magility
cyber security

Vorstellung Unternehmen und Beratungsansatz

Magility Cyber Security GmbH

Dino Munk,
Geschäftsführender Gesellschafter

Inhalte

Kurzprofil Magility Cyber Security (MCS)

Geschäftszweck der Magility Cyber Security GmbH (MCS)

Wer wir sind und was wir anstreben

- Die MCS ist eine Ausgründung der Magility GmbH, einer High-Tech Beratungsgesellschaft mit Schwerpunkt Strategie, Geschäftsmodellentwicklung und Management Consulting.
- Die MCS implementiert ganzheitliche und regelkonforme Cyber Security Management Systeme (CSMS) und Software Update Management Systeme (SUMS) entlang der Supply Chain.
- Aktuell kommen unsere Kunden aus der Automobilbranche und dem Fahrzeugbau, vom Mittelstand bis zum OEM aus dem deutschen und europäischen Markt.
- Durch das langjährig aufgebaute Eco-System unserer Gesellschafter und unsere erfahrenen Cyber Security Experten sind wir bestens aufgestellt.
- Wir sind eng vernetzt und arbeiten vertrauensvoll zusammen mit führenden Cyber Security Anbietern z.B. aus dem Cyber Hub Israel.
- Wir sind auch in anderen Branchen wie High-Tech, Maschinenbau, Luftfahrt/Transportation tätig und setzen die Standards branchen- und kundenspezifisch praxisorientiert um.
- Wir arbeiten immer am Puls der Zeit und passen unser Angebot in Echtzeit an neue Regularien und Best Practices industriespezifisch an.

Die Gesellschafter der Magility Cyber Security

„Wir glauben an die Zukunftsfähigkeit unseres Beratungsansatzes und engagieren uns persönlich, finanziell und mit langjähriger Expertise.“

Dino Munk

Geschäftsführender Gesellschafter

vormals Business Unit Director bei Staufen.AG Beratung und Beteiligung

Dr. Michael W. Müller

Gesellschafter

Geschäftsführender Gesellschafter Magility GmbH, vormals Geschäftsführer MBtech Consulting

Stefan E. Buchner

Gesellschafter

Aufsichtsrat in diversen Unternehmen wie Continental AG und thyssenkrupp AG, vormals Vorstand Daimler Trucks,

Ralf Stokar von Neuforn

Gesellschafter

Gründer Staufen.AG und zahlreicher Startups, erfolgreiche Umsetzung diverser Unternehmensnachfolgen

Typische Cyber Security Herausforderungen

Grundsätzlich muss Cyber Security auf unterschiedlichen Ebenen verankert werden

Klassische IT

z.B. Cloud, Server, Netzwerke, PCs, Laptops, mobile Geräte, Software

Infrastruktur

z.B. Gebäude, IIOT, OT, Datenbusse, Anlagen, Maschinen, Industrie 4.0, Smart Cities, Software

Produkte & Services

z.B. IoT-Produkte, End-to-End Solutions, V2X, Fahrzeugflotten, Services, Software

