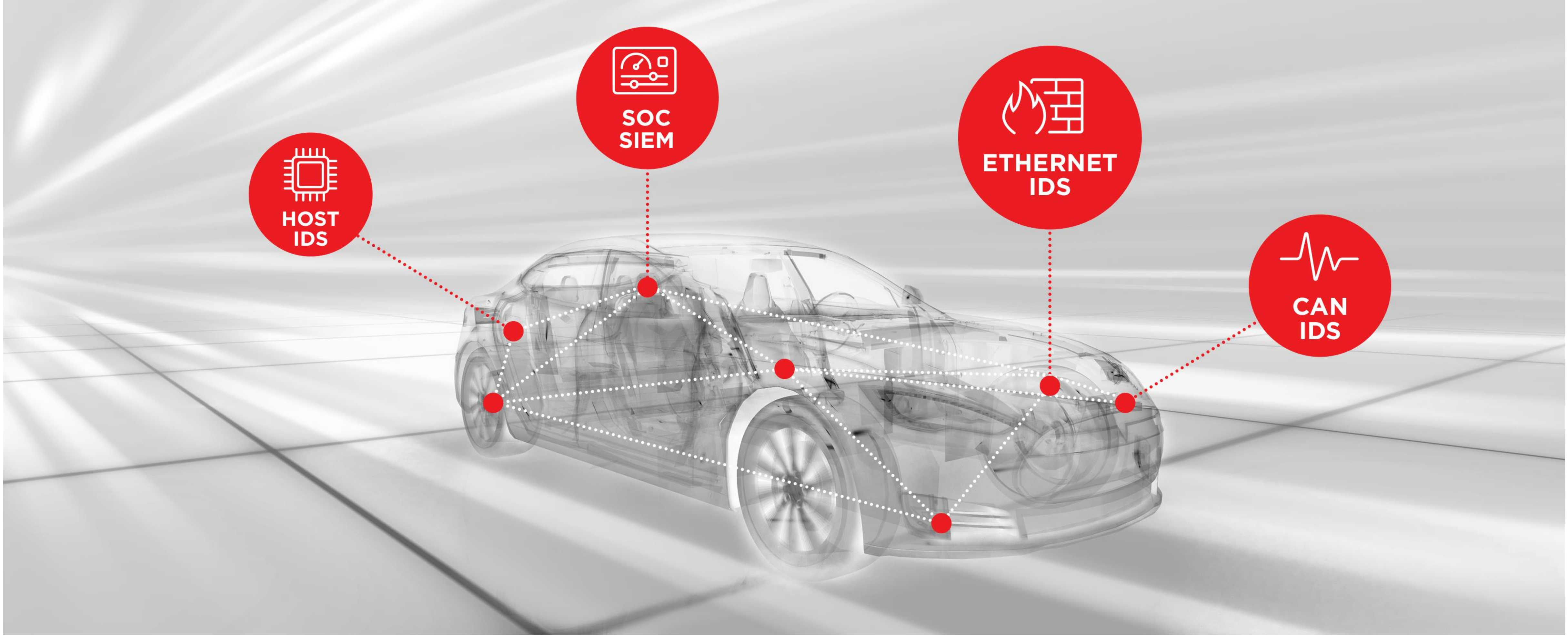


NOVEMBER 16 2022 | WAYNE KIM (김도중 팀장)

MULTI-NETWORK INTRUSION DETECTION SYSTEMS

Stay Ahead of Hackers with Adaptable, Multi-Network Vehicle Intrusion Detection System
Garrett Korea

Garrett
ADVANCING MOTION

Who are we?

