2025

Künstliche Intelligenz im Vehicle Security Operation Center

Wegbereiter einer resilienten Cyberabwehr für vernetzte Fahrzeuge und deren IT-Infrastruktur

Authors: Christian Trompler – P3 group Deutschland
Andreas Sitar – P3 group Rumänien

Warum Sie dieses Whitepaper lesen sollten:

- **Verstehen**, wie Künstliche Intelligenz (KI) den Betrieb eines Vehicle SOCs transformiert – von der Anomalieerkennung bis zur automatisierten Reaktion.
- **Erkennen**, welche organisatorischen, technischen und regulatorischen Voraussetzungen notwendig sind, um KI sicher, erklärbar und regelkonform einzusetzen.
- **Einordnen**, wie KI-basierte Verfahren zur Erfüllung aktueller und künftiger Vorgaben wie UN R155, ISO/SAE 21434, EU-AI-Act, NIS2 und Cyber Resilience Act beitragen.

2025

Inhaltsverzeichnis

1. Executive Summary

Die zunehmende Digitalisierung des Automobils hat schon vor langer Zeit eine neue Ära der Cybersecurity eingeläutet. Fahrzeuge sind heute vernetzte IT-Systeme mit einer Vielzahl an Steuergeräten, komplexen Software-Stacks und permanenter Anbindung an Cloud-Infrastrukturen, mobile Anwendungen und V2X-Kommunikation (Vehicle-to-Everything). Diese Vernetzung bietet Komfort, Sicherheit und Effizienz – erhöht aber gleichzeitig die Angriffsfläche in bislang unbekanntem Ausmaß.

Ein Vehicle Security Operation Center (Vehicle-SOC) ist die Antwort auf diese Entwicklung. Es dient als **zentrales Steuerungswerkzeug der Cyberabwehr** und überwacht die Sicherheit ganzer Fahrzeugflotten über den gesamten Lebenszyklus hinweg – von der Entwicklung bis zur Stilllegung. Seine Aufgabe ist es, sicherheitsrelevante Ereignisse aus Fahrzeug, Backend, Cloud und Lieferkette zu erkennen, zu korrelieren und kontrolliert darauf zu reagieren.

Klassische, manuell arbeitende SOCs stoßen bei dieser Datenflut an Grenzen. **Künstliche Intelligenz (KI) wird daher zum strategischen Hebel:** Sie kann Muster erkennen, die für Menschen unsichtbar bleiben, Ereignisse automatisch priorisieren und Entscheidungen datenbasiert vorbereiten. Richtig integriert, steigert KI die Effizienz, Präzision und Reaktionsgeschwindigkeit im gesamten Sicherheitsbetrieb.

Ein KI-gestütztes Vehicle-SOC ermöglicht:

- **Früherkennung** unbekannter Angriffsmuster durch Anomalie- und Verhaltensanalysen unterstützt durch Intrusion Detection Systeme (IDS).
- **Reduktion von Fehlalarmen** durch lernende Priorisierungsmodelle.
- **Automatisierte Reaktionsvorschläge** in Echtzeit unter Wahrung menschlicher Kontrolle.
- **Kontinuierliche Verbesserung** durch Rückkopplung realer Vorfälle in Trainingsdaten.
- **Regulatorische Nachvollziehbarkeit**, indem Entscheidungen dokumentiert und erklärbar gemacht werden.

Dieses Whitepaper zeigt, wo und wie KI im Vehicle-SOC den größten Nutzen entfaltet, welche technischen und organisatorischen Voraussetzungen erfüllt sein müssen und wie KI zur stabilen Umsetzung regulatorischer Anforderungen beiträgt.

2. Ausgangslage und Zielbild eines Vehicle SOC Setups

Die Cyberbedrohungen in der Automobilindustrie nehmen in Anzahl und Komplexität stetig zu. Moderne Fahrzeuge sind Teil eines global vernetzten Ökosystems – mit Backend-Servern, mobilen Apps, Werkstatt-Systemen und Lieferanten-Netzwerken. Jede dieser Schnittstellen kann zum Angriffsvektor werden.

