SECURING CONNECTED AUTONOMOUS VEHICLES AS AN INDUSTRY.

GLOBAL COLLABORATION OPPORTUNITIES FOR COMPETITORS.

Tobias Gaertner | 12.02.2021

IEEE MaaS Virtual Workshop
“Standards for Trustworthy Autonomous Vehicles“

BMW GROUP

MINI

ROLLS-ROYCE
MOTOR CARS NA LLC

YOUR SPEAKER.

Tobias Gaertner

Current Position

- Vehicle Cybersecurity Specialist
  - US Incident Response and Information Exchange between BMW’s US and German engineering teams, PoC for the Auto-ISAC and all automotive cybersecurity topics

Past Positions

- Penetration testing and auditing of BMW’s infotainment systems at BMW AG, Munich
  - Supported BMW’s ramp-up of automotive cybersecurity capabilities and developed new processes for security testing
- BMW infotainment system testing department
- Joined BMW Group for Diploma thesis in August 2011

Education

- Diploma Degree in Computer Systems Engineering from TU Braunschweig, Germany
- CISSP – Certified Information System Security Professional
- OSCP – Offensive Security Certified Professional

MEGA TRENDS RAISE FUNCTIONALITY & CONVENIENCE BUT INCREASE SYSTEM COMPLEXITY AND ATTACK SURFACE.

