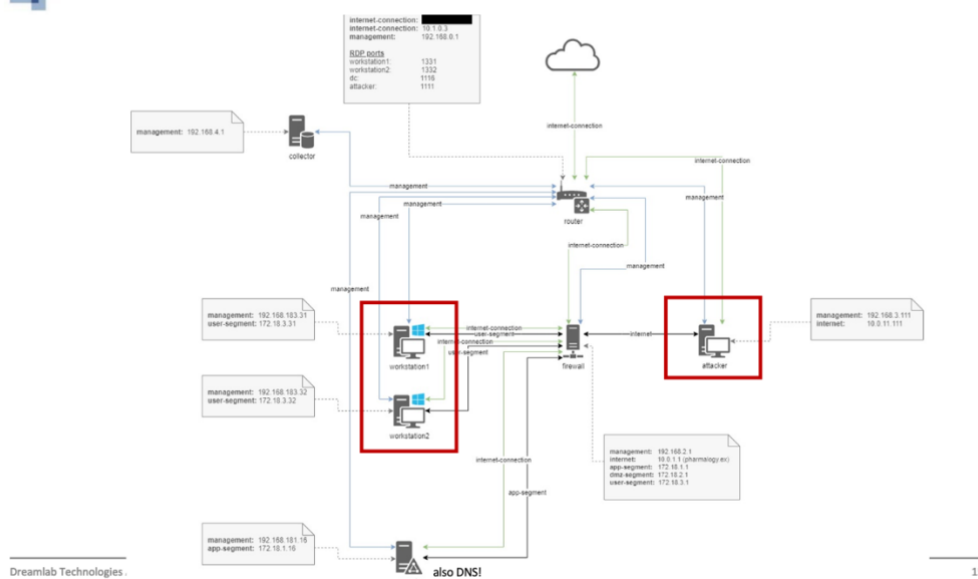
- ...
- Framework for machine readable playbooks containing response and recovery information
- Research on local detection methods
 - DGA-Detection
 - Classification of phishing URLs
 - Host- and application profiling based on network and endpoint-data
 - **Anomaly detection based on network and endpoint-data**
- Research on automation of playbooks for remediation of identified incidents
- Research on anonymization for sharing of information
- Research on federated machine learning
- ...

Dreamlab Technologies AG

www.dreamlab.net

12

Network topology for experiment



Dreamlab Technologies

15

Utilized MITRE-Att&ck Tactics

- T1204.002 - User Execution: Malicious File
- T1055.001 - Process Injection: DLL-Injection
- T1218.011 - Signed Binary Proxy Execution: Rundll32
- T1008: Fallback Channels
- T1090.002 - Connection Proxy: External Proxy
- T1119: Automated Collection
- T1005: Data from Local System
- T1041: Exfiltration Over Command and Control Channel
- T1018: Remote System Discovery
- T1059.001: Command and Scripting Interpreter: Powershell

Dreamlab Technologies AG

www.dreamlab.net

18



Take aways

- MITRE Emulation Plans can be leveraged by a technically competent reader to simulate realistic attacks
- MITRE Emulation Plans helped our purpose by allowing for efficient adoption and customization

Next steps

- If necessary further red team experiments, e.g. compromise of active directory
- Utilization of the gathered data for detection experiments (based on network as well as endpoint data)
- Experimentation regarding automated remediation of detected attacks



Become part of the SAPPAN end user committee!

What we need your help with:

- Interview after demonstration of SAPPAN results and discussion of achievements

How much time it all takes:

- 2 surveys + demonstration, 2 hours each

What you can expect in return:

- No cash
- Early access to results (papers)
- Early access to practical implementations (if open source)
- Access to new detectors as they are developed in showcases

What to do if you are interested:

- Hit me up: mischa.obrecht@dreamlab.net

10

3.3 2021+2022 TF-CSIRT Meetings & FIRST Regional Symposium Europe


Short description of the event:

TF-CSIRT Meeting & FIRST Regional Symposium Europe is an annual joint meeting of cybersecurity teams from the whole world under TF-CSIRT and FIRST. TF-CSIRT is a task force that promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions, whilst liaising with relevant organisations at the global level and in other regions. FIRST is the premier organisation and recognized global leader in incident response. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organisations. FIRST aims to foster cooperation and coordination in incident prevention, stimulate rapid reaction to incidents, and promote information sharing among members and the community at large.

- Link to the 2021 event: <https://tf-csirt.org/tf-csirt/meetings/63rd/>
- Link to the 2022 event: https://www.first.org/events/symposium/regional_europe2022/

Presentation

SAPPAN results were presented in both year events. At the 2021 event, Tomas Jirsik and Michal Pavuk from Masaryk University presented a demonstration of large-scale endpoint profiling. Some of the slides are shown as follows. Also, the complete slide set is available on the SAPPAN website: <https://sappan-project.eu/wp-content/uploads/2022/04/SAPPAN-HostProfiling.pdf>




SHARING AND AUTOMATION FOR
PRIVACY PRESERVING ATTACK
NEUTRALIZATION

Demonstration of large-scale endpoint profiling

SAPPAN @ CSIRT-MU

Tomas Jirsik and Michal Pavuk
(Masaryk University)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418



Agenda

- Data Sources
- Endpoint Profiles
- Sample Use cases
- Visual Exploration of the Profiles

1 Demonstration of large-scale endpoint profiling | 04.05.2022
Tomas Jirsik & Michal Pavuk | Masaryk University

2 This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418



How can be the profiles used?