Zudem fordern Regulatoren wie die UN-Wirtschaftskommission für Europa (UN-ECE) oder die Europäische Union (EU) den Nachweis eines durchgängigen Cybersecurity Management Systems im Fahrzeug-Lebenszyklus. Der Betrieb eines Vehicle-SOC wird damit nicht nur zum Sicherheitsfaktor, sondern auch zur gesetzlichen Pflicht

Ein modernes Vehicle-SOC verfolgt folgende Zielbilder:

- **Zentralisierung der Überwachung** aller sicherheitsrelevanten Ereignisse.
- **Integration unterschiedlicher Datenquellen** (Fahrzeug, Backend, Cloud, Lieferanten).
- **Standardisierte Prozesse** zur Erkennung, Analyse und Reaktion auf Vorfälle.
- **Automatisierung und KI-Unterstützung**, um Geschwindigkeit und Skalierbarkeit zu gewährleisten.
- **Nachweisbare Compliance** mit internationalen Normen und Gesetzen.

Die Künstliche Intelligenz ist dabei nicht Selbstzweck, sondern **Ermöglicher dieses Zielbilds**: Sie schafft die technische und organisatorische Grundlage, um diese **Anforderungen mit vertretbarem Aufwand** zu erfüllen.

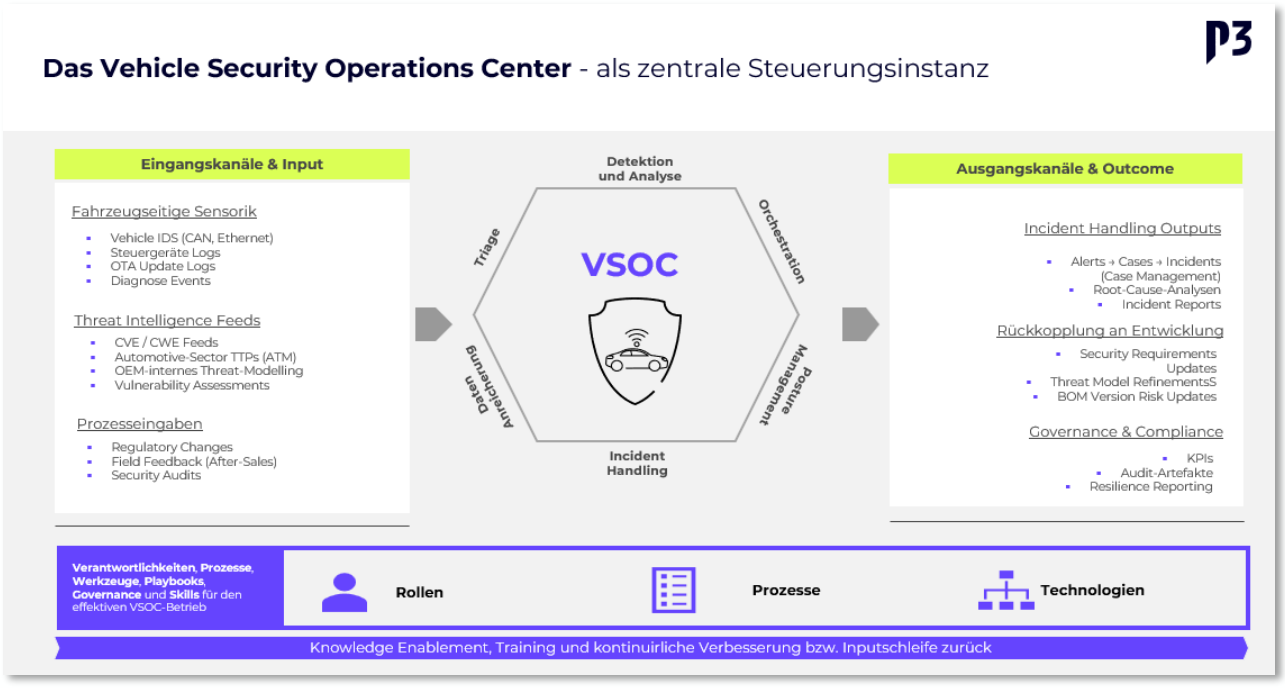

Abb. 1: Darstellung VSOC als zentrale Steuerungsinstanz

3. Einsatzfelder der KI im VSOC

KI kann entlang der gesamten SOC-Wertschöpfungskette eingesetzt werden – von der Erkennung über die Analyse bis zur Reaktion. Nachfolgend sind die wichtigsten Anwendungsfelder, Methodiken und Nutzen beschrieben.

3.1 Anomalieerkennung im Fahrzeug (Onboard)

- **Methodik**: Unüberwachtes Lernen mit Autoencoder-Netzen, One-Class Support-Vector-Machines oder Graph Neural Networks zur Modellierung normaler Kommunikationsmuster zwischen Steuergeräten.
- **Nutzen**: Erkennt Abweichungen in Echtzeit, etwa wenn ein bisher unbeteiligtes Steuergerät auf dem CAN-Bus aktiv wird oder die Kommunikationsfrequenz sich ändert. So können Manipulationen, Spoofing oder Injektionsangriffe frühzeitig erkannt werden.

