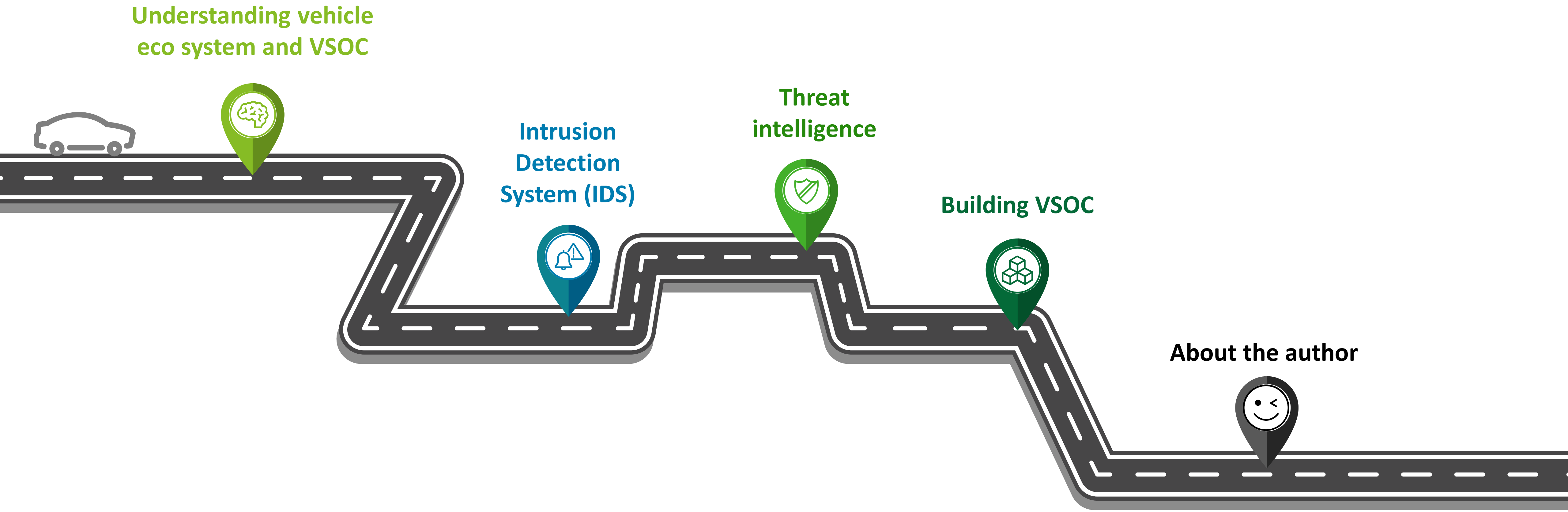
Deloitte.

Building VSOC in a connected ECO system of IDS and threat intelligence

SIP-adus Cybersecurity, 10th Nov 2021

MAKING AN IMPACT THAT MATTERS since 1845

Content journey



Understanding vehicle eco system and VSOC

Intrusion Detection System (IDS)

Threat intelligence

Building VSOC

About the author

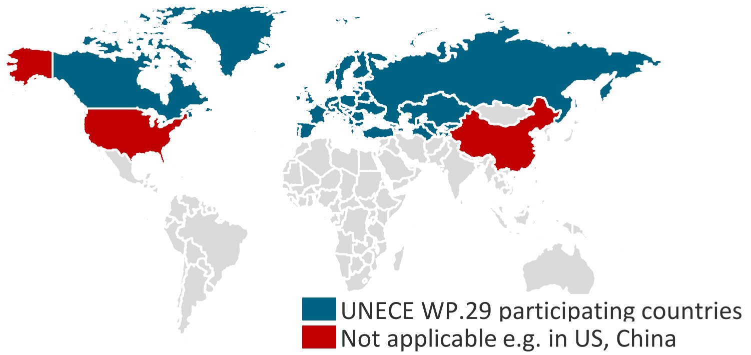
Understanding vehicle eco-system and VSOC

Challenges in fulfilling regulatory requirements

UN R155 requires vehicle cybersecurity monitoring

Vehicle data logs shall be analyzed to ensure timely and efficient incident response

- UNECE regulation for Cyber Security Management System (CSMS) mandates cyber security assurance as a prerequisite for type approval
- These requirements are set by the Working Party on Automated / Autonomous and Connected Vehicles” (GRVA) and include:
  - Requirements for a Cyber Security Management System (CSMS)
  - Type Approval Requirements (based on CSMS)


🟦 UNECE WP.29 participating countries
🟥 Not applicable e.g. in US, China

Development | Production | Post-Production

Threat detection

7.2.2.4.(b) *“…Include the capability to analyze and detect cyber threats, vulnerabilities and* ***cyber-attacks from vehicle data and vehicle logs****….”*

7.3.7. *The vehicle manufacturer shall implement measures for the vehicle type to:*
(a) ***Detect and prevent cyber-attacks against vehicles*** *of the vehicle type;*
(b) Support the monitoring capability of the vehicle manufacturer with regards to ***detecting threats****, vulnerabilities and cyber-attacks relevant to the vehicle type;*

Annex 5

- ***M13*** *Measures to detect and recover from a denial of service attack shall be employed*
- ***M15*** *Measures to detect malicious internal messages or activity should be considered*