Durch die moderne Konnektivität wird

End-to-End Sicherheit

zum kritischen Erfolgsfaktor für Unternehmen

Für Automotive: End-to-End Security entlang des Lebenszyklus und der Value Chain

Flottenmanagement und OTA Software Updates werden zum kritischen Erfolgsfaktor

HW und SW Wertschöpfungskette

OEM - Tier 1 - Tier 2 - Tier n

Produktlebenszyklus

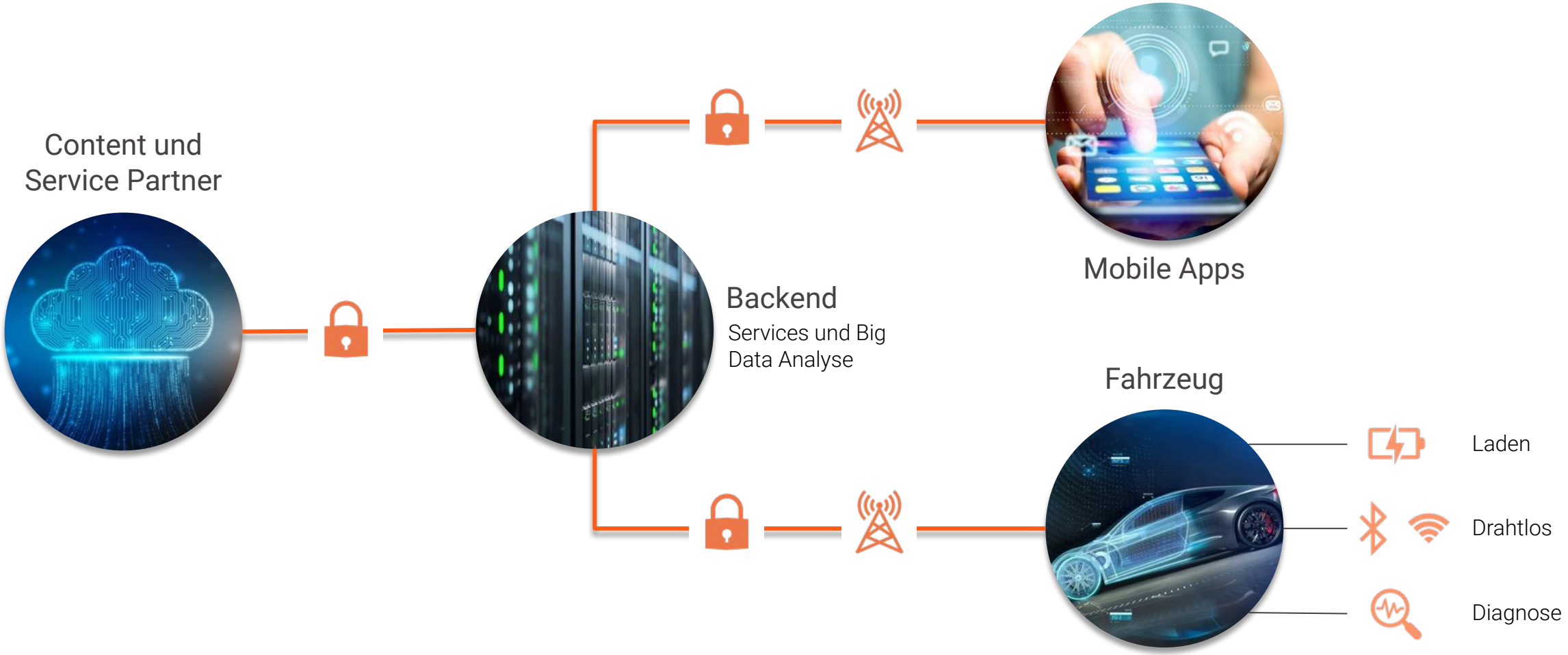
F&E, Produktion, Sales, Aftersales, Entsorgung

