From SOC to VSOC: Transferring Key Requirements for Efficient Vehicle Security Operations

Jenny Hofbauer[1,3][0009−0003−6679−3672], Kevin Gomez Buquerin[1,2,4][0000−0002−5597−3913], and Hans-Joachim Hof[1,5][0000−0002−6930−9271]

[1] CARISSMA Institute for Electric, Connected, and Secure Mobility, Technical University Ingolstadt, Ingolstadt, Germany
[2] Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
[3] jeh7703@thi.de
[4] kevin.gomez@carissma.eu
[5] hof@thi.de

Abstract. The prioritization of passenger safety and comfort in the automotive sector lead to the research and development of technologies such as seat belts, airbags, driving assistants, and autonomous driving. These technologies bring advantages and new, unique dangers in the area of Information Technology (IT) security. Most enterprises have established a Security Operations Center (SOC) to protect their IT systems from security threats. Due to the changing threat landscape, increasing hacker attacks, and unique challenges, introducing a dedicated Vehicle Security Operations Center (VSOC) is critical. This paper defines in which aspects a VSOC that specializes in protecting vehicle fleets has to be adapted to the application area compared to an enterprise IT SOC. The aspects are found by defining primary SOC capabilities from existing literature on a non-domain-specific SOC. Determined by the definition of a SOC, requirements of current regulations and best practices of IT security in the automotive sector are collected. Based on these minimum requirements, the differences between an enterprise IT SOC and a VSOC can be discerned using coverage, people, technical, governance, and compliance metrics. This approach shows that the methods, procedures, and technical solutions used in an enterprise IT SOC can, for the most part, not be directly implemented in a VSOC. By defining the minimum legal requirements of a VSOC and giving an overview of the unique challenges of protecting a vehicle fleet, this paper offers a concrete basis for the design and practical implementation of a VSOC.

Keywords: Automotive Security · Security Operations Center · Vehicle SOC · Enterprise IT SOC.

1 Introduction

Juniper Research predicts that by 2027, up to 367 million connected vehicles will be in service [1]. Above all, technologies such as 5G unlock high-speed and low-latency capabilities. Due to the increasing connectivity of vehicles, the target area for cyber attacks is correspondingly growing. The Upstream Global Automotive Cybersecurity Report 2023 shows 151 new Common Vulnerabilities and Exposures in the automotive sector for 2022 [32]. Due to the new threat landscape and the growing number of cyber attacks, Security Operations Centers (SOCs) are essential for the automotive sector.

A SOC is a central organization that provides Information Technology (IT) security services to prevent and deal with security threats. Enterprise IT SOCs function well for providing security monitoring for the IT systems in standard enterprise architectures, including perimeter, network, servers, and endpoints. Vehicle systems are fundamentally different, primarily utilizing embedded systems, a different technology ecosystem, and automotive regulations, to name a few. This paper defines the minimum legal requirements of a modern Vehicle Security Operations Center (VSOC) and shows how a SOC has to be adapted to protect vehicle fleets compared to a traditional enterprise SOC. To answer the research question, general SOC capabilities are defined and used to establish requirements for a VSOC from automotive regulations and best practices. Afterward, SOC metrics are utilized to get a structured overview of the unique needs of a VSOC. As a result, we make the following contributions:

- Definition of minimum VSOC requirements based on automotive regulations and best practices.
- Identification of similarities and differences between a VSOC and an enterprise IT SOC.
- Identification of challenges in implementing a VSOC.

2 Related Work

To the best of our knowledge, no publicly available research paper addresses the differences between an enterprise IT and a vehicle SOC. Specific literature on a current SOC in the automotive sector is also limited and is primarily part of company advertising material.

In 2019, Langer et al. [17] developed an Automotive Cyber Defense Center which manages and secures vehicles over the entire period of use. The work shows a possible interaction of SOC, Security Information and Event Management (SIEM), Cybersecurity Management System (CSMS), Over-The-Air (OTA) updates, and a Cyber Incident Response Team (CIRT) to secure public mobility, Original Equipment Manufacturer (OEM)-controlled mobility services, fleets, and single vehicles. Barletta et al. [5] further developed this work into a VSOC for Improving Automotive Security in 2022. A prototype for real-time monitoring of intra-vehicle communication in next-generation vehicles was created and evaluated with Denial-of-Service and Fuzzing attacks.

