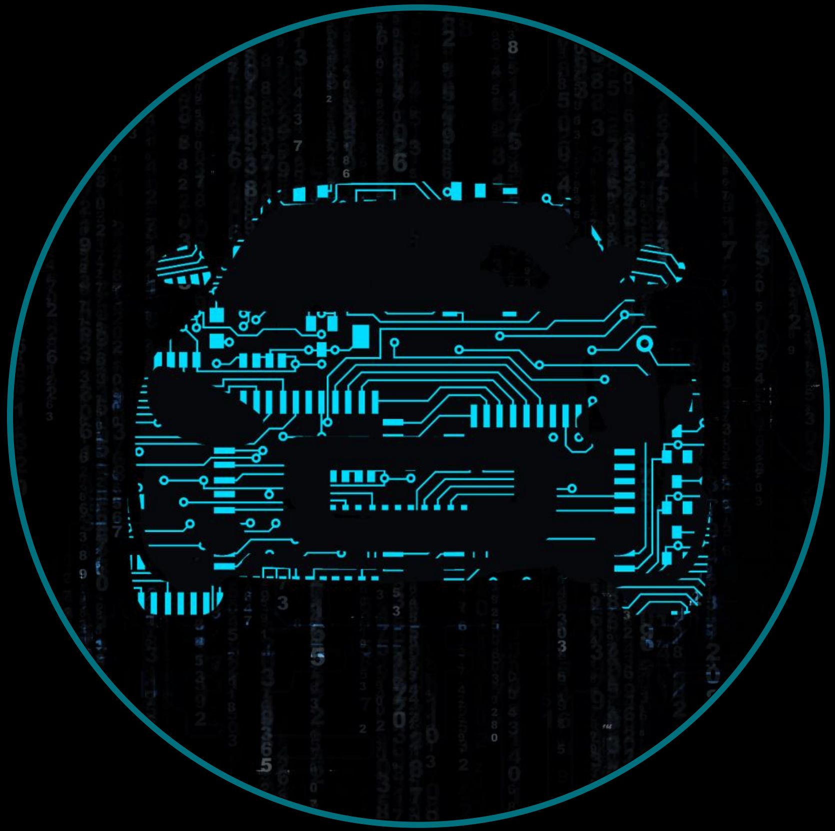
Deloitte.



