Deloitte.

IDS Overview and Approach

SIP-adus 2020, Nishant Khadria/ Ingo Dassow

Deloitte 2020

MAKING AN IMPACT THAT MATTERS since 1845

Contents

*An attempt is made to present unbiased information on vehicle IDS

2020 Deloitte

** Content of this presentation may not be accurate and/or complete and the author and his employer disclaim any liabilities arising from the use of the content.*

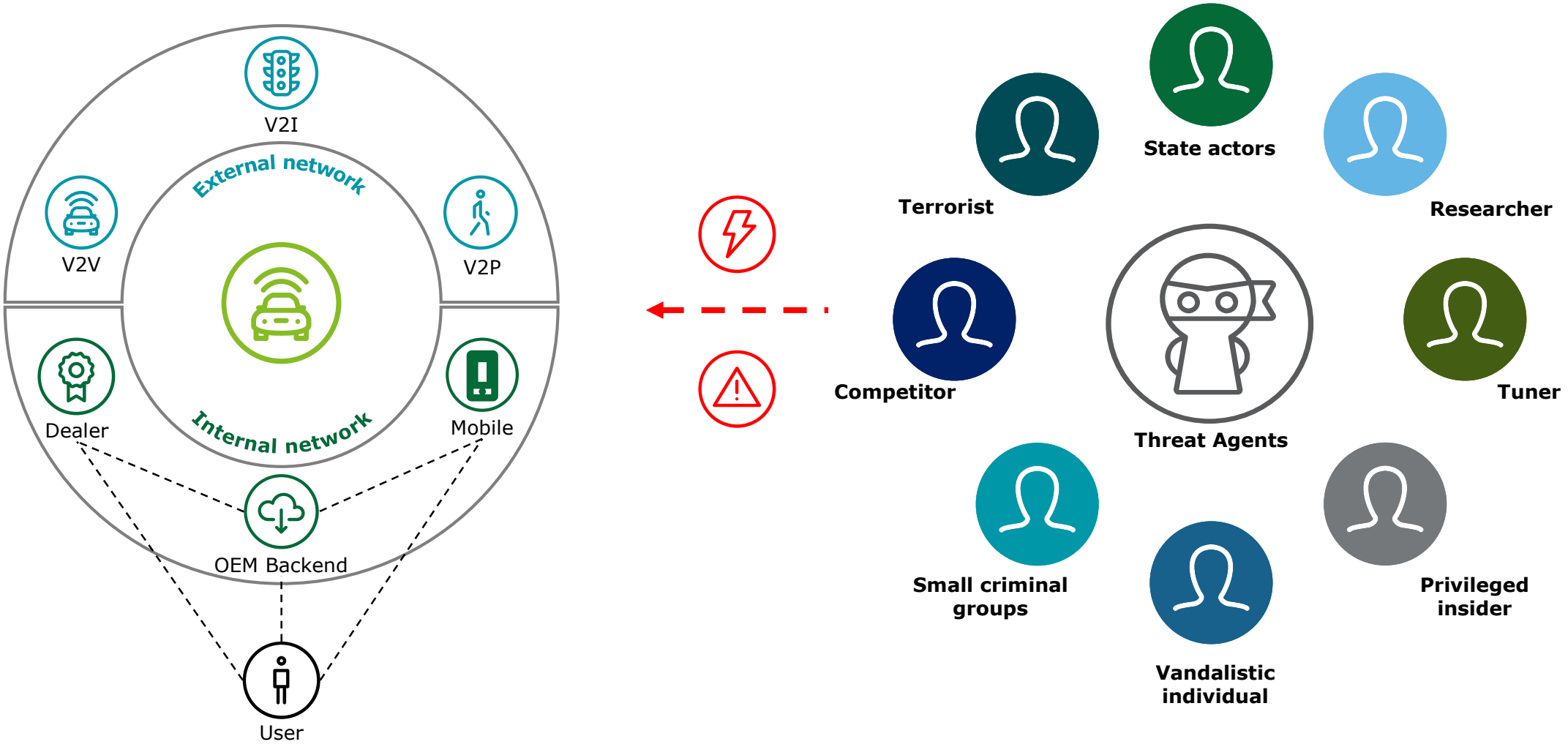
Why an Intrusion Detection System?

Increased threats and regulations advise a vehicle based detection+logging system

2020 Deloitte

Connected vehicle is an aggregation of vulnerable components

Each element and connection can open a window for cyber attack



Threats are increasing at a stunning rate

Researches and real attacks have shown growing demand for vehicle based intrusion detection

2015
- US Automaker

2016
- Leading EV maker
- Japanese OEM
- Key Relay attack on 19 OEM's 24 cars

2017
- Electric car manufacturer
- Korean OEM

2018
- German leading OEM
- Premium auto maker

2019
- Global electric carmaker

2020
- Germany based global OEM

What next?

*"Logs of all security critical operations should be kept. They should be aggregated and uploaded periodically to the fleet management server for analysis. More importantly, there needs to be **real time detection and reaction on vehicle**."*

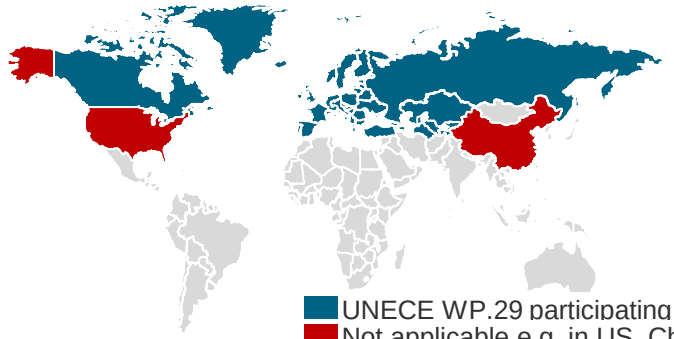
*"Like Ethernet, the **CAN network traffic should be observed in real time to identify anomalies**. All the attacks outlined in the historical section could have been detected (and prevented) with even the most trivial **CAN network intrusion detection** software."*

Securing Self-Driving Cars (one company at a time), Dr. Miller, Valasek; Aug 2018

Upcoming UNECE WP.29 CSMS (R155) requires competent detection capabilities

Though not mentioned directly in the regulation, IDS becomes inherent component of vehicle security

- 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)



Development → **Production** → **Post-Production**

Threat detection

7.2.2.4.(b) *"…Include the capability to analyse 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 capabilities

Detection mechanisms

2020 Deloitte

An efficient IDS prepares OEMs for upcoming challenges

More and more regulations impose intrusion detection and forensics

Regulatory

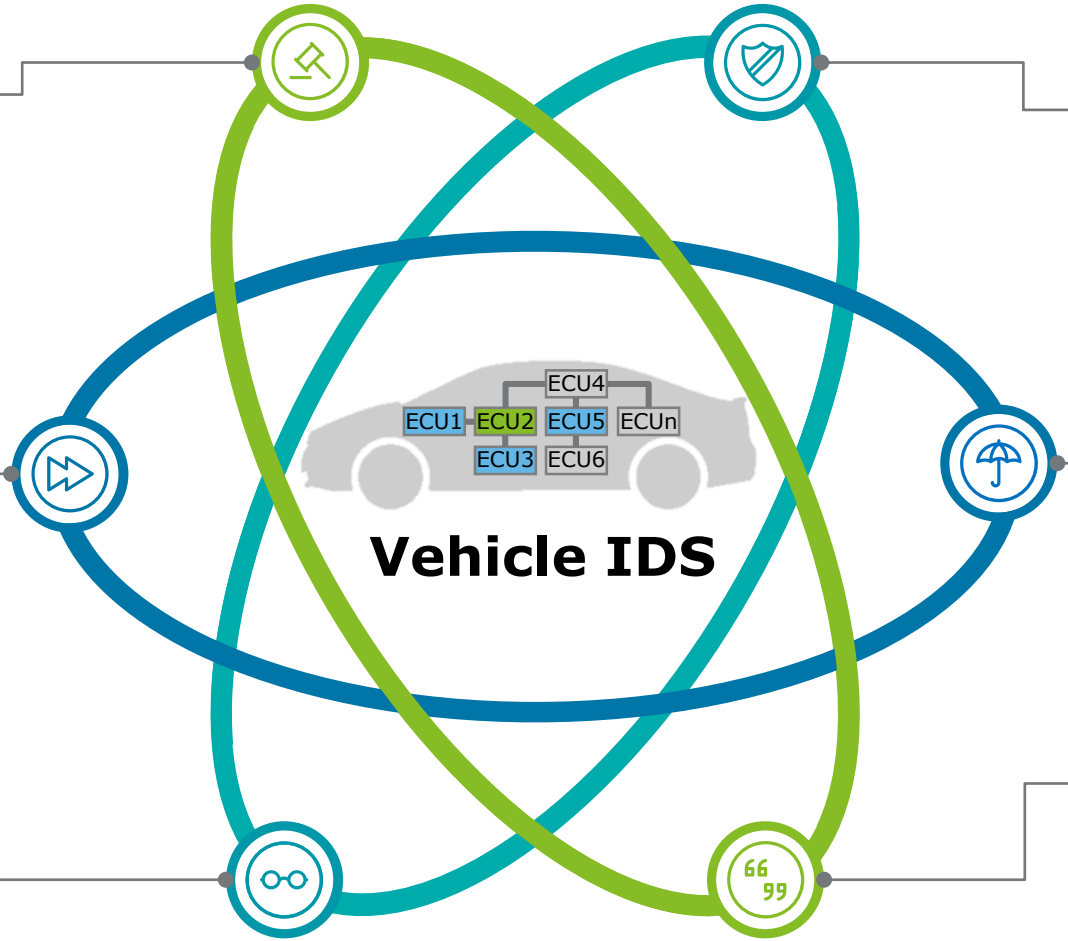
UNECE WP.29 R155 mandates vehicle manufacturers to analyze vehicle logs