The company NTT DATA provides a comprehensive white paper [21] which focuses on the specific attack surfaces, standards, and regulations of modern vehicles crucial for a VSOC. Upstream introduces another proprietary state-of-the-art VSOC concept. Their annual Global Automotive Cybersecurity Report [31] gives an overview of the Automotive Cybersecurity Solution Landscape. They chose a multi-layered approach, which bundles SIEM, Network Detection and Response, Vehicle Detection and Response, and other capabilities used in an enterprise IT SOC into a VSOC.

Several regulations and recommendations on cybersecurity for vehicles can provide information on the minimum requirements for a VSOC. Among them is the UN Regulation No. 155, "*Uniform provisions concerning the approval of vehicles regarding cybersecurity and cybersecurity management system*" [30], which sets IT security requirements for the manufacturer to comply with before new vehicles are registered. The ISO/SAE 21434 standard "*Road vehicles - Cybersecurity engineering*" [15] defines further specifications in the field of automotive cybersecurity engineering. In addition, the European Union Agency for Cybersecurity provides best practices for smart and cooperative, connected, and automated mobility (CCAM) [8, 9].

3 Primary Security Operations Center Capabilities

To obtain a uniform basis to compare an enterprise IT SOC and a VSOC, primary SOC capabilities are established. SOC capabilities have been specified independently of its application area through established security management frameworks [16, 20, 33] and information security standards [14]. Parts of these capacities fall under the remit of a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT). The precise allocation of responsibilities is fluid or overlapping in most organizations. CERT and CSIRT can be seen as specialized sub-capabilities that work based on the data and alarms collected by the SOC [3].

Our paper draws a comparison that is as universal and complete as possible by considering services attributed to CERT and CSIRT. Primary SOC capabilities include the following aspects highlighted in Table 1.

Capability	Description
Change and Asset Management	Implementing monitoring, and documenting all IT infrastructure assets to overview the environment and ensure only authorized changes.
Threat Intelligence Management	Collection, analysis, production, and sharing of cyber threat intelligence
Vulnerability Management	Identification and proactive addressing of vulnerabilities.
Data Collection and Management	Includes collecting security-related data/events and archiving for forensic and legal purposes.
Security Event Management	Real-time detection of cyber attacks and correlation of the given data for analysis and reaction to the security incident.
Incident and Crisis Management	Identification of cyber threats and reaction with necessary measures when a cyber incident or crisis occurs.
Forensic and Investigation of Security Incidents	Analysis of the root cause of security incidents to learn from and develop improvements.
Compliance Management and Reporting	Providing reports on the current threat situation and compliance with security standards and guidelines.
Recommendations and Advice	Provision of consulting services and recommendations regarding improving IT security.
Security Awareness Training	Education and sensitization of humans regarding IT security to mitigate user risk.

Table 1. Capabilities of a modern Security Operations Center (SOC).

4 Defining a Vehicle Security Operations Center to protect Vehicle Fleets

Since several sources already detail the requirements and regulations for a traditional IT SOC [16, 19, 33], this section will define the regulatory specifics and best practices of a SOC specialized in protecting vehicle fleets. Furthermore, a distinction between a VSOC and the vehicle manufacturer's SOC is established. A vehicle manufacturer should maintain two mostly separate SOCs. One of these SOCs can be classified as an enterprise IT SOC, which oversees the design and manufacture of the vehicles. This SOC can be set up relatively independently of the manufactured product and focuses on the employees, their endpoints, and servers required to produce vehicles. A VSOC specializes in protecting the manufacturer's vehicle fleet from cyber-attacks; this includes the vehicle itself and all communication with its ecosystem, including sensors and infrastructure. A VSOC is thus designed to provide security after the vehicle is manufactured and operational. Many SOC tasks overlap or must be carried out individually for the vehicle manufacturers' enterprise SOC and VSOC. The following capabilities

are classified as essential for establishing a functioning VSOC by the definition in section 3. It should be noted that only the points relevant to a VSOC are listed; further specifications must be implemented by the OEM SOC and other instances to comply with the law.