Proven Automotive Expertise

- Global supplier to a majority of major OEM globally for over 65 years
- Deep understanding of automotive processes and procedures

Strong Ecosystem Commitment

- Member of SAE, Auto-ISAC, CLEPA
- Capabilities to integrate with T1/ Chips vendors
- Experts yet neutral player

Robust Cyber Technology Foundation

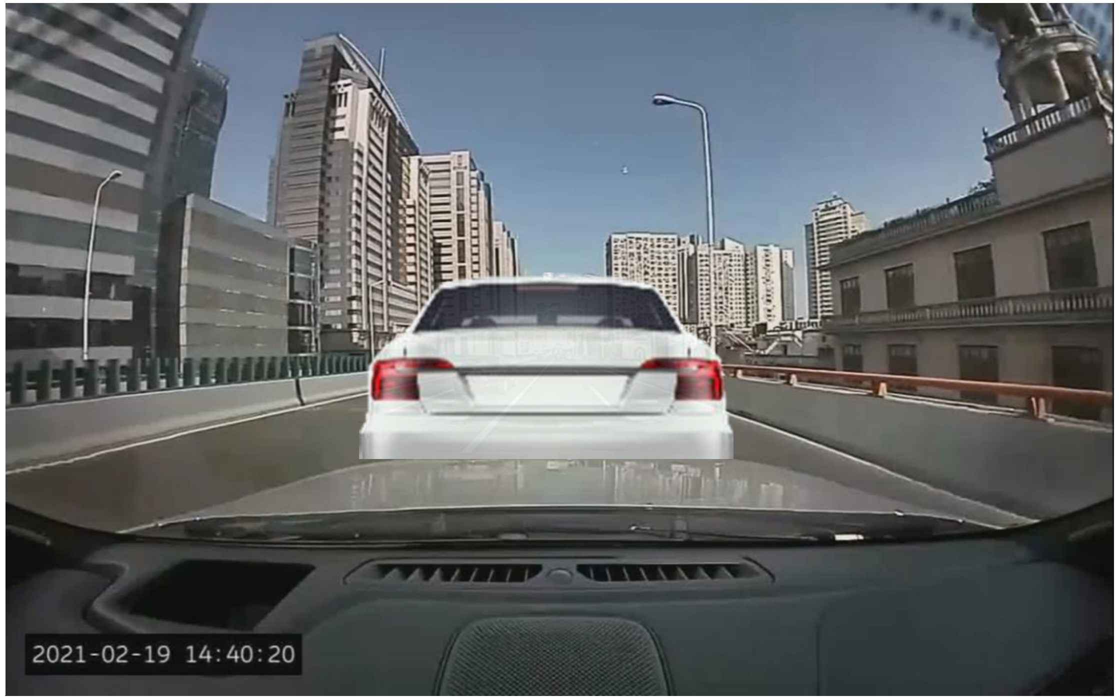
- Product built upon robust industrial application
- 25+ Years of experience in industrial cybersecurity

Garrett Cybersecurity Solutions

- Unique capabilities to segregate cyber issues from vehicle defects
- Close relationship with customers everywhere
- Class leading performance, proven by production awards

Challenge #1

When security and safety must work together: a simple illustration of a dramatic attack



The answer

An intrusion happens: an injection attack, fooling your safety system.

Your car does identify a vehicle crossing your way. It is a fake.

Market now is driven by urgency

Challenge #2

Legislation Regulatory: UNECE Requirements

OEM must answer following threats	CAN	ETH	HOST	SOC SIEM	SERVER
Back-end Servers Threats					X
Communications Channels Threats	X	X			X
Unintended human actions facilitating a cyber attack	X	X	X		
External connectivity and connections Threats	X	X			X
Vehicle Data and Code			X		X
Protection and Hardness	X	X	X		X
Monitor, detect, respond to cyber threats	X	X	X	X	X
Management System for Monitored Vehicle				X	

From UNECE WP29 R155

Market now is driven by regulations

Challenge #3

How to choose and apply an IDS system

What type of IDS do I need, and where to place it into?

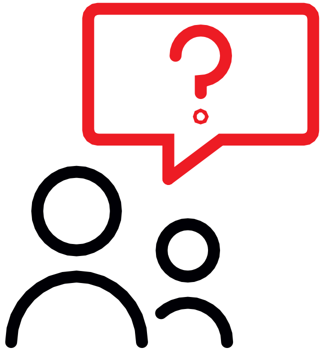
How to make IDS have the maximum performance, the best detection accuracy, and minimal system consumption?