Operational

An efficient and timely detection can prevent operational hindrance e.g. by mitigating DoS/ DDoS attacks

Forensics

IDS logs are key part of the forensic investments and help organization understand technical and processual gaps



Security

IDS logs offer unique way of detecting cyber attacks as and when it occurs, triggering immediate response activities

Safety

Safeguarding remotely controlled safety critical applications in an autonomous environment (e.g. ALKS)

Privacy

Securing/ containing leakage of customer private data can save OEMs from financial and reputational damages

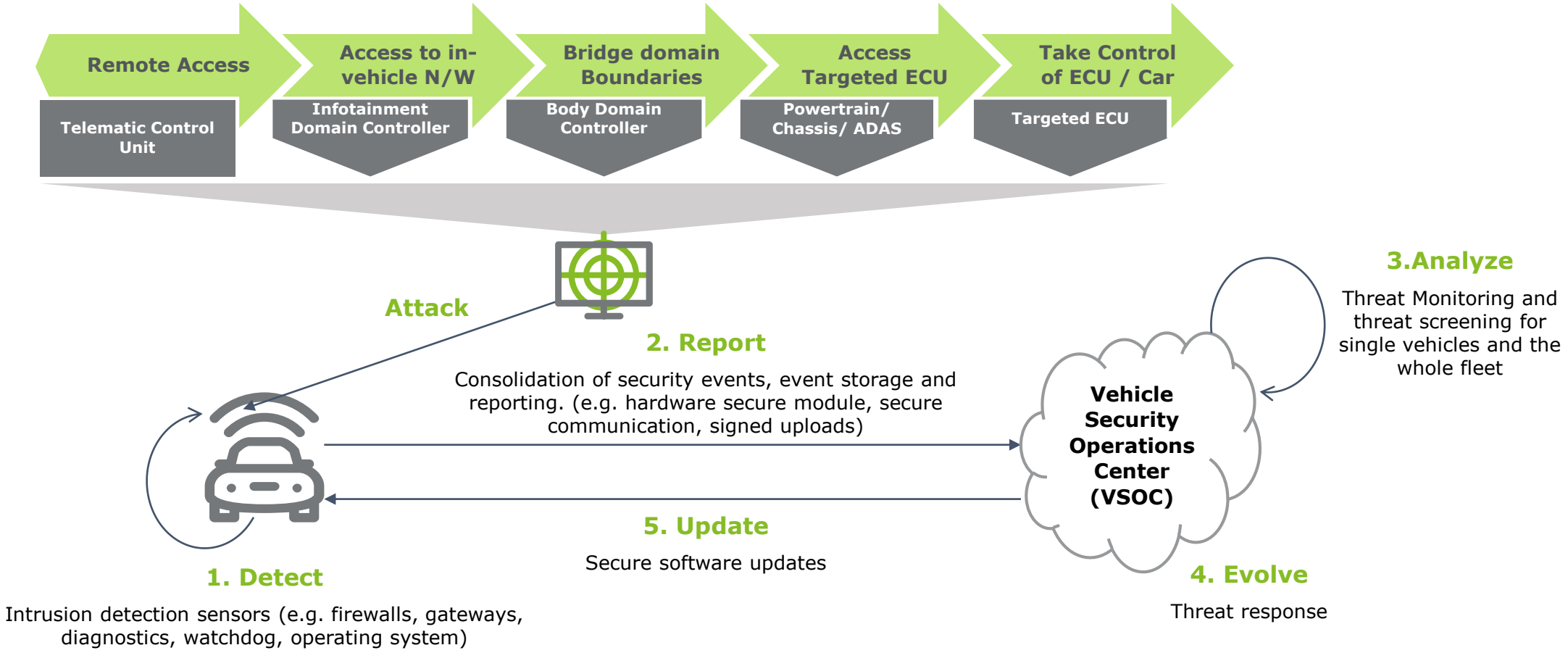
Working and information flow

Typical flow of data across various systems and components

The big picture

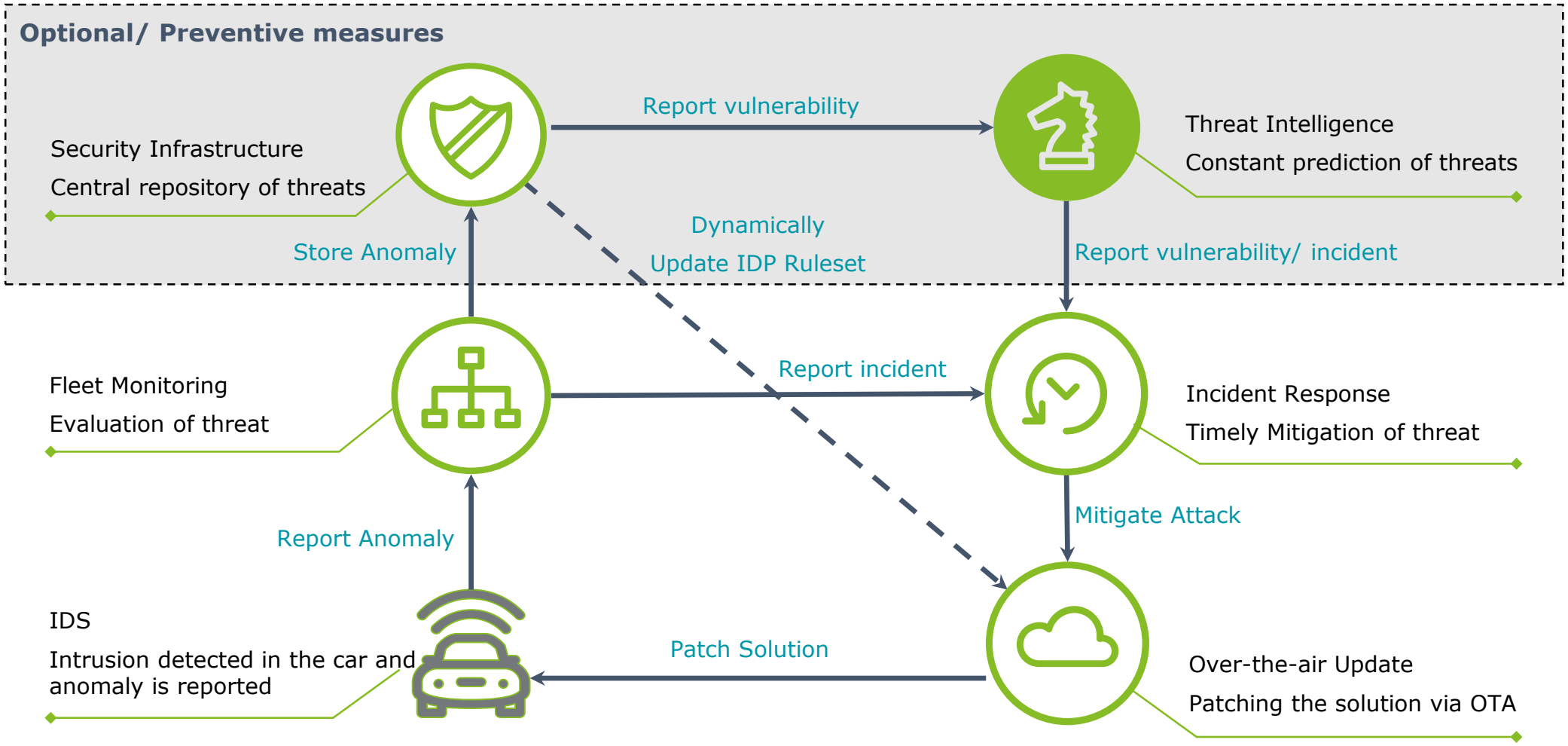
Detecting anomalies where it occurs

Once an unexpected behavior is detected, logs are fed into a Security Operations Center (SOC) where they are analyzed and correlated to other systems and vehicle logs. In case of a definite incident, patches are prepared (in association with suppliers and 3rd parties) and are applied to the ECUs either through authorized workshop and/ or using secure Over The Air update.



Flow of data in an IDS enabled environment

Eco system may also include vulnerability management to ensure preventive measures



Stakeholders involved

Relevant data is carried over mobile network from vehicle to VSOC for analysis

Tier 1/ 2 supplier

An IDS SW components are typically embedded on existing and/ or separate ECUs by the supplier

Network operator

Mobile (virtual) network operators carry data and logs from SIM card to the backend systems

OEM/ 3rd party backend

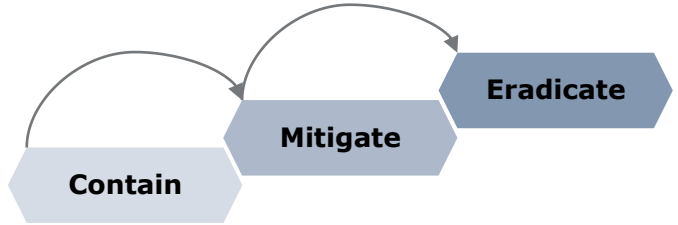
Backend can offer multiple services as well as acts as place for data lake

OEM/ 3rd party VSOC

A Vehicle Security Operations Centers is equipped with SIEM and big data analytics tool to deeply analyze vehicle logs and correlate them with other IT systems

OEM/ 3rd party incidence management/ forensics lab

During triage, if an anomaly/ incident is ascertained, the incidence response activities are trigger to contain, mitigate and eradicate the issue



Based on the organizational setup and technical eco-system, there could be fewer or more parties involved.