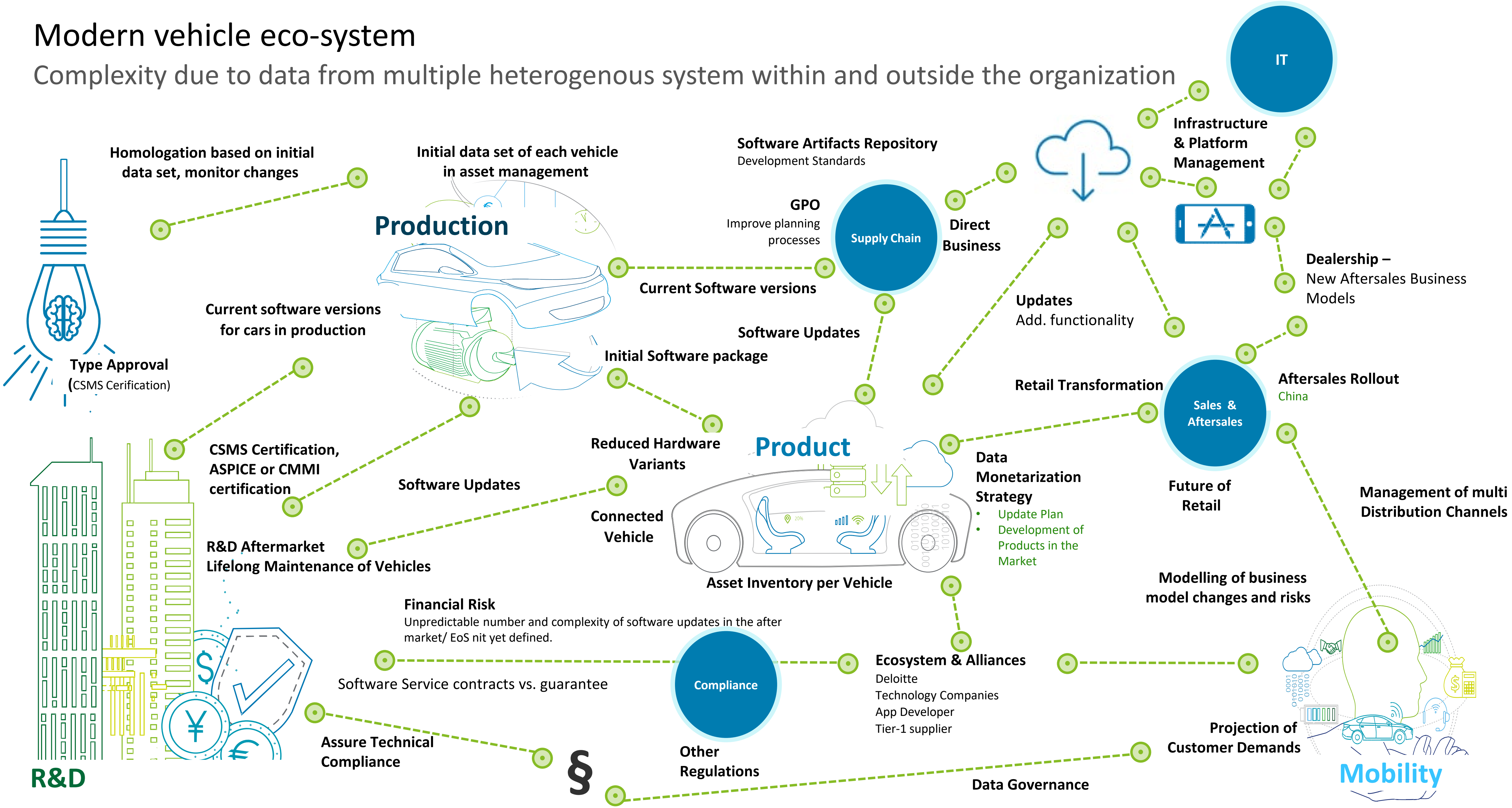
Expected Outcome

Detection mechanism

Threat intelligence

Modern vehicle eco-system

Complexity due to data from multiple heterogenous system within and outside the organization



IT

Infrastructure & Platform Management

Homologation based on initial data set, monitor changes

Initial data set of each vehicle in asset management

Software Artifacts Repository
Development Standards

Production

GPO
Improve planning processes

Supply Chain

Direct Business

Dealership –
New Aftersales Business Models

Current Software versions

Current software versions for cars in production

Updates
Add. functionality

Software Updates

Initial Software package

Type Approval
(CSMS Cerification)

Retail Transformation

Sales & Aftersales

Aftersales Rollout
China

Reduced Hardware Variants

Product

CSMS Certification, ASPICE or CMMI certification

Software Updates

Data Monetarization Strategy
- Update Plan
- Development of Products in the Market

Future of Retail

Management of multi Distribution Channels

Connected Vehicle

R&D Aftermarket
Lifelong Maintenance of Vehicles

Asset Inventory per Vehicle

Modelling of business model changes and risks

Financial Risk
Unpredictable number and complexity of software updates in the after market/ EoS nit yet defined.

Software Service contracts vs. guarantee

Compliance

Ecosystem & Alliances
Deloitte
Technology Companies
App Developer
Tier-1 supplier

Assure Technical Compliance

Other Regulations

Projection of Customer Demands

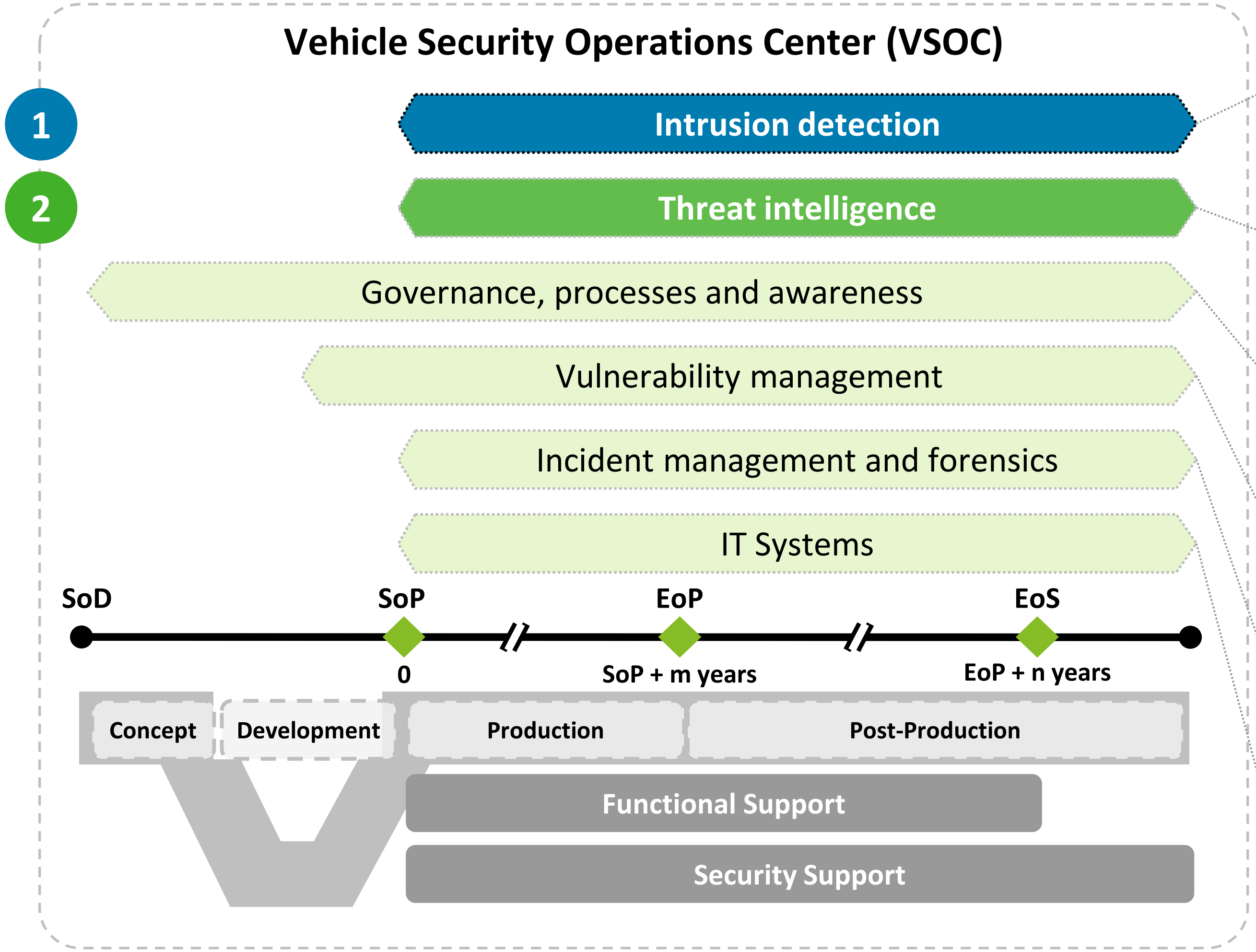
Data Governance

R&D

Mobility

Focus on critical elements while building a VSOC

Processes and technical interfaces are critical part of it



Vehicle Security Operations Center (VSOC)