- **Clustering of profiles**
 - identification of groups with similar properties
 - different purpose
 - segmentation
 - variability (security)
- **Classification**
 - profile assignment
- **Long Term Observations**
 - history of host behaviors
- **Visual Analytics**
 - explorative analysis
 - get understanding

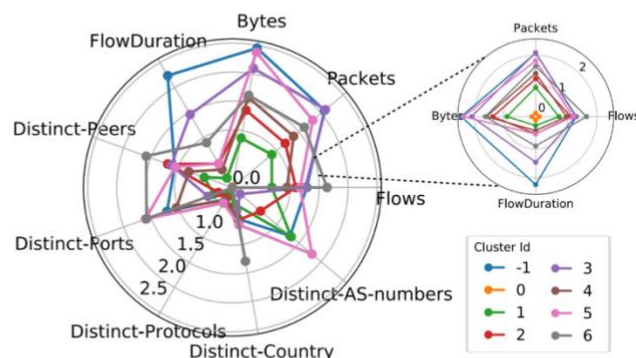


Fig. 9. Representation of clusters of hosts with similar variability of behavior characteristics.

10

Demonstration of large scale endpoint profiling | 28.05.2021
Tomas Jirsik & Michal Pavuk | Masaryk University



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418



On-going: Automated Response

- Simple playbook for Phishing attacks
- The complexity is primarily within the performed actions
- Tip of the iceberg
 - Determine if quarantined email is Phishing
 - Get distributed OSINT for *IP, domain, file*
 - Search all traffic and logs for observables from 6 months ago
 - Block *IP* via FlowSpec, Block *domain* via DNS RPZ
- Orchestration is not overly hard, but also not trivial
 - We use *Apache Airflow* for our prototypes
 - Other engines are available

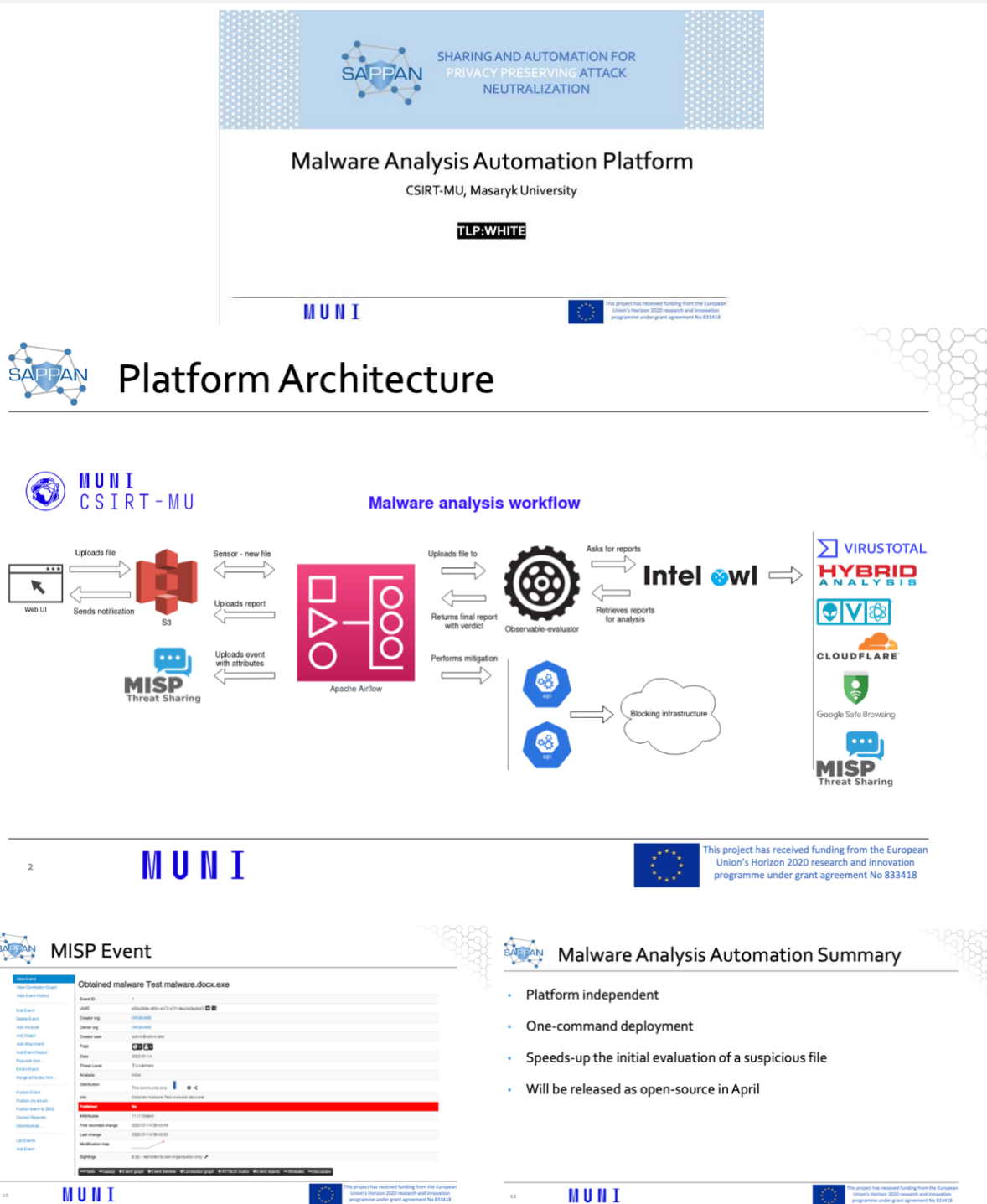
16

Demonstration of large scale endpoint profiling | 28.05.2021
Tomas Jirsik & Michal Pavuk | Masaryk University