End-to-End Gesamtsystem

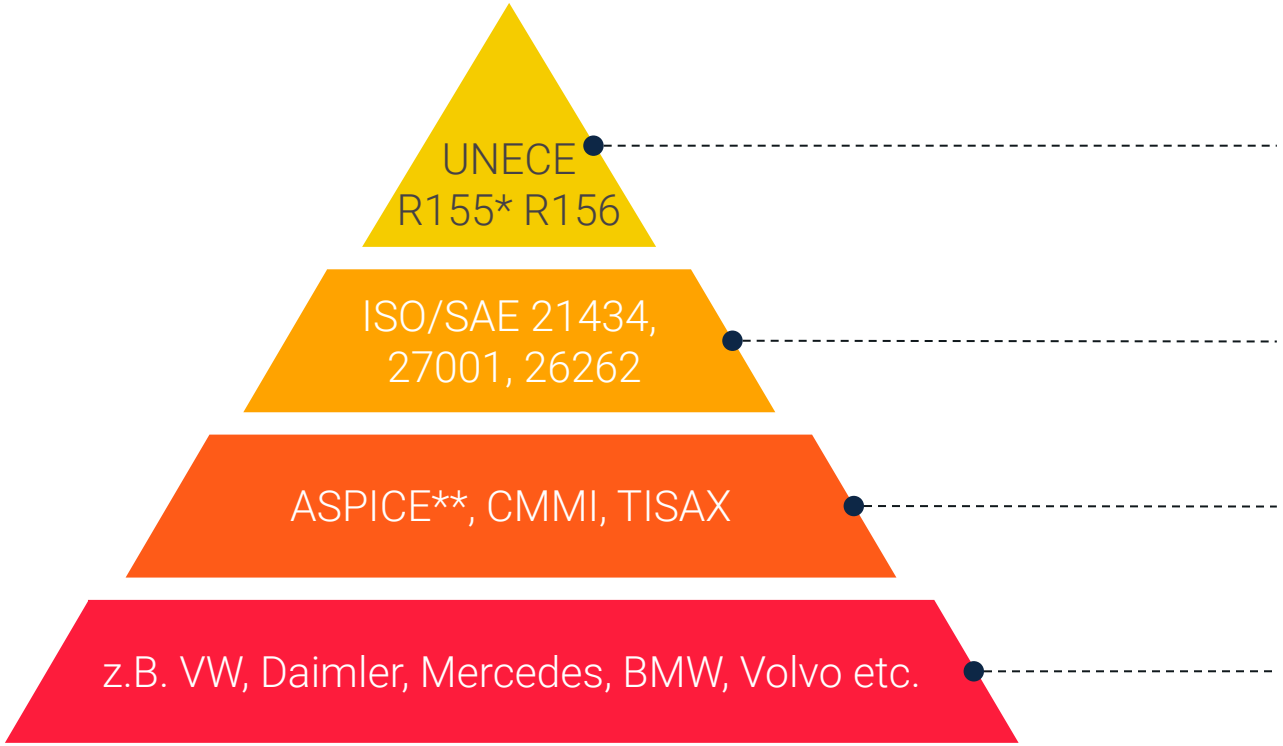
Fahrzeug, Backend, Cloud Services, mobile Applikationen

Auch das vernetzte Gesamtfahrzeugsystem setzt End-to-End Security voraus

Nicht nur das Fahrzeug, sondern auch sämtliche Verbindungen nach außen und innen müssen geschützt sein



Die von der UNECE gesetzlich festgelegten Regularien für Automotive CSMS werden durch mitgeltende Normen und übergreifende sowie firmeninterne Richtlinien umgesetzt



Gesetze (z.B. weltweit, EU-weit, staatsweit)

Normen (z.B. USA, EU, etc.)

Richtlinien/Assessments
(z.B. von Verbänden (VDA), etc.)

Firmeninterne Richtlinien

* UNECE R155 „UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (CSMS)“
** ASPICE: Automotive Software Process Improvement and Capability Determination

Die UNECE-WP.29* stellt Anforderungen an die OEM aus der Automobilindustrie

OEM müssen ihre Organisation und Prozesse anpassen

Cyber Security (ISO/SAE 21434, UN R155)

Cyber Security Management System (CSMS)

Externe Zertifizierung gültig für drei Jahre

- Risikomanagement in Prozessen ist implementiert
- Prozesse für Risikohandling sind etabliert

Fahrzeuganforderungen

Typprüfung

- Nachweis über Fahrzeugsicherheit und Cyber Security über den gesamten Produktlebenszyklus

Software Updates (ISO/SAE 24089, UN R156)

Software Update Management System (SUMS)

Externe Zertifizierung gültig für drei Jahre

- SW Update Management Prozesse sind etabliert
- Security und OTA-Anforderungen sind abgesichert

Fahrzeuganforderungen

Typprüfung

- Compliance mit Anforderungen SW Updates und OTA Updates über den gesamten Lebenszyklus