Automotive Fleet SIEM

Essential requirement for product security

László Tóth - Automotive Cyber security

Deloitte 2018

Agenda

The challenge

Introduction to Fleet SIEM

Fleet SIEM - A bird's-eye view

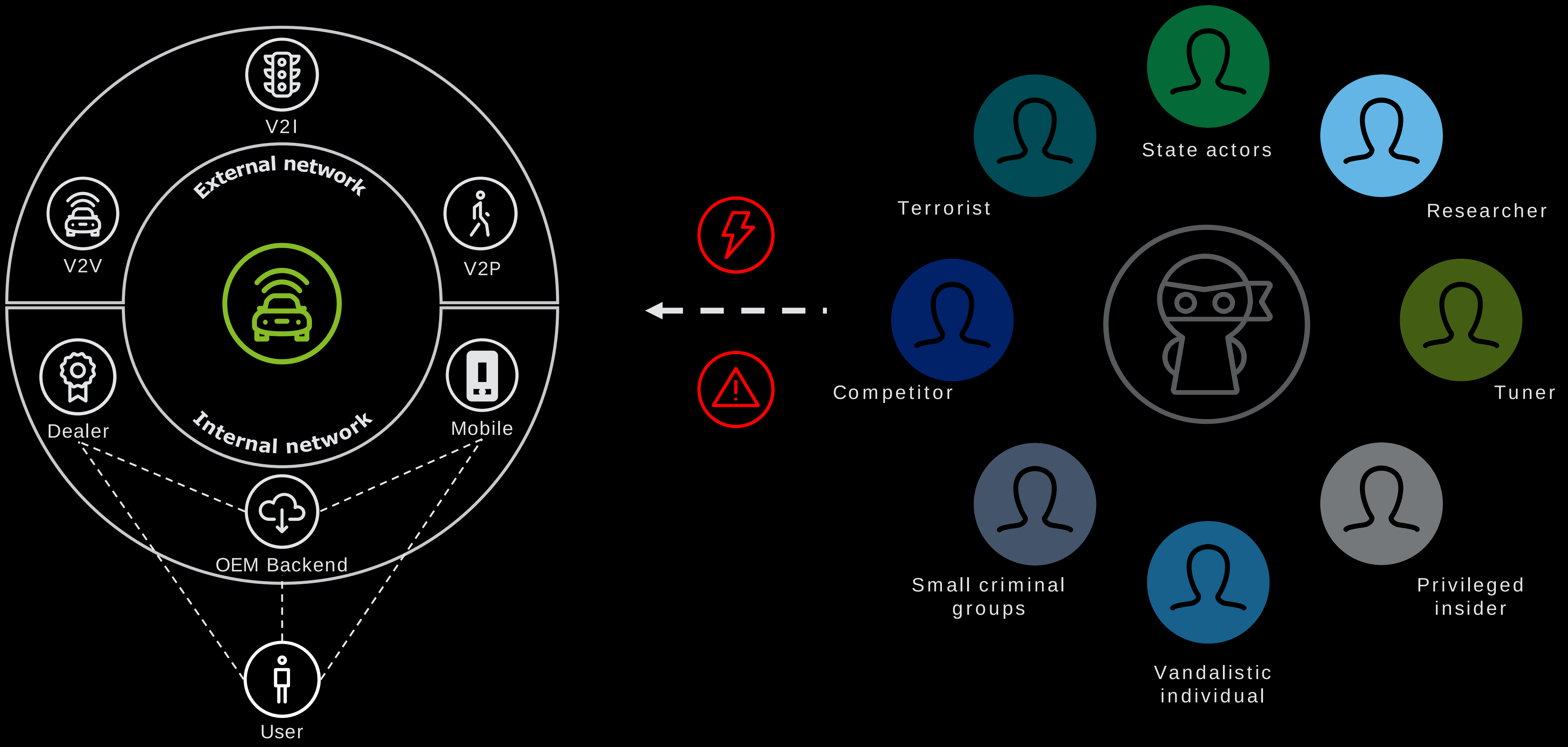
Contacts

The challenge

With connected functionalities, attack surface is much wider than it seems

Connected vehicle infrastructure

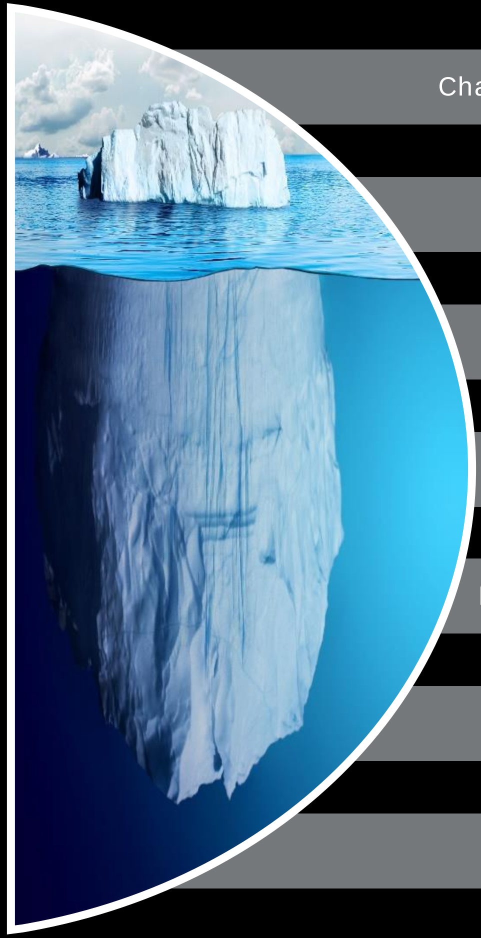
Each external or internal interface opens door for potential attack



Threat landscape for connected vehicles

The attack surface is much bigger than it seems…

Researches have proven existing vulnerabilities



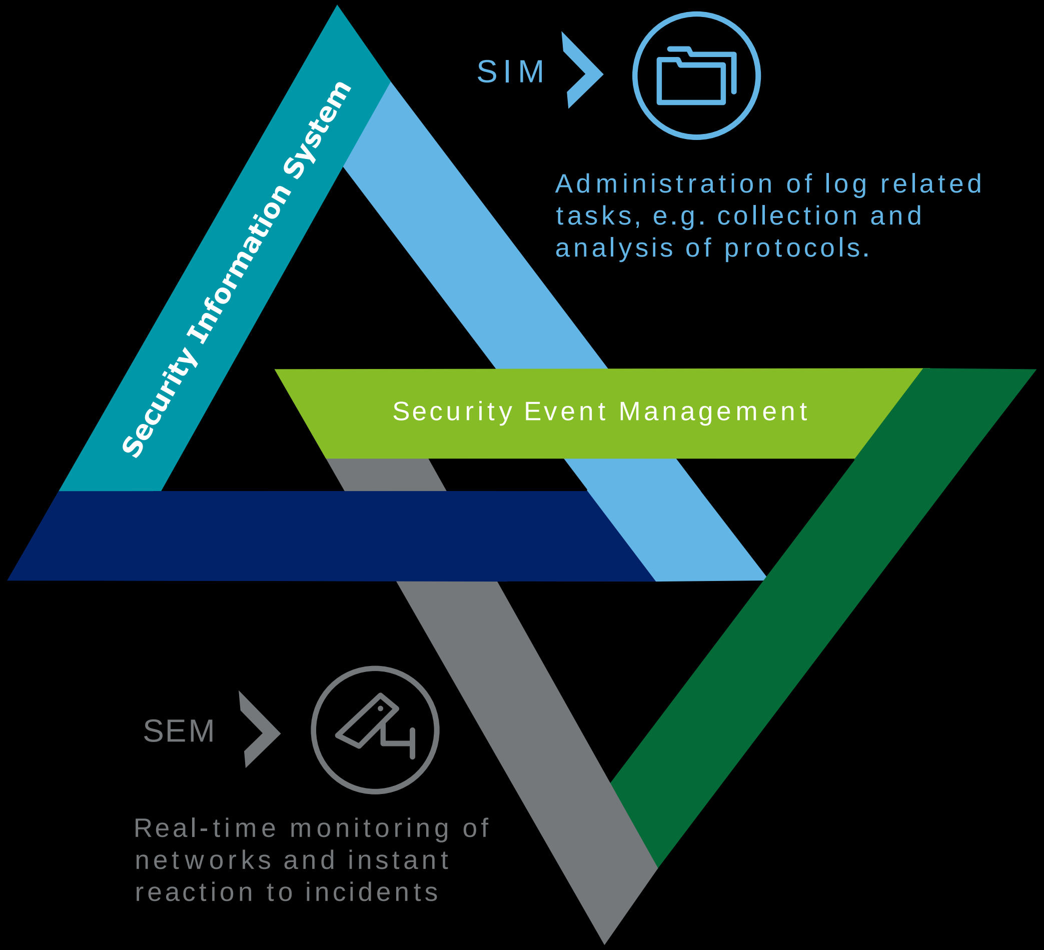
Charlie Miller, Chris Valasek, whitepaper 2015	Possible to control vehicle remotely	Improper segregation and vulnerable service on IVI of the vehicle	Send CAN message as a result of hardware hacking and reverse engineering techniques
Samy Kamar, DefCon 2015	Possible to steal credentials and open vehicle	Man-in-the-Middle attack between mobile app and the backend	SSL protection, however, server certificate validation was not implemented
Troy Hunt, 2014	Possible to call APIs, used by the mobile application, without authentication	Only VIN was necessary	Providing VIN number exposed all vehicle relevant information through the interface
Ken Munro & Dave Lodge, 2016	Possible to turn off theft alarm	Mobile app connected to the vehicle over WiFi using predictable WPA PSK, which made brute force possible	The mobile app used a binary protocol without any authentication
Michael, Shkatov, Bazhaniuk, DefCon 2017	It was possible to locate vehicles	A domain given up by the OEM which was used by a backend system for vehicles	Registering the domain name, vehicles tried to connect to a URL on the domain name
Duncan Woodbury, Nicholas Haltmeyer	Linux-Stack Based V2X Framework	SocketV2V could be used to hack connected vehicles	Emphasized the necessity to test V2X infrastructure, focusing on EU/US standards
Ron Ofir and Ofer Kapota, 2014	Remote attack on an aftermarket telematics service	The dongle used clear text over GPRS to connect to backend	Update files were not signed, backdoor could be installed

Introduction to Fleet SIEM

Process and components

SIEM – Definition, classification and components

Combined capabilities of SIM and SEM enables timely detection and efficient response



SIM

Administration of log related tasks, e.g. collection and analysis of protocols.