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

The 2022 year, the results of the malware analysis automation platform which is developed by Masaryk University CSIRT-MU as part of SAPPAN was presented by Martin Laštovička. This is a tool to automate the response and recovery actions of SOC operators for the malware use case. The following slides are part of the slide set, and the complete presentation slides are available on the SAPPAN website: <https://sappan-project.eu/wp-content/uploads/2022/04/Martin-Lastovicka-SAPPAN-Malware-Analysis-Platform.pdf>



3.4 SECRIPT 2021

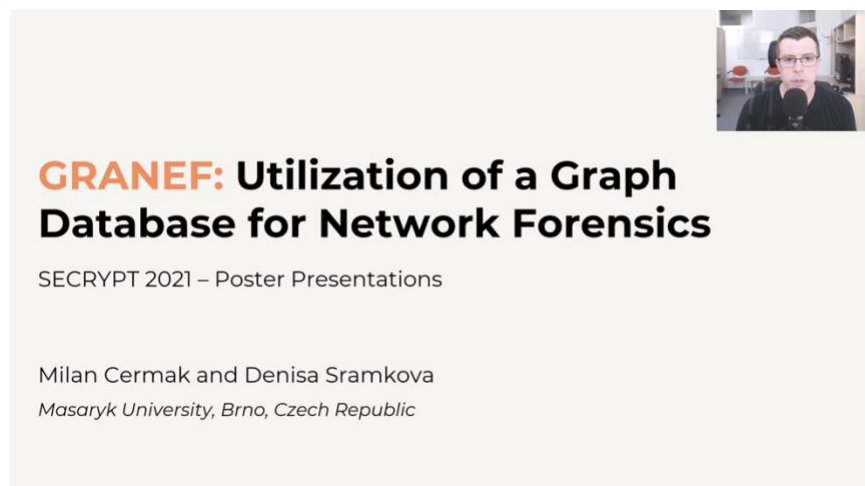
Short description of the event:

SECRIPT is an annual international conference covering research in information and communication security. The 18th International Conference on Security and Cryptography (SECRIPT 2021) seeks submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of data protection, privacy, security, and cryptography. Papers describing the application of security technology, the implementation of systems, and lessons learned are also encouraged. Papers describing new methods or technologies, advanced prototypes,

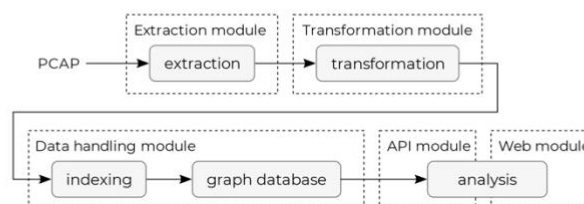
systems, tools and techniques and vision papers indicating future directions are also encouraged.

Presentation:

Understanding the information in captured network traffic, extracting the necessary data, and performing incident investigations are principal tasks of network forensics. The analysis of such data is typically performed by tools allowing manual browsing, filtering, and aggregation or tools based on statistical analyses and visualizations facilitating data comprehension. However, the human brain is used to perceiving the data in associations, which these tools can provide only in a limited form. We introduce a GRANEF toolkit that demonstrates a new approach to exploratory network data analysis based on associations stored in a graph database. In this article, we describe data transformation principles, utilization of a scalable graph database, and data analysis techniques. We then discuss and evaluate our proposed approach using a realistic dataset. Although we are at the beginning of our research, the current results show the great potential of association-based analysis. The presentation is available on SAPPAN YouTube Channel: <https://www.youtube.com/watch?v=E0eqa-o6GhE>



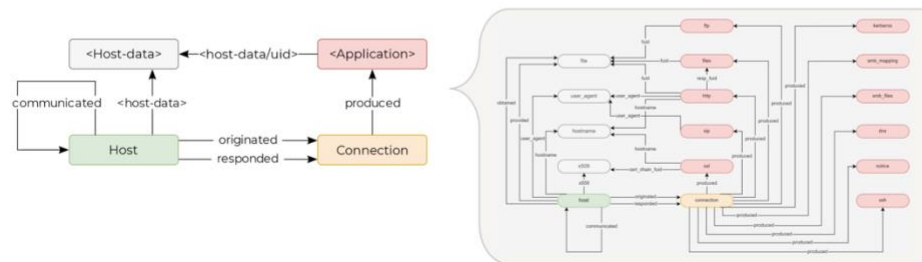
Toolkit Design



- The toolkit's core consists of a graph database **Dgraph** (<https://dgraph.io/>) that stores transformed information from network traffic captures extracted by **Zeek** (<https://zeek.org/>) network security monitor.
- Custom **Python scripts control all modules** to ease toolkit setup and usage.
- Modules are implemented as **Docker containers**.
- Web interface visualizes data as an **interactive relationship diagram**.

Database Schema

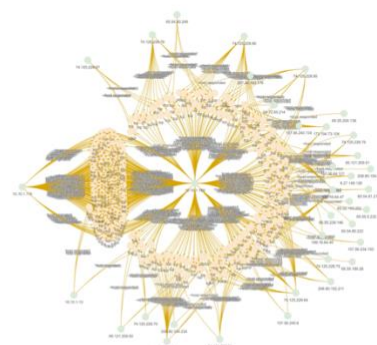
- The schema follows the format of Zeek logs, preserves their relation, and eases extension.
- All edges are directional but allow reverse processing.
- **Host** – a device with IP address observed in the network traffic capture.
- **Host-data** – data related to the host extracted from network traffic (hostname, certificate, ...).
- **Connection** – information about individual network connections (statistics, flags, ...).
- **Application** – application data extracted from the connection (DNS, HTTP, TLS, ...).