Can IDS cover all or most of the attacking cases?

Is IDS ruleset easy to update independently of Over The Air(OTA)?

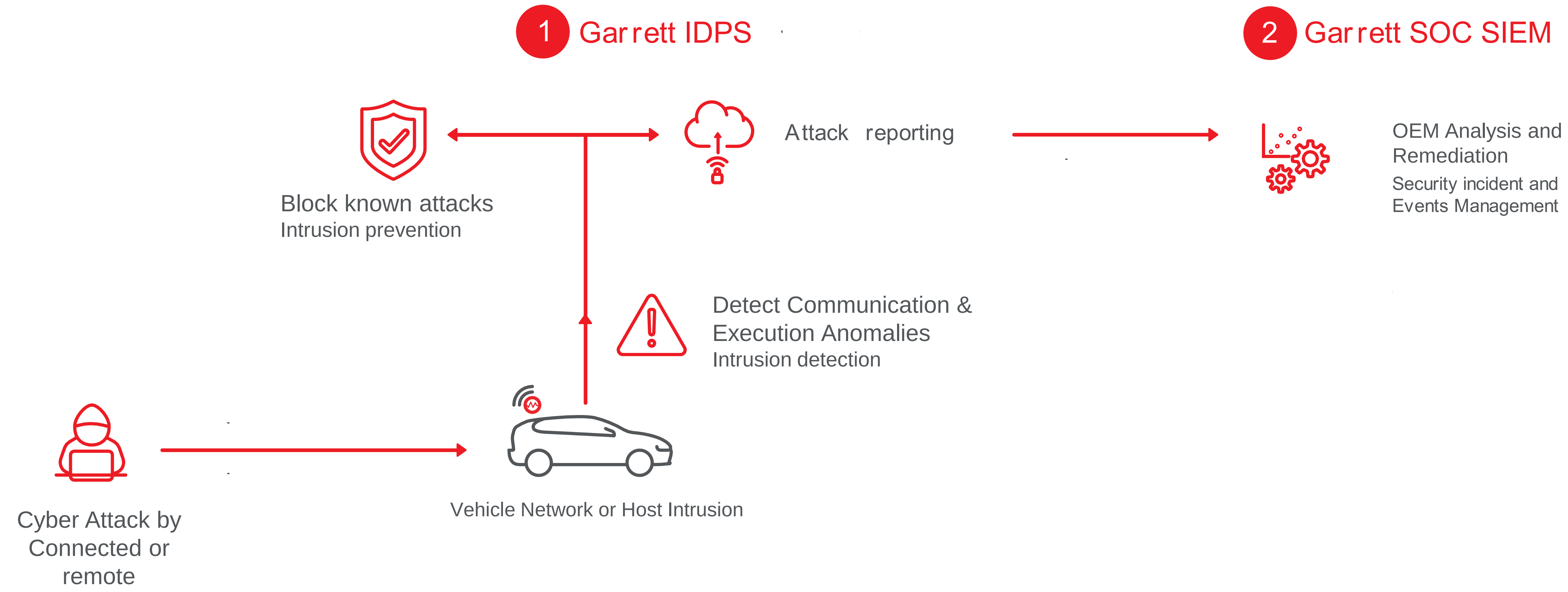
Is IDS easy for porting from one vehicle model or one type of component to another?

Is IDS easy for extending ruleset or even detection algorithms by customers themselves



Garrett cybersecurity products

Garrett
ADVANCING MOTION


1 Garrett IDPS
2 Garrett SOC SIEM
Block known attacks
Intrusion prevention
Attack reporting
OEM Analysis and Remediation
Security incident and Events Management
Detect Communication & Execution Anomalies
Intrusion detection
Cyber Attack by Connected or remote
Vehicle Network or Host Intrusion

1

- 50+ advanced algorithms, cross-bus detection
- Independent of system hardware and operating system, easy to integrate
- Full lifecycle security management and related configuration tools
- Suitable for CAN, CAN FD, Ethernet and HPC
- SOA Service Anomaly Monitoring and Control