SEM

Real-time monitoring of networks and instant reaction to incidents

1 Collect

- Data collection from different sources e.g. vehicle, backend, external networks
- Long-term storage of aggregated log data to provide the retention necessary to fulfill compliance requirement

2 Correlate

- Correlating different data sources like log, threat intelligence, vulnerability and asset information
- Generating alarms based on implemented use cases

3 Recover

- Contain damage by shutting some services
- Patch affected systems/ components
- Bring business to normal

4 Report

- Generate KPI based management reporting
- Create compliance reports based on existing security, governance and audit processes
- Feedback in corporate strategy to strengthen security measures

Information eco system

A complex pool of data from various sources are available for analysis

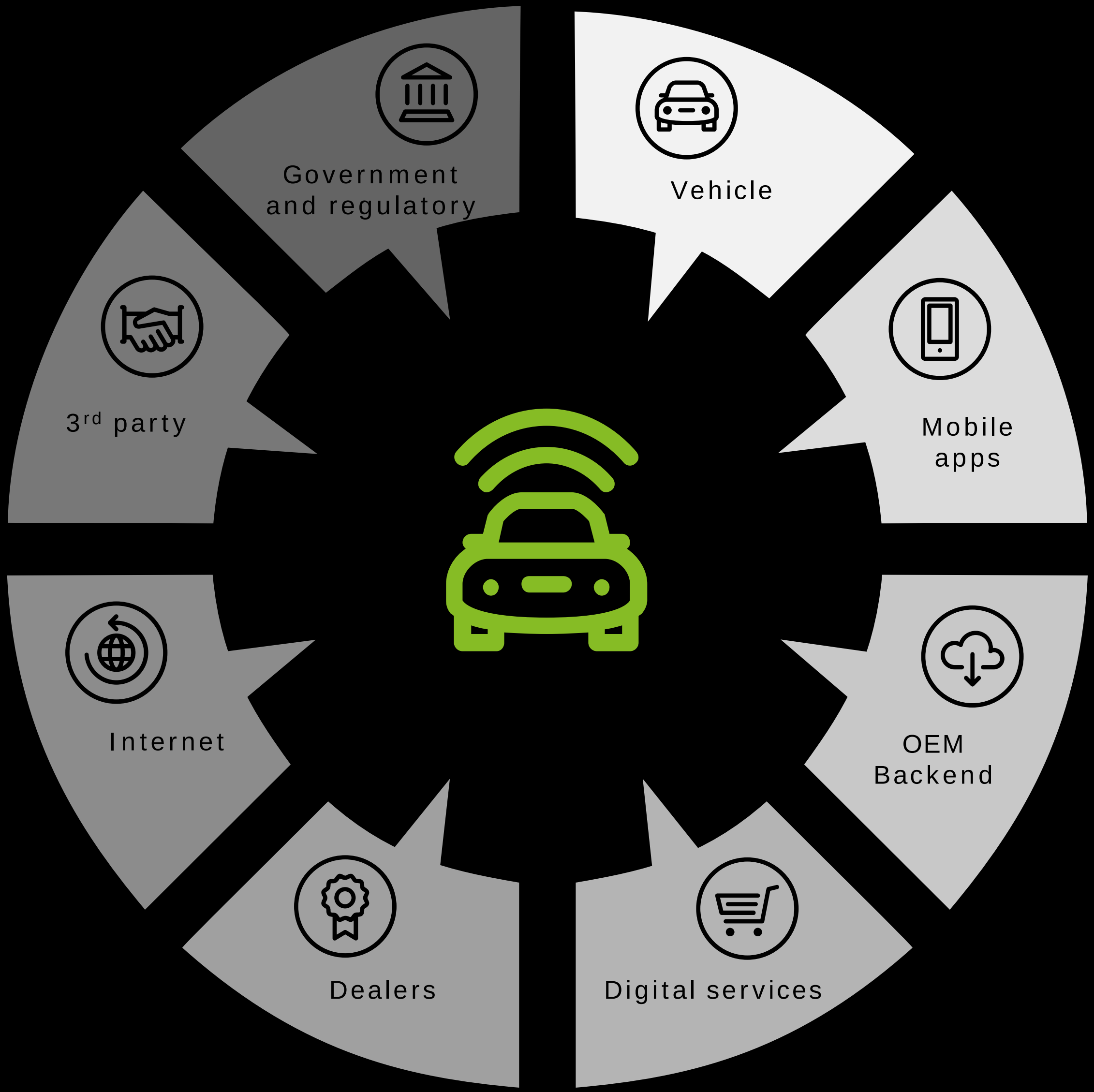
1 Collect

- Mandatory standards
- Legal compliance
- Known threats
- Activists database

- Vulnerabilities
- Use cases
- Threat intelligence

- Dark Net
- Hacking communities
- Social media
- News feeds

- Maintenance
- Car configuration
- Updated profile



- Infotainment
- Maintenance
- Errors
- V2X

- Driving behavior
- User preferences
- Backend access

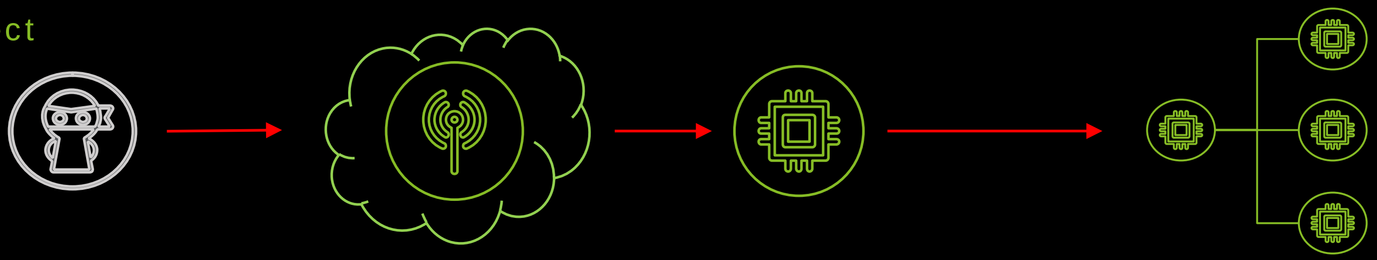
- Software configuration
- Hardware configuration
- Activated services
- Authentication matrix
- Spare parts and accessories