3

Network Forensics

- The interactive relationship visualization allows the analyst to **get details** about any selected node, **go into the graph's depth**, and gain **new observations**.
- The API includes additional functionality to get **initial insights** about network connections and perform anomalies detection.



5

Additionally, the poster is available on the SAPPAN website: https://sappan-project.eu/wp-content/uploads/2022/04/2021_SECRIPT-poster.pdf

GRANEF: Utilization of a Graph Database for Network Forensics

Milan Cermak and Denisa Sramkova

Institute of Computer Science, Masaryk University, Brno, Czech Republic
cermak@ics.muni.cz, denisa.sramkova@mail.muni.cz

Abstract

Understanding the information in captured network traffic, extracting the necessary data, and performing incident investigations are principal tasks of network forensics. The analysis of such data is typically performed by tools allowing manual browsing, filtering, and aggregation or tools based on statistical analyses and visualizations facilitating data comprehension. However, the human brain is used to perceive the characteristics of the data in associations, which these tools can provide only in a limited form. To overcome this issue, we introduce a GRANEF toolkit that demonstrates a new approach to exploratory network data analysis based on associations stored in a graph database.

Toolkit Design

- The toolkit's core is a graph database **Dgraph** (<https://dgraph.io/>) that stores transformed information from network traffic captures extracted by **Zeek** (<https://zeek.org/>) network security monitor.
- Modules are implemented as **Docker containers**.
- Web interface visualizes data as an **interactive relationship diagram**.

Database Schema

- Host** – a device with IP address observed in the network traffic capture.
- Host-data** – data related to the host extracted from network traffic.
- Connection** – information about individual network connections.
- Application** – application data extracted from the connection.
- The schema follows the format of Zeek logs and eases their extension.
- All edges are directional but allow reverse processing.

Analysis Query

- DQL query with a selection of TCP connections with a file transfer from a local network:

```
{getConn(func: allof(host.ip, cidr, "192.168.0.0/16")) {
  name: host.ip
  host: originated @filter(eq(connection.proto, "tcp")) {
    expand(connection)
    connection: produced {
      expand(all_)
      files: fluid { expand(file) }
    }
    ~host.responded { responded_ip: host.ip }
  }
}}
```

- The toolkit contains an **abstract layer API** with common analysis functions to ease investigation.
- Results are provided as **JSON** or visualized in an **interactive relationship diagram**.

Network Forensics

- The interactive relationship visualization allows the analyst to **get details** about any selected node, **go into the graph's depth**, and gain **new observations**.
- The API includes additional functionality to get **initial insights** about network connections and perform anomaly detections.
- Network traffic data can be **easily enriched** with additional information from external sources linked to existing nodes (e.g., asset management, OSINT, device logs, notes).
- The visualization allows the analyst to **distinguish regular network traffic** from suspicious one just at first glance based solely on the **resulting pattern**.
- The approach is not only the new method of data storage and querying, but it is a **shift of mindset** that enables the analyst to perceive network data in a new way.

Sharing and Automation for
Privacy Preserving Attack
Neutralization

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418.

3.5 PST 2021 Conference

Short description of the event:

18th International Conference on Privacy, Security and Trust (PST) was held virtually due to COVID-19 restrictions on December 13-15, 2021. However, it was planned to be held in person in Auckland, New Zealand. The conference continued the tradition of bringing together researchers around the three themes of privacy, security, and trust, together with a new blockchain special theme to present their latest findings and discuss their results and application in practice.

Presentation:

Domain Generation Algorithms (DGAs) are operated by botnets to rotate Command and Control (C2) domains. Blocking or seizing such dynamic and random-looking C2 domains is a significant challenge for defenders and law enforcement. Utilising machine learning can ease the DGA detection with very accurate results. The main challenge is a well-trained model relies on high-quality data which is hard to find for individuals. Also, training data on resource-constrained devices is a huge restriction. On the other hand, models are usually confidential and part of intellectual property. Therefore, the trainer has not willing to share it. DGA-Detector-as-a-Service can be a solution, using a cloud-based service for the detection of DGAs. In this scenario, privacy plays a significant role when the URLs are usually privacy-critical data and cannot be shared in a raw format. We investigate privacy-preserving machine learning libraries and utilise them to train DGA classifiers based on the state-of-the-art available models. Then we modified the models to increase the performance with a very low penalty in the accuracy. Some slides of the talk titled "Towards Privacy-Preserving Classification-as-a-Service for DGA Detection" are as follows. The presentation is available on the SAPPAN YouTube channel: <https://www.youtube.com/watch?v=5NUywNi1nzQ>

Towards Privacy-Preserving Classification-as-a-Service for DGA Detection

PST 2021: 18TH ANNUAL INTERNATIONAL CONFERENCE ON PRIVACY, SECURITY, AND TRUST 2021

December 2021

Arthur Drichel
Mehdi Akbari Gurabi
Tim Amelung
Ulrike Meyer

Evaluation Setup

Selection of Privacy-Preserving ML Frameworks

Framework	Parties	Approach	Conv1D	Max Pool 1D	Avg Pool 1D	ReLU	Sigmoid
PySyft ¹	3	MPC*	Only 2D	Only 2D	Yes	Yes	No
TF-Encrypted ²	3	MPC	Only 2D	Only 2D	Only 2D	Yes	Yes
MP2ML ³	2	HE** & MPC	Yes	Yes	Yes	Yes	No
SecureQ8 ⁴	2 or 3	MPC	Only 2D	Only 2D	Only 2D	Yes	Yes

+ All of them support Dense and none of them supports LSTM and embedding

* Secure Multi Party Computation (MPC)

** Homomorphic Encryption (HE)

1. T. Ryffel et al. "A generic framework for privacy preserving deep learning," arXiv:1811.04017, 2018.

2. M. Dahl et al. "Private machine learning in tensorflow using secure computation," arXiv:1810.08130, 2018.

3. F. Boemer et al. "Mp2ml: A mixed-protocol machine learning framework for private inference," in ARES. ACM, 2020.

4. A. Dalskov, et al. "Secure evaluation of quantized neural networks," Privacy Enhancing Technologies, vol. 2020, no. 4, 2020.