3.2 Anomalien in Backend- und Cloud (Offboard)

- **Methodik**: Sequenzmodelle (Long Short-Term Memory, Temporal Convolutional Networks) lernen typische Authentifizierungs- und Zugriffsmuster auf APIs und Cloud-Dienste.
- **Nutzen**: Unerwartete Login-Folgen, ungewöhnliche Gerät:Account Beziehungen oder fehlerhafte Token-Verwendung werden automatisch erkannt und korreliert. Das reduziert die durchschnittliche Erkennungszeit enorm.

3.3 Überwachung der Software-Lieferkette

- **Methodik**: Natural-Language-Processing-Modelle verknüpfen Software Stücklisten (Software Bill of Materials) mit bekannten Schwachstellen-Feeds (CVE, CWE).
- **Nutzen:** KI erkennt automatisch, welche Fahrzeugvarianten von einer Schwachstelle betroffen sind, und priorisiert Gegenmaßnahmen nach Risiko und, Impakt und Flottenumfang

3.4 Korrelation und Priorisierung

- **Methodik**: Kombination aus Regressions- und Klassifikationsmodellen (Learning-to-Rank-Ansätze), die Alarmereignisse nach Relevanz bewerten und gruppieren.
- **Nutzen**: Reduziert das Alarmaufkommen um bis zu 80 %, indem gleichartige oder redundante Meldungen zusammengeführt werden. Analysten können sich auf tatsächliche Bedrohungen konzentrieren.

3.5 Automatisierte Incident-Response

Der Incident-Response-Prozess ist in der Regel organisatorisch entkoppelt aus den Monitoring Aktivitäten, jedoch eng an den VSOC-Monitoring-Prozess angebunden, um eine nahtlose Reaktionskette sicherzustellen.

- **Methodik**: Reinforcement-Learning-Modelle (bestärkendes Lernen) und regelbasierte Entscheidungsbäume trainieren auf historische Reaktionsmuster.
- **Nutzen**: KI schlägt konkrete Gegenmaßnahmen vor (z. B. OTA-Update stoppen, Feature deaktivieren, ECU isolieren) und bewertet deren Risiko. Menschen behalten die Freigabe, aber die Entscheidung wird erheblich beschleunigt.

3.6 Bedrohungsanalyse/Threat Intelligence

- **Methodik**: Sprachmodelle (Natural Language Processing) verarbeiten Bedrohungsberichte, Sicherheits-Advisories und Forenbeiträge.
- **Nutzen**: KI extrahiert automatisch relevante Indikatoren (z. B. IoCs, TTPs) und mappt sie auf das MITRE-ATT&CK-Framework für Automotive. Damit kann der SOC proaktiv neue Angriffstrends erkennen.

3.7 Flotten- und Risiko-Analytik

- **Methodik**: Scoring-Modelle kombinieren Expositionsdaten, Angriffswahrscheinlichkeit und Sicherheits-auswirkungen zu einem Risikowert je VIN-Gruppe.
- **Nutzen**: Unterstützt strategische Entscheidungen, welche Fahrzeuge zuerst gepatcht oder untersucht werden sollen.

Zusätzlich von den oben genannten Einsatzfelder wird mit der zunehmender Datenmenge die manuelle Triage schnell zum Engpass. KI-Modelle automatisieren Vorfilterung und Kontextanreicherung und helfen Analysten, echte Bedrohungen früher und zuverlässiger zu identifizieren.

KI-unterstützte Incident-Triage im Vehicle SOC - von Rohsignalen zu priorisierten Incidents

Abb. 2: Darstellung KI-unterstütze Triage im VSOC

4. VSOC Design: Daten, Modelle und Qualitätssicherung

Der Erfolg von Künstlicher Intelligenz im Vehicle-SOC hängt weniger von der Wahl des Algorithmus als von einer **durchdachten Systemarchitektur und Governance** ab. Ein tragfähiges KI-System basiert auf drei Säulen: **Datenqualität, Modellmanagement und Erklärbarkeit.**

Erstens braucht es eine verlässliche **Datenbasis**. Fahrzeug- und Backend-Telemetrie müssen standardisiert, zeitlich synchronisiert und mit Metadaten (Quelle, Vertrauensstufe, Kontext) versehen werden. Nur so lassen sich Modelle über unterschiedliche Fahrzeugplattformen hinweg stabil trainieren. Zentral ist die Definition sogenannter Data Contracts – verbindliche Vereinbarungen darüber, welche Ereignisse, Formate und Auflösungen dem SOC zur Verfügung stehen.