- Parking
- Car sharing
- Marketing

Example research results

Attack scenarios and affected components

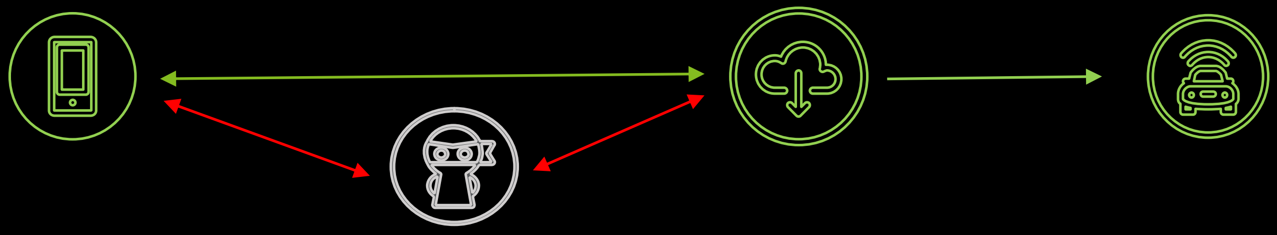
1 Collect



Backend system was not affected

In-vehicle buses were affected

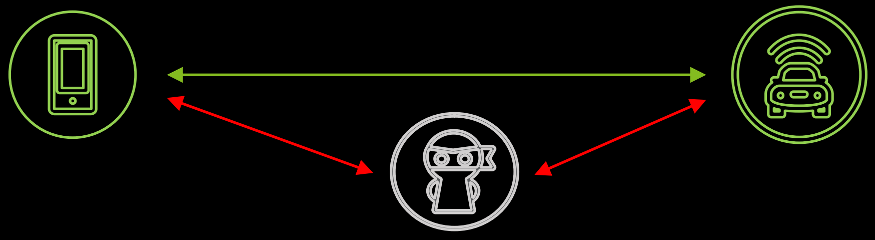
ECUs were affected



Vehicle saw only legitimate traffic

Backend system was affected

Mobile application was affected



Backend system was not affected

In-vehicle buses were not affected

In-vehicle Wi-Fi was affected

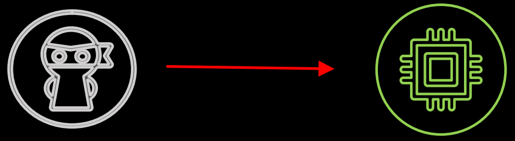
Mobile application was affected

2018 Deloitte

Example research results

Attack scenarios and affected components

1 Collect



There can be attack scenarios when just the infotainment system is affected and attacker is interested in the data stored there only

Infotainment system can run various operating system with various security architecture and application frameworks. For example:

AUTOMOTIVE GRADE LINUX

GENIVI

QNX

Analysing data to detect potential risks

Aritifical intelligence, machine learning and security analysts extract meaningful information from collected data

1

2 Correlate

Information derived from threat, risk and vulnerability analysis is used to identify and process security incidents.

Information collected about the underlying assets is important to calculate the associated risks.

Identifying new risks with the fleet is possible by correlating actual data sets with benchmarks or reference data (e.g. anomaly detection).

Newly discovered vulnerabilities can be used to create new use cases in order to take proactive measures.

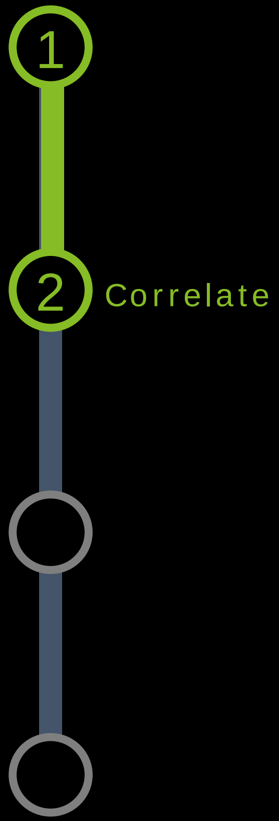
An efficient administration of identified vulnerabilities requires ongoing maintenance, attention and connecting with other processes