2

- Log reading, parsing, correlation
- Identify severity levels, prioritization, incident escalation
- Vehicle abnormal signal cause analysis module
- Rule based is the mainstay, supplemented by machine learning

Garrett cybersecurity software solutions

| 4 CORE PRODUCTS |

CAN IDS

On board Garrett CAN IDS monitors CAN traffic, detects and or blocks anomalies

Supported by off-board lifetime ruleset management tool

ETH IDS

Garrett Ethernet Firewall and IDS solutions inspect Ethernet traffic and block malicious messages on board

Supported by off board lifetime ruleset management tool

HOST IDS

Garrett host IDS solutions monitor and detect anomaly cyber-attacks on automotive high-performance Computer

Supported by off board lifetime ruleset management tool

SOC SIEM

Garrett SOC SIEM tools analyses cyber alerts from millions of vehicles in a human actionable way

Garrett cybersecurity solutions provide best-in-class protection for connected vehicles

Garrett IDS and SOC system in-vehicle

CAN IDS : CAN Network IDS

- ✓ Automotive CAN network anomaly detection

ETH IDS : Ethernet IDS

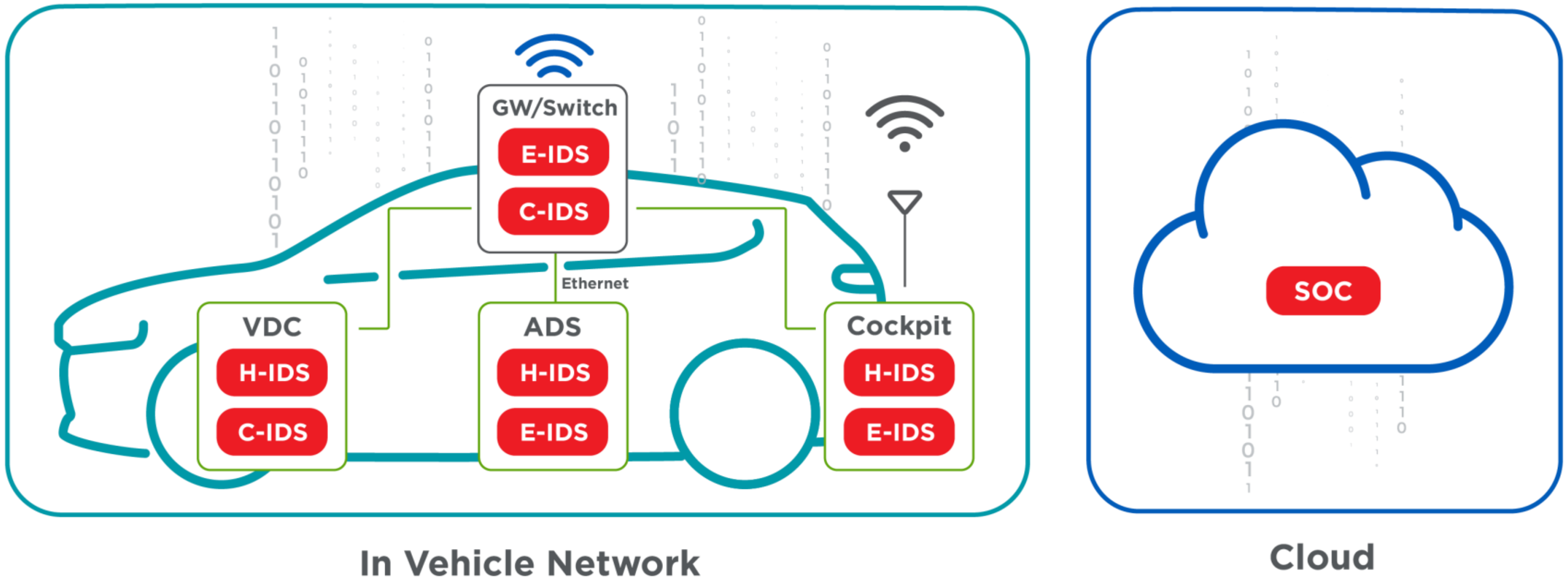
- ✓ Automotive Ethernet anomaly detection

