DefCamp where hacking & security collide Cluj Napoca

Many thanks to our sponsors and partners!

Powered by orange™

PLATINUM SPONSORS

BIT SENTINEL

3CYBER

CYBER LIFE HACKS

HACKING VILLAGE PARTNERS

cyber EDU

electron

HACKOUT Portalul Atacurilor Cibernetice

SILVER SPONSORS

efect

PFG FINANCE

wantsome the friendly IT academy

MOBILITY PARTNER

TOYOTA Cluj-Napoca prin Profi Auto

COMMUNITY & MEDIA PARTNERS

GUVERNUL ROMÂNIEI DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

CLUJ IT

UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

BRCC British Romanian Chamber of Commerce

ISACA Trust in, and value from, information systems Romania Chapter

(ISC)² CHAPTER ROMANIA

CLOUD SECURITY ALLIANCE OFFICIAL CHAPTER Romania Chapter CSA

CARTEA DALIEI

x86 GENERATION

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION ROMANIA

ȘCOALA INFORMALĂ DE IT®

TSM TODAY SOFTWARE MAGAZINE

DevExperience

ITCAMP

MOBZINE.RO

SecurityPatch

ROTSA The highway of Romanian Tech Startups

techcelerator

DRIVING FORWARD

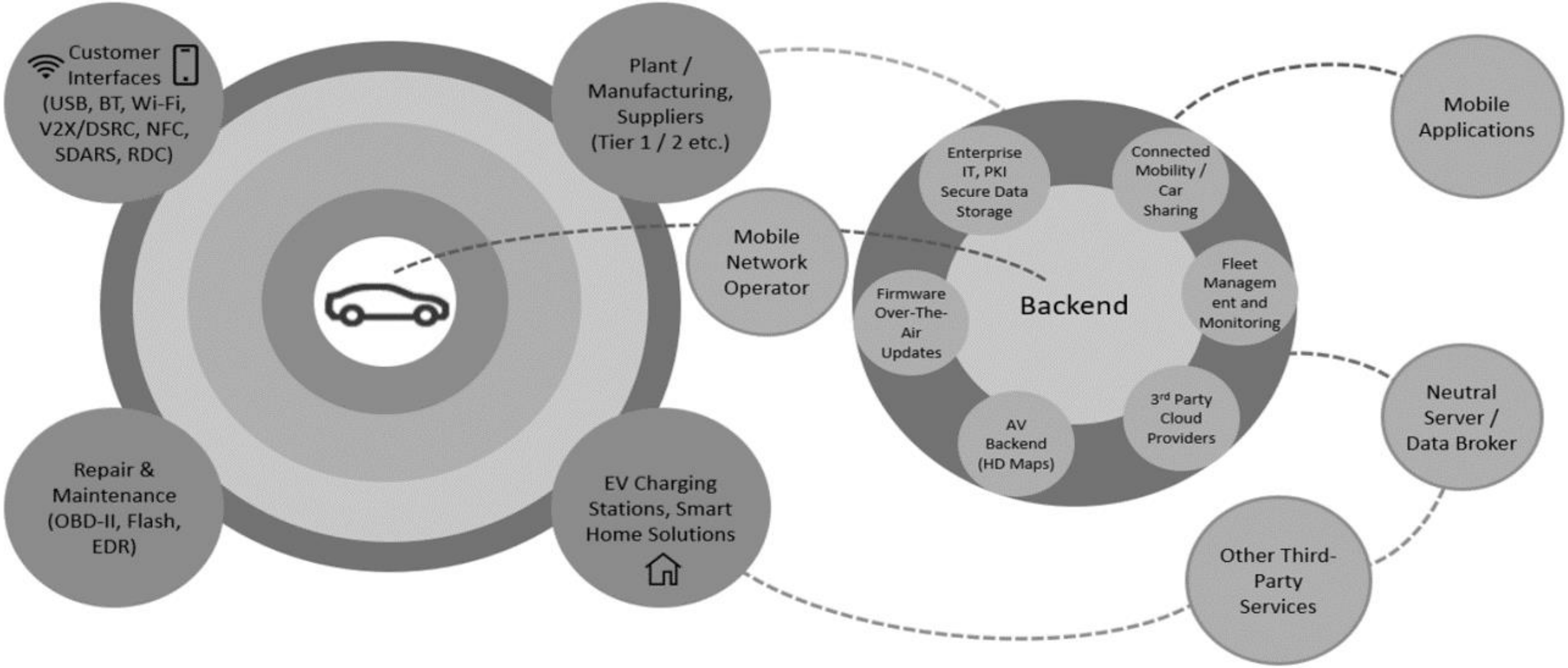
Automotive Security in the Digital Era

MARIUS STRATILA,
Sr. Technology Consultant,
Cybersecurity,
BearingPoint

> “We can call them cars, or we can call them laptops on wheels”