Autonomous

Connected

Electrified

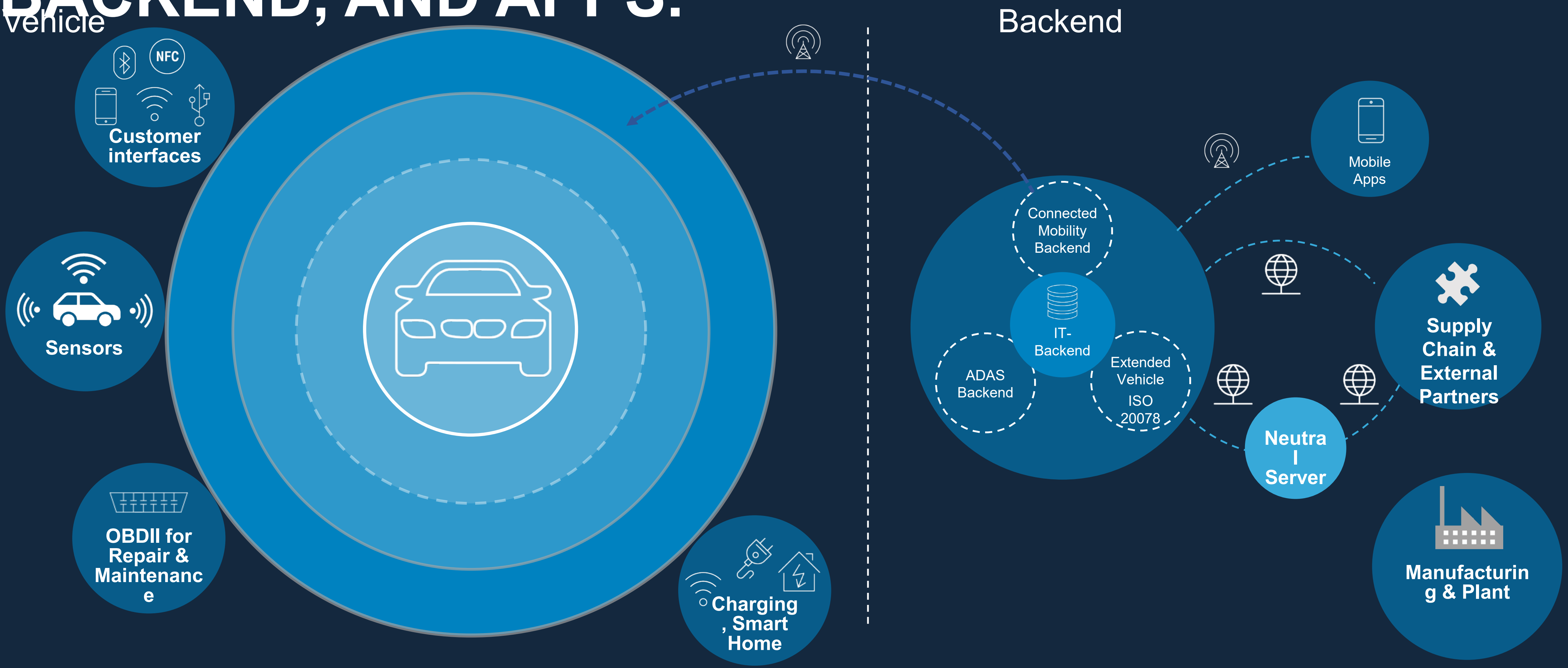
Shared

→ Autonomous driving requires massive onboard data processing and broadband communication to IT backend systems.

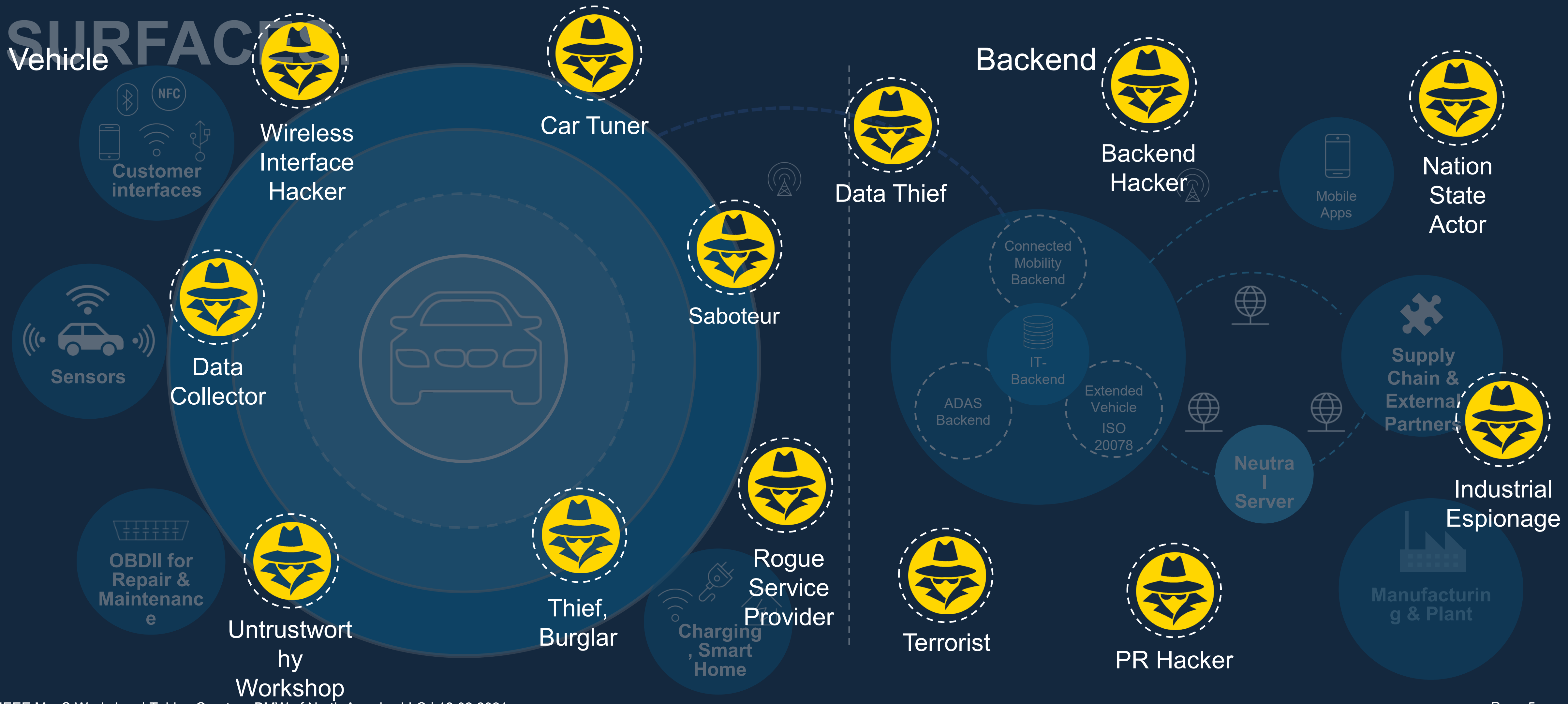
→ New mobility functions need a multitude of new interfaces.