2020 Deloitte

IDS Types and Design considerations

In general there exist, Network and Host based IDS

Mostly there are Network and Host based IDS to detect intra/ inter ECU anomalies

In certain cases hybrid capabilities can be built using “hybrid IDS”

The intrusions may come from **internal**, which resides inside the targeted system components having legal access privilege to the network.

External intruders may 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 communication)

- Ethernet
- CAN/ CAN FD
- LIN/ FlexRay

Hybrid IDS

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

Host based (ECU internals)

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

Current trends show use of anomaly based network IDS solutions

Artificial Intelligence and Machine Learning algorithms are finding their place

State of the Art anomaly detection techniques: Most of them are based on the Machine learning algorithms, having the advantage of, the normal behaviour is learned from training data.

"In-vehicle networks are a well defined Environment. There are also several standards available to specify the communication between ECUs in a semi-formal manner"

1

Signature Based

With the help of attack database, previously occured attacked patterns are used for pattern matching to detect and prevent upcoming intrusion.

Set-back: Effective only for known attacks

2

Anomaly Based

Very similar to blacklisting approach in signature based systems, with a difference that here rules are defined to have much broader scope which results in detection of events that have never occurred.

Set-back: Frequent rule updates

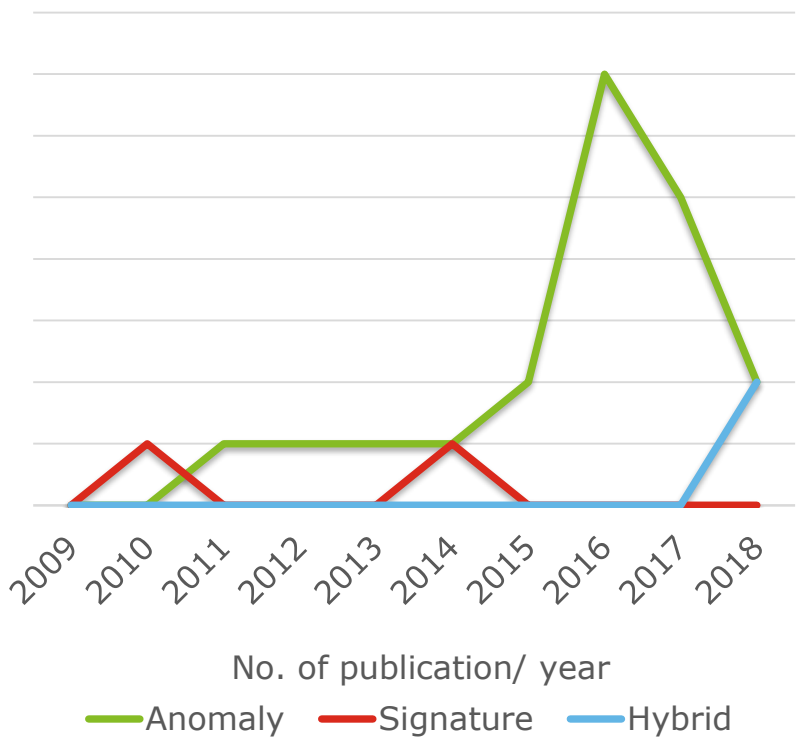
3

Specification Based

Expected behavior of the system is defined as the set of rules. The classification and detection is then performed by observing a deviation of the execution from the defined properties.

Set-back: False positives

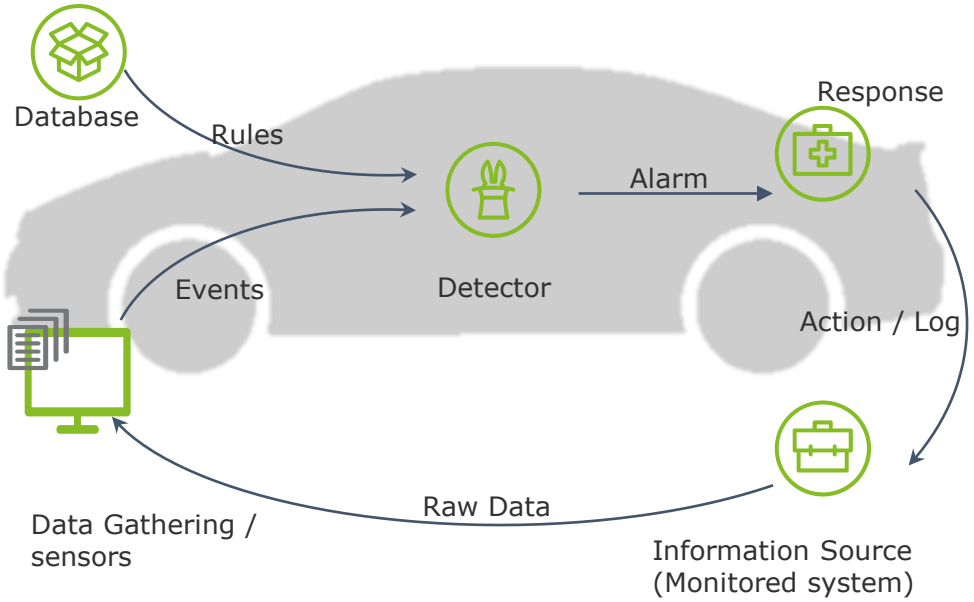
Example: CAN based IDS



Design considerations and in-vehicle architecture

A more robust and stringent system prevents „false positives" transferred to SOC

Basic Architecture within the Car



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.

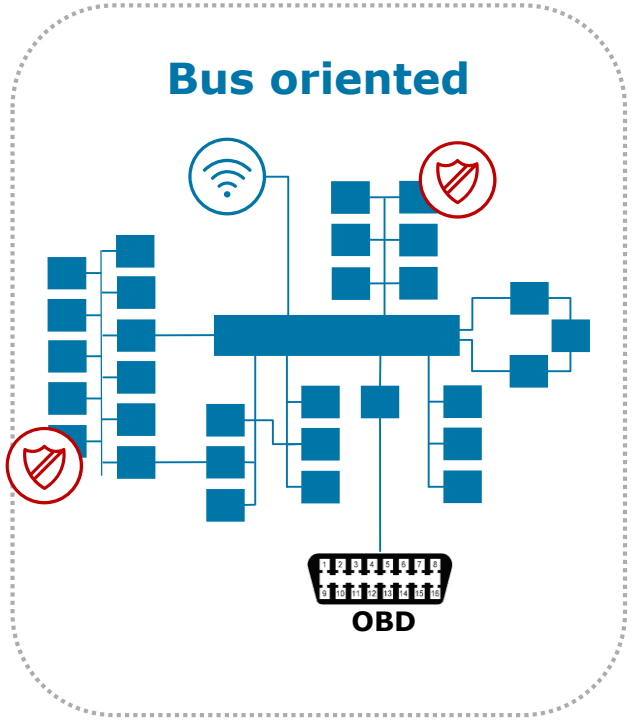
Database: is a storage module that contains the rule-sets or the IDs which the detector uses when comparing the received data.

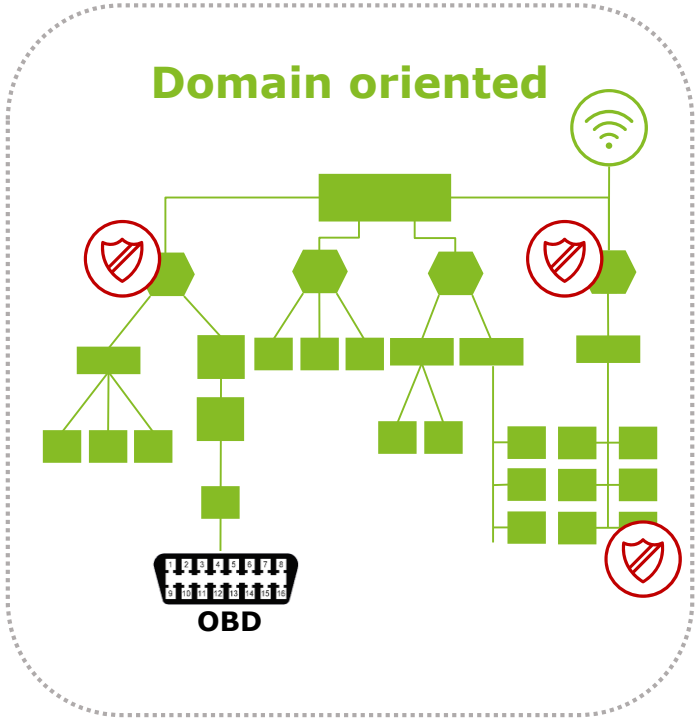
Output / Response: When an alarm is raised a proper action is taken. This could be an active response where the IDS performs a predefined action such as drop the packet, or an inactive response such as logging for later inspection by a human factor to determine the appropriate response.