HOST IDS

- ✓ Automotive high-performance Controller anomaly detection

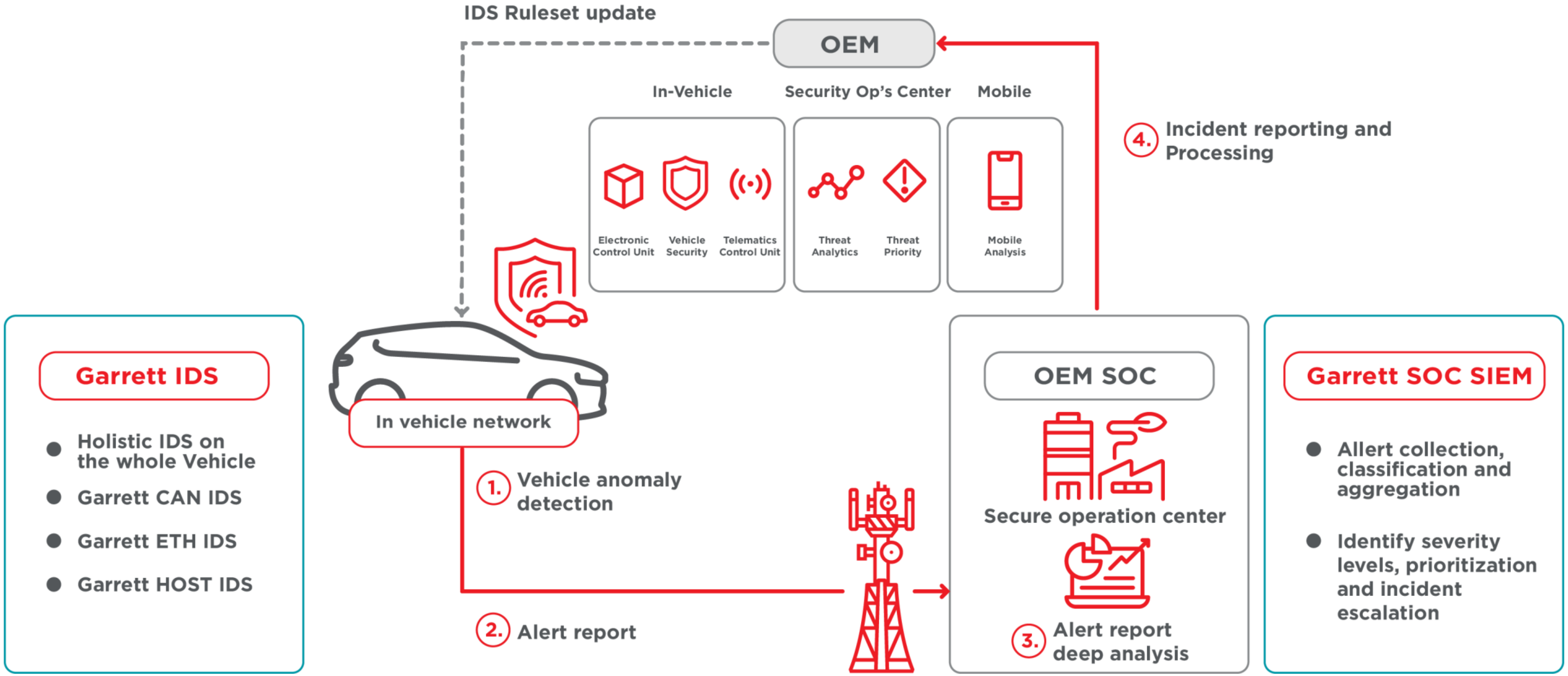
SOC SIEM

- ✓ Anomaly alert aggregation, analysis and processing, identify the real attack



Use Case 1: Garrett IDS solution for OEM

Garrett
ADVANCING MOTION