1 Intrusion detection

2 Threat intelligence

Governance, processes and awareness

Vulnerability management

Incident management and forensics

IT Systems

IDS (Intrusion Detection System)

- Network/ host based
- Rules for use cases
- Machine learning
- Artificial intelligence

Threat Intelligence

- List of input sources and access
- Data model/ Correlation methods
- Attack vector and tree
- Report generation

Governance, Processes and Awareness

- Governance model
- End-to-end process definition
- Roles and Responsibilities
- Regional challenges and guidelines

Vulnerability Management

- Risk assessment
- Penetration tests
- Definition of digital twin
- Complementary services (3rd party)

Incidence Response

- Incident response plan
- Impact analysis and strategies
- Prioritization matrix
- Workflow management

IT Systems

- Backend
- Workshops
- Dealer management
- Production

1

Intrusion Detection System (IDS)

Detailed content is available on SIP-adus 2020 download area

https://en.sip-adus.go.jp/evt/workshop2020/file/cs/10CS_02_Khadria.pdf

Types of IDS

Network, host based or “hybrid”

Intrusions may come from **internal**, which reside inside the targeted system components having legal access privilege to the network.

External intruders come from the outside of the targeted network, attempting to gain illegitimate access to the system components

The detection methods can be classified as

- Anomaly type: Detect unexpected behavior
- Signature type: Detect from history
- Specification type: Detect out of rules

Network based (inter ECU)

- Ethernet
- CAN/ CAN FD
- LIN/ FlexRay

Hybrid IDS

- Detects ECU as well as network anomalies
- Spread across vehicle EE architecture

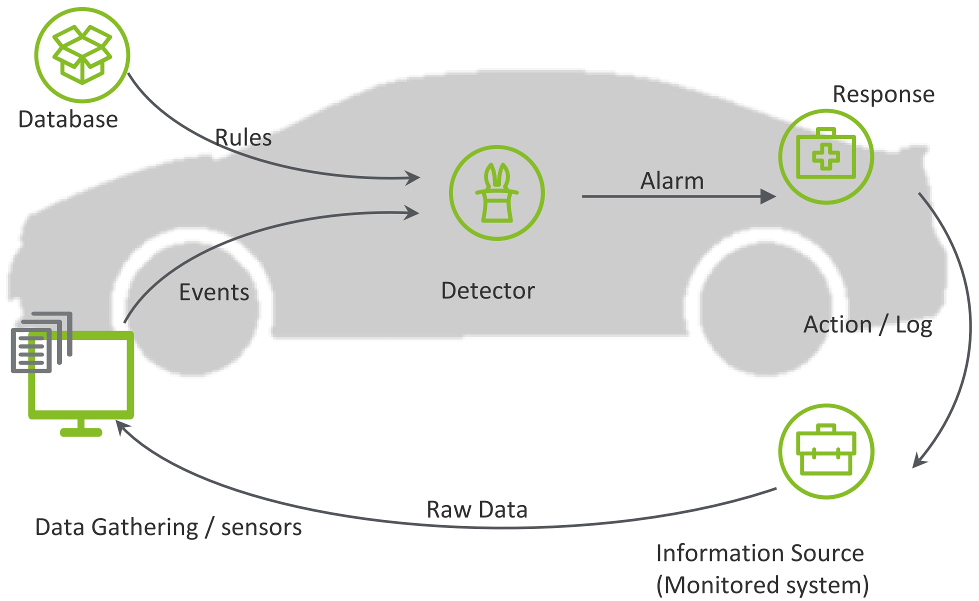
Host based (intra ECU)

- Control Flow
- CPU Runtime
- Memory Consumption
- ECU-internal communication

IDS design considerations

A more robust and stringent system prevents „false positives“ transferred to VSOC

Basic IDS architecture within a vehicle



Data Gathering: Used for monitoring the source environment. The data gathering is performed using different sensors that observe specific application(s) and/ or protocol(s). A pre-processing module can also be included, that performs basic classification of the data type received from the source.

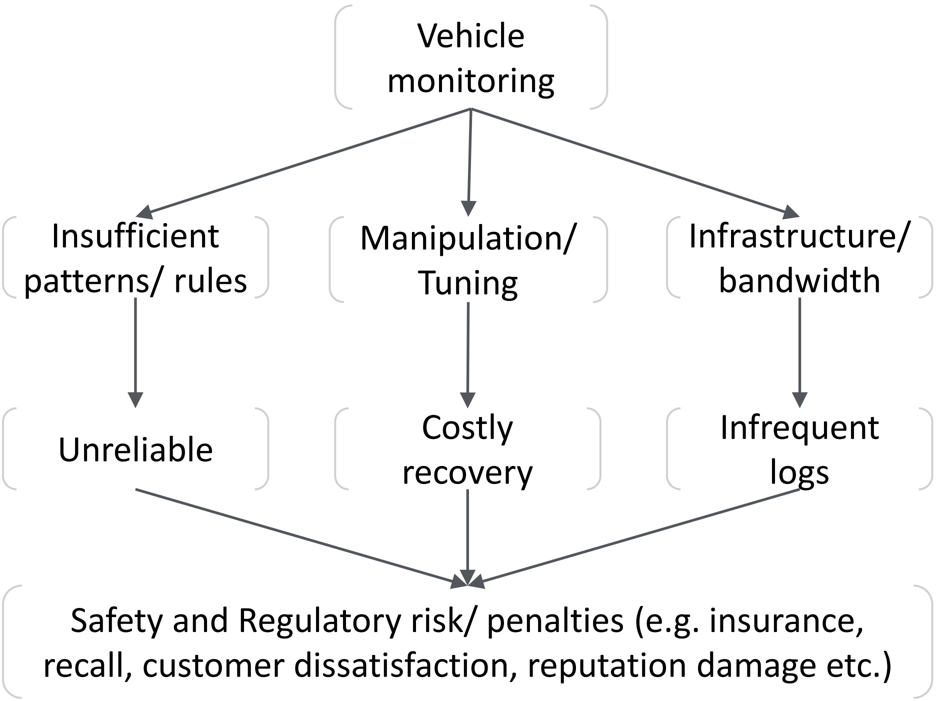
Detector: is a module that performs the comparison between the gathered data and the defined rules set and raises alarms in case a deviation is found.