Anthony Battle, JLR’s chief digital officer,
The Times, 14th Jan 2023

The Automotive Ecosystem


Customer Interfaces (USB, BT, Wi-Fi, V2X/DSRC, NFC, SDARS, RDC)
Plant / Manufacturing, Suppliers (Tier 1 / 2 etc.)
Mobile Network Operator
Repair & Maintenance (OBD-II, Flash, EDR)
EV Charging Stations, Smart Home Solutions
Backend
Enterprise IT, PKI Secure Data Storage
Connected Mobility / Car Sharing
Fleet Management and Monitoring
Firmware Over-The-Air Updates
AV Backend (HD Maps)
3rd Party Cloud Providers
Mobile Applications
Neutral Server / Data Broker
Other Third-Party Services

Source: Automotive ISAC

Essential Aspects within Automotive

SAFETY-CRITICAL SYSTEMS

Systems prioritizes safety for drivers & road users. Ensures reliability during accidents, manoeuvres & extreme weather.

SHARED COMPONENTS

Extensive ECU reuse leads to potential vulnerabilities affecting both older and new vehicle models.

LONG LIFECYCLE / CONSUMER USAGE

OEMs invest 3-4 years in new products, supporting security for years even after production ends. Challenge: maintaining security over 8+ year lifespan.

HIGHLY COMPLEX SYSTEMS

Modern vehicles with numerous ECUs and complex networks pose challenges: rising software, multiple OS, real-time demands, and availability needs.