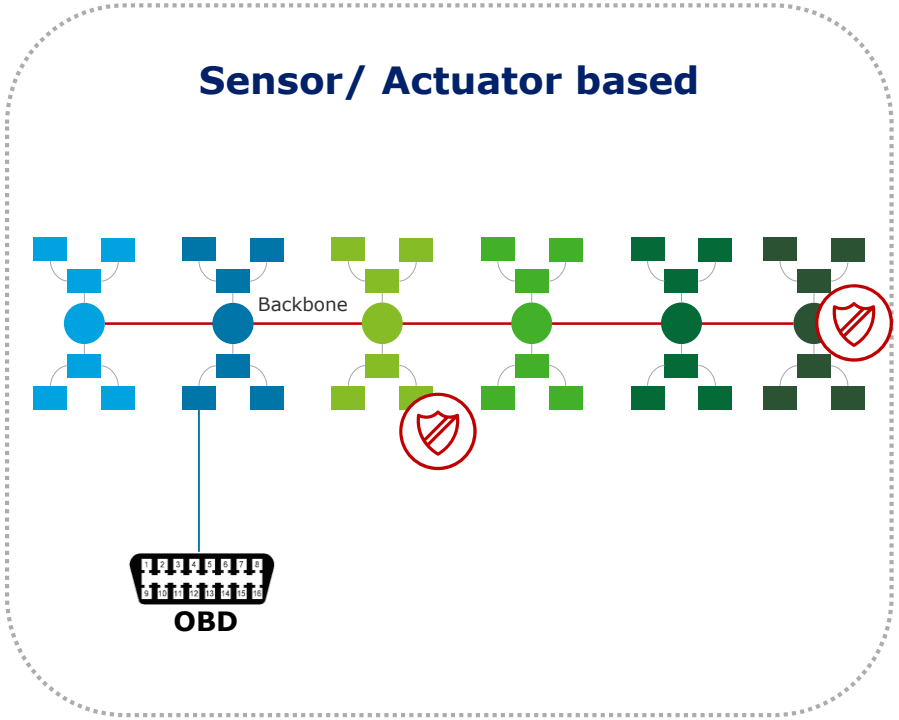
2020 Deloitte

Placement of a Network IDS (NIDS) in the EE architecture

Based on the platform and network topology, a NIDS could be placed on multiple ECUs. Logs should be assembled before transferring to the SOC.







Possible placement of IDS module for network anomaly detection

Challenges and Future

Technical expertise and collaboration is the key to success

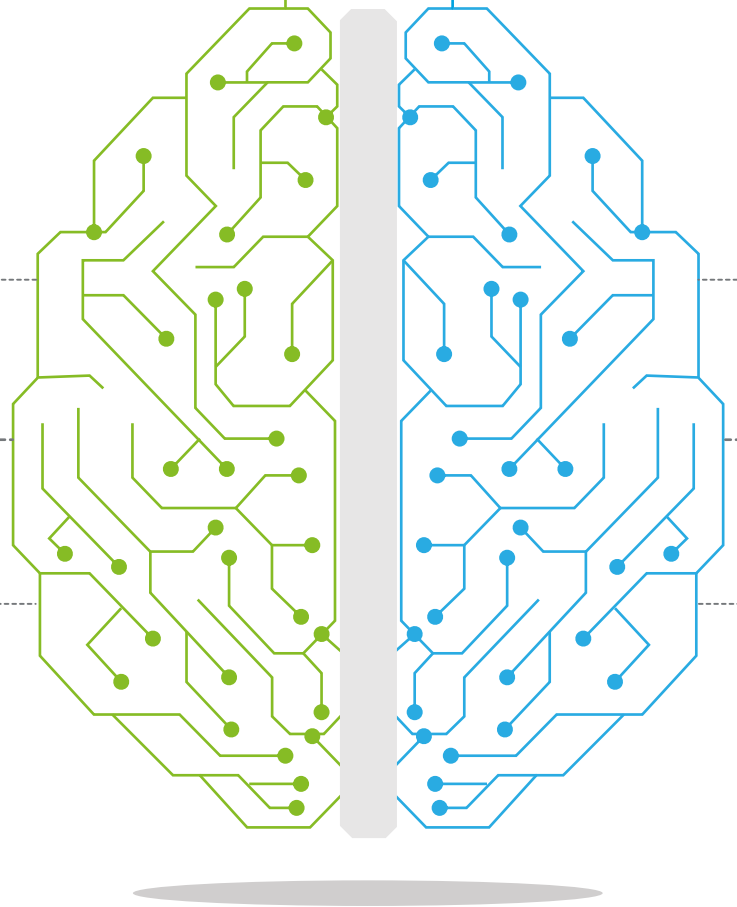
2020 Deloitte

Challenges for an effective and efficient IDS

A dynamic approach is required to deliver performance with limited embedded resources

Physical

Technical



Placement

- For optimum traffic log collection, ECU and domain selection is not easy because not all EE domains are interconnected

Resource constraints

- Effective and sufficient analysis of real time logs is quite taxing with limited computing power

Data storage and transfer

- Secure log storage and transfer is an overhead on the ECU as it has to then manage several crypto keys and do special memory management

Accuracy and Performance

- ~100% true-positive and true-negative rates are expected. Even a deviation of 0.3% may become unacceptable
- Zero-day attacks cannot be solved using signature/ anomaly based systems

Attack response

- Improper/ insufficient response can endanger road users' life
- A response may unexpectedly interrupt normal vehicle operation

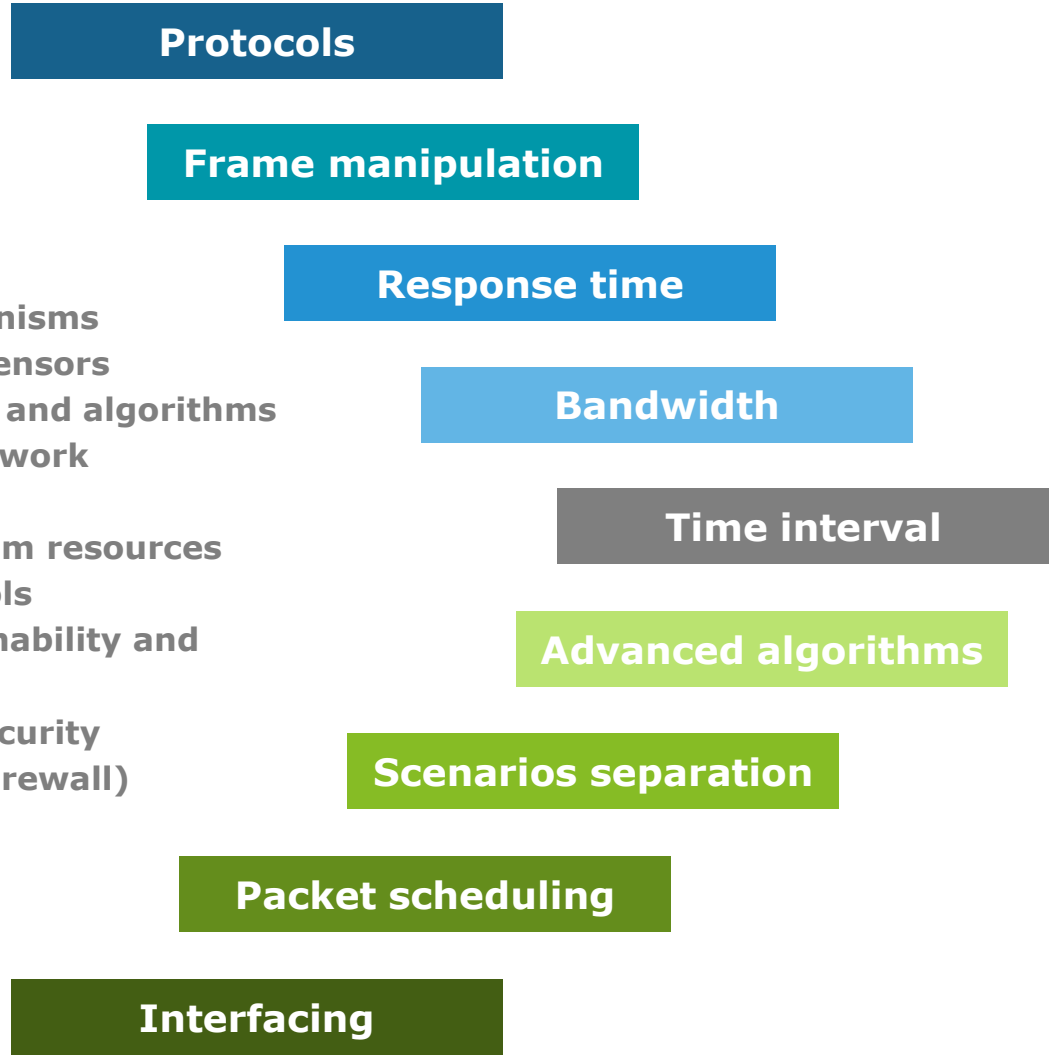
Data selection

- With increased complexity of EE architecture and value added services, data selection methods become challenging for a dynamically changing eco system

Future with supported features for effective detection

No specific standards, however innovations are sprouting in all directions

- Deployment mechanisms
- Placement of IDS sensors
- Location of IDS SW and algorithms
- Access to host/ network parameters
- Availability of system resources
- Support for protocols
- Reliability, maintainability and portability
- Dependencies of security gatekeepers (e.g. firewall)



No Automotive IDPS standard!

But the there are common recommendations from standard making organizations and industry leaders for automotive IDPS design or testing of a new Architecture which help in delivering realistic workloads.