→ Increasing system complexity and interdependence enlarges the attack surface.

THE VEHICLE ECOSYSTEM INCLUDES THE VEHICLE, ITS INTERFACES & COMPONENTS, THE IT BACKEND, AND APPS.



ATTACKERS THREATEN THE VEHICLE ECOSYSTEM AND ACTIVELY SEARCH FOR NEW ATTACK SURFACES



Vehicle

NFC

Customer interfaces

Sensors

OBDII for Repair & Maintenance

Wireless Interface Hacker

Car Tuner

Data Collector

Saboteur

Untrustworthy Workshop

Thief, Burglar

Rogue Service Provider

Charging, Smart Home

Backend

Data Thief

Backend Hacker

Mobile Apps

Nation State Actor

Connected Mobility Backend

IT-Backend

ADAS Backend

Extended Vehicle ISO 20078

Supply Chain & External Partners

Neutral Server

Industrial Espionage

Manufacturing & Plant

Terrorist

PR Hacker

COLLABORATION ON CYBERSECURITY IN A HIGHLY COMPETITIVE INDUSTRY TO OVERCOME CHALLENGES.

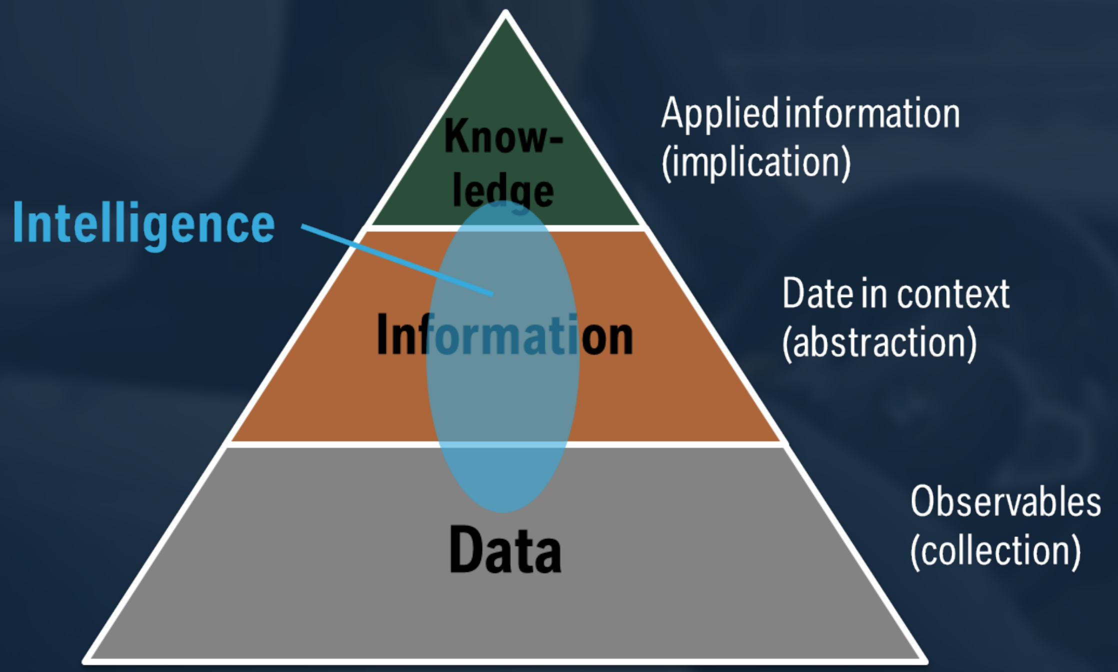
- Automotive has a complex supply chain
- “Attack on one of us is an attack on all of us”
- Automotive companies are mostly global
- Contrast of “cybersecurity ownership” and “vehicle ownershi
- Attackers collaborate too (e.g. they trade exploits and credentials)