HIGHLY CONSTRAINED OPERATIONAL PARAMETERS

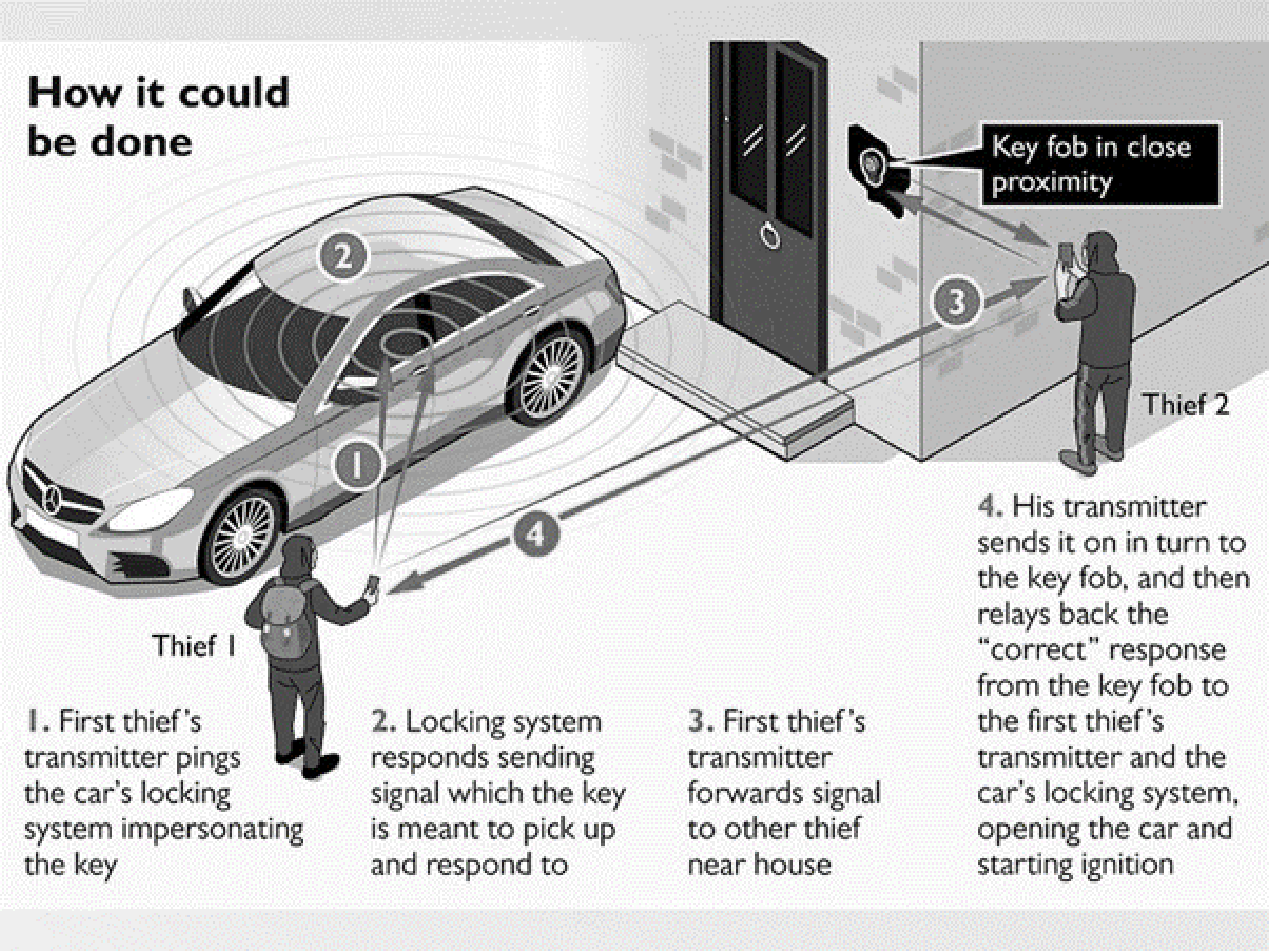
Post-production countermeasures pose challenges: limited computing power, diverse owners, varied repair centres, and updates not guaranteed.

COMPLEX SUPPLY CHAIN

Product development involves multiple global suppliers with various tiers. Concurrently, Tier 1 suppliers and OEMs develop multiple vehicle ECUs.

REAL-WORLD AUTOMOTIVE CYBERCRIME CASE

Source: CNN Youtube



How it could be done

1. First thief's transmitter pings the car's locking system impersonating the key

2. Locking system responds sending signal which the key is meant to pick up and respond to

3. First thief's transmitter forwards signal to other thief near house

4. His transmitter sends it on in turn to the key fob, and then relays back the "correct" response from the key fob to the first thief's transmitter and the car's locking system, opening the car and starting ignition