Garrett IDS

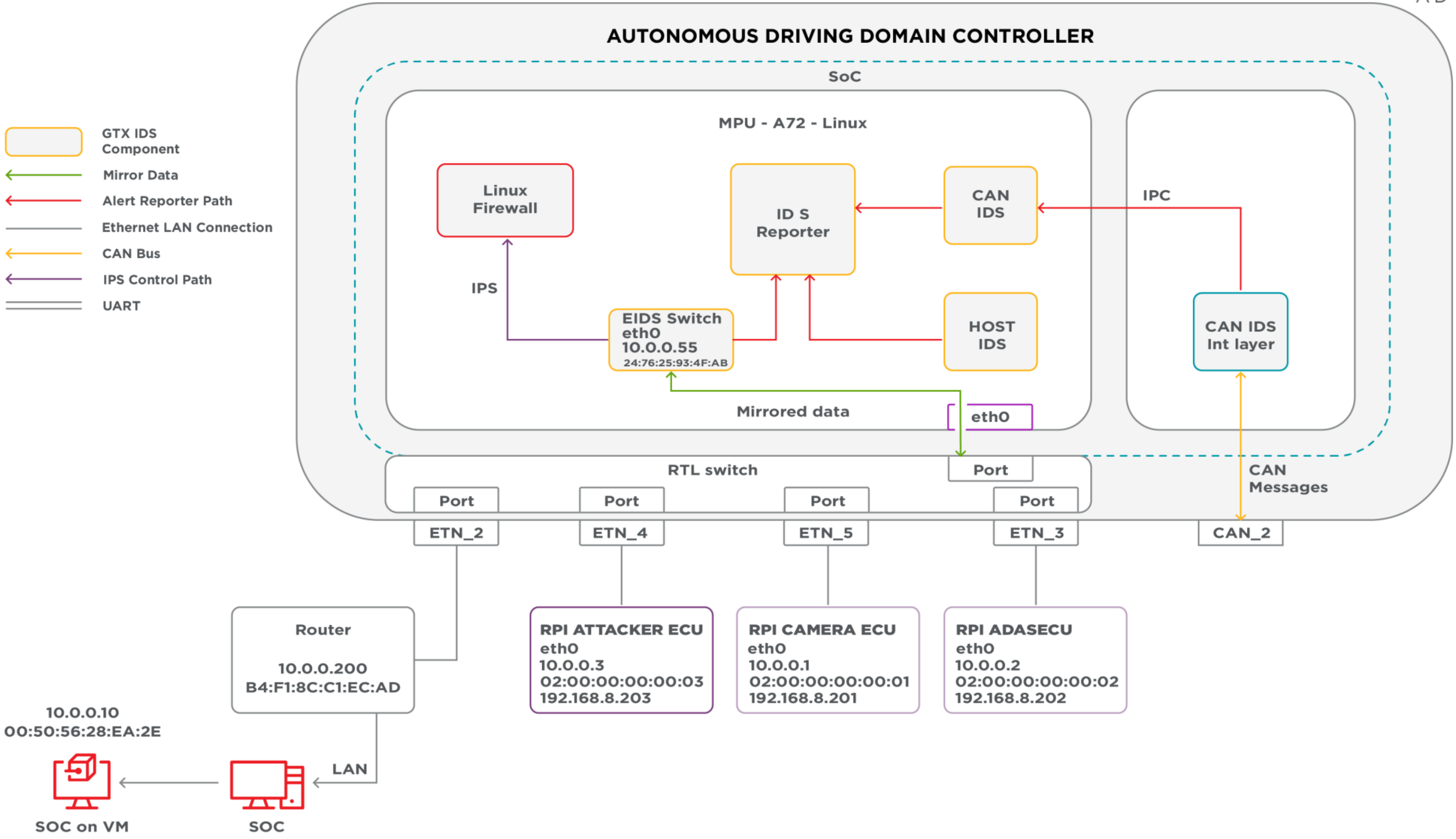
- Holistic IDS on the whole Vehicle
- Garrett CAN IDS
- Garrett ETH IDS
- Garrett HOST IDS

Garrett SOC SIEM

- Allert collection, classification and aggregation
- Identify severity levels, prioritization and incident escalation