KPIs have an influence on evaluating the scope of vulnerabilities

A Security Operation Center (SOC) helps proceeding efficiently

Threat intelligence is significantly enhanced by using valid use cases

Through simulation with real time data, many attacks can be prevented



1

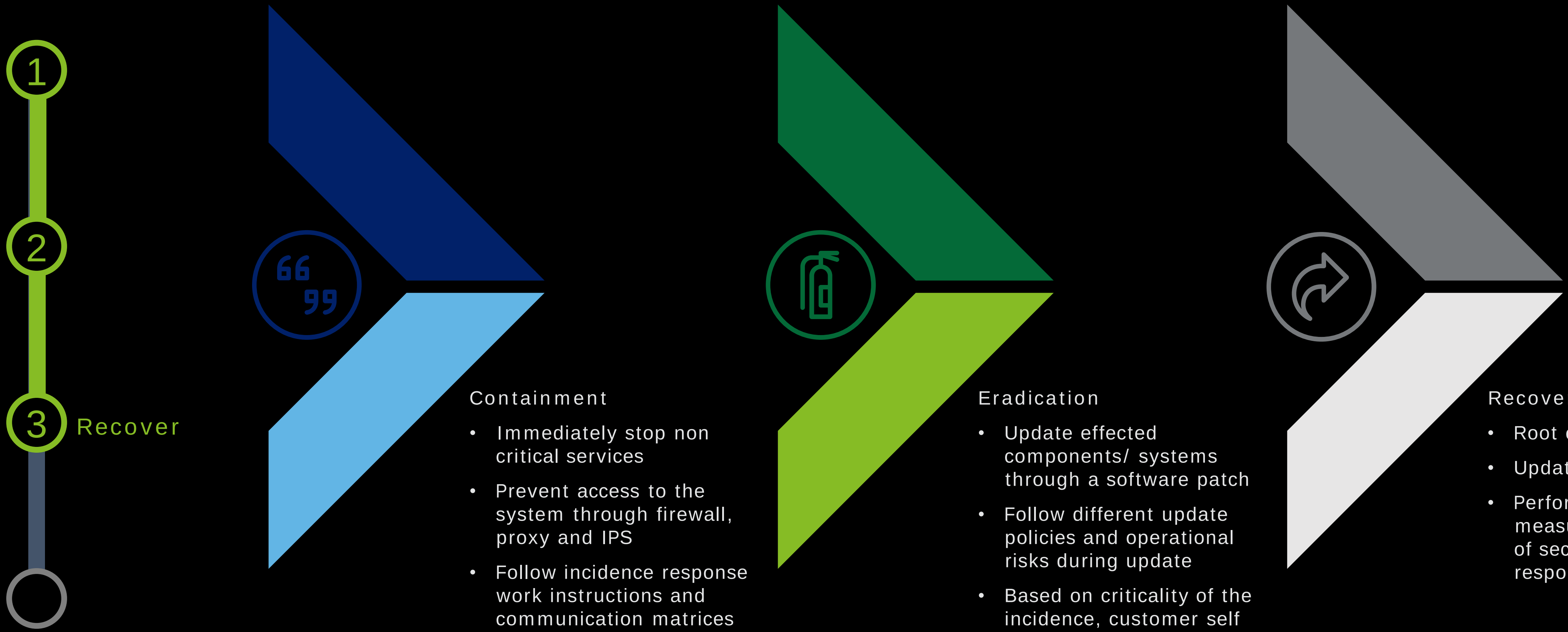
2 Correlate

Code injection to the infotainment system

Vulnerability	• Malicious code execution through a vulnerable service or application • Bypassing the security controls of the update process
Involved components	• Infotainment system • Gateway ECU • DCU/TCU
Stakeholder	• Driver and passengers • Supplier/ Producer of the infotainment system • FOTA update engineering team
Threat vector	• Wireless connectivity via Bluetooth, GPS, GSM, WiFi • Physical connections via USB, CD, SD-Cards or OBDII
Impact	• Spoofing or DoS-attacks on ECUs • Unauthorized access to sensitive information • Reputation damage • Enabling restricted features
Log sources	• Privilege escalation attempts • Application error logs • Feature activation/deactivation logs • Memory corruption logs • User activity logs on the owner portal
Environmental data	• Planned software maintenance / updates • Vulnerability information about the software components of the infotainment system • Version/configuration information of the firmware and components
Threshold	• Feature activation without purchase
KPI	• # unauthorized feature activation < 1
Incident Response	• Remediate the vulnerability to prevent update without valid signature • Reset firmware to factory adjustment/ last validated version

A structured solution approach for incidents is essential before actual incident occurs

Effective patch management and business continuity are keys to efficient operations



Containment

- Immediately stop non critical services
- Prevent access to the system through firewall, proxy and IPS
- Follow incidence response work instructions and communication matrices

Eradication

- Update effected components/ systems through a software patch
- Follow different update policies and operational risks during update
- Based on criticality of the incidence, customer self update, dealer workshop support or recall might be necessary

Recovery

- Root cause analysis
- Update of response plan
- Perform KPI based measurement of efficiency of security incidence response process

Structure of reporting and feedback shall be part of corporate governance

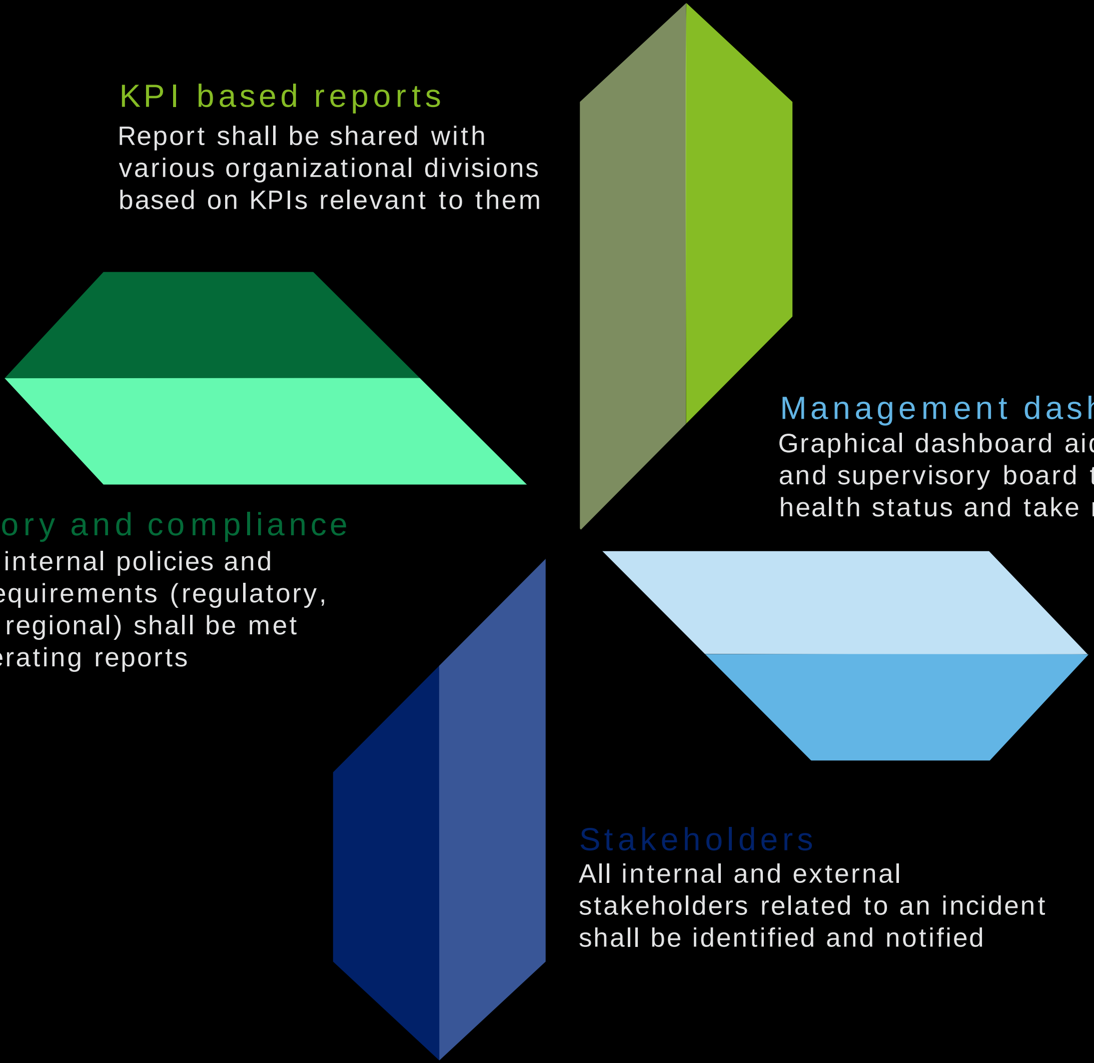
Notification shall be sent to all relevant stakeholders and management team and must abide by policies and regulations