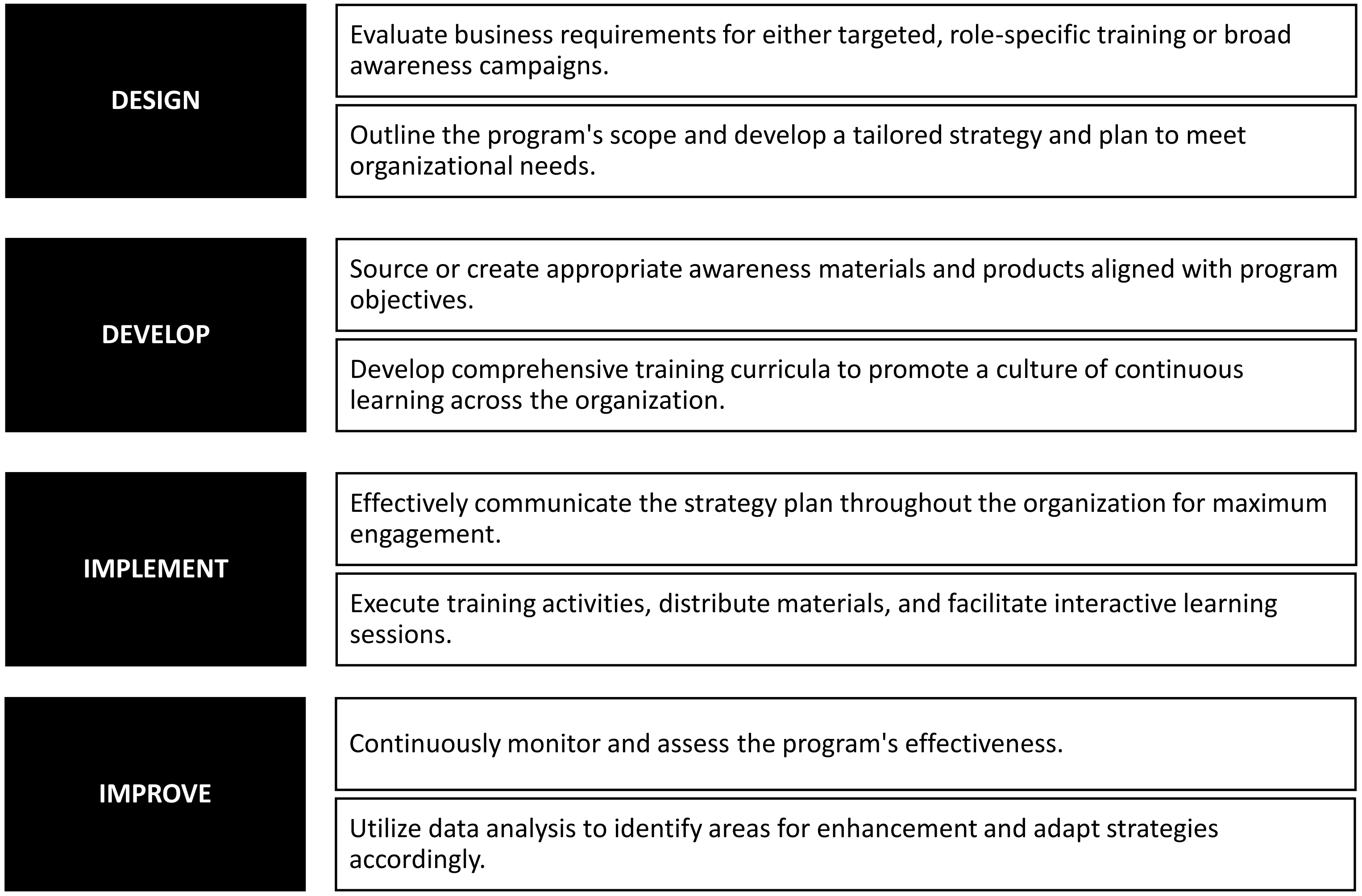
Source: CBC

Cybersecurity Defense: Customer & OEM Actions

What Customers Can Do	Physical barriers can be added by utilizing a steering wheel lock.
	Shield electronic key fob signals using Faraday-style devices.
	Place your key fob at a considerable distance from exterior walls and doors.
	Consider purchasing a tracking device.
	Double-check the car to ensure its locked.
What OEMs Can Do	Enhance security with an additional layer of protection: a unique code to start the car.
	Implement a sleep mode feature where the key fob automatically switches off after a few seconds.
	Incorporate a physical button on the key fob for easy on/off switching.

INTEGRATING CYBERSECURITY IN AUTOMOTIVE

Promoting Cybersecurity Through Training and Awareness



DESIGN

- Evaluate business requirements for either targeted, role-specific training or broad awareness campaigns.
- Outline the program's scope and develop a tailored strategy and plan to meet organizational needs.