Database: is a storage module that contains the rule-sets or the IDs which the detector uses when comparing the received data.

Output / Response: When an alarm is raised a proper action is taken. This could be an active response where the IDS performs a predefined action such as drop the packet, or an inactive response such as logging for later inspection by a human factor to determine the appropriate response.

Using AI and machine learning in IDA

Bias: detection false positives may lead to inefficiency and true negatives may lead to safety risks to road users



Vehicle monitoring

Insufficient patterns/ rules

Manipulation/ Tuning

Infrastructure/ bandwidth

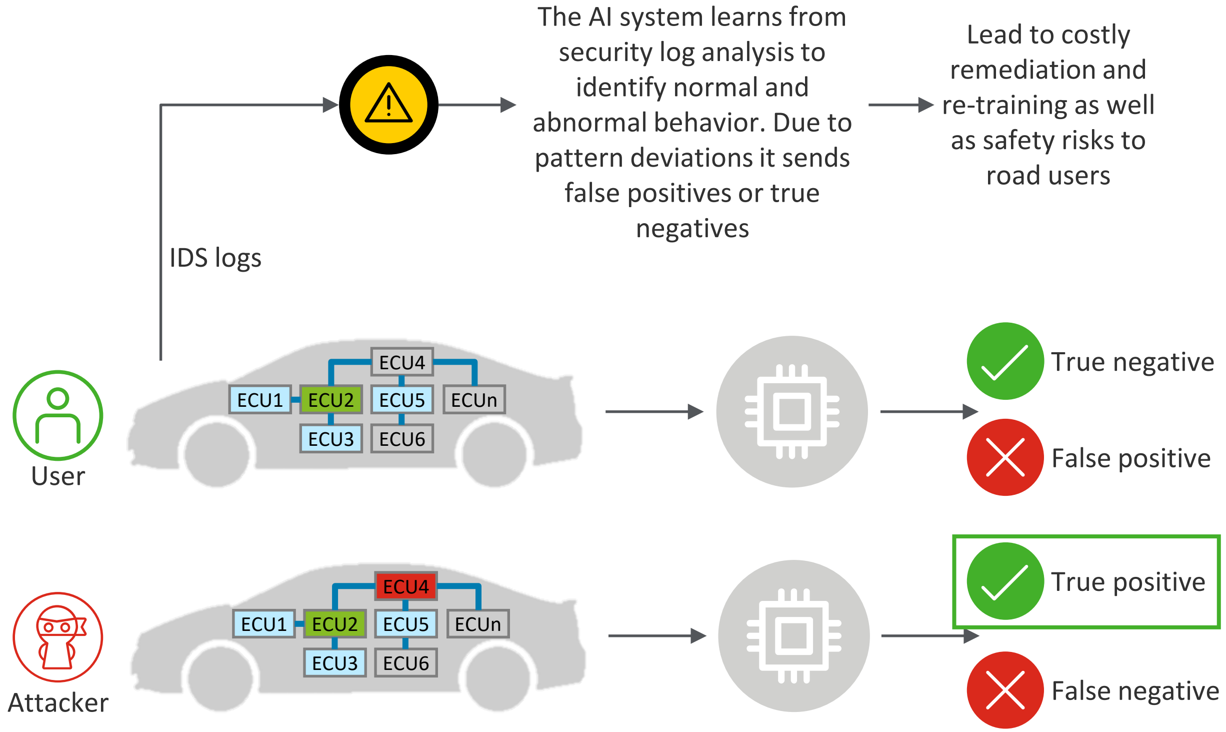
Unreliable

Costly recovery

Infrequent logs

Safety and Regulatory risk/ penalties (e.g. insurance, recall, customer dissatisfaction, reputation damage etc.)

Case	Attack	Detected	Impact	Desired
False negative	Yes	No	Safety/ financial losses	No
False positive	No	Yes	Unnecessary cost of analyzing data	No
True positive	Yes	Yes	An attack is detected and responded	Yes
True negative	No	No	No impact	Yes



The AI system learns from security log analysis to identify normal and abnormal behavior. Due to pattern deviations it sends false positives or true negatives

Lead to costly remediation and re-training as well as safety risks to road users

Based on historic data and rules, AI system decides whether or not an activity can be flagged as abnormal

Introduction of new service/ feature can lead to undesired behavior – an attack is missed (true negative) OR an expected behavior is flagged as ATTACK (false positive)

2

Threat intelligence

Threat intelligence methodology

Foundation elements should be highlighted to service flexibility and possibility to adapt given approach

THREAT DETECTION

Intelligence Network Through global network based on collaboration with other OT/IoT laboratories and automotive customers globally.