Zweitens ist der **Modelllebenszyklus** zu managen. Hier geht es um Planung, Training, Freigabe und Überwachung von KI-Modellen. Ein gereiftes SOC etabliert dazu MLOps-Prozesse (Machine-Learning-Operations), die sicherstellen, dass jedes Modell dokumentiert, versioniert und auditierbar bleibt. Modelle werden regelmäßig auf Leistungsfähigkeit, Drift und Stabilität geprüft. Entscheidend ist die Kopplung an einen Human-in-the-Loop-Mechanismus: Bei Unsicherheiten oder kritischen Bewertungen entscheidet immer ein Analyst.

Drittens bildet die **Qualitätssicherung und Erklärbarkeit** die Basis für Vertrauen. Erklärbare KI-Verfahren (Explainable AI) machen nachvollziehbar, warum ein Alarm ausgelöst wurde – ein zentraler Aspekt für Analysten und für regulatorische Audits. Jede Modellversion erhält eine „Model Card“ mit Zweck, Gültigkeit und Leistungskennzahlen. Diese Transparenz ist Voraussetzung dafür, dass KI-Entscheidungen als Bestandteil des Cybersecurity Managementsystems akzeptiert werden. Darüber hinaus sollte das Systemdesign den **Betriebsaspekt** aktiv mitdenken: KI-Modelle benötigen eine gesicherte Infrastruktur für Datenaufnahme, Berechnung und Rückkopplung. Dies umfasst skalierbare Datenpipelines, definierte Latenzzeiten und Mechanismen zur Priorisierung sicherheitsrelevanter Informationen.

Zudem sollte jedes Modell über einen „Safe Fail“-Modus verfügen – also klare Regeln, wie es sich bei Unsicherheiten verhält, etwa durch Rückfall auf konservative Schwellwerte oder Übergabe an manuelle Prüfung. Damit wird KI zu einem stabilen Bestandteil der SOC-Architektur, ohne neue operative Risiken einzuführen.

Ein konzeptionell sauber aufgebautes Systemdesign ist daher keine technische Randfrage, sondern die Grundlage, um KI im Vehicle-SOC **nachhaltig, reproduzierbar und vertrauenswürdig zu betreiben.**

5. Sicherheit, Adversarial Machine Learning & Governance

Mit dem Einsatz von KI entsteht ein neues Schutzziel: **die Sicherheit der KI selbst**. Da Modelle aus Daten lernen, können Manipulationen in den Eingangsdaten oder im Trainingsprozess das Verhalten unbemerkt verändern – sogenannte Adversarial Attacks. Diese Bedrohung verlangt, dass Sicherheit und Governance von Anfang an integraler Bestandteil des KI-Betriebs sind.

Ein wirksames Schutzkonzept kombiniert **technische Robustheit und organisatorische Verantwortung.** Technisch bedeutet das: Trainingsdaten werden auf Integrität geprüft, Modelle werden vor dem Rollout getestet und in Betrieb kontinuierlich überwacht. Drift-Analysen erkennen schleichende Veränderungen; Integritätsprüfungen und Prüfsummen sichern Modelle gegen Manipulation. So entsteht ein Kontrollrahmen, der sicherstellt, dass Entscheidungen stets auf vertrauenswürdigen Daten basieren.

Organisatorisch wird die Verantwortung in einem **Governance Rahmen** verankert. Ein interdisziplinäres AI Assurance Board – bestehend aus Security-, Data-Science-, Legal- und Compliance-Vertretern – bewertet Risiken, prüft Freigaben und dokumentiert Entscheidungen. Damit wird gewährleistet, dass KI-Modelle denselben Qualitäts- und Revisionsstandards unterliegen wie klassische sicherheitsrelevante Systeme. Darüber hinaus sollte Governance auch die **Verknüpfung zu bestehenden Sicherheits- und Entwicklungsprozessen herstellen.** KI-Ergebnisse aus dem Betrieb – etwa neu erkannte Angriffsmuster oder Verhaltensänderungen – müssen zurück in die Entwicklungsabteilungen fließen, um Produkte und Sicherheitskonzepte kontinuierlich anzupassen. Dieser Rückkanal verankert KI im Lebenszyklusmanagement und macht sie zu einem Bindeglied zwischen Betrieb und Engineering. Im Zusammenspiel mit bestehenden Normen wie ISO/SAE 21434 unterstützt diese Governance die Rückkopplung zwischen Betrieb und Entwicklung: Efließen in Risikoanalysen und Sicherheitskonzepte ein, während neue Bedrohungen direkt in die Modellpflege zurückgespielt werden. Einige Beispiele von Erkentnissen sind u.a. neue Angriffsvektoren, Schwachstellen in Steuergeräten oder unzureichend abgesicherte Kommunikationspfade.