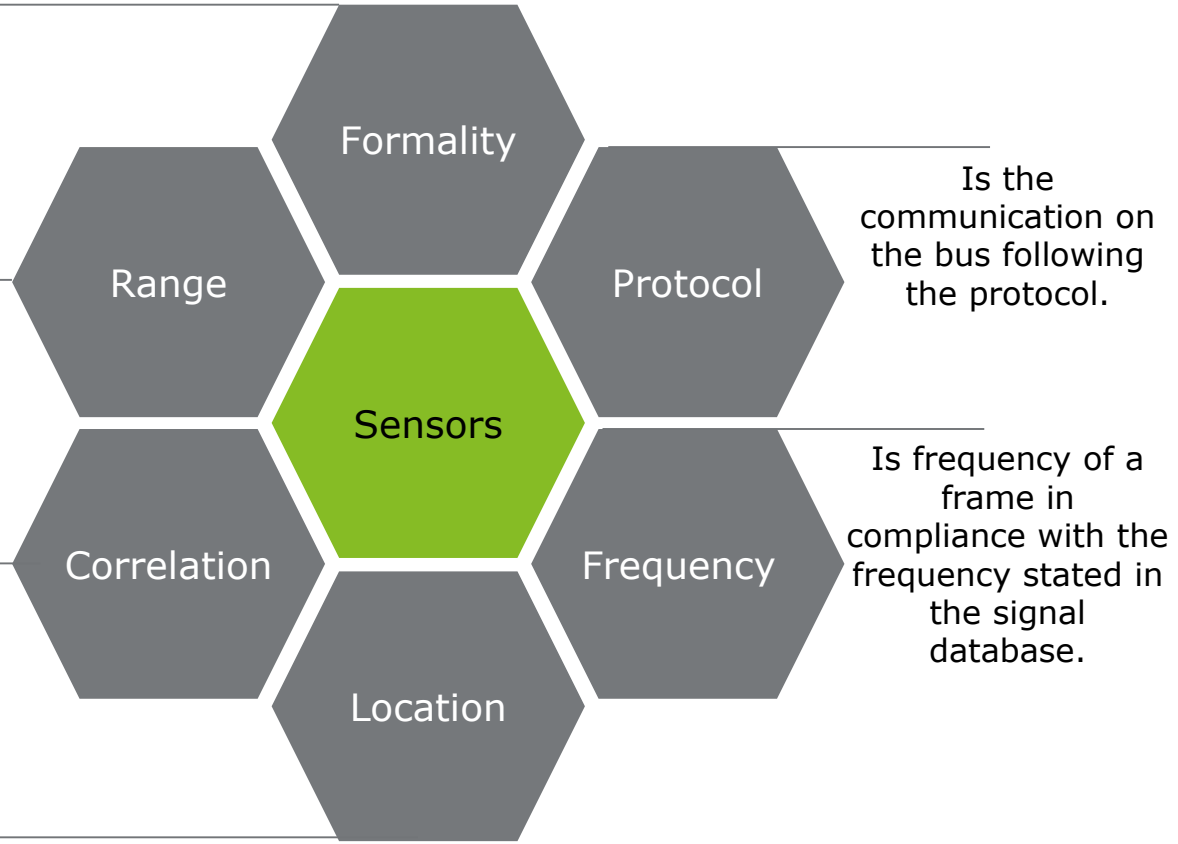
2020 Deloitte

Future of sensors and data collection mechanisms

To be implemented on ECUs and network to detect an abnormal behavior

The Goal is to make use of sensors / to come up with the techniques to watch the abnormalities for these conditions

Provide almost 100% data. They can be extracted and utilzed in the security for this process.



Plausibility Consistency

There are No sensors to provide data on these two conditions

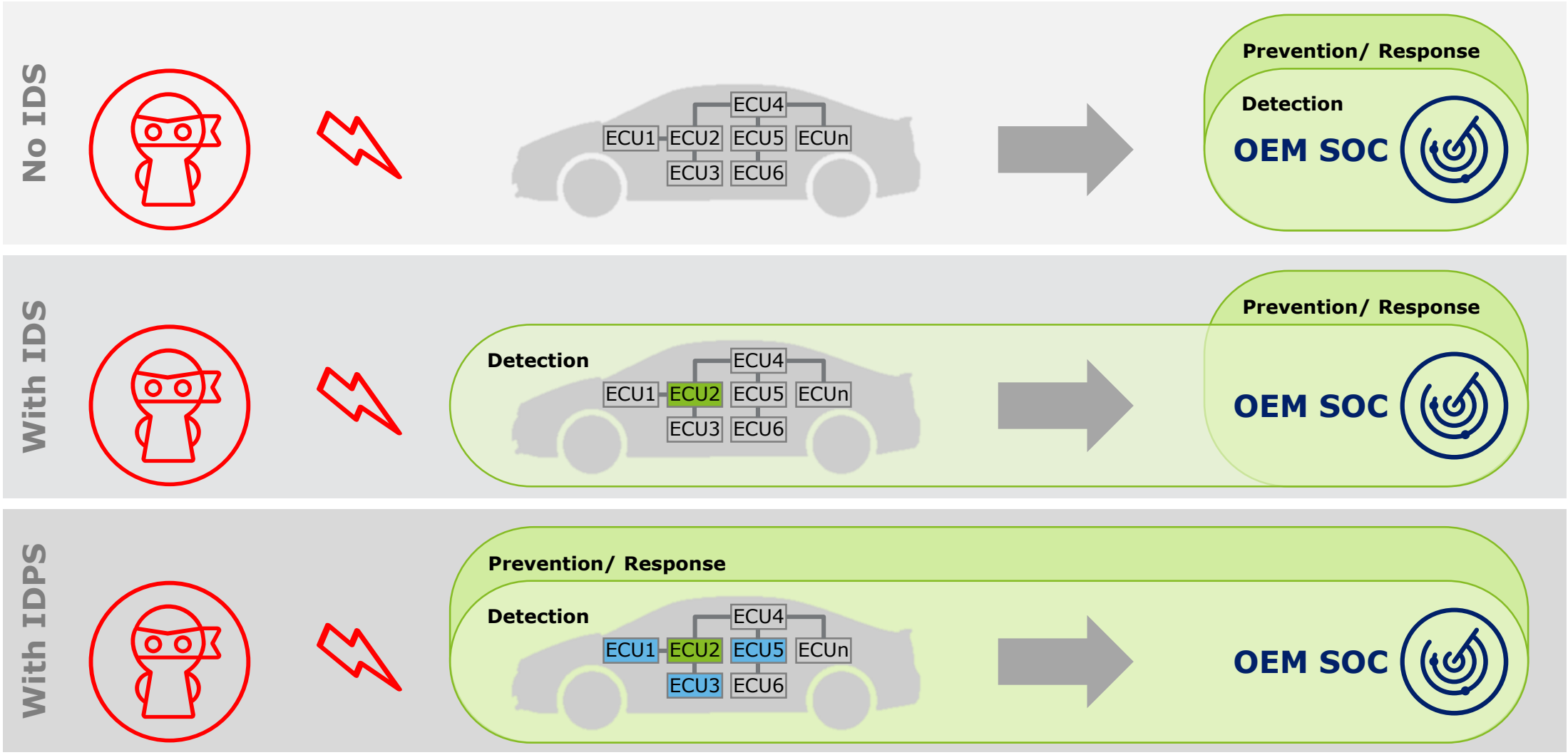
The Machine learning and neural networks are utilized by different vendors to provide the solution.

The best solutions are achieved through: **Anomaly** or **specification** based methods complemented by Machine Learning. But the latest trend is to combine both, to provide a **Hybrid solution**.

