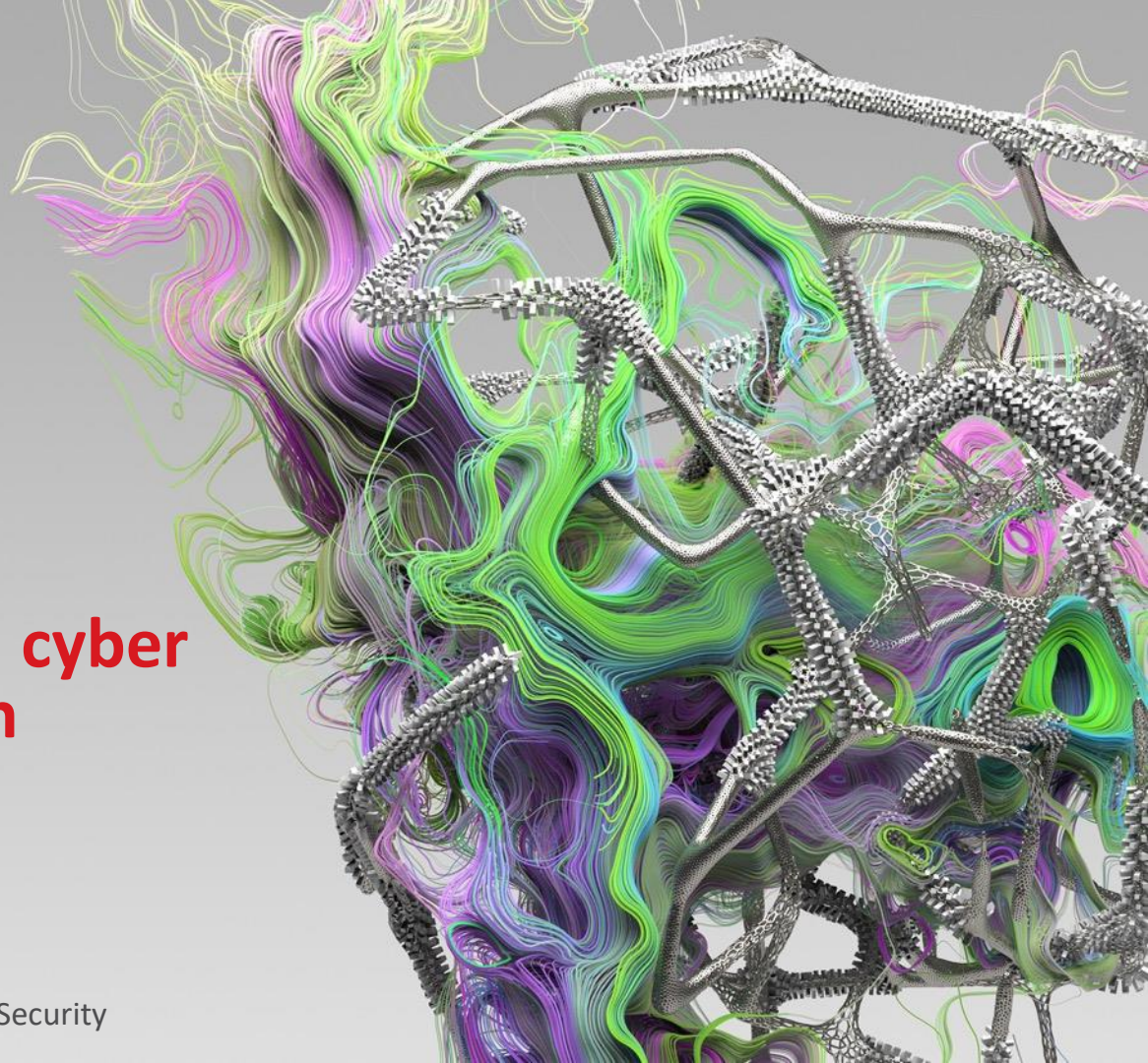


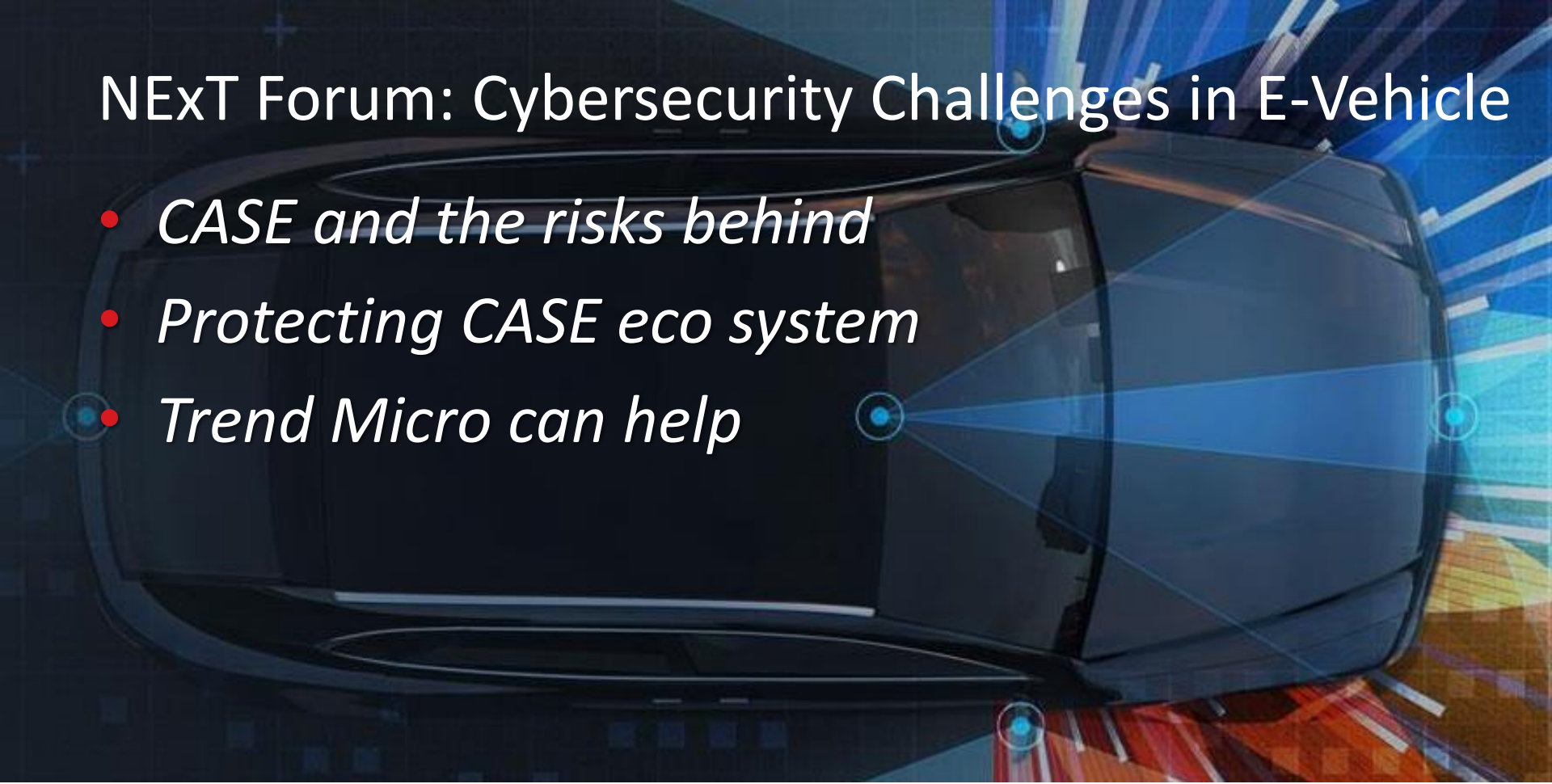
Securing CASE: Putting the brakes on cyber threats to keep you in the fast lane