So entsteht ein **geschlossener Regelkreis zwischen KI, Sicherheit und Organisation**, in dem Modelle nicht nur erkennen und reagieren, sondern sich selbstständig an ein verändertes Bedrohungsumfeld anpassen – stets unter menschlicher Kontrolle und dokumentierter Nachvollziehbarkeit.

Die Absicherung von KI-Systemen ist nicht nur eine technische, sondern zunehmend auch eine regulatorische Verpflichtung. Entsprechend ist die Einbettung in geltende Standards ein zentraler Erfolgsfaktor und wir im folgenden Kapitel betrachtet.

6. Regulatorik – KI als Enabler der Compliance

KI kann maßgeblich dazu beitragen, regulatorische **Anforderungen nachhaltig und automatisiert umzusetzen**. Die nachfolgende Tabelle beschreibt beispielhaft das Mapping zentraler KI-Funktionalitäten zu relevanten Regularien:

Regulatorik	Zentrale Anforderung	Beitrag der KI-Funktion im Vehicle-SOC
UN R155	Kontinuierliche Überwachung und Bewertung von Cyber-Risiken	Anomalieerkennung und KI-gestützte Risikoanalysen liefern Echtzeit-Evidenz für das CSMS-Monitoring.
ISO/SAE 21434	Nachvollziehbare Risikoanalyse, kontinuierliche Verbesserung in Betrieb & Wartung	MLOps-Prozesse mit Drift-Erkennung und Feedback-Loops erfüllen Abschnitt 8 (Operation & Maintenance).
EU AI Act	Transparenz, Nachvollziehbarkeit und menschliche Aufsicht bei Hochrisiko-Systemen	XAI-Methoden (Erklärbarkeit), Model Cards und Human-in-the-Loop-Freigaben sichern Compliance mit Artikeln 13 & 14.
NIS2-Richtlinie	Risikomanagement und Meldepflichten für sicherheitsrelevante Ereignisse	KI-gestützte Erkennung und automatische Klassifizierung von Vorfällen ermöglicht fristgerechtes Reporting.
Cyber Resilience Act (CRA)	Sicherheit während des gesamten Lebenszyklus von Produkten	KI-basierte Schwachstellenkorrelation (SBOM + CVE) unterstützt die laufende Produkt- und Patch-Überwachung.

7. Betrieb, Prozesse und KPIs

Rollen und Verantwortlichkeiten müssen mit dem Einsatz von KI neu gedacht werden, denn der Einsatz von Künstlicher Intelligenz verändert diese grundlegend. **Tier-1-Analysten** werden durch KI bei der Voranalyse und Priorisierung von Alarmen unterstützt. Dabei ist zu beachten, dass nicht jeder Alarm einen Sicherheitsvorfall darstellt, entscheidend ist die frühzeitige Unterscheidung zwischen False Positives und True Positives, um Ressourcen gezielt einzusetzenAnstatt Meldungen manuell zu sichten, konzentrieren sie sich auf die Bewertung sicherheitsrelevanter Fälle. Der **Tier-2-Analyst oder Incident-Responder** erhält automatisiert Kontextdaten zu betroffenen Steuergeräten, Kommunikationspfaden und möglichen Angriffs-szenarien. Dadurch beschleunigt sich die Ursachenanalyse und verbessert sich die Reaktionsqualität.

Der Threat Hunter nutzt KI, um historische Daten nach bisher unbekannten Mustern zu durchsuchen und neue Angriffspfade zu identifizieren. So entsteht ein proaktiver Ansatz zur Bedrohungserkennung. Der **AI Operations Engineer** verantwortet die Pflege und Überwachung der KI-Modelle. Er steuert Trainingszyklen, kontrolliert Daten-Drift und sorgt für die technische Nachvollziehbarkeit und Dokumentation.

Auch der **Compliance Officer** profitiert: KI erstellt automatisierte Reports und Audit-Nachweise, wodurch regulatorische Anforderungen effizienter erfüllt werden können. Damit verschiebt sich der Fokus im SOC von manueller Eventbearbeitung zu einer überwachenden, datengetriebenen Sicherheits-steuerung, in der menschlichen Expertise gezielt für kritische Entscheidungen eingesetzt wird.