Garrett provides the entire IDS solution from vehicle side to cloud side for OEMs

Use Case 2: Garrett IDS solution Tier-1



Garrett provides customized IDS solution for ICV Tier-1 suppliers

Use Case 3: Garrett IDS solution for SOA use case

ETH-IDS:

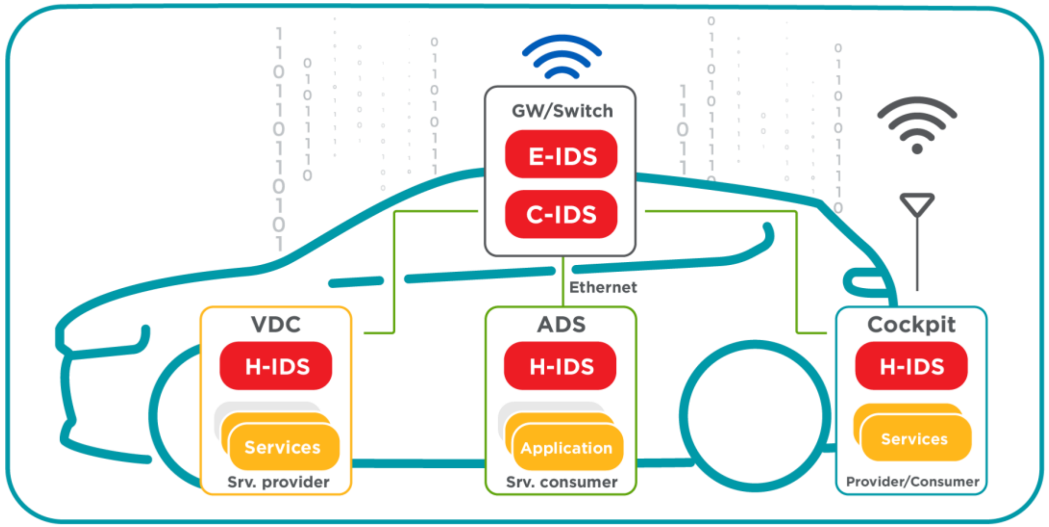
- ✓ SOME/IP protocol monitor
- ✓ SOA service content monitor

HOST-IDS: HOST IDS

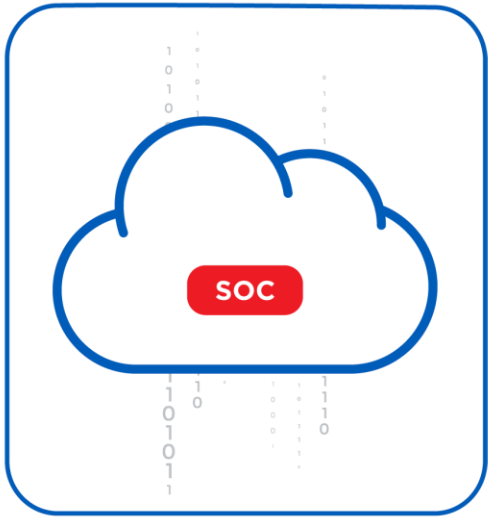
- ✓ SOA service resources consumption monitor
- ✓ SOA service access monitor both outside and inside

SIEM SOC:

- ✓ SOA attacking Identification with monitoring of SOA alert from ETH-IDS and HOST-IDS



In Vehicle Network



Cloud

Use Case 4: assist customer for obtaining VTA certificate

Garrett Cybersecurity Solutions	CAN IDS	ETHERNET IDS	HOST IDS	SOC SIEM
Back-end Servers Threats				
Communications Channels Threats	✓	✓		
Unintended human actions facilitating a cyber attack	✓	✓	✓	
External connectivity and connections Threats	✓	✓		
Vehicle Data and Code			✓	
Protection and Hardness	✓	✓	✓	
Monitor, detect, respond to cyber threats	✓	✓	✓	✓
Management System for Monitored Vehicle				✓

Garrett assist OEM to pass VTA as proof of security measures

Garrett

ADVANCING MOTION

www.garrettmotion.com

garrettmotion