DEVELOP

- Source or create appropriate awareness materials and products aligned with program objectives.
- Develop comprehensive training curricula to promote a culture of continuous learning across the organization.

IMPLEMENT

- Effectively communicate the strategy plan throughout the organization for maximum engagement.
- Execute training activities, distribute materials, and facilitate interactive learning sessions.

IMPROVE

- Continuously monitor and assess the program's effectiveness.
- Utilize data analysis to identify areas for enhancement and adapt strategies accordingly.

Strengthening Governance

DESIGNING PHASE

- Clearly define and communicate the program’s scope to all stakeholders.
- Articulate the mission and vision to align with organizational goals.
- Identify key functions essential for effective governance.

BUILDING PHASE

- Establish internal structures by activating leadership and assigning decision-making authorities.
- Foster collaboration across business units by integrating with key partners and setting communication expectations.

OPERATING PHASE

- Develop robust policies and processes to guide governance activities.
- Monitor performance using metrics to ensure accountability.
- Maintain transparent resource allocation processes for efficiency.

Finding and Mitigating Risks

SCOPE DEFINITION

Clearly outline the scope and requirements for implementing cyber risk assessment methodologies.

INTEGRATION

Seamlessly integrate security assessments into various stages of the vehicle or product lifecycle.

DOCUMENTATION

Clearly document roles and responsibilities to ensure clarity and accountability among stakeholders.

FREQUENCY DETERMINATION

Determine the optimal frequency for conducting risk assessments throughout the lifecycle.

RISK TOLERANCE PROFILING

Establish a formal risk tolerance profile to guide decision-making across lifecycle phases.

TREATMENT PLAN DEVELOPMENT

Develop methodologies for evaluating assessment results and devising appropriate risk treatment plans.

INTEGRATION AND COMPLIANCE

Integrate risk management processes into broader business operations governance and ensure adherence to standards.

Security Development Lifecycle

PRE-DEVELOPMENT	Consider existing system architectures and incorporate lessons learned from previous cycles. Define acceptable and unacceptable cyber risks for the final product.
DESIGN AND DEVELOPMENT PHASE	Develop comprehensive cybersecurity specifications tailored to component features. Ensure clear and testable requirements, understanding of threats, and utilization of mitigating architectures. Emphasize security in implementation through coding standards and analysis mechanisms. Conduct security testing and verification to ensure compliance with requirements and proper implementation of security principles.
POST-DEVELOPMENT	Monitor cybersecurity issues during vehicle operations and maintenance to inform continuous improvements in security.