Diese Kennzahlen verdeutlichen, dass KI nicht nur Effizienz steigert, sondern **messbar zur Betriebsstabilität und Compliance-Reife beiträgt:**

Kennzahl	Bedeutung	Einfluss der KI
MTTD (Mean Time to Detect)	Zeitspanne von Angriff bis Erkennung	KI reduziert MTTD durch Echtzeit-Anomalieerkennung um bis zu 70 %.
MTTR (Mean Time to Respond)	Zeitspanne bis zur Reaktion	Automatisierte Vorschläge und SOAR-Integration verkürzen MTTR signifikant.
False-Positive-Rate	Anteil irrtümlicher Alarme	Lernende Modelle erkennen wiederkehrende Muster und senken Fehlalarme um Faktor 5.
Coverage Rate	Anteil überwachter Fahrzeuge/Systeme	KI-gestützte Datennormalisierung ermöglicht breitere Abdeckung bei gleichbleibender Analystenzahl.
Explainability Rate	Anteil erklärbarer Entscheidungen	Durch XAI-Methoden steigt der Anteil nachvollziehbarer KI-Entscheidungen auf > 95 %.

8. Implementierung – Worauf ist zu achten?

Die erfolgreiche Einführung von KI im SOC Umfeld ist kein reines Technologie-, sondern vor allem ein **Transformationsprojekt**. Für ein effizientes Rollout müssen Mensch, Prozess und Toolchain gleichermaßen betrachtet und aufeinander abgestimmt werden. Neben der Auswahl geeigneter Use Cases entscheiden organisatorische Reife, Datenstrategie und Governance über den Erfolg. Unternehmen sollten den Aufbau eines KI-gestützten SOC daher als **mehrstufigen Reifeprozess** verstehen: Von der Etablierung verlässlicher Datenflüsse über den Aufbau interdisziplinärer Teams bis hin zur Implementierung klarer Freigabe- und Kontrollmechanismen.

Wichtig ist, technische Innovation mit kulturellem Wandel zu verbinden – denn Vertrauen in KI entsteht nur, wenn ihre Ergebnisse nachvollziehbar, überprüfbar und in bestehende Entscheidungsprozesse eingebettet sind.

- ✓ **Datenqualität als Fundament:**
  Ohne saubere, standardisierte Telemetrie keine belastbare KI-Erkennung.
- ✓ **Integration der Lieferkette:**
  Klare Verträge zu Datenlieferung, Schwachstellen-Meldung und Incident-Response.
- ✓ **Datenschutz & Ethik:**
  Pseudonymisierung, regionale Verarbeitung, menschliche Verantwortung.
- ✓ **Organisatorische Verankerung:**
  Enge Verzahnung von IT-, Fahrzeugentwicklung-, Sicherheits- und Rechtsabteilungen.
- ✓ **Qualifizierung:**
  Analysten müssen die Arbeitsweise der KI verstehen und Ergebnisse interpretieren können.
- ✓ **Skalierbarkeit:**
  Architekturen müssen GPU-Kapazitäten und Datenvolumen bewältigen.
- ✓ **Reifegradmodelle:**
  Einführung schrittweise nach Data-&-AI-Capability-Maturity-Frameworks planen.
- ✓ **Kontinuierliche Verbesserung:**
  Modelle altern – regelmäßige Überprüfung und Nachtraining sind Pflicht.

Aus diesen praktischen Anforderungen ergibt sich eine klare strategische Richtung für die Branche – von der Experimentierphase hin zu strukturierten, KI-gestützten Sicherheitsoperationen

9. Herausforderungen im VSOC-Betrieb und mögliche Lösungsansätze

Der operative **Betrieb** eines **Vehicle Security Operations Centers** (VSOC) ist mit mehreren **Herausforderungen** verbunden, die die Wirksamkeit der Cyberabwehr beeinflussen. Eine zentrale Schwierigkeit besteht in der heterogenen **Datenqualität** entlang von Fahrzeug-, Backend- und Lieferkettenartefakten: Unterschiede in Format, Granularität und Versionierung erschweren die korrekte Einordnung und Priorisierung sicherheitsrelevanter Ereignisse.

Gleichzeitig führt die stetig wachsende Alarmmenge zu „Alarm Fatigue“, wodurch Analysten echte Vorfälle schwerer von harmlosen Anomalien unterscheiden können.

Zusätzlich beeinträchtigen fragmentierte Toolchains, manuelle Übergaben und historisch gewachsene Prozesslandschaften die Reaktionsgeschwindigkeit. Der Mangel an spezialisierten Analysten mit fahrzeugdomänenspezifischem Wissen verstärkt diese Situation – es kommt zu Verzögerungen, mehr Fehlern und Lücken in der VIN- oder ‚Fahrzeugflottensteuerung‘.