London Marathon 2017

Source: https://www.bbc.com/news/health-43583620

> **“It’s good to learn from your mistakes. It’s better to learn from other people’s mistakes”**
>
> – Warren Buffet

THREAT INTELLIGENCE HELPS THE INDUSTRY TO DESIGN APPROPRIATE SECURITY MEASURES.

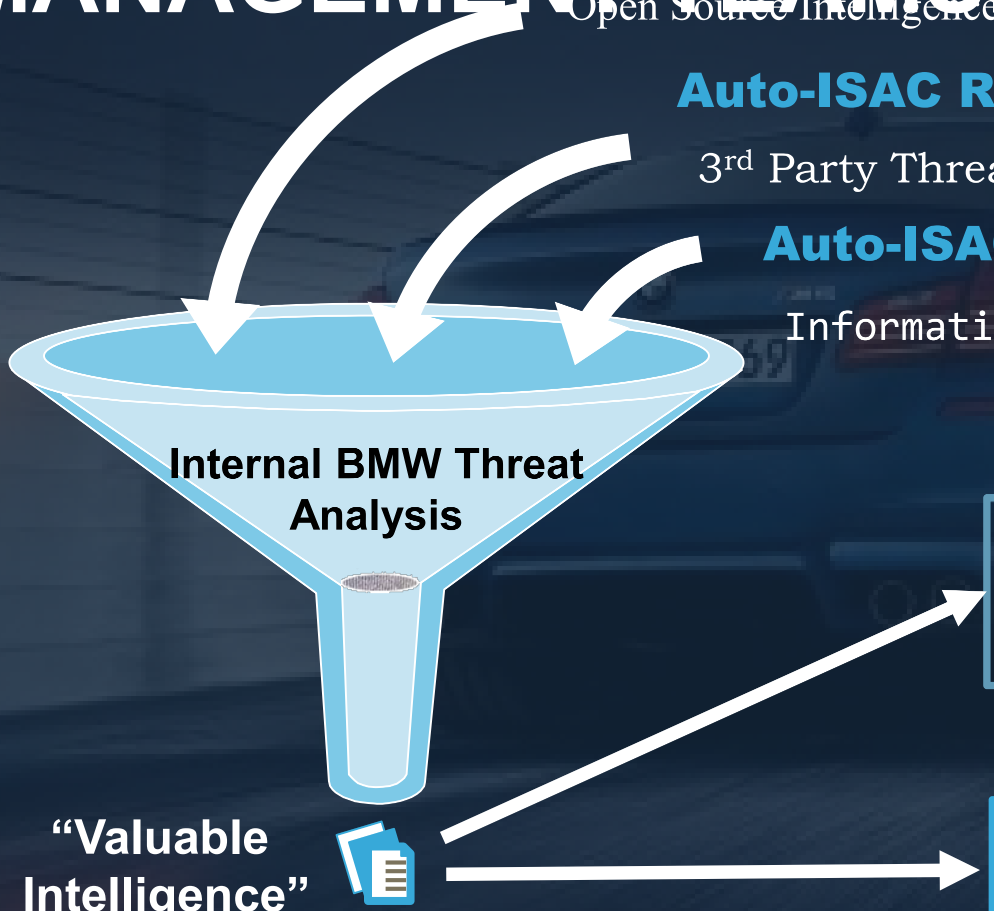

Know-ledge
Intelligence
Information
Data
Applied information (implication)
Date in context (abstraction)
Observables (collection)

Threat Intelligence Analysis helps us to understand attacks, attackers and improves overall vehicle security.