Lab Obtaining feeds related to automotive and IoT environments in our OT/IoT Lab

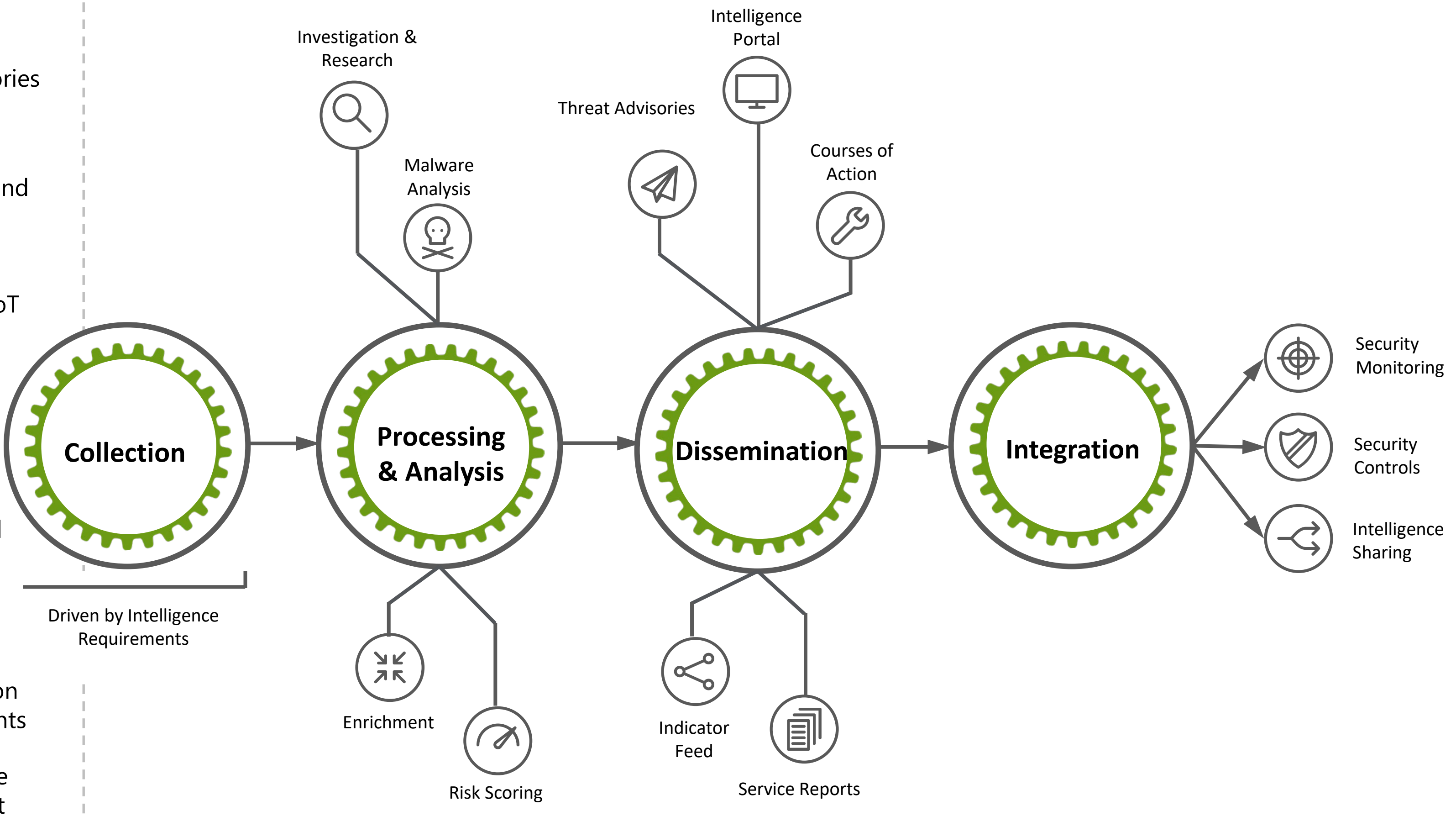
Honeynet A specific Honeypot designed for OT / IoT environments is created

Crawlers Detection of new automotive threat sources and Intelligence tools to retrieve information from social media

Other monitoring services Expanded search for sources, trends and indicators specific to the automotive environment through synergies with ot monitoring equipment

Manual investigation Malware analysis and manual search fc threats in the deep/dark web, focusing on those that affect automotive environments

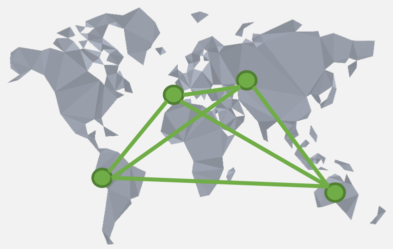
Specialized feeds 3rd party alliance in the cyber automotive industry to leverage an exhaustive threat landscape



Typical threat intelligence capabilities

A global network of analysts, collaboration with alliance partners and rich data base

Analyst network and languages



German, English, Spanish, Russian, Chinese, Arabic, French, Italian, Portuguese, Persian, Japanese

Search capabilities

- ✓ Search relevant information
- ✓ Actors tracking
- ✓ Interaction with actors

- Forums & Markets
- Dark web sites
- Telegram channels
- IRC channels

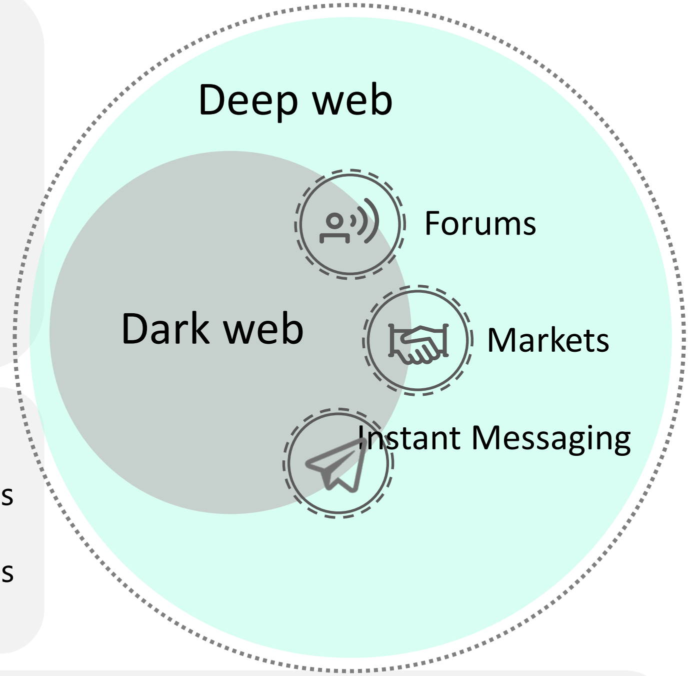
Target

Malware attacks
- ✓ Profiles tracking
- ✓ Interaction with actors
- ✓ Botnets credentials

Sensitive data
- ✓ Files
- ✓ Credentials
- ✓ Credit cards
- ✓ Emails

Attack vectors
- ✓ Malware kits
- ✓ Phishing kits
- ✓ Carding
- ✓ Scamming
- ✓ Exploits
- ✓ Vulnerabilities
- ✓ SIM cards

Compromised Systems
- ✓ BPC Panels
- ✓ SMTP solutions
- ✓ SSL Connections
- ✓ VPN Solutions
- ✓ VPS solutions
- ✓ RDP Connections
- ✓ https Shell

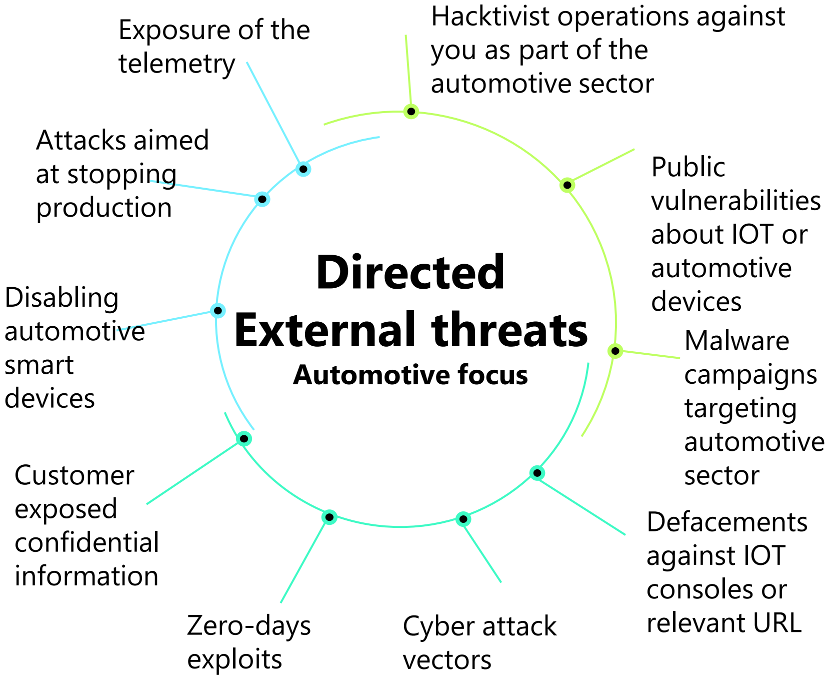


Client specific Intelligence

Control your brand and your assets

24/7 CRITICAL ALERTS | MONTHLY REPORTS

24/7 Client-specific cyber reconnaissance to search for evidence of malicious cyber activity directed against the client, with a focused lens on client-specific **automotive threats and exposures.**