1

2

3

4 Report



KPI based reports

Report shall be shared with various organizational divisions based on KPIs relevant to them

Management dashboard

Graphical dashboard aids senior management and supervisory board to instantly check fleet health status and take necessary measures

Regulatory and compliance

Corporate internal policies and external requirements (regulatory, industrial, regional) shall be met while generating reports

Stakeholders

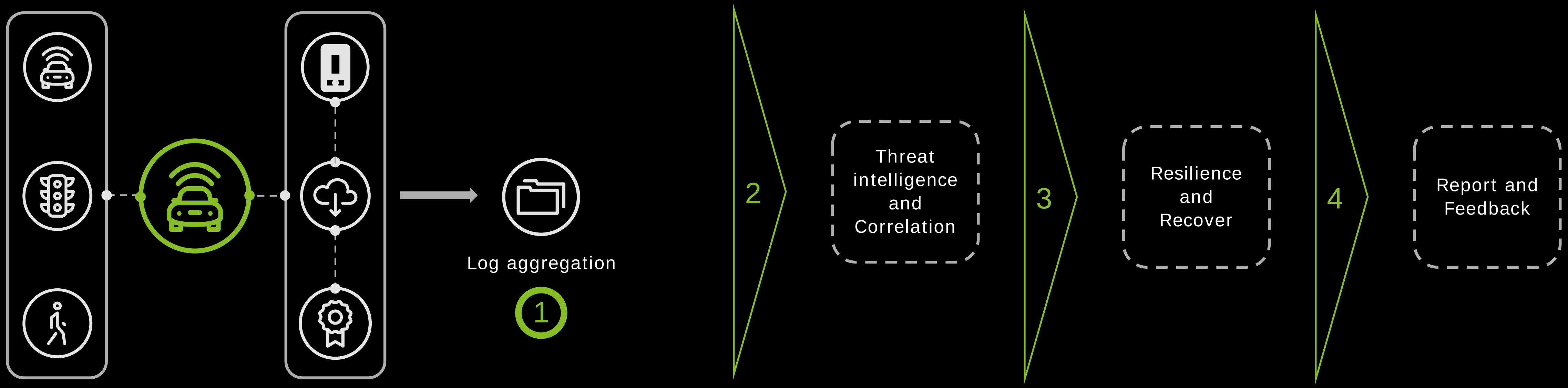
All internal and external stakeholders related to an incident shall be identified and notified

