Vehicle Security Operations Center for Cooperative, Connected and Automated Mobility

Kevin Mayer, Tina Volkersdorfer, Jenny Hofbauer, Patrizia Heinl, Hans-Joachim Hof
e-mail: *kevin.mayer@carissma.eu*

November 4th, 2024

CARISSMA Institute of Electric, Connected and Secure Mobility (C-ECOS)

Technische Hochschule Ingolstadt, Germany

Dr. Kevin Mayer

Experience:

- **12.2023–present**: Postdoctoral researcher at the Technische Hochschule Ingolstadt, Germany
- **11.2022–today**: Research assistant in the EU research project SELFY, Technische Hochschule Ingolstadt
- **03.2018–10.2022**: Security Analyst and Incident Response, AUDI AG
- **10.2016–03.2018**: Security Research, Airbus Defense & Space

Education:

- **04.2020–12.2023**: Dr.Ing. Friedrich-Alexander University Erlangen-Nürnberg
- **03.2018–03.2020**: M.Sc., Computer Science at the Technical University of Ingolstadt.
- **10.2014–02.2018**: B.Sc., Computer Science for Automotive and Avionics aat the Technical Univer- sity of Ingolstadt.

Cybersecurity monitoring in CCAM

- Increasing Digitalization in Vehicles
  - Modern vehicles are becoming highly digitalized with advanced features.
  - This growth increases the risk of cybersecurity incidents in vehicles and their ecosystems.
- Need for Enhanced Cybersecurity
  - Traditional Security Operations Centers (SOCs) are not sufficient for vehicle-related cybersecurity.
  - Dedicated responses are required for the complex and interconnected nature of Cooperative, Connected, and Automated Mobility (CCAM).
- Gap in Existing Solutions
  - Existing IT-based SOCs lack vehicle-specific threat detection and response capabilities.
  - There is a need for specialized solutions addressing the unique characteristics of vehicle ecosystems.

Research questions

RQ1: What data streams are relevant for a VSOC?

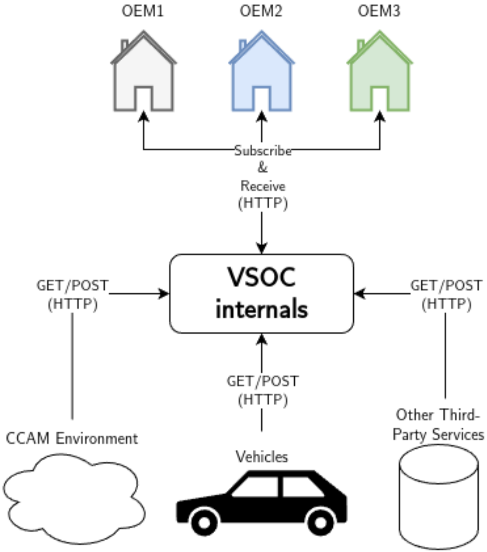
RQ2: Which components of an VSOC are required in a CCAM environment?

RQ3: Which information of a VSOC are beneficial to provide to CCAM participants?

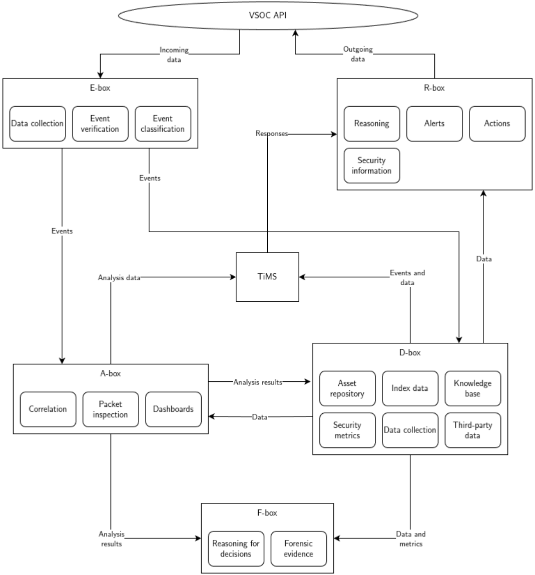
Metrics for VSOC

Metric	Source
Reaction time	Langer et al.
Criticality	Langer et al.
Autonomy	Langer et al.
Data aggregation	Langer et al.
Control-flow	Langer et al.
Coverage	Hofbauer et al.
People	Hofbauer et al.
Technical	Hofbauer et al.
Governance and compliance	Hofbauer et al.
Data privacy concern	Menges et al.
Physical assets	Our contribution
Real-time safety	Our contribution
Complex supply chain	Our contribution
Attack vectors	Our contribution

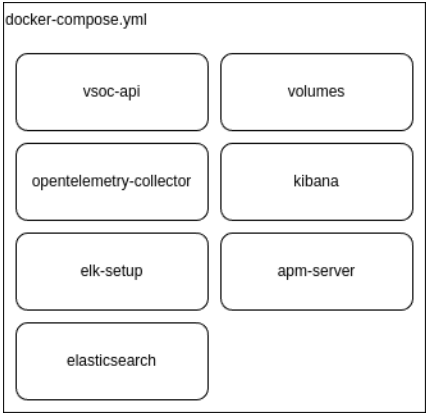
Outside view of the VSOC



Inside view of the VSOC



Docker compose components



docker-compose.yml

vsoc-api

volumes

opentelemetry-collector

kibana

elk-setup

apm-server

elasticsearch

Evaluating the VSOC

Fulfillment	Metric	Source
●	Reaction time	Langer et al.
✓	Criticality	Langer et al.
✓	Autonomy	Langer et al.
✓	Data aggregation	Langer et al.
✓	Control-flow	Langer et al.
✓	Coverage	Hofbauer et al.
●	People	Hofbauer et al.
✓	Technical	Hofbauer et al.
✓	Governance and compliance	Hofbauer et al.
●	Data privacy	Menges et al.
✓	Physical assets	Our contribution
●	Real-time safety	Our contribution
●	Complex supply chain	Our contribution
●	Attack vectors	Our contribution

Conclusion

RQ1: What data streams are relevant for a VSOC?
A1: Communication with external tools (e.g., SELFY tools), manufacturers (OEMs), and backend systems.

RQ2: Which components of an VSOC are required in a CCAM environment?
A2: E-box (events), R-box (responses), A-box (analysis), D-box (data), F-box (digital forensics), TiMS (threat management), and VSOC API (communication interface).

RQ3: Which information of a VSOC are beneficial to provide to CCAM participants?
A3: Analysis results, security events, trust information, metrics, and (raw) data.

SELFY Project

SELFY

This project has received funding from the European Union’s Horizon Europe research and innovation program under grant agreement No 101069748.

IARIA

CARISSMA
Automotive Safety Research