Directed External threats

Automotive focus

Exposure of the telemetry

Hacktivist operations against you as part of the automotive sector

Attacks aimed at stopping production

Public vulnerabilities about IOT or automotive devices

Disabling automotive smart devices

Malware campaigns targeting automotive sector

Customer exposed confidential information

Defacements against IOT consoles or relevant URL

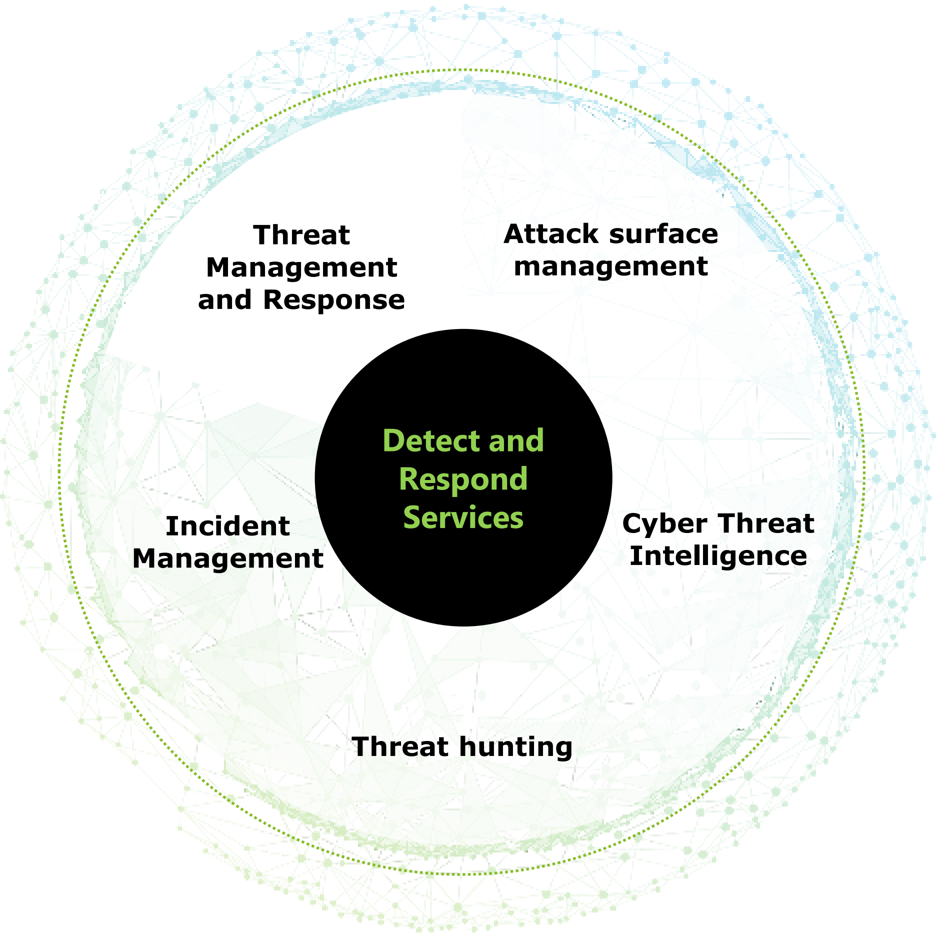
Zero-days exploits

Cyber attack vectors

Tool landscape

Wide variety of tools can be deployed based on organizational requirements and existing infrastructure

- splunk
- ArcSight
- IBM QRadar
- exabeam
- SECURONIX
- Resilient an IBM Company
- servicenow
- CORTEX XSOAR BY PALO ALTO NETWORKS
- splunk phantom
- Carbon Black.
- PRISMA CLOUD
- cybereason malops protection
- DARKTRACE
- NOZOMI NETWORKS
- Indegy
- CLAROTY Clarity for OT Networks



Detect and Respond Services

Threat Management and Response

Attack surface management

Incident Management

Cyber Threat Intelligence

Threat hunting

- tenable
- KENNA Security
- Qualys.

- DISP.
- Recorded Future
- THREAT LIBRARY
- MISP Threat Sharing
- INTEL471
- THREAT CONNECT
- CODEX

- elastic
- DEVO

Logos and trademarks are properties of their respective owners and are used here for information purpose only

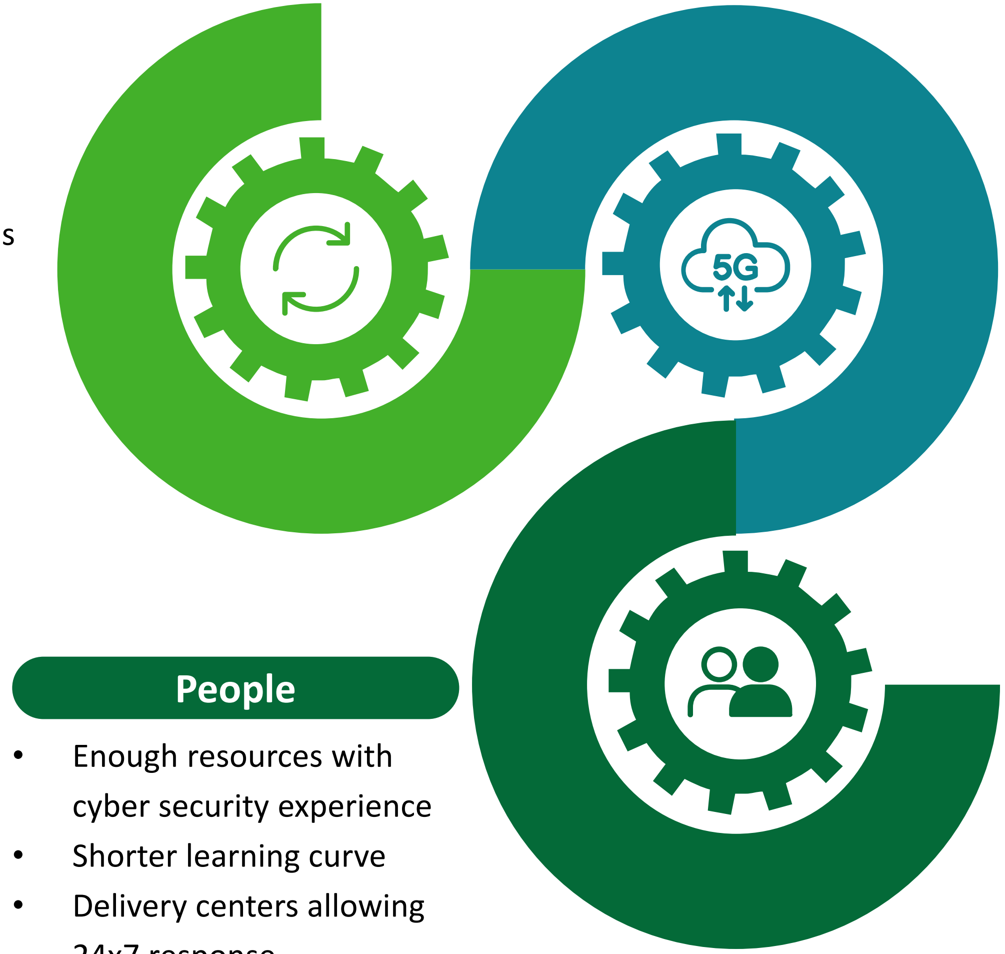
Build VSOC using IDS and Threat intelligence