UNECE

UNECE-WP.29 ("World Forum for Harmonization of Vehicle Regulations")
Working Group GRVA ("Working Party on Automated/Autonomous and Connected Vehicles")

*WP.29 Arbeitsgruppe der UNECE, **Weltforum für die Harmonisierung von Fahrzeugvorschriften**

Fokus auf Organisation und Prozessen

Fokus auf Fahrzeug und End-to-End Technologien

magility cyber security

WP.29* – Compliance für Automotive Cyber Security Management Systeme

Inhalte der gesamten Dokumentation für CSMS nach UNR 144 Annex 1 / Appendix 1, Annex 4

VEHICLE CYBERSECURITY MANAGEMENT

Nachweis, wie die Prozesse im Zusammenhang mit dem Cyber Security Management einem ständigem Aktuallisierungspro-zesses unterliegen und somit immer up to date sind

SUPPLY CHAIN CYBER-RISK

Nachweis eines angemessenen Ansatzes für das Risikomanagement im Zusammenhang mit Lieferanten, Dienstleistern oder anderen Dritten

RISK MANAGEMENT PROCESSES

Nachweis, wie Cyber-Risiken von der Identifizierung bis zur Kategorisierung, Bewertung und Behandlung gehandhabt werden,

CYBERSECURITY TESTING PROCESSES

Nachweis, wie die Cyber Security von der Entwicklung über die Produktionsphasen überprüft und validiert wird

CYBERSECURITY MONITORING & RESPONSE

Nachweis der Cyber Security Werkzeuge, Prozesse und Technologien zur Überwachung, Erkennung und Reaktion auf Cyber-Bedrohungen, Schwachstellen und Angriffe

OTHER CUSTOM PROCESSES

Demonstration von Prozessen, die für spezielle Anwendungsfälle geeignet sind

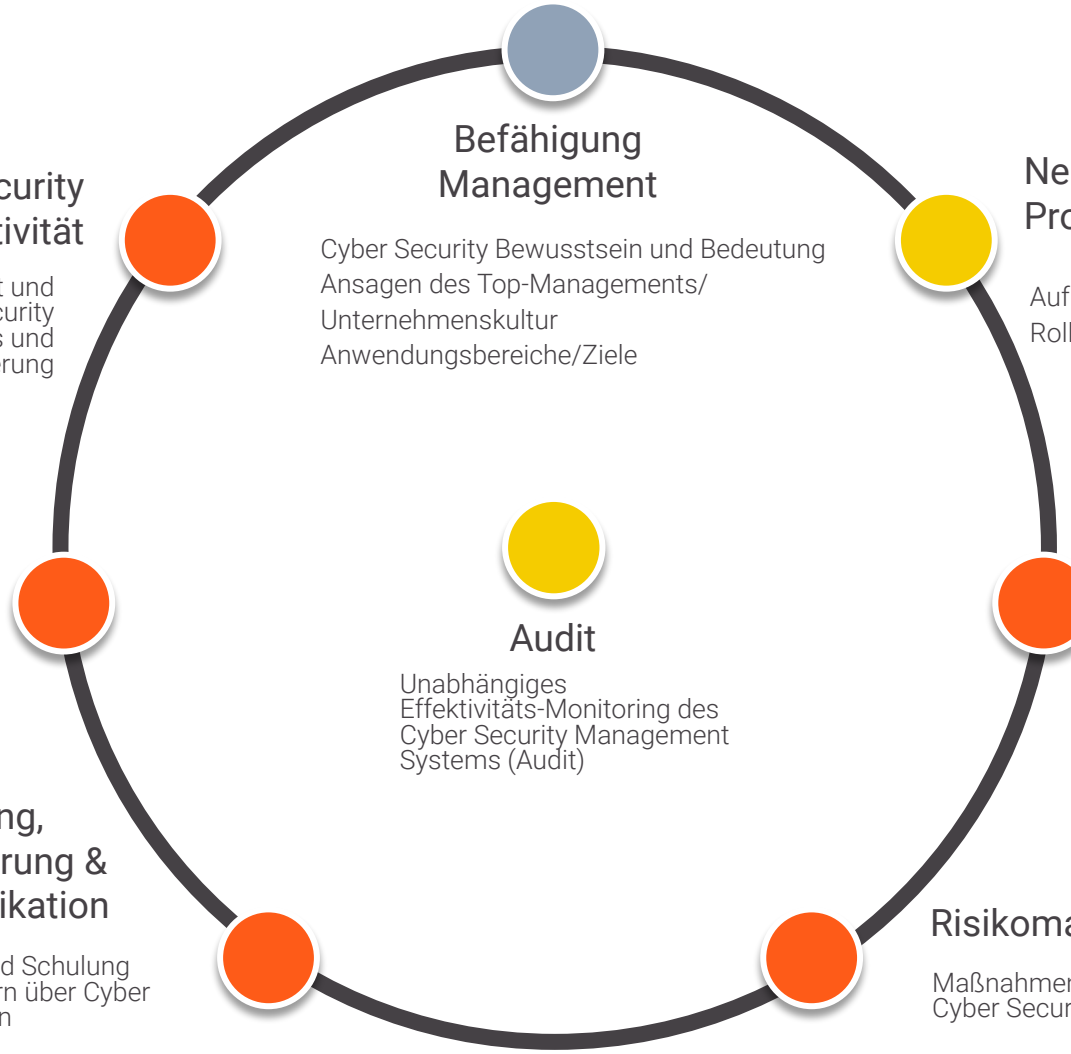
*WP.29 Arbeitsgruppe der UNECE, **Weltforum für die Harmonisierung von Fahrzeugvorschriften**