楊豐愷, 車聯網資安防護解決方案產品經理

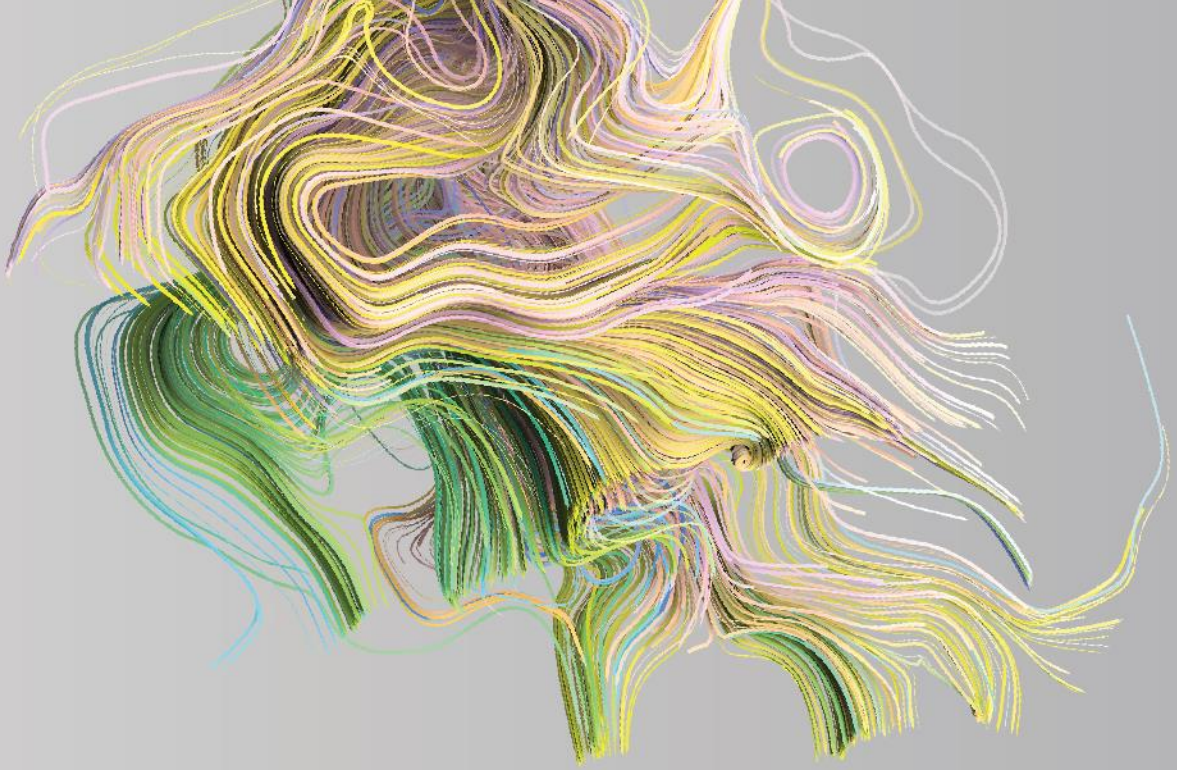
Peter Yang

Sr. Product Manager, IoT & Connected Vehicle Security

NExT Forum: Cybersecurity Challenges in E-Vehicle



- *CASE and the risks behind*
- *Protecting CASE eco system*
- *Trend Micro can help*



CASE and The Risks Behind

Hacker's Motivation

Global Mega Trend: CASE

The Mobility Revolution

Connected

- Infotainment
- Navigation
- Remote diagnostics
- FOTA/ SOTA
- Use Based Insurance
- Fleet management