Some Lessons Learned:

- **Collect** and **process cyber-intelligence** to improve your product's defense to find specific answers.
- Hybrid skillsets for the "Automotive Cybersecurity Intelligence Analyst" are needed.
- Be **open** to talk to ethical researchers and have a **vulnerability disclosure or bug bounty program**.
- **Stay-up-to-date** with threat reports, CVEs, CERT newsletters and vulnerability notifications, etc.
- Categorize attacks and attack paths to detect

CYBERSECURITY INTELLIGENCE FEEDS INTO SECURITY ENGINEERING AND INCIDENT MANAGEMENT TEAMS



Open Source Intelligence (OSINT)

Auto-ISAC RED Platform

3rd Party Threat Intelligence Providers

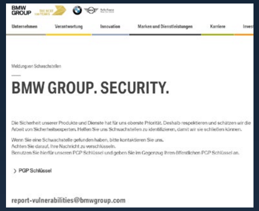
Auto-ISAC Intelligence Products

Information Security Conferences

Internal BMW Threat Analysis

“Valuable Intelligence”

BMW Vulnerability Disclosure Program



Meldung von Schwachstellen

BMW GROUP. SECURITY.

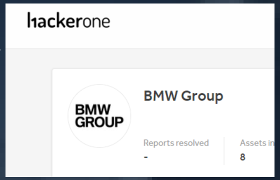
Die Sicherheit unserer Produkte und Dienste hat für uns oberste Priorität. Deshalb respektieren und schätzen wir die Arbeit von Sicherheitsexperten. Helfen Sie uns Schwachstellen zu identifizieren, damit wir sie schließen können.

Wenn Sie eine Schwachstelle gefunden haben, bitte kontaktieren Sie uns.
Achten Sie darauf, Ihre Nachricht zu verschlüsseln.
Benutzen Sie hierfür unseren PGP Schlüssel und geben Sie im Gegenzug Ihren öffentlichen PGP Schlüssel an.

> PGP Schlüssel

report-vulnerabilities@bmwgroup.com

BMW Bug Bounty Program



BMW Group

Reports resolved
-

Assets in
8

Automotive Security Engineers
for improved future vehicle security architecture and defense against specific threats

Automotive Incident Response Team
for further investigations and remediation

“Feedback loop”
as required by UN-ECE WP.29, NHTSA AV Guidelines, ISO/SAE 21434 standard, etc.

THE AUTOMOTIVE INFORMATION SHARING & ANALYSIS CENTER FACILITATES INDUSTRY COLLABORATION.

Originates

in 1998 President Clinton issued Critical Infrastructure Protection (PDD-63), that aimed to raise the national critical infrastructure's resilience (85% privately owned) against cyber-attacks

AUTO-ISAC

Automotive Information Sharing and Analysis Center

NHTSA pushed the industry in 2015 to develop automotive cyber-security best-practices, Auto Alliance decided to form an ISAC, BMW Group is one of its founding members, Jeep hack accelerated foundation

56 Auto-ISAC Members

Most US-based OEMs and Suppliers, Strong Partnership Program with private and public sector, Global Expansion ongoing with Focus on European Stakeholders

ISAC's for Multiple Sectors

24 ISAC's exist today, such as Financial, Energy, Aviation, etc.

What is an ISAC?

ISACs are private non-profit organizations that provide trusted information exchanges in a private-public partnership

What is shared?

Sector-specific information about physical and cyber-threats, Vulnerabilities, Incidents on a voluntarily basis, Industry Best practices, Online Collaboration Platform, Workshops, Table-top Exercises, Templates, etc.

Compliance

Auto-ISAC and its members strictly comply with global anti-trust laws. A Legal Working Group advises

Membership important for BMW

NHTSA recommends vehicle manufacturers in its best-practices to exchange cybersecurity-relevant information within the industry and refers to Auto-ISAC's Best Practice Guides

THE AUTO-ISAC STRENGTHENS BMW GROUP.