magility cyber security

MCS Beratungsansatz

CSMS – Cyber Security Management System

Unser Ansatz integriert Cyber Sicherheit ganzheitlich und nachhaltig in die Organisation



Befähigung Management

Cyber Security Bewusstsein und Bedeutung
Ansagen des Top-Managements/ Unternehmenskultur
Anwendungsbereiche/Ziele

Neugestaltung Organisation & Prozesse

Aufbau der Organisationsstruktur
Rollen, Verantwortlichkeiten und Prozesse

Risikoidentifikation

Systematischer und ganzheitlicher Ansatz zur Identifizierung und Bewertung von Cyber Security Risiken

Risikomamagement

Maßnahmen zur Minderung der Cyber Security Risiken

Befähigung, Qualifizierung & Kommunikation

Information und Schulung von Mitarbeitern über Cyber Security Risiken

Cyber Security Transformation

Implementierung von Cyber Security Maßnahmen

Monitoring Cyber Security Effektivität

Monitoring der Effektivität und Effizienz des Cyber Security Management Systems und kontinuierliche Verbesserung

Audit

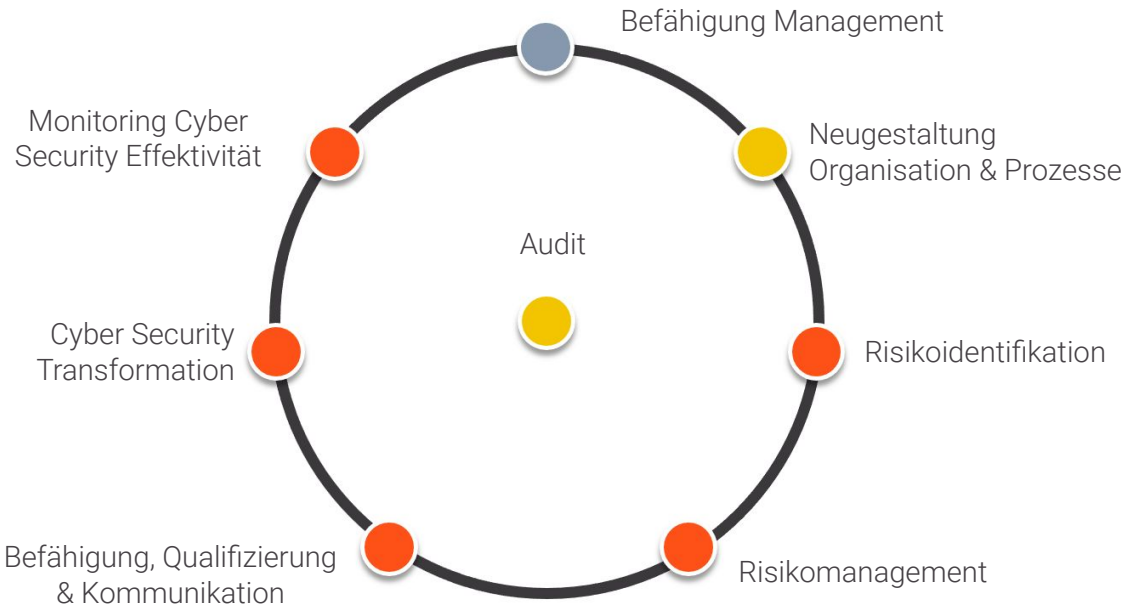
Unabhängiges Effektivitäts-Monitoring des Cyber Security Management Systems (Audit)

- CSMS Zielvorgaben des Managements
- Organisations-Setup
- Cyber Security Framework

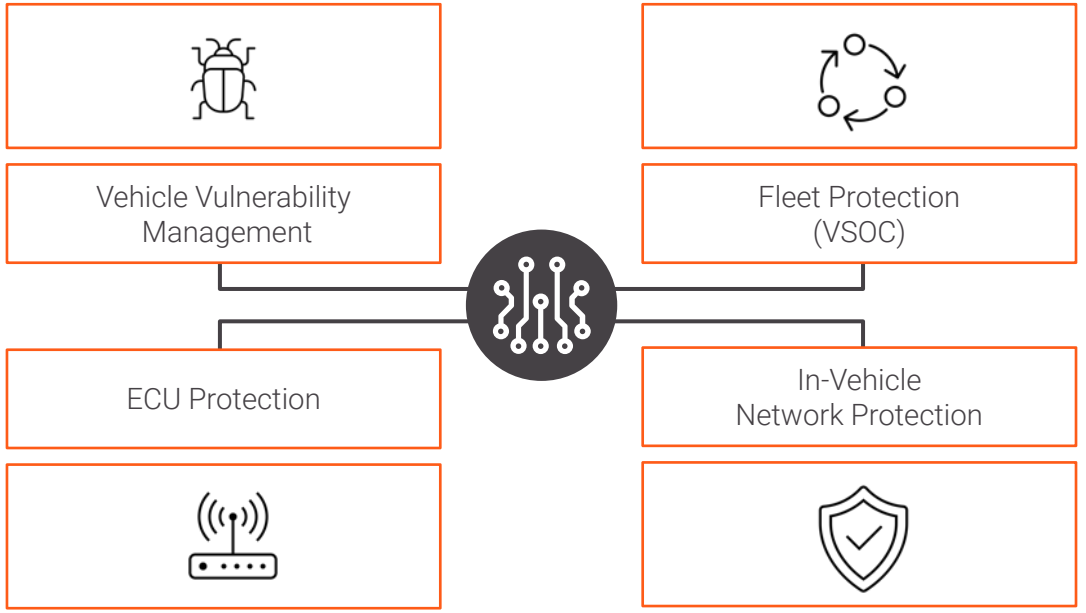
Das magility Ecosystem ermöglicht eine CSMS-Implementierung als One-Stop-Shop

Ganzheitlich gedachter Technologie Footprint über gesamte Wertschöpfungskette und End-to-End