Proactive Threat Detection and Incident Response

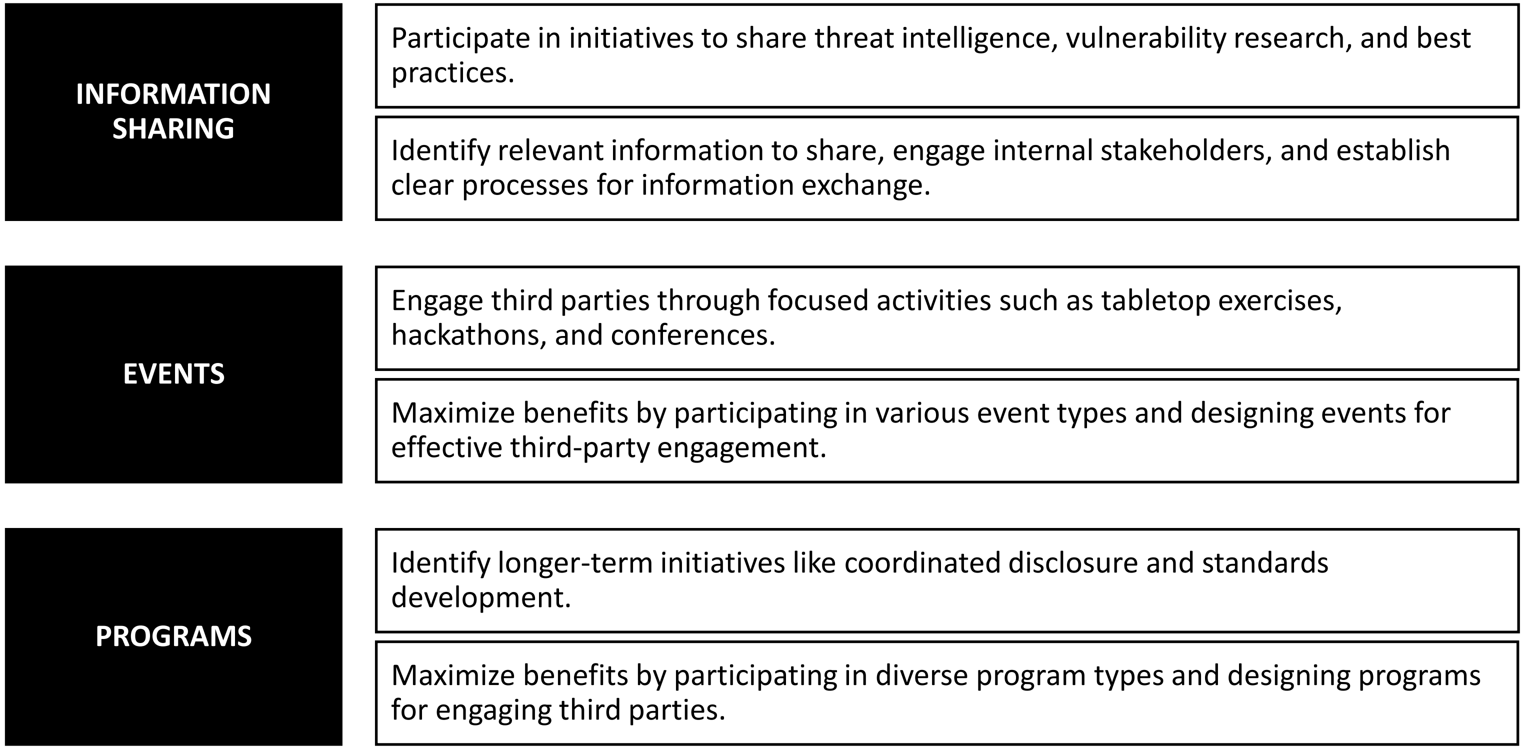
THREAT DETECTION

- Define a comprehensive threat detection and analysis process, understanding the automotive threat landscape and establishing stakeholder roles.
- Determine threat intelligence requirements for identifying sources and collection processes.
- Establish a robust threat monitoring process, prioritizing activities and employing various techniques.
- Develop a systematic threat analysis methodology, including identification, validation, verification, and necessary actions.
- Implement a process and acquire appropriate tools for organizing, storing, and sharing threat information effectively.

INCIDENT RESPONSE

- Prepare by documenting plans, establishing roles, and conducting exercises and training for efficient response.
- Quickly identify incidents through validation, classification, and escalation using severity matrices and clear protocols.
- Rapidly contain, mitigate, remediate, and recover from incidents through technical and corporate response activities.
- Close each incident by conducting debriefs, implementing long-term remediation actions, and updating response plans.

Collaboration and Engagement with Appropriate Third Parties



INFORMATION SHARING

- Participate in initiatives to share threat intelligence, vulnerability research, and best practices.
- Identify relevant information to share, engage internal stakeholders, and establish clear processes for information exchange.

EVENTS

- Engage third parties through focused activities such as tabletop exercises, hackathons, and conferences.
- Maximize benefits by participating in various event types and designing events for effective third-party engagement.

PROGRAMS

- Identify longer-term initiatives like coordinated disclosure and standards development.
- Maximize benefits by participating in diverse program types and designing programs for engaging third parties.

Q&A.
Thank you!