4.1 UN Regulation No. 155

One of the primary points of reference for defining the capabilities of a modern VSOC is the UN Regulation No. 155 [7, 30]. This document specifies the United Nations Economic Commission for Europe (UNECE) cybersecurity regulations for car manufacturers who are members of UNECE WP.29. Implementing processes defined in the regulation is mandatory for market access and approval of new vehicles. Annex 5 defines a list of explicit threats and corresponding mitigations; since this work only overviews mandatory VSOC capabilities and does not detail technologies, only the high-level processes are listed below.

- Establish processes to manage the implementation of cybersecurity.
- Regularly identify risks and threats to vehicle types.
- Establish processes to assess, categorize and treat identified risks.
- Establish processes to verify that identified risks are managed.
- Regularly test the cybersecurity and risk assessment of a vehicle type.
- Monitor, detect and respond to cyberattacks, threats, and vulnerabilities.
- Provide forensic data capability to analyze cyberattacks.
- Manage cybersecurity dependencies with suppliers, service providers and sub-organizations.

4.2 ISO/SAE 21434

Further requirements come from the ISO/SAE 21434:2021 standard [15] developed by the ISO and SAE working group. This standard affects vehicle manufacturers, suppliers, engineering, software, and infrastructure service providers in the automotive sector and establishes minimum requirements for automotive cybersecurity engineering. The following aspects were considered mandatory for a VSOC. Those are *Organizational Cybersecurity Management* (Table 2), *Continual Cybersecurity Activities* (Table 3), *Operations and Maintenance* (Table 4), *End of Cybersecurity Support and Decommissioning* (Table 5), and *Threat Analysis and Risk Assessment Methods* (Table 6).

Aspect	Description
Cybersecurity Culture	Employ and train cybersecurity roles to continuously improve a strong cybersecurity culture.
Information Sharing	Establish rules regarding information sharing.
Management Systems	Institute and maintain change management, documentation management, and configuration management.
Information Security Management	Establish an information security management system.
Organizational Cybersecurity Audit	Perform independent cybersecurity audits.

Table 2. Organizational Cybersecurity Management in ISO/SAE 21434.

Aspect	Description
Cybersecurity Monitoring	Establish triggers for triaging cybersecurity information and determine if it is a cybersecurity event.
Cybersecurity Event Evaluation	Evaluate cybersecurity events to identify weaknesses.
Vulnerability Analysis	Analyse weaknesses to identify and manage vulnerabilities.
Vulnerability Management	Mitigate vulnerabilities or apply cybersecurity incident response.

Table 3. Continual Cybersecurity Activities in ISO/SAE 21434.

Aspect	Description
Cybersecurity Incident Response	Develop and implement cybersecurity incident response plans.
Updates	Develop update-related capabilities.

Table 4. Operations and Maintenance in ISO/SAE 21434.

Aspect	Description
End of Cybersecurity Support	Establish procedures to communicate the end of cybersecurity support to customers.
Decommissioning	Provide cybersecurity requirements for post-development.

Table 5. End of Cybersecurity Support and Decommissioning in ISO/SAE 21434.

Aspect	Description
Asset Identification	Identify damage scenarios and cybersecurity properties that lead to it.
Threat Scenario Identification	Identify threat scenarios and their components.
Impact Rating	Asses impact of damage scenario.
Attack Path Analysis	Identify attack paths for threat scenarios.
Attack Feasibility Rating	Conduct an effort rating for each attack path.
Risk Value Determination	Identify a risk value based on impact and attack feasibility.
Risk Treatment Decision	Determine risk treatment option for every threat scenario.

Table 6. Threat Analysis and Risk Assessment Methods in ISO/SAE 21434.

4.3 European Union Agency for Cybersecurity

European Union Agency for Cybersecurity [10] was founded in 2014 to achieve a high IT security level across Europe. They contribute by publishing EU cyber policies, recommendations, and best practices in many areas of IT security. Two of the publications that are important for the automotive sector are "*ENISA Good practices for security of Smart Cars*" [8] from 2019 and "*How to Secure the Connected & Automated Mobility (CAM) Ecosystem*" [9] from 2021. These contain detailed best practices and security measures that a mature VSOC should implement, but enforcing the recommendations is optional. Table 7 summarizes the practices.