7 | Towards Privacy-Preserving Classification-as-a-Service for DGA Detection

Context & Motivation | Evaluation Setup | Results | Conclusion



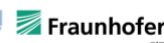
Results

Inference Latency

Classifier	Experiments	3 party setting				2 party setting		
		PySyft	TF-E	Q8-2	Q8-3	MP2ML	Q8-0	Q8-1
Inline	No modification (s)	2.3	1.3	2.1	4.2	296.6	98.2	208.4
	Simp. improvement	68%	80%	5%	16%	68%	67%	64%
NYU	No modification (s)	6.9	3.7	2.5	10.3	191.4	374.6	793.3
	Simp. improvement	95%	87%	14%	45%	73%	81%	78%
ResNet	No modification (s)	9.8	-	-	-	174.8	-	-
	Simp. improvement	93%	-	-	-	84%	-	-
FANCI	No modification (s)	0.1	0.1	0.6	0.6	0.1	0.6	0.9
	Simp. improvement	71%	71%	0%	0%	8%	3%	0%

10 | Towards Privacy-Preserving Classification-as-a-Service for DGA Detection

Context & Motivation | Evaluation Setup | Results | Conclusion



Results

Accuracy Penalty

Classifier	Experiments	Accuracy	TPR	FPR
Inline	No modification (%)	99.77%	99.97%	0.43%
	Simp. Applied (%)	99.66%	99.97%	0.65%
NYU	No modification (%)	99.81%	99.98%	0.36%
	Simp. Applied (%)	99.65%	99.80%	0.50%
ResNet	No modification (%)	99.85%	99.93%	0.23%
	Simp. Applied (%)	99.68%	99.99%	0.63%
FANCI	No modification (%)	98.58%	99.24%	2.08%
	Simp. Applied (%)	98.02%	97.87%	1.83%

12 | Towards Privacy-Preserving Classification-as-a-Service for DGA Detection

Context & Motivation | Evaluation Setup | Results | Conclusion



3.6 DFRWS EU 2022

Short description of the event:

DFRWS is a non-profit, volunteer organisation dedicated to bringing together everyone with a legitimate interest in digital forensics to address the emerging challenges of our field. DFRWS organises digital forensic conferences, challenges, and international collaboration to help drive the direction of research and development. DFRWS conferences provide a friendly atmosphere to share research papers, practitioner presentations and works in progress. Every gathering includes technical workshops, demos, panels, and other “breakout sessions” covering various issues related to digital forensics. Ultimately, it is the goal of DFRWS to cultivate transdisciplinary co-production of knowledge that stimulates healthy growth in this rapidly evolving field. Notably, many novel developments in the field have their roots in works and breakout sessions at DFRWS conferences. As such, DFRWS conferences are not only a snapshot of the state of the research in the field but are also a useful pointer toward the future. Link to the event: <https://dfrws.org/conferences/dfrws-eu-2022/>

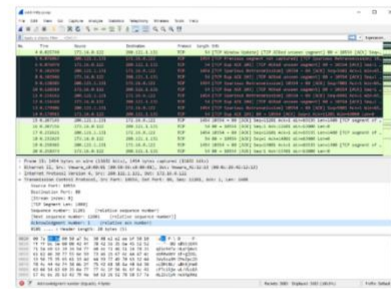
Presentation:

Even though network traffic is typically encrypted, and it is almost impossible to look into the content of transmitted data, the analysis of metadata and characteristics of individual connections still plays an essential role in an incident or criminal investigation. In recent years, we have seen a significant development of various approaches for storing and analysing large-scale data, including graph databases. Such an approach offers great potential for expert analysts performing digital forensics and network traffic investigation, as it corresponds to their natural perception of the data. In addition, it allows a simple connection of different types and sources of data, which represents the primary focus of our research. The slide set is available on the SAPPAN website (Link: <https://sappan-project.eu/wp-content/uploads/2022/04/2022-DFRWS-EU-toward-graph-based-network-traffic-analysis-and-incident-investigation.pdf>). The following figures show sample slides from the presentation.



Wireshark

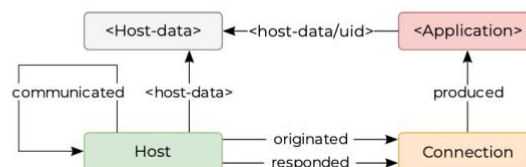
- A widely-used network protocol analyzer providing insights into network activity at a **microscopic level**
- **De facto standard** for packet trace analysis
- + Rich and detailed support of many different protocols
- + Ability to analyze all network traffic metadata
- Performance issues in analyzing large packet traces
- Limited overview of the whole packet trace
- Missing connection to other information sources



Wireshark: <https://www.wireshark.org/>

5

Representation of Network Traffic Data



- Initial version was proposed by **Niese** and further developed by **Leichtnam et al.**
- We have further developed these proposals and simplified them to ease data understanding
- **Host** – a device with IP address observed in the network traffic capture
- **Host-data** – data related to the host extracted from network traffic (hostname, certificate, ...)
- **Connection** – information about individual network connections (statistics, flags, ...)
- **Application** – application data extracted from the connection (DNS, HTTP, TLS, ...)
- All edges should be directional to ease analysis, but reverse processing could be possible