Fleet SIEM - A bird's-eye view

Infrastructure and Information flow

Data collection is a critical part of the whole process

A flaw at this step can risk huge time and money to the company



Log aggregation

1

2

Threat intelligence and Correlation

3

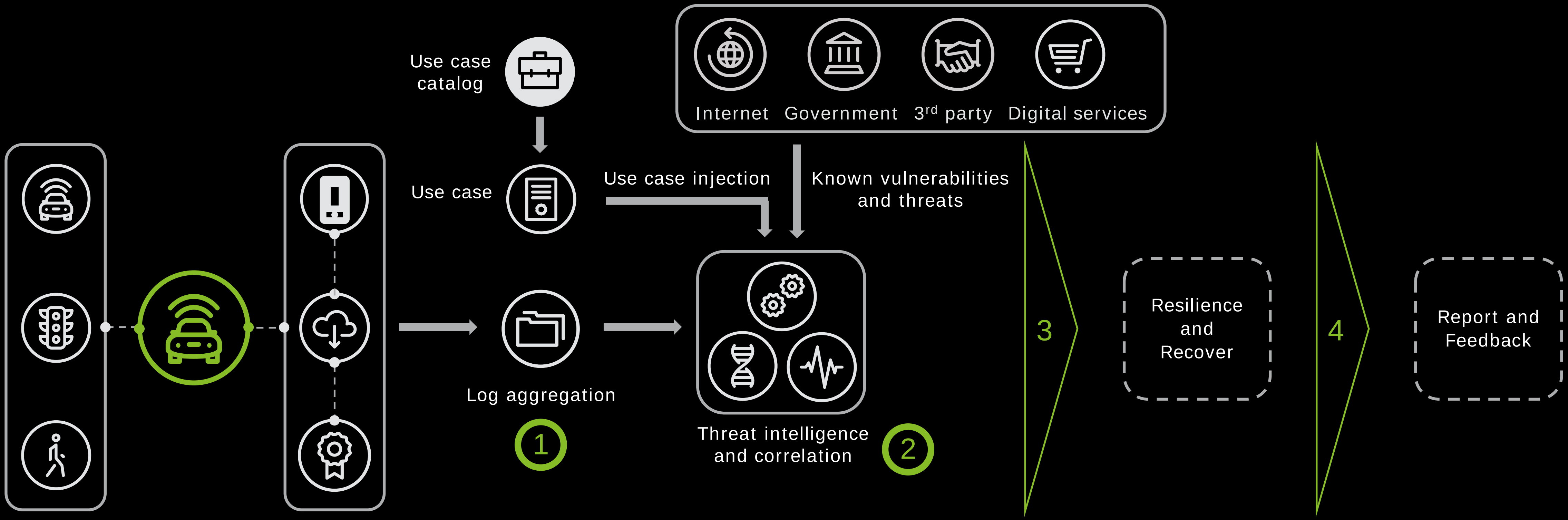
Resilience and Recover

4

Report and Feedback

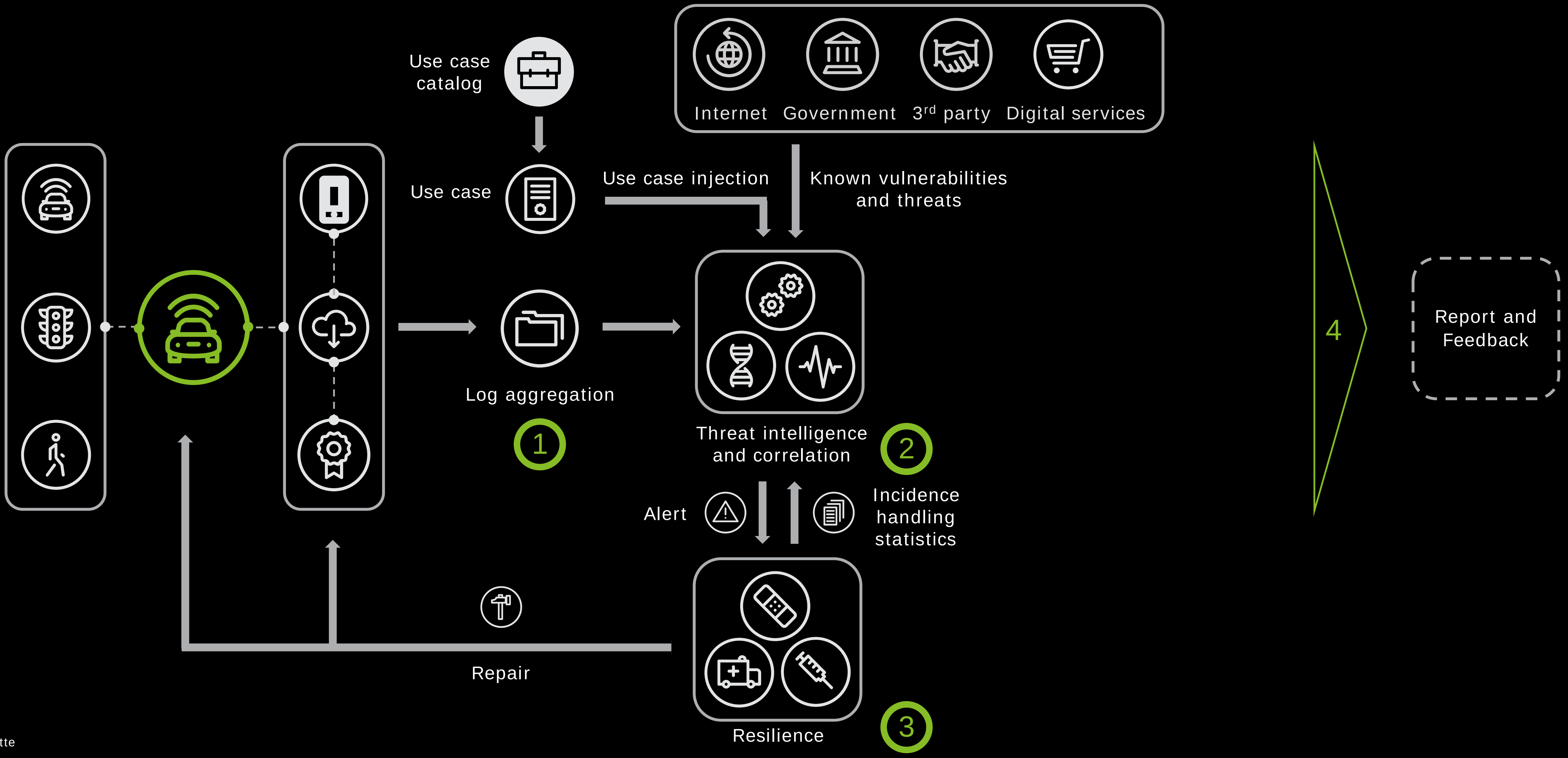
Threat intelligence and correlation are brain of a fleet SIEM system

It also acts as the hub for almost all internal and external interfaces



Bird‘s eye view of data flow and structure in fleet monitoring and reporting

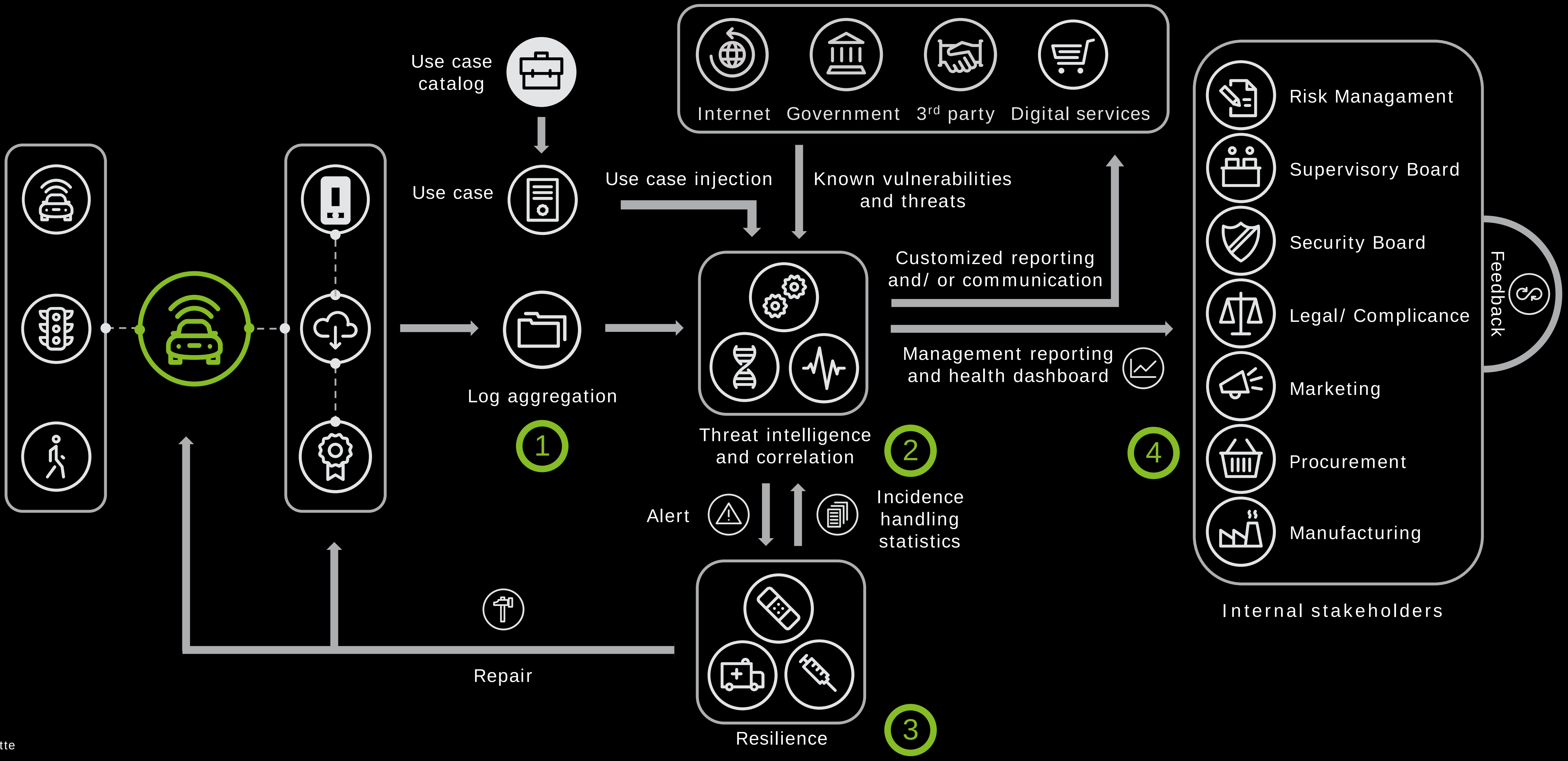
Approach towards secure, vigilence and resilience