Best Automotive Threat Intelligence Source

Fast-growing & Expanding Community

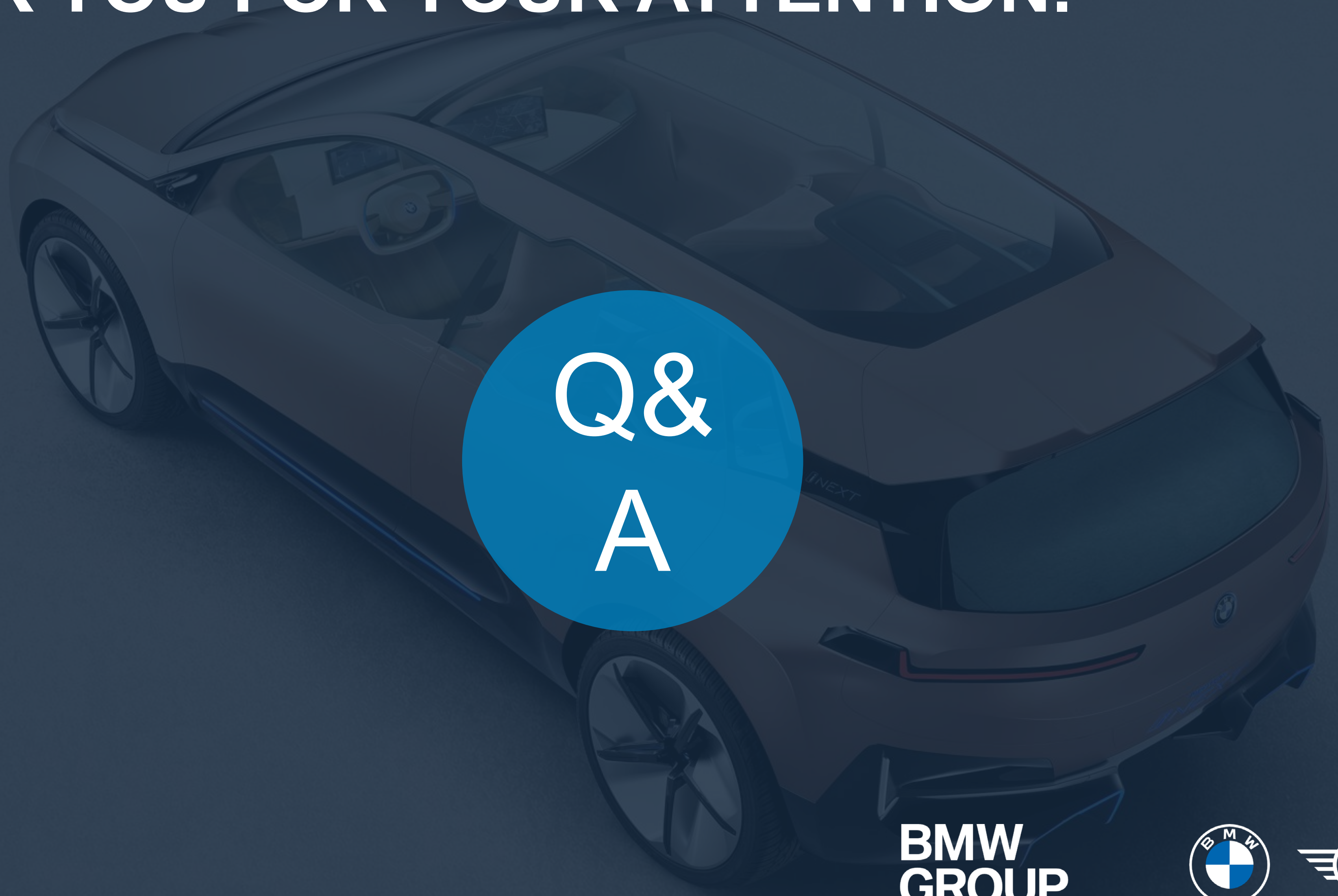
Best Practice Guides

PIRs & Playbooks

Interesting Projects & Events

Members-teach-Members Workshops

THANK YOU FOR YOUR ATTENTION.



Q&
A