SAPPAN

SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

SAPPAN Project Presentation

Dr. Avikarsha Mandal

Senior Researcher

Fraunhofer FIT, Germany

Project Information

SAPPAN → **S**haring and **A**utomation for **P**rivacy **P**reserving **A**ttack **N**eutralization

H2020 Call SU-ICT-01-2018 (IA) - Dynamic countering of cyber-attacks

- **Scope:** Cyber-attacks management – advanced response and recovery
- **Timeline**: May 2019 until April 2022
- **Overall Budget:** € 4 700 053,39

Project Highlights:

- Support **human operators, CSIRTs** to find optimal responses to and ways to recover from cyberattacks
- Platform for **privacy-preserving threat intelligence sharing** among organisations
- **Local and Federated detection tools** for effective response and recovery
- **Visual, interactive support tools** for SOC operators
- Improve **scalability** of massive data and logs processing for intrusion detection approaches
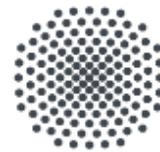- Tools for optimal **response recommendation** and **automation**

Consortium

Fraunhofer FIT

cesnet

Hewlett Packard Enterprise

DREAMLAB TECHNOLOGIES

F-Secure

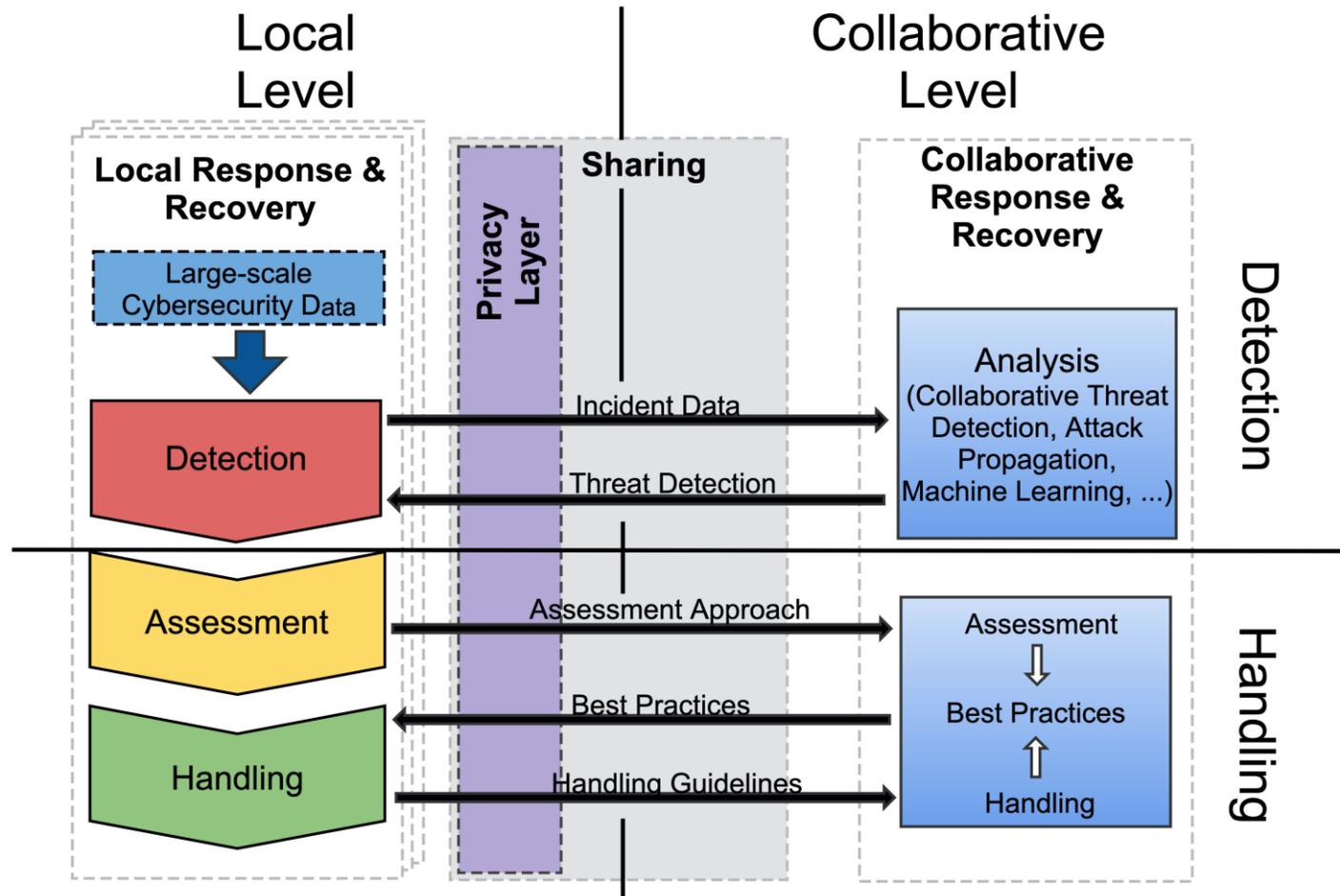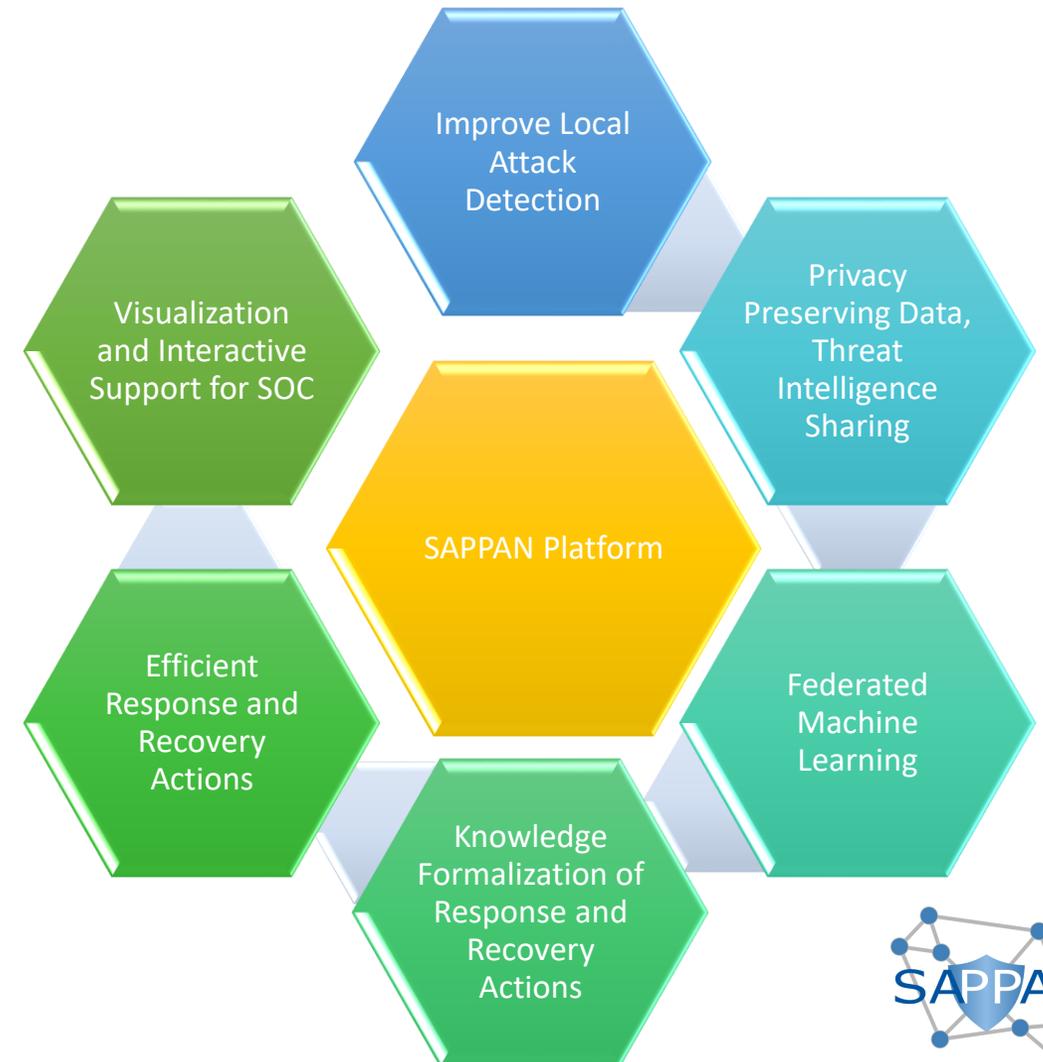Universität Stuttgart