2018 Deloitte

Data flow and subsystems in fleet security information and event management

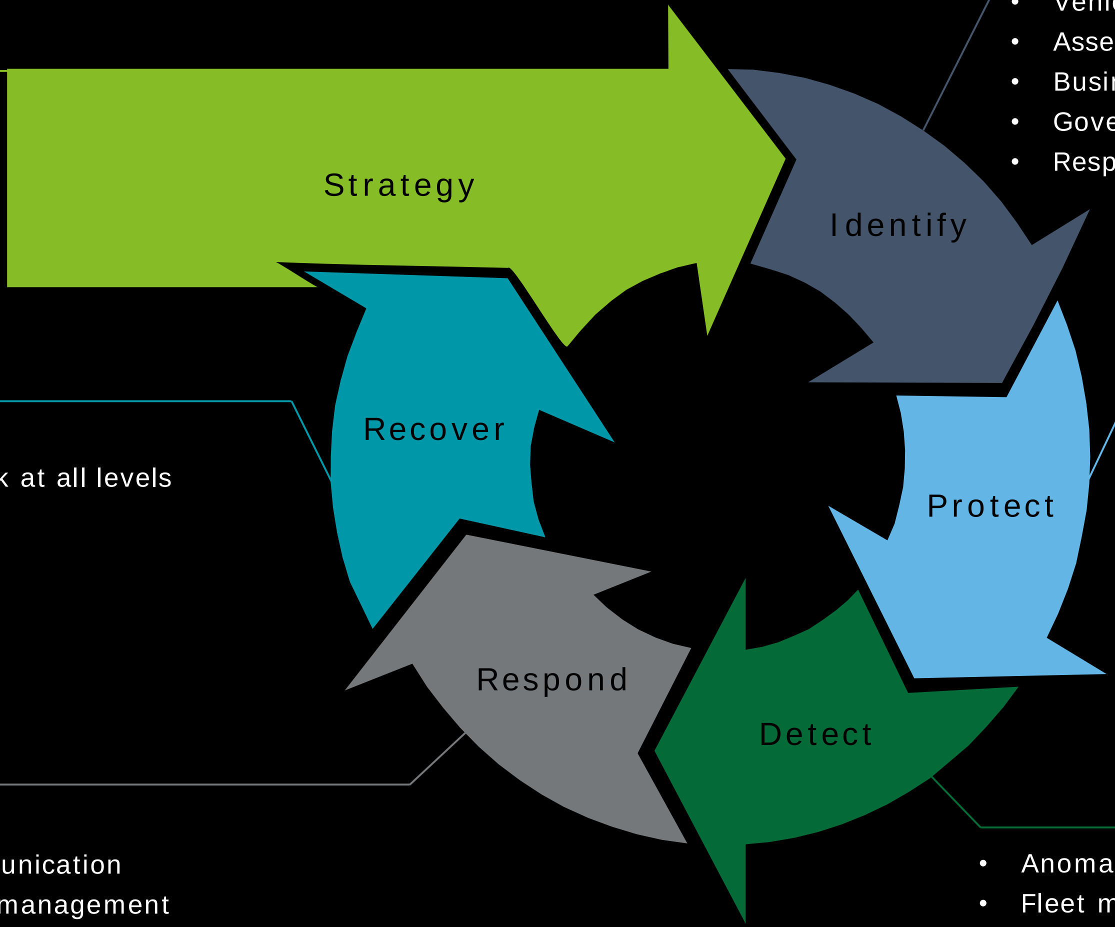
Organization shall go for a secure, vigilent and resilient approach



2018 Deloitte

Security framework observed during fleet monitoring and reporting

Continuous vigilance and updates are key to achieve security goals



Strategy

- Company objectives
- Understand benefits and costs
- Phase wise implementation
- Analysis of stakeholders and beneficiaries
- Legal and regulatory compliance

Identify

- Vehicle eco system
- Assets in and around vehicle
- Business environment
- Governance model
- Response plan

Protect

- Access controls
- Awareness
- Security by design
- Continuous update

Detect

- Anomalies and events
- Fleet monitoring
- Vulnerability database
- External intelligence

Respond

- Prevent spread
- Effective communication
- Efficient patch management
- Recall (if necessary)

Recover

- Gap analysis
- Improvement feedback at all levels
- Implementation plan

Contacts

László Tóth
Partner - Cyber Risk Services

Deloitte PLC
Dózsa György 84/c
H-1057 Budapest
Hungary

ltoth@deloittece.com

Ingo Dassow
EMEA Lead Automotive Cybersecurity
Director - Cyber Risk Services

Deloitte GmbH
Wirtschaftsprüfungsgesellschaft
Kurfürstendamm 23
10719 Berlin

idassow@deloitte.de

Deloitte.

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 more than 244,000 professionals are committed to making an impact that matters.

This presentation contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.