Gezielte Maßnahmen adressieren typische Herausforderungen und erhöhen Effizienz, Skalierbarkeit und Resilienz:

- **Datenqualität steigern** durch Normalisierung, Data-Quality-KPIs und verbindliche Supplier-Schnittstellen.
- **SBOM-Versionierung standardisieren** (z. B. SPDX/CycloneDX) und automatisiert gegen CVEs korrelieren.
- **Alarmflut reduzieren** via KI-gestützter Triage, kontextueller Anreicherung und adaptiver Schwellenwerte.
- **Skills ausbauen** mittels Rollen-Enablement, Playbooks und regelmäßigen Tabletop-Exercises.
- **Toolchain-Fragmentierung** reduzieren durch API-basierte Integration, konsolidiertes Case-Management und einheitliche Workspaces.

Dadurch steigt die organisatorische Resilienz, während Effizienz, Skalierbarkeit und Reaktionsgeschwindigkeit deutlich verbessert werden.

10. Schlussfolgerungen

KI ist der entscheidende Hebel, um den steigenden Anforderungen an Sicherheit, Geschwindigkeit und Compliance in der Fahrzeug-Cybersecurity gerecht zu werden. Sie **ergänzt menschliche Expertise** durch datenbasierte Erkenntnis, entlastet Analysten und ermöglicht **skalierbare Sicherheitsüberwachung** über Millionen Fahrzeuge hinweg.

Seit der verpflichtenden Anwendung der UN R155 auf neue Fahrzeugtypen haben die meisten Hersteller tragfähige CSMS-Strukturen etabliert, Audit-Trails aufgebaut und VSOC-Funktionen — intern oder über spezialisierte Dienstleister — in Betrieb genommen. Parallel wurden Software-Update-Management-Systeme nach UN R156 verankert, OTA-Pipelines gehärtet und erste KI-gestützte Funktionen in Alarmkorrelation, Anomalie Erkennung und Threat Intelligence eingeführt. Brancheninitiativen wie Auto-ISAC liefern aktualisierte Best-Practice-Guides und SBOM-Orientierung, wodurch sich ein gemeinsames Vokabular und Erwartungsniveau über die Lieferkette herausbildet.

10.1 Handlungsbedarfe

VSOC-Reife mit KI professionalisieren: Vom punktuellen KI-Einsatz (z. B. Triage) zu durchgängigem, messbarem Nutzen über Detection, Investigation, Response und Evidence-Automation. Zielbild: erklärbare Modelle mit Human-in-the-Loop, belastbare Drift-Überwachung und versionsgeführte Nachweise für Audits.

Regulatorische Zukunftsfähigkeit sichern: EU-AI-Act (Hochrisiko-Systeme), NIS2 (Melde- und Risikomanagementpflichten) und CRA (lebenszyklusweite Produkt-Cybersecurity) erfordern belastbare Dokumentation, Transparenz und kontinuierliche Überwachung. KI wird hier Enabler — sofern Governance, Explainability und Logging konsistent nachweisbar sind.

SBOM-gestützte Kampagnenfähigkeit ausbauen: Kontinuierliche Schwachstellen-Korrelation (CVE - SBOM) auf VIN-Ebene heben, um Rückruf- und OTA-Kampagnen risikobasiert zu priorisieren und regulatorische Reportings zu speisen.

Lieferketten-Integration vertiefen: Einheitliche Datenverträge, TTP/IoC-Austausch und gemeinsame Testszenarien mit Tier-1/2-Zulieferern; VSOC-Sichten über Organisationsgrenzen heben, um End-to-End-Angriffsketten zu erkennen.

Betriebsresilienz & Kollaboration: Teilnahme an Branchenforen, gemeinsame Übungen, abgestimmte Incident-Playbooks (OEM–Zulieferer–Händler) und einheitliche Kennzahlen zur Wirksamkeit. Somit ist Training die beste Verteidigung in Friedenszeiten. Regelmäßige TTXs (Monitoring & Incident Response Table Top Exercises) stärken die Reaktionsfähigkeit der Security-Analysten im VSOC durch simulierte Angriffe und tragen somit zur Erhöhung der Resilienz sowie zur Verbesserung relevanter KPIs bei.