2020 Deloitte

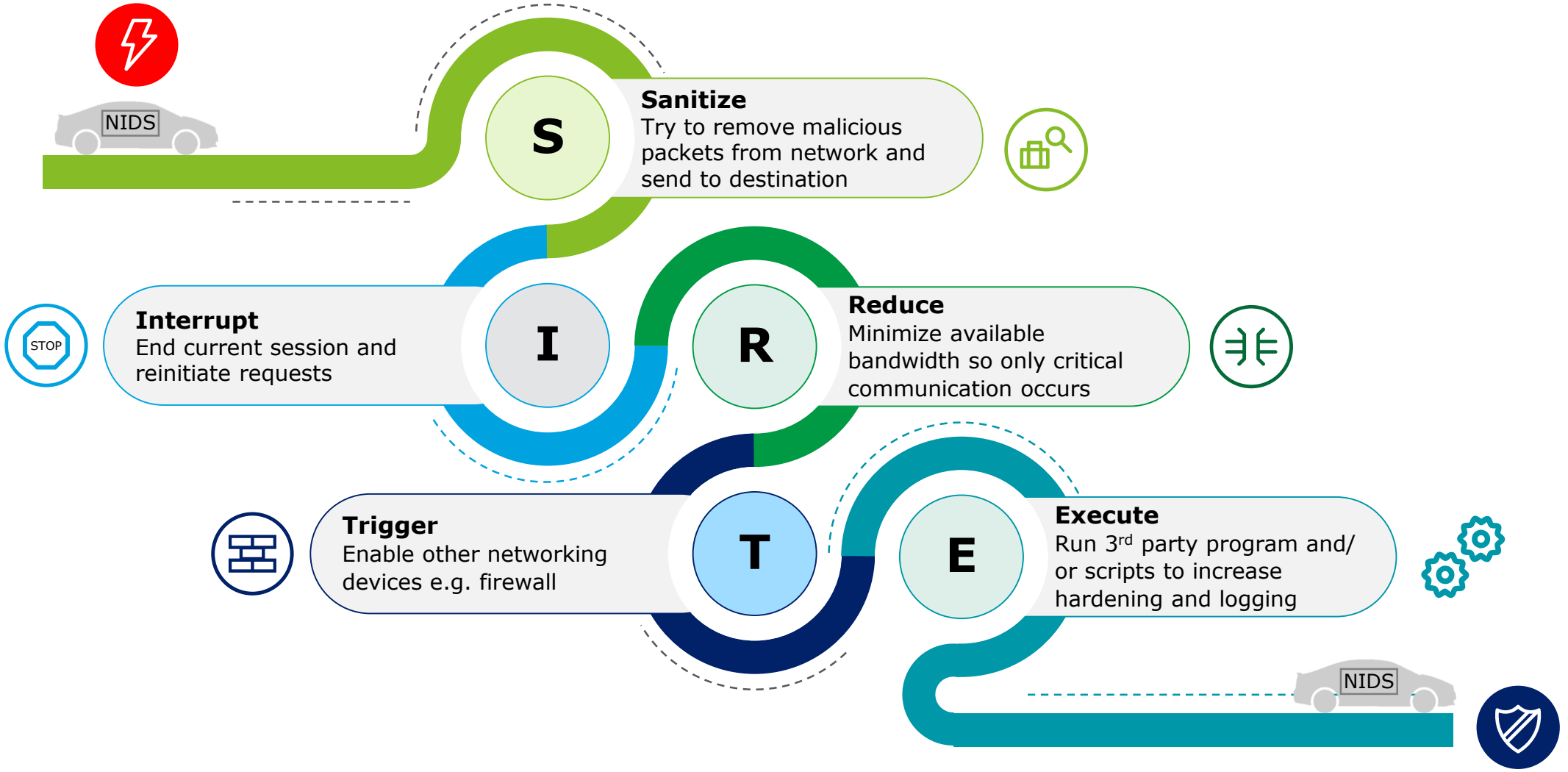
IDS with in built prevention capabilities

Significantly enhances real time response and decreases attack scenarios



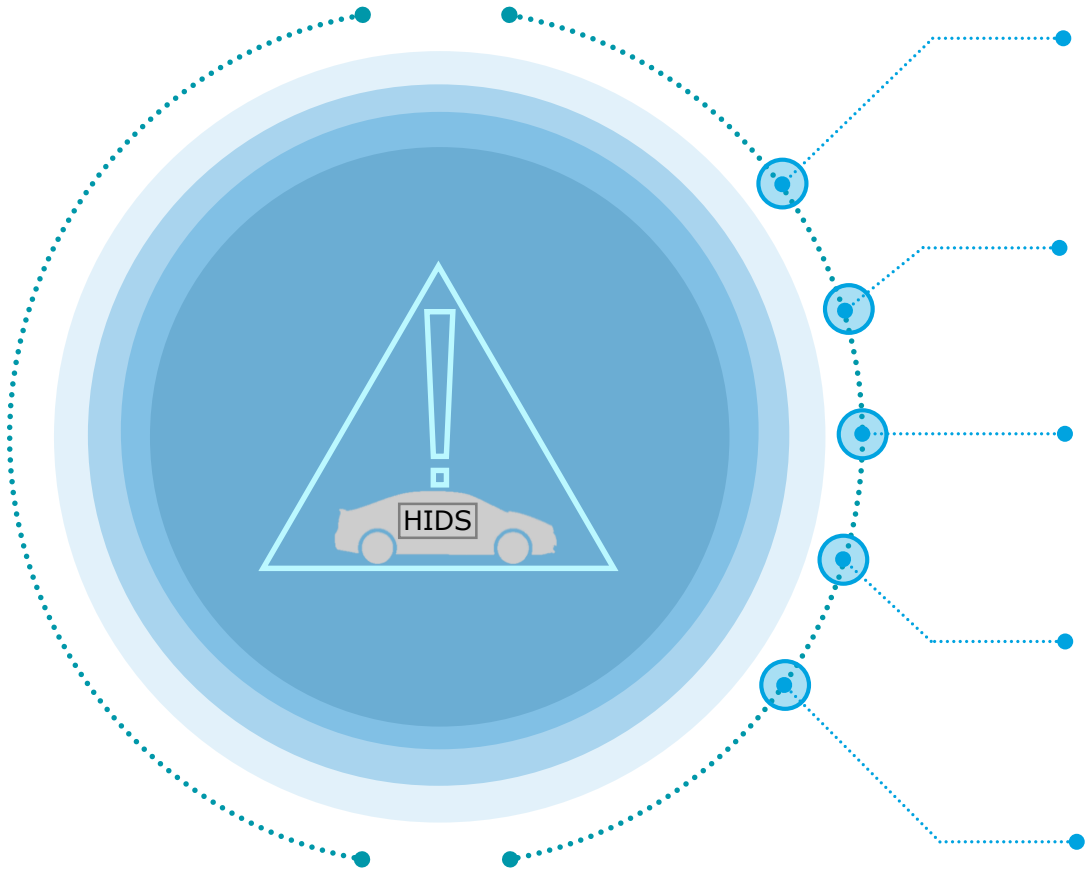
Possible approach and preventive measures in a NIDS

Based on the architecture and attack, **S-I-R-T-E** execution order will change



Possible approach and preventive measures in a HIDS

Threat surface and KPIs shall be identified carefully to protect the assets



Code analysis

Binary code scanning for vulnerability exploits

Traffic filtering

Observing and filtering in/outbound traffic data

Filesystem monitoring

Controlling identity, access and authorization on filesystem

Memory management

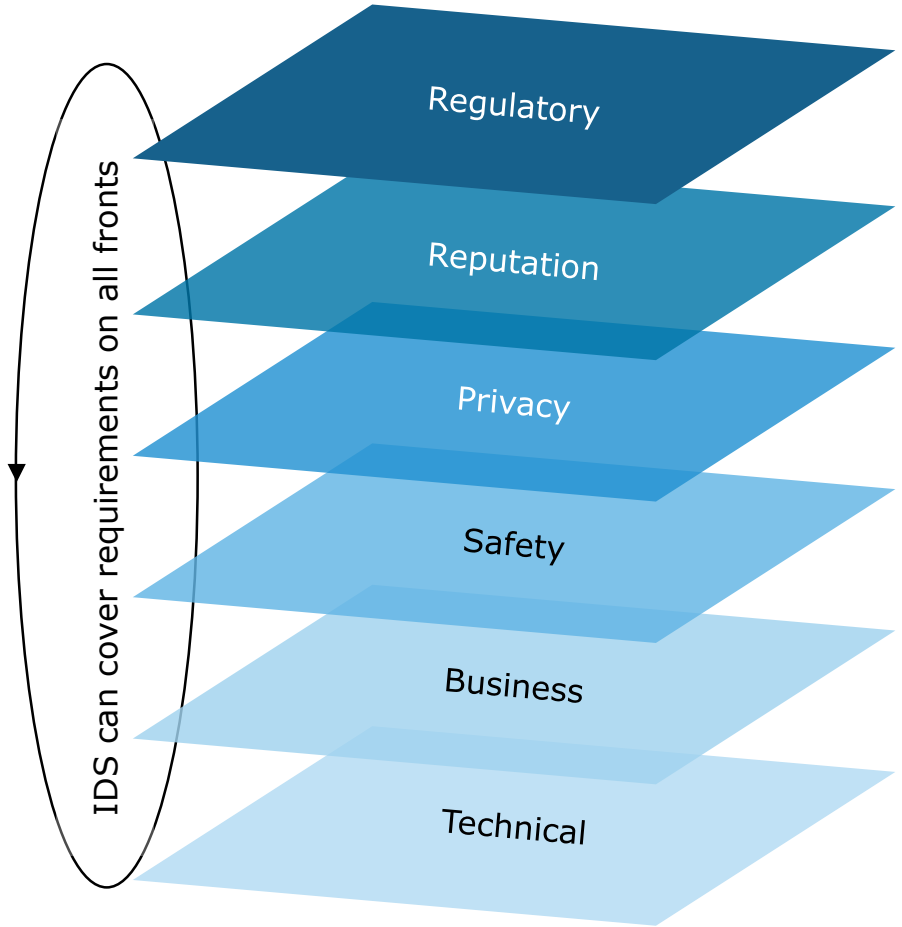
Guarding partial/ complete memory locations

Process watchdog

Supervising KPIs for unexpected behavior

Use cases

IDS shall be designed in a flexible way, enabling easy adaption to different network technologies, as well as embedded environment in different application areas



UNECE R155	• Vehicle logs for vehicle monitoring • Forensic analysis
Brand value	• Predictive maintenance through regular health checks and history
GDPR	• Data privacy leakage detection
FuSa, SOTIF	• Securing safety critical functions
ROI	• Execution of authentic value added services • Tuning prevention
Reliability	• Software patch management • Support in crypto key management