Autonomous

- Logistics
- Cargo
- Haling service
- Passenger car

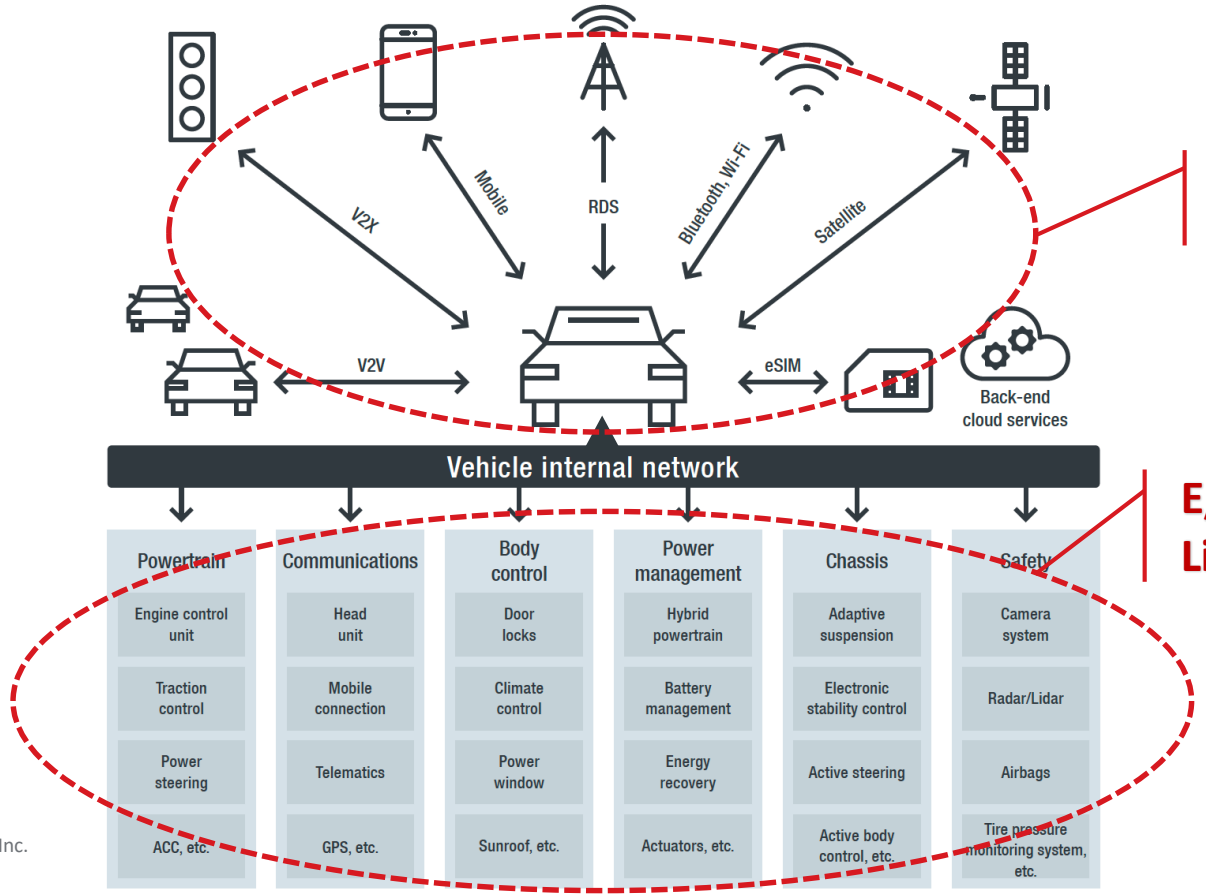
Shared

- Ride share
- Car share
- Shared parking
- Shared energy

Electrification

- Reduce emission
- Reduce noise
- Lower maintenance

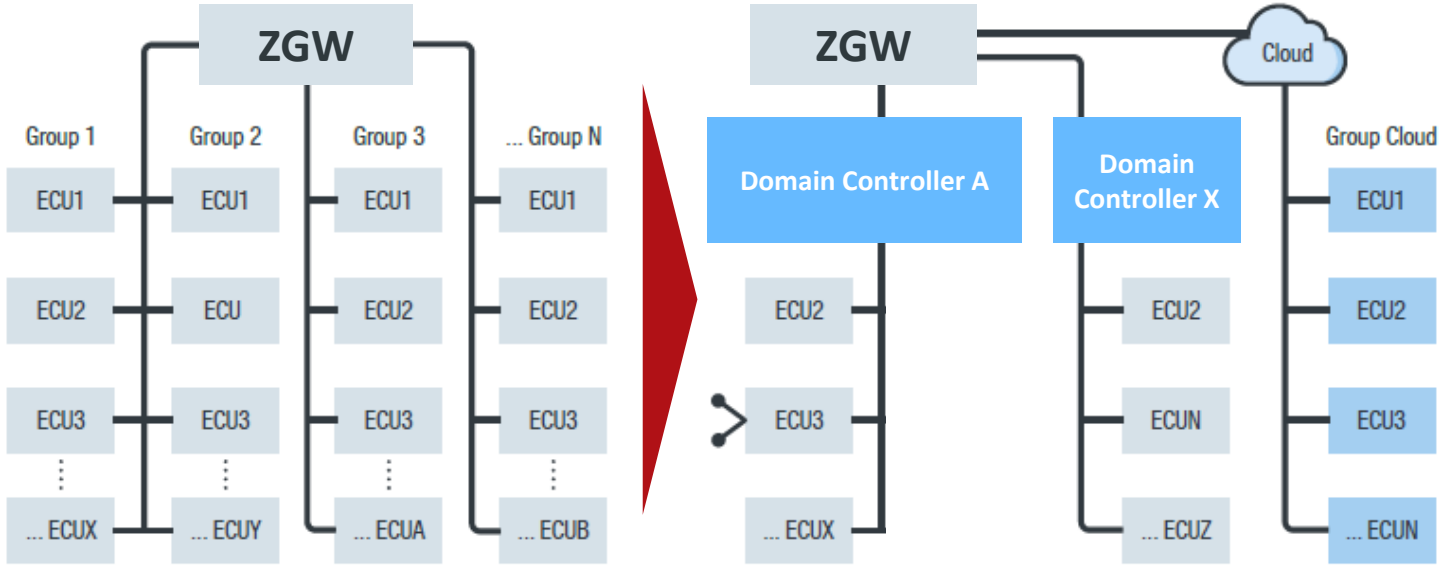
Behind CASE