9

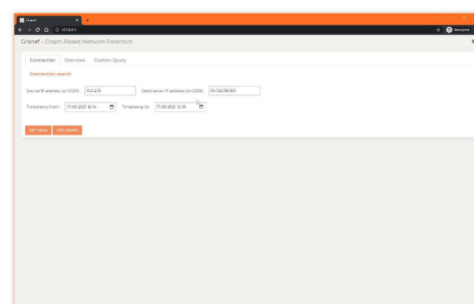
Interactive Data Exploration

- The analyst can **use predefined queries** or custom **DQL queries** (Dgraph Query Language)
- The interactive relationship visualization allows the analyst to **get details** about any selected node, **go into the graph's depth**, and gain **new observations**
- Various types of attacks and anomalies can be spotted at first glance based on **visual patterns**

```

{getConn(func: allof(host.ip, cidr, "192.168.0.0/16"))
  name : host.ip
  host.Originated @filter(eq(connection.proto, "tcp"))
  expand(connection)
  connection.produced {
    expand(_all_)
    files.fuid { expand(File) }
  }
  ~host.responded { responded_ip : host.ip }
}
}
}

```



11

3.7 SLUSH 2021

Short description of the event:

Slush is the focal point for European and Asian startups and tech talent to meet with top-tier international influencers, investors and media. ECSO Cyber Investor Days run at Slush 2021 trade fair included expert discussions on cybersecurity investment in Europe, European cybersecurity funding and concrete strategies for strengthening investment activities in the EU, plus pitch sessions of the pre-selected European cybersecurity startups and SMEs. Slush is a large multi-day matchmaking exhibition for companies and investors. Link of the event: <https://www.businessfinland.fi/en/whats-new/events/2021/ecso-cyber-investor-days>

Presentation:

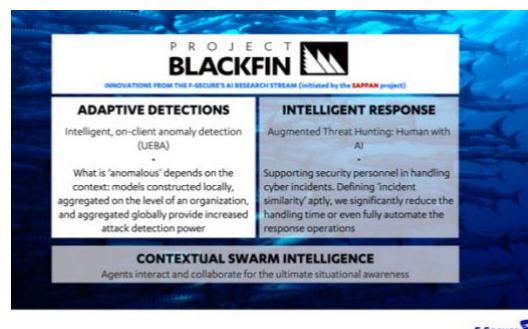
The talk focused on innovation in cybersecurity based on collaboration and joint R&I activities and presented examples of EU-funded projects which enabled research in new domains and directions. SAPPAN was the talk's highlight, illustrating the alignment of the project objectives with the WithSecure (formerly F-secure Business) strategy. The slide set is available on the SAPPAN website: <https://sappan-project.eu/wp-content/uploads/2022/04/Cybersecurity-Innovation-in-the-Nordics-ECSO-2021-12-01-1.pdf>

CASE EXAMPLE: SAPPAN PROJECT

Sharing and Automation for Privacy-Preserving Attack Neutralization

(received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement no. 833418)

- Consortium: Fraunhofer FIT (DE), Masaryk University (CZ), F-Secure (FI), RWTH Aachen University (DE), Hewlett Packard Enterprise (IE), CESNET (CZ), University of Stuttgart (DE), Dreamlab Technologies (CH)
- Main objectives:
 - Distributing of attack detection and response capabilities among endpoints, organizational security backends and security service provider backends
 - Sharing of cybersecurity data and detection and response models (ML) in confidentiality- and privacy-preserving ways



3.8 HPE Security Summit 2021

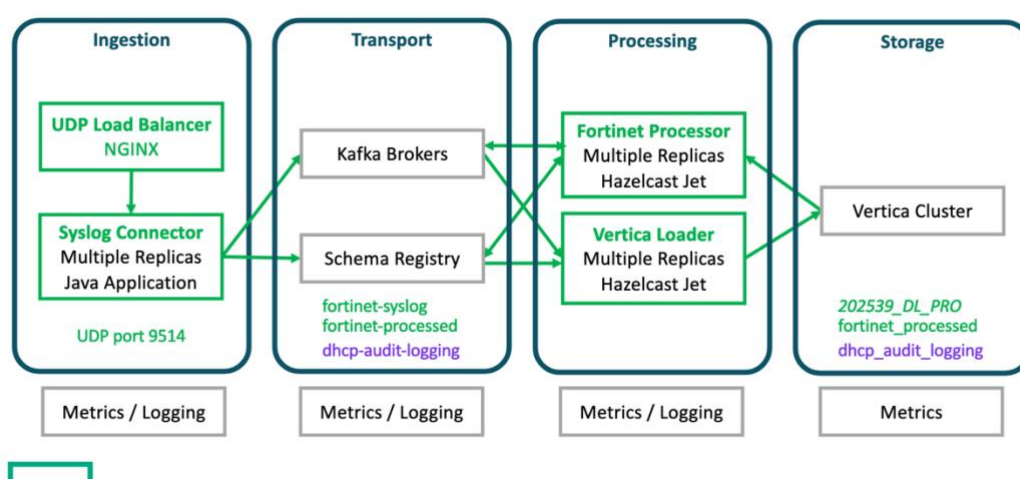
Short description of the event:

The conference brought together representatives and security practitioners from HPE groups including Cyber Security, Engineering, Labs, Aruba, Pointnext Technology Services, and GreenLake Cloud Services to learn about security capabilities, products, and services to exchange experiences and ideas with one another. The event aimed to provide a combination of deep technical content, as well as higher-level content for those with less experience in the field. This is a unique opportunity for the HPE team to get together and share their expertise with a focused audience and help them to shape the security culture that HPE will stand for in the marketplace. The Summit provided an ideal opportunity to find out more about what HPE is doing in the realm of cyber security. It has a particular focus on HPE's shift to 'Everything as a Service' and the role that security will have to play, enabling them to create alignment across HPE and understand the cyber challenges facing the customers and how they are evolving each day. They utilise the event to share new cyber innovations in their critical portfolio growth areas, as well as the value they bring to the customers and partners.