MUNI

RWTH AACHEN UNIVERSITY

SAPPAN Threat Intelligence Sharing Approach

Project Goals

Goals:

- Privacy-preserving sharing of threat intelligence (e.g., ML detection models, playbooks) between organisations
- Develop advanced ML-based tools for attack detection and response
- Visualization components to support human operators

Improve Local Attack Detection

Privacy Preserving Data, Threat Intelligence Sharing

Visualization and Interactive Support for SOC

SAPPAN Platform

Federated Machine Learning

Efficient Response and Recovery Actions

Knowledge Formalization of Response and Recovery Actions

SAPPAN

SAPPAN via Cyberwatching.eu

- Project of the Week from 17th-21th Aug. 2020

- Promoted in the Project Rader

- MTRL based Cluster meeting for lightweight synergies on 9th July 2020 (FENTEC, SealedGRID, PAPAYA, DEFEND, PANACEA, GUARD and SAPPAN)

- Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Project on 22th Jan. 2021 (C4IIoT, CARAMEL, GUARD, SAPPAN, SIMARGL, and SOCCRATES.)

- SAPPAN included in Threat Intelligence Cluster and interested in participating "Threat Intelligence and Information Sharing" webinar

- SAPPAN and SOCCARATES project will jointly organize NG-SOC workshop@ARES 2021 on 17th Aug. and a webinar on "DGA related threats" on 28th Sept

Thank you

SAPPAN