Aspect	Requirements
Asset Management	Establish tools for automatic asset management. Keep an up-to-date overview of all assets. Establish a change management process for new devices and software.
Risk and Threat Management	Adopt risk management and consider automotive threat and attack scenarios. Perform regular cybersecurity risk analysis. Monitor security vulnerabilities. Perform event-driven security evaluations. Establishing a threat intelligence process. Perform regular security control assessments and deploy patches if needed. Regularly evaluate security assumptions and define end-of-life processes.
Relationships with Suppliers	Establish security-related information sharing with suppliers without disclosing intellectual property.
Training and Awareness	Establish security-related information sharing between all involved organizations. Raise awareness about the importance and impact of cybersecurity among employees and suppliers. Promote certification schemes for automotive security. Regularly update security training. Perform security awareness training for vehicle operators and passengers.
Security Management	Establish a SOC and dedicated security teams. Designate specialists for security-related topics. Define an information security management system for the entire lifecycle. Establish an internal task force for security-related decisions to facilitate accountability. Track and implement up-to-date cybersecurity regulations, standards, and best practices.
Incident Management	Regularly revise OEM and 3rd party supplier incident handling processes. Regularly revise OEM and 3rd party supplier CSIRT. Report incidents. Classify cybersecurity incidents to enable prioritization. Establish a process for misbehaving Intelligent Transport Systems and Services (ITS).

Table 7. General Practises in the European Union Agency Standard.

As a result, the European Union Agency for Cybersecuritys defines different technical practices. Table 8 summarizes those.

Practice	Description
Detection	Establish and monitor properly protected detection and logging mechanisms at the vehicle and back-end level.
Protection of Networks and Protocols	Establish and maintain protection for vehicle communication and administration tools.
Software Security	Ensure that software is configured and updated securely and can not be tampered with.
Cloud Security	Protect and monitor cloud data and communication.
Access Control	Apply security controls, prevent privilege abuse and encourage Multi-Factor Authentication.
Self-Protection and Cyber Resilience	Apply to harden, reinforce interfaces robustness, strengthen applications isolation at runtime and network segregation.
(Semi-) Autonomous Systems Self Protection and Cyber Resilience	Protect Artificial Intelligence and Machine Learning against data falsifications and adversarial attacks.
Continuity of Operations	Establish a Business Continuity Plan and a Business Recovery Plan.

Table 8. Technical Practices in the European Union Agency Standard.

5 Security Operations Center (SOC) Metrics

The two types of SOCs are compared with the general SOC metrics proposed by Vielberth et al. [33] in his study about SOCs and their open challenges. SOC metrics deemed valid for evaluation are coverage, people, technical, governance, and compliance. An enterprise IT SOC provides the fundamental capabilities defined in section 3; the following listing only covers VSOC-specific additional requirements.

5.1 Coverage

The coverage metric represents how many assets are monitored and in what context. An enterprise IT SOC protects a few thousand fully managed endpoints of employees, servers, and infrastructure during regular working hours and on-call duty. Vehicle fleets scale this task across millions of vehicles, monitoring these assets 24/7 and in near real-time. In addition to monitoring, resources for analysis, mitigation, and incident responses must be made available. The assets to be protected are not located in a limited area, like in a company, but are distributed worldwide. As a result, restricting physical access and a remote connection cannot be guaranteed. Furthermore, vehicle owners have the Right to Repair leading to modified hardware and software. Many vehicle models and individually configurable equipment contribute to various environments that must be considered. This level of protection must be provided throughout the

entire vehicle's lifecycle, which is on average 18 years [28], a lot longer than enterprise devices. [6, 9, 22]

5.2 People

Since a SOC primarily provides IT security services, employees are among the most critical aspects. The following section highlights the resulting challenges.

Domain Knowledge SOC analysts can be divided into three different tiers. Tier 1 analysts are responsible for the first level of monitoring. They open tickets for events and do rudimentary investigation and mitigation using predefined workbooks or automation. If events are not defined in a workbook or require more profound analysis, they are passed on to tier 2. These analysts have in-depth IT security knowledge and CSIRT experience. They are capable of mitigating more complex threats and recommending changes. Analysts with specialized expert knowledge sit in the third tier. These analysts can actively find and prevent threats through threat hunting and provide forensic analysis such as malware reverse engineering and counter-intelligence [4]. Only the first tier can be carried out without special domain knowledge of the automotive field and how vehicles operate. Skilled and in the automotive sector specialized resources are hard to find and retain in the labor market [9]. In an enterprise IT SOC, tasks are relatively similar regardless of the product manufactured in the company so that employees can move between individual industries without extensive retraining.