Presentation:

Modern Cyber Security relies on combining Cyber Intel with massive amounts of streaming event data to help detect security incidents. At the enterprise scale in HPE, these streaming data feeds are delivering more than 100,000 Events Per Second (EPS). HPE's Cyber Security team have built a Data Staging Platform (DSP) to ingest these data feeds, enrich them with additional details such as asset and identity, organisational and vulnerability information, aggregate the feeds where appropriate to reduce volume while preserving utility and then make them available in a standard data model to the SIEM, Data Lake and other consumers. Conor Owens, Anne Moelle, Gabriela Aumayr, and Hugo Hromic from SAPPAN presented a talk titled "Building a Data Staging Platform for Enterprise-scale streaming security data" at the event. The presentation is available on the SAPPAN website: <https://sappan-project.eu/wp-content/uploads/2022/04/2021-techx-DSP-FortinetAggregation-GabrielaAumayr-HugoHromic.pdf>

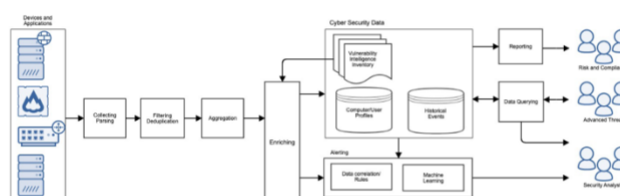
HOW WE INGEST, PROCESS AND STORE FORTINET SYSLOG EVENTS



BACKGROUND

Iterative process

- First iteration – Hortonworks, Spark/Scala
 - PROS
 - Scalable, performant
 - CONS
 - Shared platform, unstable environment
 - At the limit of available resources
- Second iteration – MapR, Spark/Scala
 - PROS
 - our own platform
 - CONS
 - non-transferable technology
 - different Kafka libraries in MapR
 - difficult to maintain



3.9 HPE WiS Group (Women in Security) Webinar

Short description of the event:

This webinar is organised by the CodePlus project. This project is organised by the National University of Ireland Galway (NUIG), Dublin City University (DCU) and the University of Limerick (UL) with the following goals:

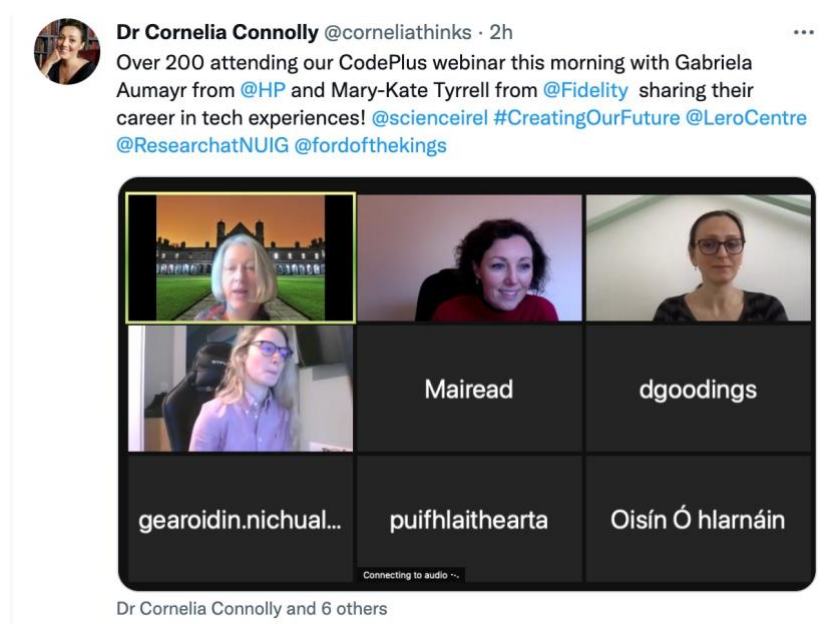
- Offer purposefully designed coding workshops (20 hours in duration) to cohorts of female students. The workshops used a collaborative approach to teaching & learning which has proved effective in helping learners engage with CS and more general 21st-century skills. Due to COVID-19 restrictions, both face-to-face and online modes of delivery were available.
- Collaborate with tech companies to organise interactive webinars for students to engage with female IT professionals.
- Work with tech companies to organise visits, for students, to company offices for tours and talks with female IT professionals (subject to COVID restrictions).

On December 9, 2021, there was a Webinar presented by the Women in Security (WiS) group at HPE for secondary school girls. The organisers aim to repeat the event with new schools next year.

Presentation:

Gabriela Aumayr (HPE/SAPPAN) talked about her professional paths toward Computer Science careers, including her involvement with the SAPPAN project.

The event saw attendance from about 200 secondary school girls from the west coast of Ireland. The talks were very well received, and the organisers suggested there might be a similar event with new schools next year (2022). Link to the post on the SAPPAN website: <https://sappan-project.eu/?p=2060>



3.10 GRASEC Workshop (at NOMS 2022 Conference)

Short description of the event:

The workshop serves to bring together people from industry and academia including researchers, developers, and practitioners from a variety of fields working on graphs and their applications to network security and cybersecurity in general as well as blockchain. Moreover, the workshop allows attendees to share and discuss their latest findings from both theoretical and practical perspectives in several techniques and methods for graph modelling, mining, learning, and visualizing. The main goal of GraSec is to present research and experience results in graph applications on network and cybersecurity as well as the defensive and offensive tools.