2020 Deloitte

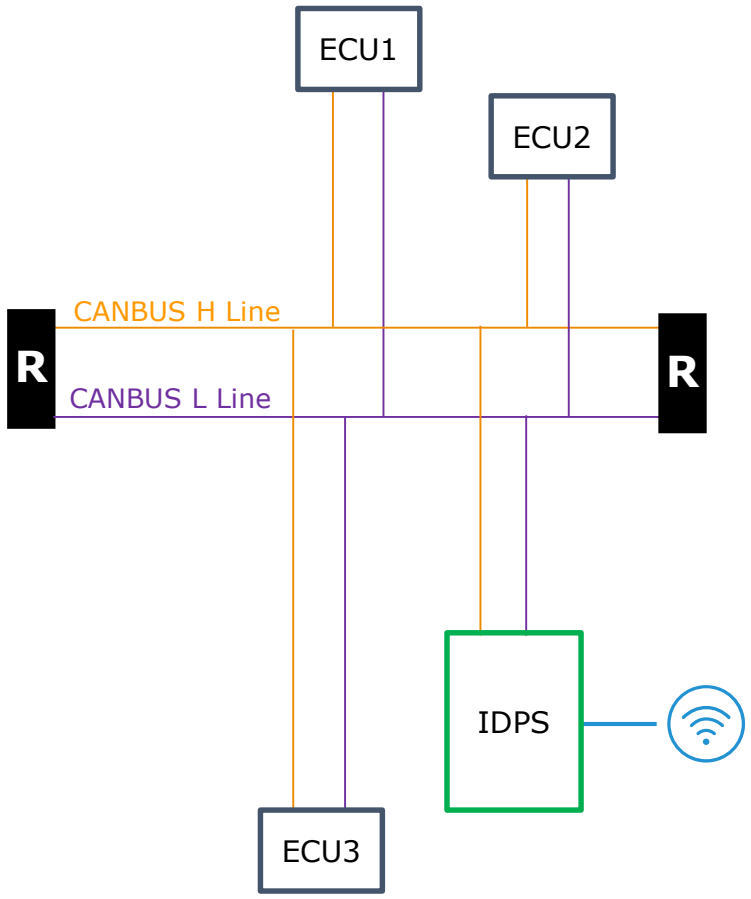
Illustration

How an NIDS can detect CAN timing anomalies

2020 Deloitte

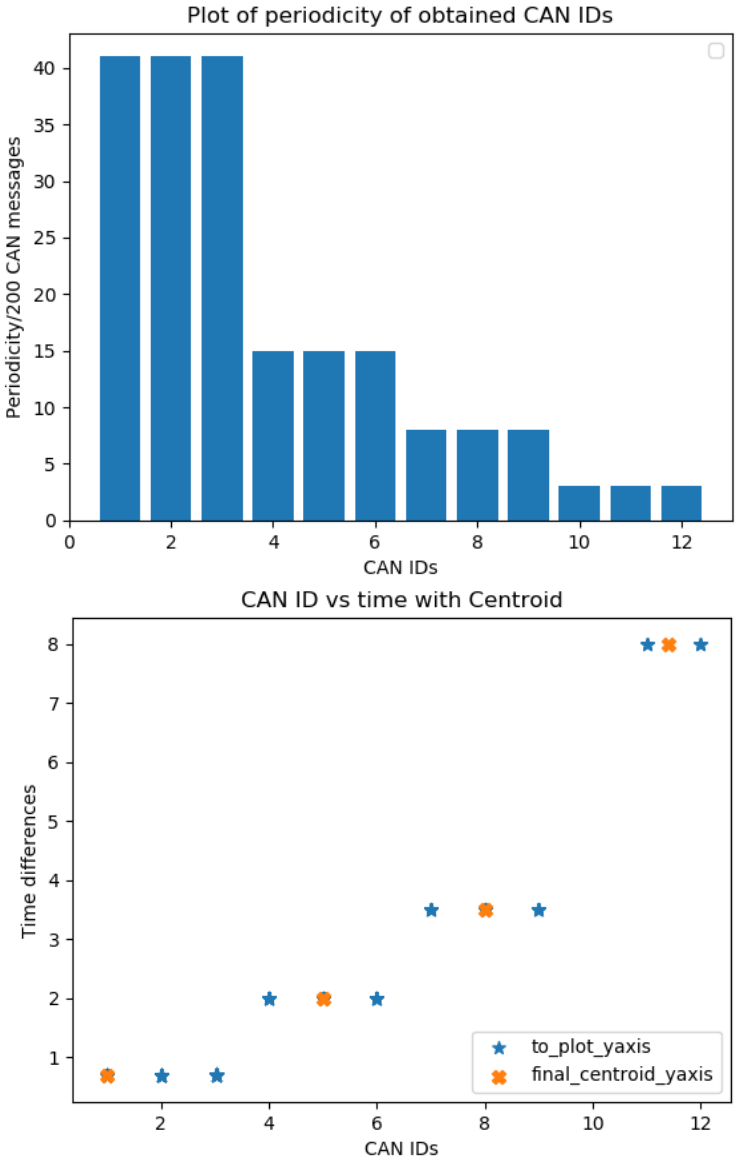
Network IDS for CAN based anomaly detection

In it's simple form, a network based ID(P)S can detect timing anomalies



ECU	CAN ID	Interval
1	1, 2, 3	Every 0.7 sec
2	4, 5, 6	Every 2 sec
2	7, 8, 9	Every 3.5 sec
3	10, 11, 12	Every 8 sec