Cyber Security Prozess-Footprint – Kernkompetenz MCS



Cyber Security Technologie-Footprint– Kernkompetenz Ecosystem



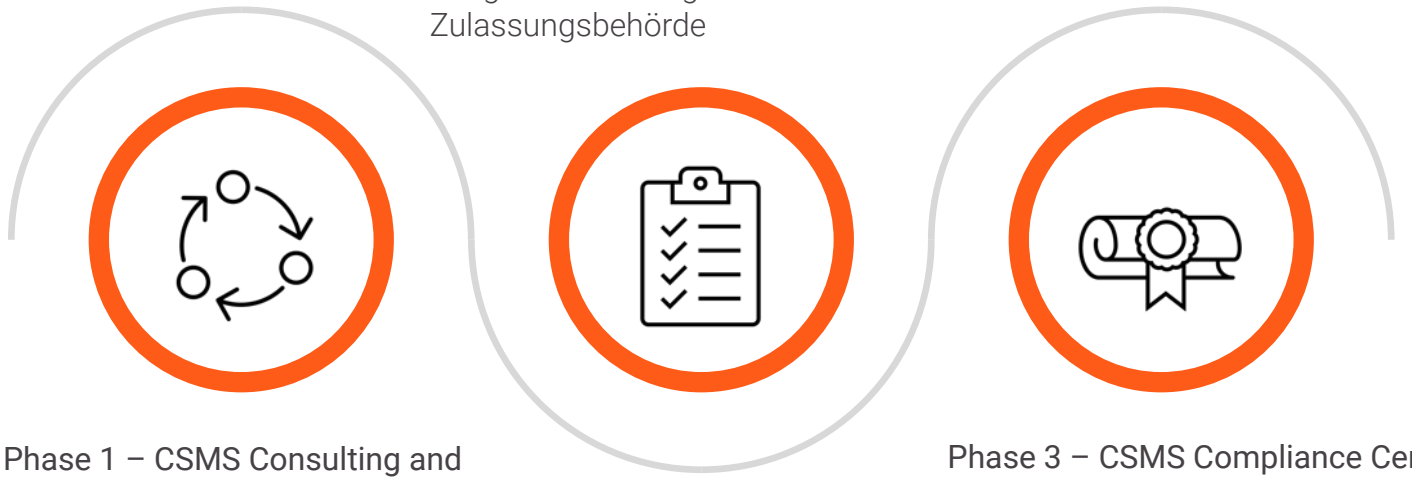
Unsere Referenzen – eine Auswahl

Der Zertifizierungsprozess für OEM für eine CSMS Konformitätsprüfung

OEM müssen die Konformität jederzeit bei einer zertifizierten Behörde oder einem Dienst nachweisen können

Phase 2 – CSMS Evaluation and Review

- durch technischen Dienst und Bewertung anhand des Reifegrades im Bezug auf nötige Anforderungen durch Zulassungsbehörde



Phase 1 – CSMS Consulting and Implementation

- Sicherstellung von Cyber Security im gesamten Lebenszyklus und der Wertschöpfungskette
- Prozesse für Risikobewertung, Testing, Monitoring und Reaktion
- OEM wird unterstützt von MCS

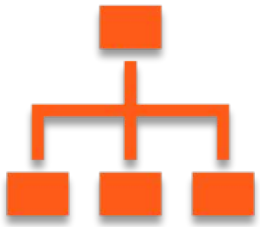
Phase 3 – CSMS Compliance Certificate

- Wird für zukünftige Zulassung für Typprüfung benötigt
- Staatliche Behörde kann Validität jederzeit prüfen, neu vergeben oder entziehen
- Staatliche Behörde: KBA (Federal Motor Transport Authority)

Die MCS unterstützt bei der Implementierung eines CSMS

Phasenmodell-Ansatz für einen nachhaltigen Projektfortschritt

1. Schaffung eines **Verständnisses** für WP.29 und **Bewertung der Anforderungen**



2. Ableiten der entsprechenden **organisationalen Auswirkungen**

3. Aufsetzen eines **Maßnahmenplans**, angepasst an den **Reifegrad der Organisation**

4. Interner **Check-Audit** und nachfolgende **Implementierung der Maßnahmen**

Der MCS Beratungsansatz ist kundenspezifisch skalierbar

Detaillierte und nachhaltige Unterstützung in allen oder auch nur einzelnen Phasen