Enabling factors for building a VSOC

Process, People and Platform

Process

- Standardized processes, implemented and followed
- Linking static programs vs. continuous improvement
- Alignment of VSOC activities with business goals
- Information sharing across groups/ departments
- Keeping up with changing regulations
- Training and awareness



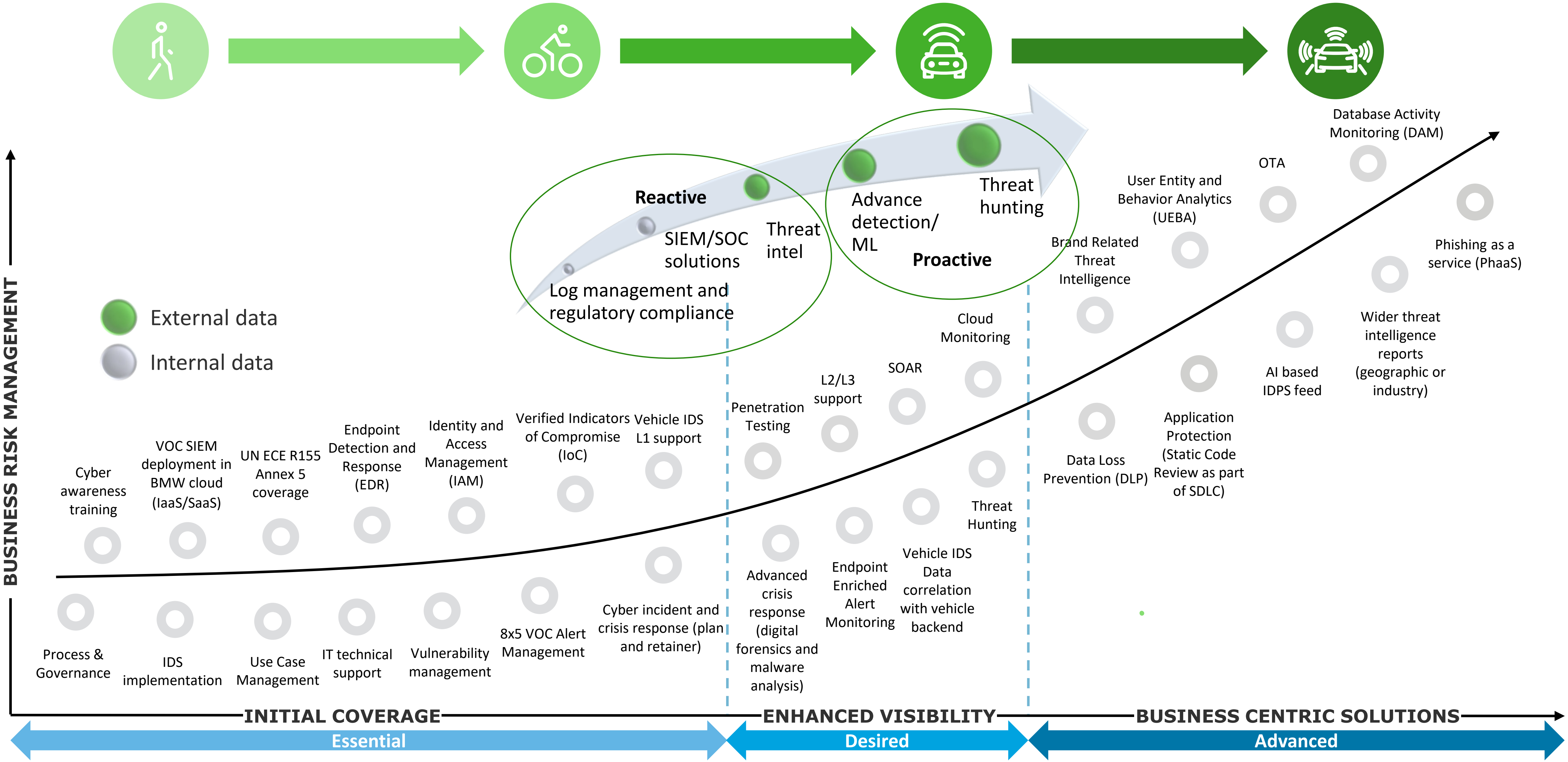
Platform

- Hybrid environment with cloud and on premise
- Hands on with new technologies
- Incubate innovations
- Tool management
- Integration of diverse data sources and technologies
- Automation and orchestration at different levels

People

- Enough resources with cyber security experience
- Shorter learning curve
- Delivery centers allowing 24x7 response

Building VSOC step by step in a scalable manner



BUSINESS RISK MANAGEMENT

🟢 External data

⚪ Internal data

Reactive

Log management and regulatory compliance

SIEM/SOC solutions

Threat intel

Advance detection/ ML

Threat hunting

Proactive

Cyber awareness training

VOC SIEM deployment in BMW cloud (IaaS/SaaS)

UN ECE R155 Annex 5 coverage

Endpoint Detection and Response (EDR)

Identity and Access Management (IAM)

Verified Indicators of Compromise (IoC)

Vehicle IDS L1 support

Process & Governance

IDS implementation

Use Case Management

IT technical support

Vulnerability management

8x5 VOC Alert Management

Cyber incident and crisis response (plan and retainer)

Penetration Testing

L2/L3 support

SOAR

Cloud Monitoring

Threat Hunting

Advanced crisis response (digital forensics and malware analysis)