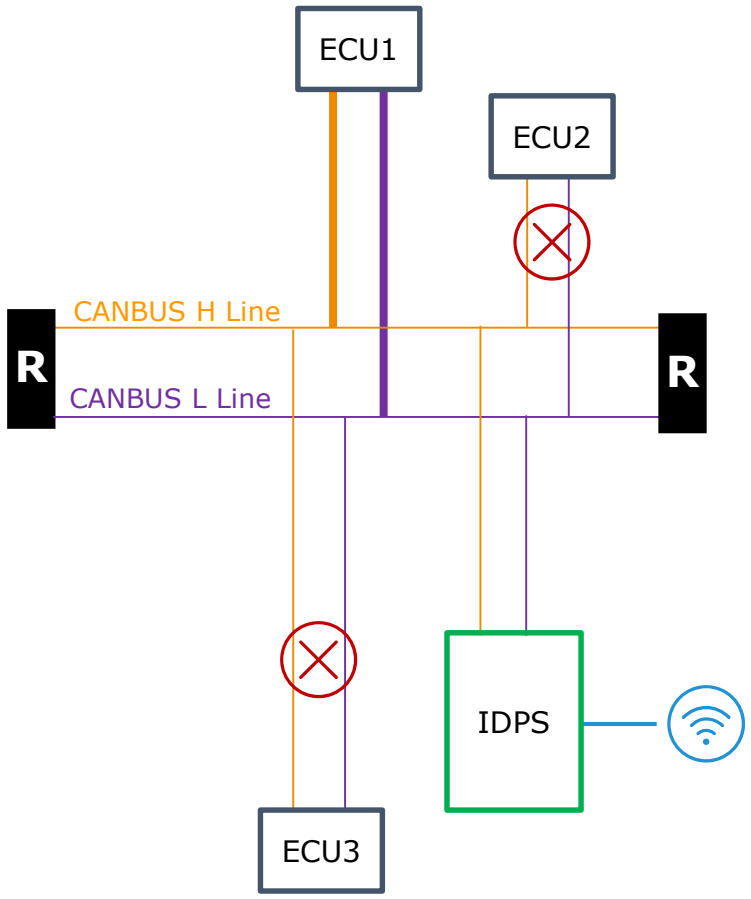
CAN message broadcast interval

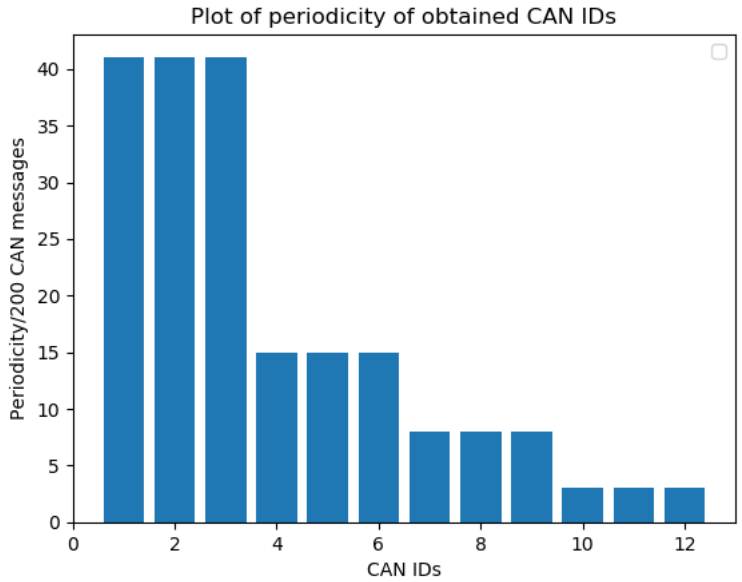


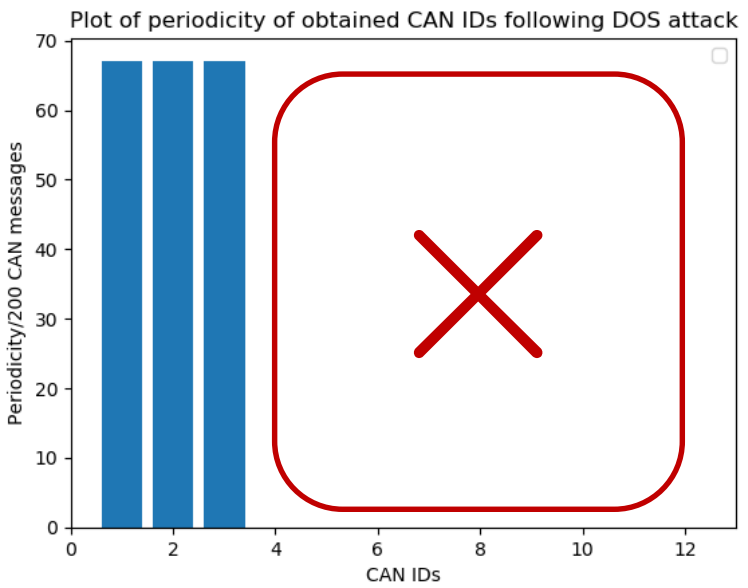
2020 Deloitte

Scenario 1: Denial of Service/ CAN flooding

Assuming ECU1 dominates the bus and prevents other nodes to send messages

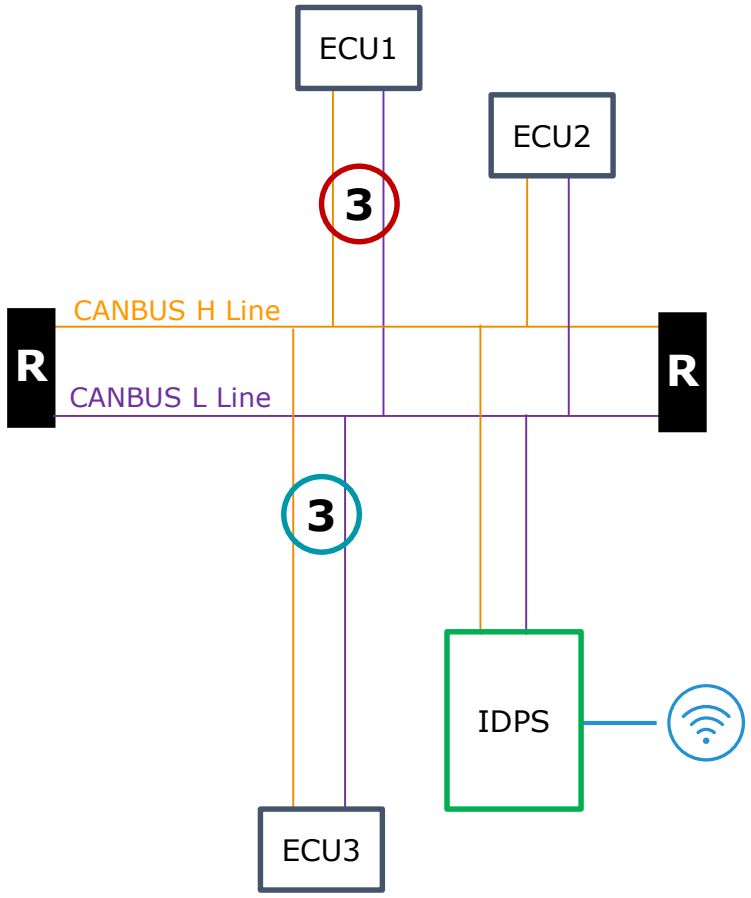


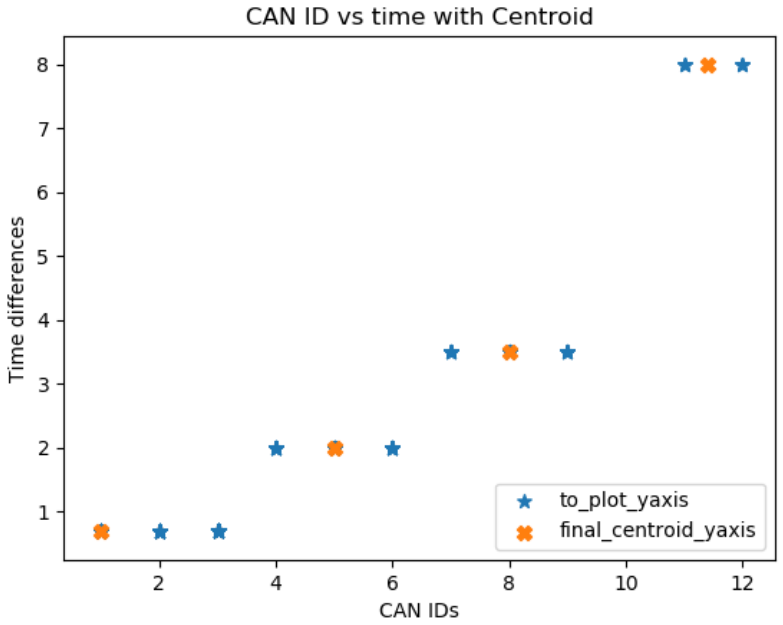


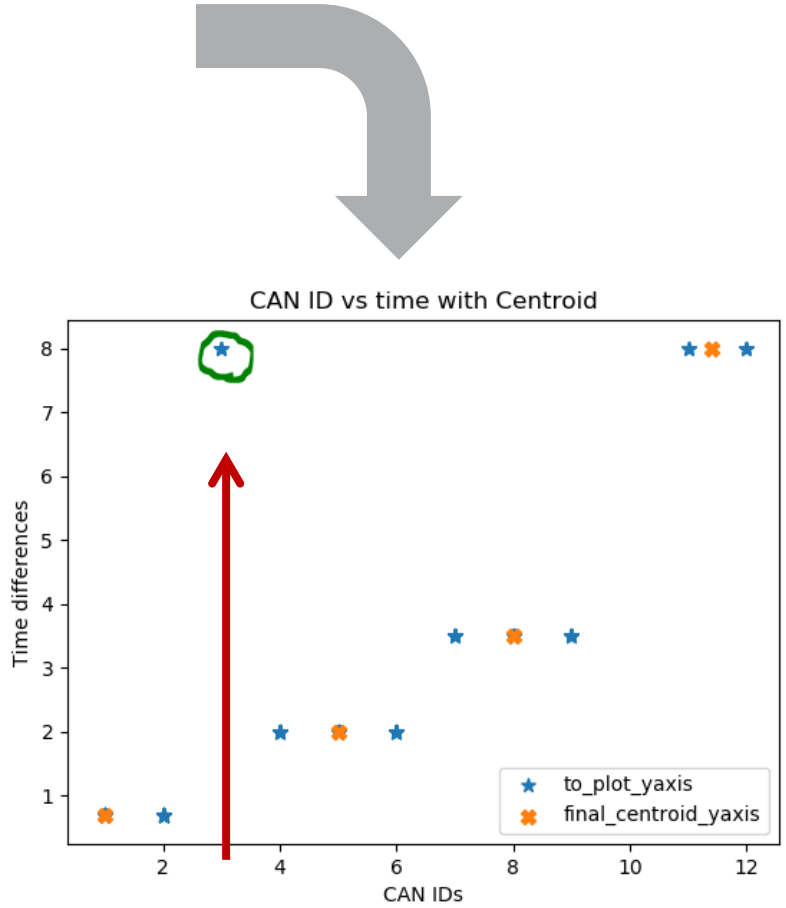


Scenario 2: Man in Middle/ Suspension/ Replay

Assuming message from ECU1 is suspended and/ or replayed by ECU3







Author bio

Part of Deloitte Germany automotive cyber risk team

About the author

Nishant Khadria
Senior Manager
Cyber Risk Automotive

Deloitte GmbH
Wirtschaftsprüfungsgesellschaft
Aegidientorplatz 2a
30159 Hannover
Deutschland

Phone: +49 (0)511 3023 4386
Mobile: +49 (0)151 5807 3554
nkhadria@deloitte.de

Summary of Professional Experience

Nishant has over 20 years of experience in the automotive industry with focus on vehicle security, software quality, supplier management, and vehicle monitoring serving automotive OEMs and suppliers across the globe. He has deep understanding of software development lifecycle and has reviewed use cases, requirements, architecture, design and tests to ensure timely implementation. He has been key contact between OEMs and their suppliers to bridge technical gap and establish security measures. He has been leading AUTOSAR team in Deloitte.

Education, Trainings and Certificates

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

Ingo Dasssow
Director
Lead EMEA Cyber Risk Automotive

Deloitte GmbH
Wirtschaftsprüfungsgesellschaft
Kurfürstendamm 23
10719 Berlin
Deutschland

Phone: +49 (0)30 25468 451
Mobile: +49 (0)151 5800 1451
idassow@deloitte.de

Summary of Professional Experience

Ingo Dassow is responsible for the implementation of management systems for clients in the automotive industry. He supports for example the implementation of a group policy management system for IT architecture as well as the implementation of a group-wide ISMS. He also gained additional expertise in the automotive sector in the areas of information security, enterprise architecture and mobile on-line services in the last five years. For a German automotive OEM he is responsible for the implementation of an ISMS in the E/E function and runs a project for vulnerability assessments vehicles architecture.

Education, Trainings and Certificates

- Diplom-Kaufmann with focus on Information Management, Uni Lüneburg
- ISO 27001 Lead Implementer/ Lead Auditor

2020 Deloitte

Deloitte.

This presentation contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited ("DTTL"), any of DTTL's member firms, or any of the foregoing's affiliates (collectively, the "Deloitte Network") are, by means of this presentation, rendering professional advice or services. In particular this presentation cannot be used as a substitute for such professional advice. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this presentation. This presentation is to be treated confidential. Any disclosure to third parties - in whole or in part – is subject to our prior written consent.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 312,000 professionals are committed to making an impact that matters.