10.2 Zwischen Fortschritt und Nachholbedarf

Viele OEMs haben CSMS/SUMS formalisiert, VSOC-Grundelemente etabliert, First-Line-Triage durch KI beschleunigt und Richtlinien zur Dokumentation (Model Cards, Audit-Trails) eingeführt. Zudem verdichten sich Programme zur SBOM-Pflege, und es existiert breite Übereinkunft zu rollenbasierten Verantwortlichkeiten (Tier-Modelle, AI-Ops, Compliance). Diese Basis ermöglicht, dass KI nicht nur punktuell hilft, sondern in den Kernbetrieb überführt werden kann.

Datenvertrags-Tiefe & Telemetrie-Harmonisierung: Viele VSOCs leiden unter heterogener Fahrzeug- und Backend-Telemetrie, was KI-Wirksamkeit und Vergleichbarkeit zwischen Baureihen einschränkt. Fehlende, verbindliche Data Contracts verzögern Labeling, Training und Evidenzbildung. (Branchenbest-Practices adressieren dies, werden aber uneinheitlich umgesetzt.)

Evidence-Automation für Regulatorik: Für AI-Act-Konformität (Transparenz, Logging, Human Oversight) und NIS2-Reporting bestehen oft Insellösungen. Durchgängige, versionssichere Verknüpfungen zwischen Alarm, Modellentscheidung, menschlicher Freigabe und Maßnahmennachweis sind noch selten.

Adversarial-Test & Red-Team-Routinen: AML-spezifische Prüfungen (Data-Poisoning, Evasion) sind noch nicht flächendeckend in SOPs verankert; Bench- und HIL-basierte KI-Stresstests werden punktuell, aber nicht systematisch betrieben. (Summits betonen den Bedarf.)

Lieferketten-Durchgriff: SBOM-Vollständigkeit, Patch-SLAs und bidirektionales Incident-Sharing schwanken entlang der Kette; dadurch entstehen Lücken bei VIN-genauer Risiko-Priorisierung und Kampagnensteuerung. Eine weitere Lücke zeigt sich bei der SBOM-Versionierung – jede neue Softwareversion kann neue Schwachstellen einführen, wenn die Versionsbezüge nicht konsequent gepflegt werden.

Dealer- und After-Sales-Integration: Playbooks enden häufig am Werkstor; Rückmeldungen aus Werkstatt/Aftersales fließen nicht standardisiert in das Lernsystem, sodass wertvolle Labels und Kontext verloren gehen. (Mehrarbeit an End-to-End-Prozessen nötig.)

10.3 Ausblick – KI als Tragsäule des zukünftigen V-SOC

Im Jahr 2025 ist KI in der Cybersecurity **kein Zukunftsversprechen mehr, sondern ein unmittelbarer Handlungsbedarf.**

Angesichts der steigenden Komplexität vernetzter Fahrzeugarchitekturen und der regulatorischen Anforderungen wird KI zum entscheidenden Faktor, um Erkennung, Reaktion und Nachweisführung im Vehicle-SOC effizient zu steuern.

Die Entwicklung geht klar in Richtung **integrierter, datengetriebener Sicherheitsplattformen,** in denen KI nicht nur Muster erkennt, sondern die Verbindung zwischen Technik, Governance und Compliance bildet. Der Fokus verschiebt sich dabei von der reinen Modellleistung hin zu **nachvollziehbaren, kontrollierten und erklärbaren Prozessen, die den Menschen bewusst im Entscheidungszyklus halten.**

OEMs stehen vor der Aufgabe, KI von punktuellen Projekten **in den operativen SOC-Kern zu überführen** – mit standardisierten Datenflüssen, konsistenten Governance-Regeln und kontinuierlicher Qualifizierung der Teams. Nur so lässt sich die Balance zwischen Automatisierung und Verantwortung sichern.

Damit wird KI in den kommenden Jahren zur **tragenden Säule einer resilienten Cyberabwehr**: Sie verknüpft Bedrohungserkennung, Risikoanalyse und regulatorische Nachweisfähigkeit zu einem geschlossenen Regelkreis – und markiert den Übergang vom reaktiven Schutz zur proaktiven, lernfähigen Sicherheit im vernetzten Fahrzeug.

Ihre Ansprechpartner

Christian Trompler

Senior Consultant
Cyber Security

T: +49 1511 9569 075
@: Christian.Trompler@p3-group.com
Christan Trompler

Andreas Sitar

Senior Consultant
Cyber Security

T: +40 749 022 667
@: andreas.sitar@p3-group.com
Andreas Sitar

KONTAKT

P3 group GmbH
Heilbronner Straße 86
70191 Stuttgart
Germany

+49 711 252 749-0
mail@p3-group.com
www.p3-group.com