Interactive keynote:

Analysis of network traffic allows us to explore events in the monitored network (even retrospectively). It benefits from the fact that it is almost impossible to maliciously affect the captured data (as opposed to system logs, for example). Therefore, it is a reliable source that suitably complements cyber incident investigation. The analysis of network traffic is currently performed by the use of tools such as Wireshark or Arkime, which allow manual data browsing, filtering, aggregation, and provide interactive visualizations but don't account for the fact that the human brain perceives the data as associations/graphs.

This interactive keynote will show you how network traffic is typically analyzed today and how it can be adapted to human thinking by using a graph database. In the introductory part, you will see what a typical network attack looks like, how it can be analyzed using Wireshark, and what the advantages and disadvantages of today's analysis techniques are. We will then show you how to transform network data into a format suitable for a graph database while at the same time preserving the natural perception of network traffic. In the final part of the keynote, we will introduce the Granef toolkit (<https://granef.csirt.muni.cz/>) and use it to analyze the given data. Through simple tutorial exercises, participants will have the opportunity to explore graph-based analysis on their own and gain new insights into network traffic data. Link: <https://granef.gitlab-pages.ics.muni.cz/grasec-keynote/>

Granef: GraSec Keynote

Incident Investigation: From Packets to Graph-Based Analysis

The main page of the Granef toolkit: <https://granef.csirt.muni.cz/>

Abstract

Analysis of network traffic allows us to explore events in the monitored network (even retrospectively). It benefits from the fact that it is almost impossible to maliciously affect the captured data (as opposed to system logs, for example). Therefore, it is a reliable source that suitably complements cyber incident investigation. The analysis of network traffic is currently performed by the use of tools such as Wireshark or Arkime, which allow manual data browsing, filtering, aggregation, and provide interactive visualizations but don't account for the fact that the human brain perceives the data as associations/graphs.

This interactive keynote will show you how network traffic is typically analyzed today and how it can be adapted to human thinking by using a graph database. In the introductory part, you will see what a typical network attack looks like, how it can be analyzed using Wireshark, and what the advantages and disadvantages of today's analysis techniques are. We will then show you how to transform network data into a format suitable for a graph database while at the same time preserving the natural perception of network traffic. In the final part of the keynote, we will introduce the Granef toolkit (<https://granef.csirt.muni.cz/>) and use it to analyze the given data. Through simple tutorial exercises, participants will have the opportunity to explore graph-based analysis on their own and gain new insights into network traffic data.

Whoami

Biography: Milan Cermak received a Ph.D. degree from the Faculty of Informatics of Masaryk University in 2020 and works as a cybersecurity researcher at the university's Computer Security Incident Response Team (CSIRT-CU). His main research interests include the development of advanced methods for a forensic analysis of network traffic using modern approaches and techniques such as a stream or graph-based analysis frameworks. In addition to detecting attacks and anomalies in network traffic, he is also interested in various cybersecurity areas, including web penetration testing or criminal investigation. He also teaches courses focused on network traffic analysis and forensics, both at the university and as a part of commercial training.

Social: [ORCID](#), [Google Scholar](#), [LinkedIn](#)

Current status: Looking for a post-doc position 🍌

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No [101019150](#).

4 Future Plans for Information and Presentation Materials

In this section, we list the planned activities after the project's lifetime.

Type of presentation activities	Planned Activities
The organisation of a Conference or Workshop	4th International Workshop on Next Generation Security Operations Centers (NG-SOC 2022): Joint workshop with the SOCCRATES and CyberSEAS H2020 EU projects. It will be held in conjunction with the 17 th International Conference on Availability, Reliability and Security (ARES 2022 – http://www.ares-conference.eu) The workshop will take place on August 23, 2022.
Participation in activities organised jointly with other EU projects	4th International Workshop on Next Generation Security Operations Centers (NG-SOC 2022): details mentioned in the above row
Training	Use of project knowledge and experiences in security and privacy courses and proposing bachelor and master theses related to project topics for further exploitation of the results (E.g., in line with the follow-up projects)
Social Media	Continuous updates on Twitter and LinkedIn about the future dissemination activities of the project
Website	Continuous updates on the project related materials (E.g., further publications) and disseminating the remaining public deliverables after EC approval.
Participation in conferences and workshop	Participation in future conferences and workshops for the SAPPAN publications that are still under review, or has not been submitted yet.
Video/Film	Providing further videos on SAPPAN YouTube channel: presentation of the results in the future conference, if applicable.

5 Conclusion

Provided information and presentation materials in the third year of the project are the template and guideline for the SAPPAN blog post series, updates on the project website and its contents, and social media activities. Further, SAPPAN-related content is mentioned on partners' websites and other dissemination channels to increase the visibility of the project. SAPPAN co-organised NG-SOC 2021 workshop in conjunction with ARES 2021 with another H2020 project and will organise it for the third consecutive year after the end of the project. Additionally, SAPPAN participated in the

second joint workshop on Dynamic Countering of Cyber-attacks with other EU H2020 projects. Finally, we organised the final stakeholder event to disseminate our results to the interested audience in the domain.

SAPPAN objectives, initiatives, and results were presented in several workshops, networking events and conferences that are described in this report. Also, a SAPPAN member present a motivational talk in a webinar to motivate and encourage young females for more involvement in computer science subjects held in the Republic of Ireland.

In the last part of the document, planned activities regarding information and presentation after the project lifetime are listed in a table.