Endpoint Enriched Alert Monitoring

Vehicle IDS Data correlation with vehicle backend

Brand Related Threat Intelligence

User Entity and Behavior Analytics (UEBA)

OTA

Database Activity Monitoring (DAM)

Phishing as a service (PhaaS)

Wider threat intelligence reports (geographic or industry)

AI based IDPS feed

Application Protection (Static Code Review as part of SDLC)

Data Loss Prevention (DLP)

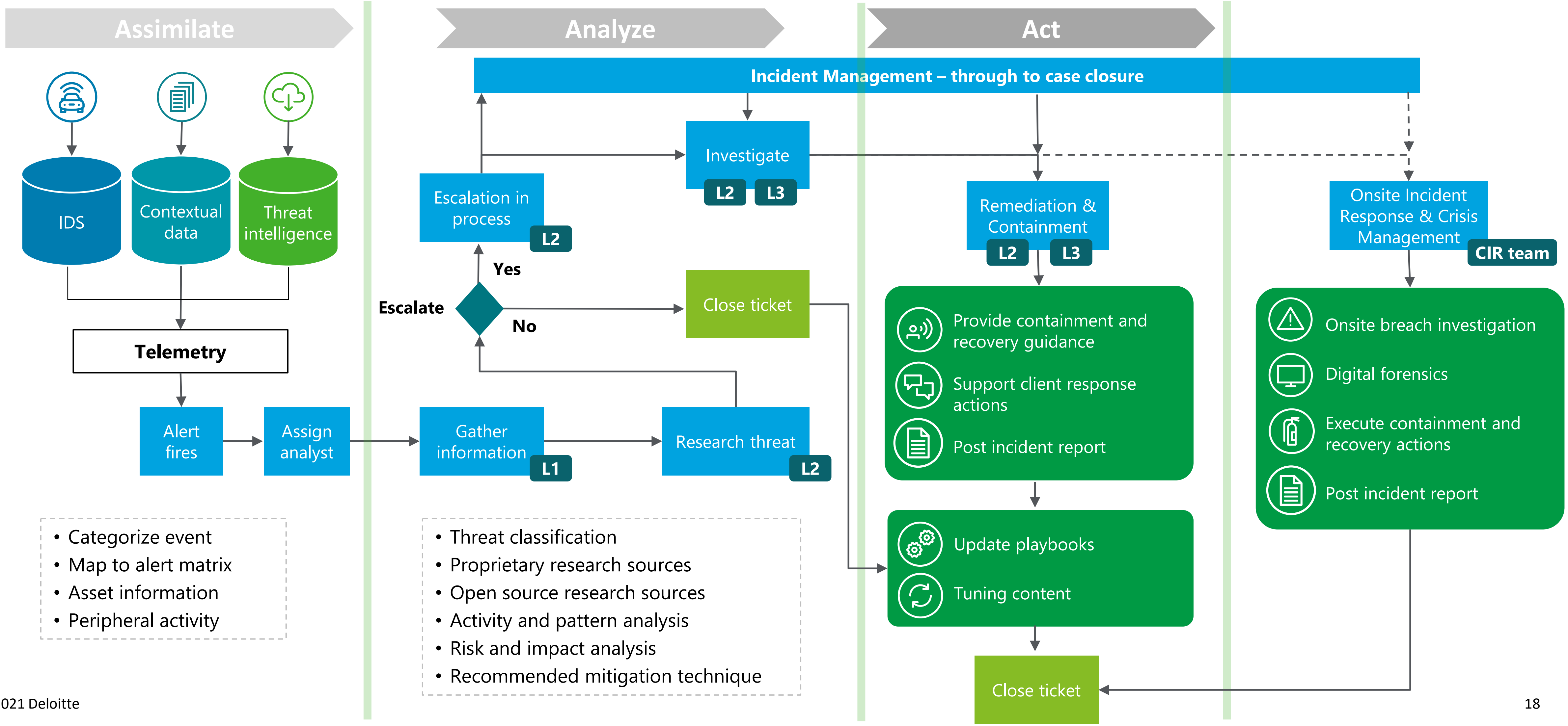
INITIAL COVERAGE – **ENHANCED VISIBILITY** – **BUSINESS CENTRIC SOLUTIONS**

Essential – **Desired** – **Advanced**

2021 Deloitte

VSOC workflow

Synergize by getting an end-to-end blueprint including IT systems and data transfer



Assimilate

IDS

Contextual data

Threat intelligence

Telemetry

Alert fires

Assign analyst

- Categorize event
- Map to alert matrix
- Asset information
- Peripheral activity

Analyze

Incident Management – through to case closure

Escalation in process L2

Investigate L2 L3

Escalate

Yes

No

Close ticket

Gather information L1

Research threat L2

- Threat classification
- Proprietary research sources
- Open source research sources
- Activity and pattern analysis
- Risk and impact analysis
- Recommended mitigation technique

Act

Remediation & Containment L2 L3

Provide containment and recovery guidance

Support client response actions

Post incident report

Update playbooks

Tuning content

Close ticket

Onsite Incident Response & Crisis Management CIR team

Onsite breach investigation

Digital forensics

Execute containment and recovery actions

Post incident report

About the author

About the Author

Nishant Khadria

Director

Deloitte GmbH Wirtschaftsprüfungsgesellschaft

Aegidientorplatz 2a

30159 Hannover

nkhadria@deloitte.de

Professional experience

- 22+ years of experience in automotive industry with focus on vehicle security, software quality, supplier management, security assessment and vehicle cyber monitoring (VSOC) serving automotive OEMs and suppliers across the globe.
- Deep understanding of software development lifecycle including use cases, requirements, architecture, design and tests to ensure timely implementation.
- Key contact between OEMs and their suppliers to bridge technical gap and establish software quality measures (based on automotive standards and guidelines) to accomplish software performance.
- Leading AUTOSAR initiative for Deloitte.

Selected projects

- UN R155 based vehicle cyber security monitoring and reporting
- Supplier quality management including process and assessment framework
- Security benchmarking of vehicle EE architecture
- ISO 21434 based Threat Analysis and Risk Assessment (TARA)
- ISO-26262 based Functional Safety recommendations for software quality
- Supplier assessment with respect to secure software development lifecycle
- Adaptive AUTOSAR system test cases for security
- Quality metrics - Software Projects, Processes, Products
- OEM driven supplier strategy and end-to-end reviews
- Requirement analysis and design for navigation infotainment systems
- Design and development of vehicle embedded functional modules on RTOS

Industry certifications

- AWS Certified Solutions Architect and Cloud Practitioner
- Automotive SPICE Provisional Assessor
- ISO 27001 Lead Auditor and Implementer

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services; legal advisory services in Germany are provided by Deloitte Legal. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

175

MAKING AN
IMPACT THAT
MATTERS
since 1845