Analyst Bias Cognitive biases can be divided into two types [12]. Availability bias is the tendency to rely on information that comes readily to mind. This information is often repeated or has higher value through personal experience. Another type is confirmation bias, defined as looking for specific information in data that supports our beliefs rather than looking at the complete picture. Rosoff et al. [24] showed in their paper about heuristics and bias in cyber that prior experiences shape future decisions. In a traditional enterprise IT SOC, employees can apply the knowledge they have acquired in various industries. And thus get the opportunity to analyze diverse information and interact with colleagues with different backgrounds and experiences. On the other hand, the automotive industry only has a limited number of vehicle manufacturers who employ workers in a VSOC. Since domain knowledge is required, individuals are less likely to have much experience outside the automotive domain. This characteristic establishes a certain level of bias, leading to incorrect analysis, primarily due to the rapid development of vehicles towards cooperative, connected and automated mobility (CCAM) which brings new technologies and attack vectors. Since no studies explicitly address bias in automotive security, this could be a good area for further research.

5.3 Technical

The different technological ecosystems bring individual challenges and cyber attack vectors, which this section examines.

Limitation Enterprise IT networks have the advantage of being able to provide a lot of bandwidth and storage relatively inexpensively. In a vehicle, storage capacity and data transmission are limited, as is the volume of data that can be processed in a VSOC. Millions of modern connected vehicles will each generate an estimated 25 GB of data per hour [23]. Integrating intelligent capabilities is necessary to efficiently retain and transfer relevant data from the vehicles to the OEM. Due to a large number of vehicles, OEMs have to spend a significant amount of money to equip all vehicles with the hardware required to ensure IT security and set up a VSOC. [21]

Vulnerability Besides entertainment and multimedia systems, most vehicle components consist of embedded systems and specially manufactured hardware and software. This leads to an extensive attack surface that offers many attack possibilities due to the large number of vehicles produced and the easy physical access. The attack surface of an enterprise IT SOC is significantly smaller and only overlaps with a VSOC in a few assets. Summer et al. [27] provide an overview of the extent of possible attack vectors in their classification of automotive cyberattacks. A rough outline of the additional attack surface of modern smart cars is summarized in the following listing, without considering OEM and traffic infrastructure. [18]

- **Electronic Control Unit:** Steering and Breaking ECU, Vehicle Access System ECU, ADAS System ECU, Lightning System ECU, Airbag ECU, Engine and Transmission ECU
- **Wireless Communication:** Bluetooth/WIFI, Remote Link Type App, eCall Service, DSCR-Based Receiver (V2X), GNSS
- **Wired Communication:** Can Bus, Ethernet, USB, FlexRay
- **Consumer Technology:** Smartphone, Infotainment System
- **Vehicle Components and Sensors:** Battery, Speedometer, Central Locking, Driving Support, OBD 2, TPMS

As a result of the expanded attack surfaces, more vulnerabilities and attack vectors must be considered. In addition, it has to be noted that the persistence of threats, especially if not made public, has a more significant impact due to the prolonged use of vehicles. This must also be regarded in threat intelligence; an enterprise IT SOC can choose between many sources and cyber professionals who share their knowledge. There are also mature frameworks, such as MITRE ATT&CK [2], for classifying and describing cyber attacks that facilitate the exchange of information. Automotive-focused data feeds are limited and expensive but provide essential and relevant information. [21, 13, 32]

Risk and Safety An incident in an enterprise environment can lead to equipment failure, data exfiltration, or financial losses. In a vehicle, vulnerabilities or faulty updates can cause consequences such as traffic disturbance or deaths from a car accident. The potential impact is also far more significant due to a fleet's many vehicles. For this reason, risks and safety in the automotive environment must be valued higher, limiting a VSOC's scope of action. [25]

Incident SOC analysts can act directly in an enterprise environment and import the manufacturer's forced patches or workarounds in case of an incident or a vulnerability. In the automotive domain, this is often a lengthy process. First, it must be ensured that a connection to the vehicle can be established and that the owner allows the update. If a vulnerability is detected, a root-cause analysis must be carried out, with the help of which new software or fixes can be built. This software must be subjected to extensive testing and validation before it is distributed to the vehicle fleet via an OTA update or an auto repair shop. [25]

5.4 Governance and Compliance

This section deals with the agreement between IT security and economic interests and mandatory regulatory guidelines and standards in the automotive sector.