Number of interface

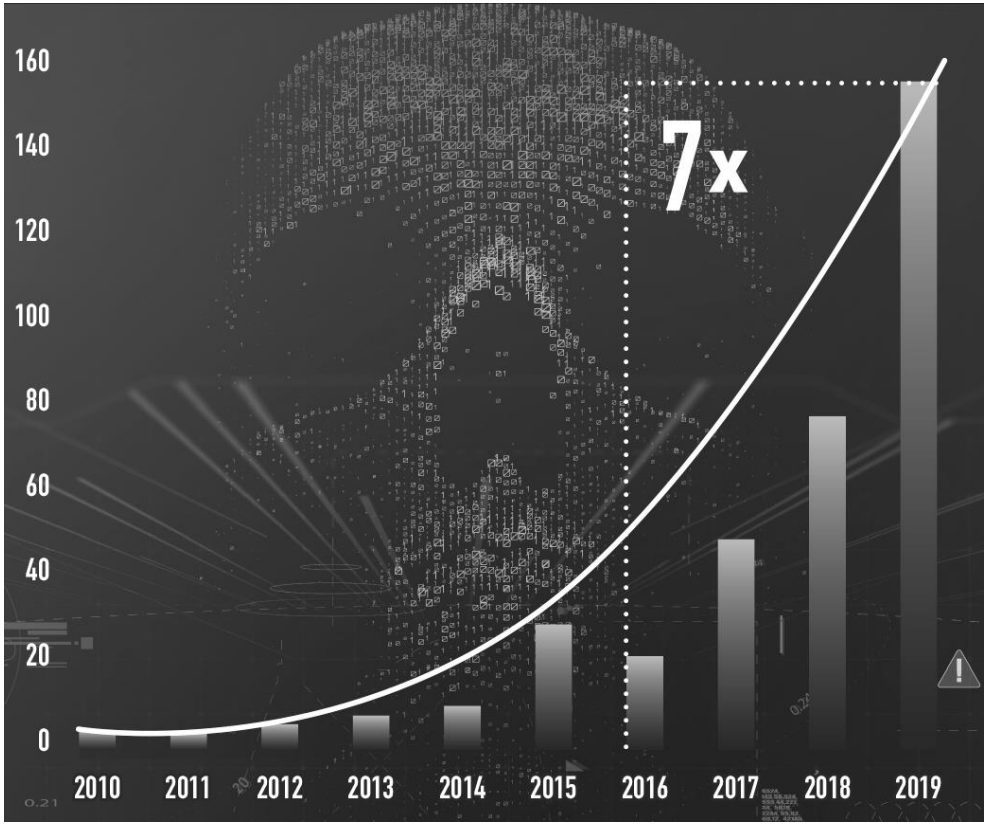
E/E Component Line of code

The E/E Architecture is Evolving



Automotive industry is transforming into Next Data Goldmine

Behind CASE - Automotive Cyberattacks



https://upstream.auto/news/press-release-global-automotive-cybersecurity-report-2020/

