

SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

SAPPAN Project Presentation

Avikarsha Mandal

Fraunhofer FIT, Germany



SAPPAN (Sharing and Automation for Privacy Preserving Attack Neutralization)

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





RNTHAACHEN UNIVERSITY



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



SAPPAN Approach





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



SAPPAN Innovations

- Advanced ML-based tools for attack detection and response
- Privacy-preserving sharing of threat intelligence between organisations
- Visualization components to support human operators

THANK YOU!

• Response recommendation and automation