Compliance While an enterprise IT SOC benefits from various tools and processes created explicitly for their use cases, a large part of the options in the automotive industry are developed by the vehicle manufacturers themselves and kept internally. The lack of standardization brings further disadvantages, such as the increased difficulty of developing security solutions in an individual and complex ecosystem. This behavior can also be observed with best practices and standards regarding IT security. While an enterprise IT SOC has established frameworks and guides, options in the automotive industry are limited. Only in recent years have dedicated IT security regulations and standards been introduced in the automotive domain. More automotive security laws and the corresponding incentives through punishment would encourage OEMs to allocate sufficient resources to a VSOC. [8, 29, 31]

Identity and Asset Management Another problem is the lack of full access to the identity and functionality of the vehicle. Due to privacy regulations like GDPR [11] or Car Spy Act [26] and the vehicle manufacturer's wish to keep their vehicle's components secret, information sharing is challenging to implement and primarily anonymous. In an enterprise SOC, the IT assets belong to the company and are managed by it. The SOC employees have full access and all rights to make changes at any time. However, the OEM does not own vehicles and depends on the buyer. Due to sales, a VSOC can not pinpoint who currently owns the vehicle. In addition, if an endpoint or server fails, the company loses money; in a vehicle, this can endanger the driver's life. As a result, the actions a SOC can take are limited while the vehicle is in use. [8, 29]

6 Conclusion

This paper demonstrates which capabilities and domain-specific properties a VSOC must have compared to an enterprise IT SOC to protect vehicle fleets effectively. Primary challenges have been identified that must be considered when implementing a VSOC. These challenges show that methods, procedures, and technical solutions used in an enterprise IT SOC cannot be directly transferred to a VSOC. The main differences identified are that a VSOC must monitor and protect several million vehicles around the clock over decades. Furthermore, monitoring, intrusion detection, and incident response must occur in various environments due to modified hardware and software. In addition to scaling the monitoring, finding and retaining a workforce specialized in the automotive sector without fostering analyst bias is challenging. Protecting vehicle fleets brings a different attack surface, which also differs regarding risks and vulnerabilities. Limitations such as storage, bandwidth, and update options require dedicated technical solutions and processes. Governance and compliance lack manufacturer-independent predefined procedures, tools, guides, and best practices. IT security regulations for the automotive sector have only recently been introduced and bring difficulties such as data protection and limitations on the intervention of a SOC in the vehicle. The limited literature on a VSOC describes a superficial implementation without directly addressing the challenge of protecting a vehicle fleet. Further basic research in the VSOC area is necessary to achieve an ideal adaptation of a traditional enterprise SOC for the automotive sector. This work intends to serve as a basis for finding a solution by defining the minimum requirements for a VSOC and summarizing the challenges in this area.

Acknowledgment

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

References

1. Connected vehicles to surpass 367 million globally by 2027 (03/04/2023), https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally
2. Mitre att&ck (04/06/2023), https://attack.mitre.org/
3. E-CMIRC: Towards a Model for the Integration of Services Between SOCs and CSIRTs. Academic Conferences International Limited (07 2016)
4. Agyepong, E., Cherdantseva, Y., Reinecke, P., Burnap, P.: Towards a framework for measuring the performance of a security operations center analyst. pp. 1–8 (2020), https://api.semanticscholar.org/CorpusID:220606696