1 IST-ANALYSE

- Durchführung der detaillierten CSMS Ist-Analyse des Unternehmens
- Bestandsaufnahme für weitere Strategiedefinition

2 KONZEPT/ BUSINESS MODEL

- Weiterentwicklung des CSMS durch Festlegung der Ziele
- Ableitung der Strategie in den Bereichen: Produkte, Services, Prozesse, Kompetenzen

3 UMSETZUNG/ TRANSFORMATION

- Begleitung des CSMS Umsetzungs- und Transformationsprozesses
- Einbindung aller Beteiligten zur zielgerichteten und ganzheitlichen Implementierung

Kontakt

Ihr Kontakt zu magility cyber security

Magility Cyber Security GmbH | Heinrich-Otto-Str. 71 |
73240 Wendlingen am Neckar | Deutschland

+49 177 698 2021 | contact@magility-mcs.com | www.magility-mcs.com

magility

together. cyber. secure.

Disclaimer

Magility Cyber Security GmbH

Haftung für Inhalte

Als Diensteanbieter sind wir gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG sind wir als Diensteanbieter jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Bei der Ausarbeitung dieser Präsentation wurde größtmögliche Sorgfalt angewandt, dennoch können wir keine Gewähr für die Vollständigkeit, Aktualität oder Richtigkeit der darin enthaltenen Informationen übernehmen. Die Angaben in dieser Dokumentation dienen lediglich Informationszwecken und sind weder als Angebot, noch als öffentliche Werbung, die zur Inanspruchnahme von Dienstleistungen auffordert, aufzufassen.
Die Haftung für sämtliche Schäden oder Verluste, welche auf der Grundlage der in dieser Dokumentation enthaltenen Informationen geltend gemacht werden, ist ausgeschlossen.

Haftung für Links

Falls Links zu externen Websites in unserer Präsentation vorhanden sind, haben wir auf deren Inhalte keinen Einfluss. Wir übernehmen für fremde Inhalte keine Gewähr. Die Verantwortung für die Inhalte von verlinkten Seiten liegt stets beim jeweiligen Anbieter und Betreiber der Seiten. Die ständige inhaltliche Kontrolle der verlinkten Seiten ist nicht zumutbar, solange keine konkreten Anhaltspunkte für eine Rechtsverletzung vorliegen. Werden solche bekannt, so werden wir derartige Links unverzüglich entfernen.

Urheberrecht

Die durch die Magility Cyber Security GmbH erstellten Inhalte und Werke auf diesen Seiten unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Downloads und Kopien dieser Seite sind nur für den privaten, nicht kommerziellen Gebrauch gestattet.

Soweit Inhalte dieser Seite nicht vom Betreiber erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir sie um einen entsprechenden Hinweis. Bei bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

Ohne vorherige ausdrückliche schriftliche Genehmigung von der Magility Cyber Security GmbH, darf kein Teil des Inhaltes dieses Dokumentes für andere Zwecke verwendet, an Personen oder Unternehmen außerhalb der empfangenden Gesellschaft verteilt oder auf irgendeine andere Weise vervielfältigt, bearbeitet oder verbreitet werden. Die in der Präsentation erhaltenen Texte und Grafiken dienen nur zum Zweck der Veranschaulichung und Referenz.

Managing Director: Dino Munk | Magility Cyber Security GmbH | European Metropolitan Region Stuttgart
Heinrich-Otto-Str. 71 | 73240 Wendlingen am Neckar | Germany
E-Mail: dino.munk@magility-mcs.com | Tel. +49 177 698 2021
Stuttgart | HRB-Nummer 78 4630
www.magility-mcs.com