5. Barletta, V.S., Caivano, D., de Vincentiis, M., Ragone, A., Scalera, M., Martín, M.Á.S.: V-soc4as: A vehicle-soc for improving automotive security. Algorithms **16**(2), 112 (2023). https://doi.org/10.3390/a16020112, https://www.mdpi.com/1999-4893/16/2/112
6. Burkacky, O., Pototzky, K., Johannes, D., Klein, B., Scherf, G.: Automotive cybersecurity: Mastering the challenge (30/03/2023), https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge
7. Economic, Council, S.: Proposal for interpretation documents for un regulation no 155 (07/06/2023), https://globalautoregs.com/documents/24474
8. ENISA: Enisa good practices for security of smart cars (10/05/2023), https://www.enisa.europa.eu/publications/smart-cars
9. ENISA: How to secure the connected & automated mobility (cam) ecosystem (10/05/2023), https://www.enisa.europa.eu/news/enisa-news/how-to-secure-the-connected-automated-mobility-cam-ecosystem
10. ENISA: Enisa (14/05/2023), https://www.enisa.europa.eu/
11. GDPR.eu: General data protection regulation (gdpr) compliance guidelines (08/06/2023), https://gdpr.eu/
12. Grindstaff, L.: Through your mind's eye: What biases are impacting your security posture? McAfee (2052021), https://www.mcafee.com/blogs/other-blogs/executive-perspectives/through-your-minds-eye-what-biases-are-impacting-your-security-posture/
13. Huq, N., Gibson, C., Kropotov, V., Vosseler, R.: Cybersecurity for connected cars: Exploring risks in 5g, cloud, and other connected technologies https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf
14. ISO: Iso/iec 27000:2018 (03/04/2023), https://www.iso.org/standard/73906.html
15. ISO: Iso/sae 21434:2021 (03/04/2023), https://www.iso.org/standard/70918.html
16. Jacobs, P., Arnab, A., Irwin, B.: Classification of security operation centers. In: 2013 Information Security for South Africa. pp. 1–7 (2013). https://doi.org/10.1109/ISSA.2013.6641054
17. Langer, F., Schüppel, F., Stahlbock, L.: Establishing an automotive cyber defense center (2019), https://api.semanticscholar.org/CorpusID:210967824
18. Malatras, D.A.: Efforts on automotive cybersecurity (13092019), https://www.headstart-project.eu/wp-content/uploads/2019/09/2019-09-13_ENISA_Automotive_Cybersecurity_HEADSTART_EU.pdf
19. Nathans, D., Limbert, M.: Designing and building a security operations center. Syngress, Waltham, Massachusetts (2015). https://doi.org/https://doi.org/10.1016/B978-0-12-800899-7.00008-2, https://www.sciencedirect.com/book/9780128008997/designing-and-building-security-operations-center
20. NIST: The five functions https://www.nist.gov/cyberframework/online-learning/five-functions
21. NTT-DATA: Höhere automotive cybersecurity mit v-soc von ntt data (28/03/2023), https://de.nttdata.com/insights/whitepapers/hoehere-automotive-cybersecurity-mit-v-soc-von-ntt-data
22. Oancea, I.G., Simion, E.: Challenges in automotive security. In: 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). pp. 1–6 (2018). https://doi.org/10.1109/ECAI.2018.8679052
23. Richter, F.: Big data on wheels. Statista (02/09/2017), https://www.statista.com/chart/8018/connected-car-data-generation/

24. Rosoff, H., Cui, J., John, R.S.: Heuristics and biases in cyber security dilemmas. Environment Systems and Decisions **33**, 517–529 (2013), https://api.semanticscholar.org/CorpusID:12736922
25. Segal, S.: 10 biggest challenges facing automotive cisos tasked with vehicle cyber security (10/02/2023), https://argus-sec.com/blog/cyber-security-blog/automotive-security-10-biggest-challenges-facing-oem-cisos/
26. Sen. Markey, E.J.: S.680 - 115th congress (2017-2018): Spy car act of 2017 (2017), https://www.congress.gov/bill/115th-congress/senate-bill/680
27. Sommer, F., Dürrwang, J., Kriesten, R.: Survey and classification of automotive security attacks. Inf. **10**, 148 (2019), https://api.semanticscholar.org/CorpusID:145897673
28. Statista: Lebensdauer von autos in deutschland (29/05/2023), https://de.statista.com/statistik/daten/studie/316498/umfrage/lebensdauer-von-autos-deutschland/
29. Turgeman, N.: 3 approaches to building a vehicle security operations center. Upstream (04/08/2019), https://upstream.auto/blog/3-approaches-to-building-an-automotive-soc/
30. UNECE: Un regulation no. 155 (10/05/2023), https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
31. Upstream Security: 2022 global automotive cybersecurity report (15/02/2022), https://upstream.auto/2022report/
32. Upstream Security: Upstream's 2023 global automotive cybersecurity report (23/03/2023), https://upstream.auto/reports/global-automotive-cybersecurity-report/
33. Vielberth, M., Bohm, F., Fichtinger, I., Pernul, G.: Security operations center: A systematic study and open challenges. IEEE Access **8**, 227756–227779 (2020). https://doi.org/10.1109/ACCESS.2020.3045514