Monetizing Cyberattacks on CASE

User PII & user data (non-PII)

- Phone contact, call history, text message, driving history, schedule…etc.
- App data & cloud data (Apple CarPlay, Android Auto), driving video recorder (Tesla's Sentry Mode)…etc.

Car itself & goods inside

- Remotely unlock the door steal the car itself or valuable goods that transport by autonomous car

Driving services

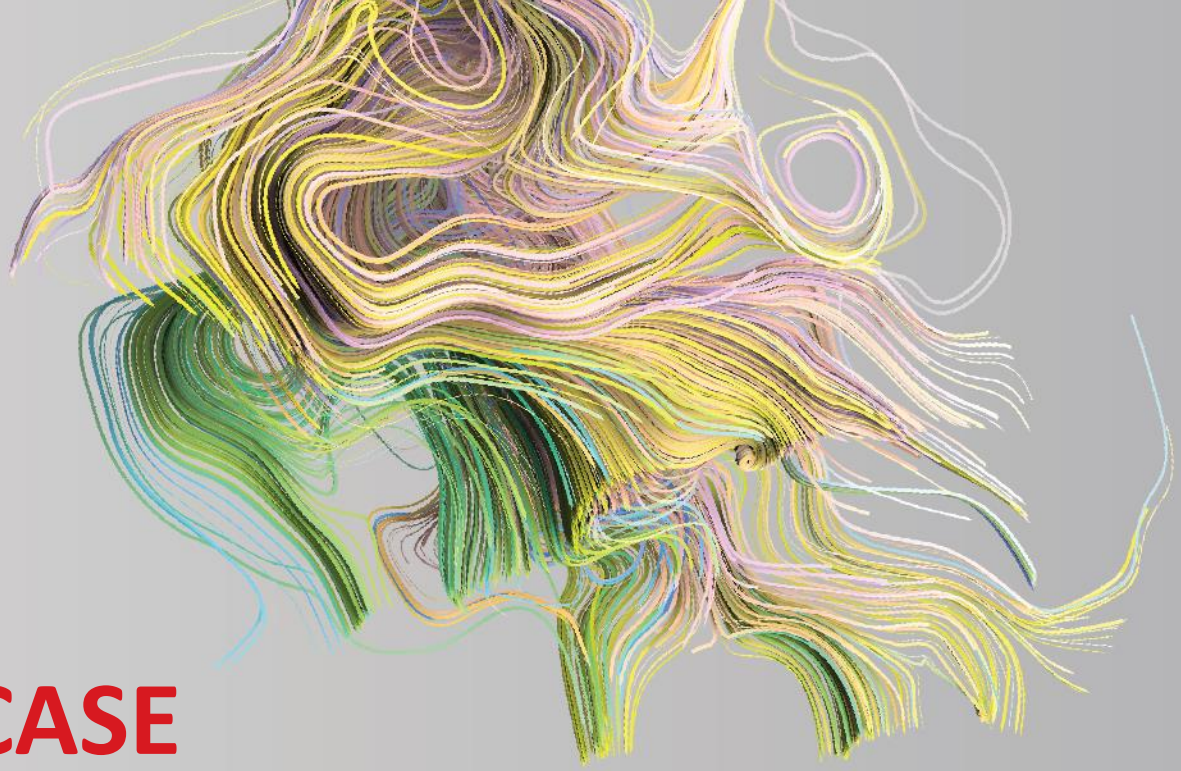
- Hacking and using cars' services for moving contraband items, committing crimes, performing anonymous movements, and other illegal acts

Stored energy

- Stored battery energy in cars could potentially become a valuable commodity (V2G)

Network and processor resources

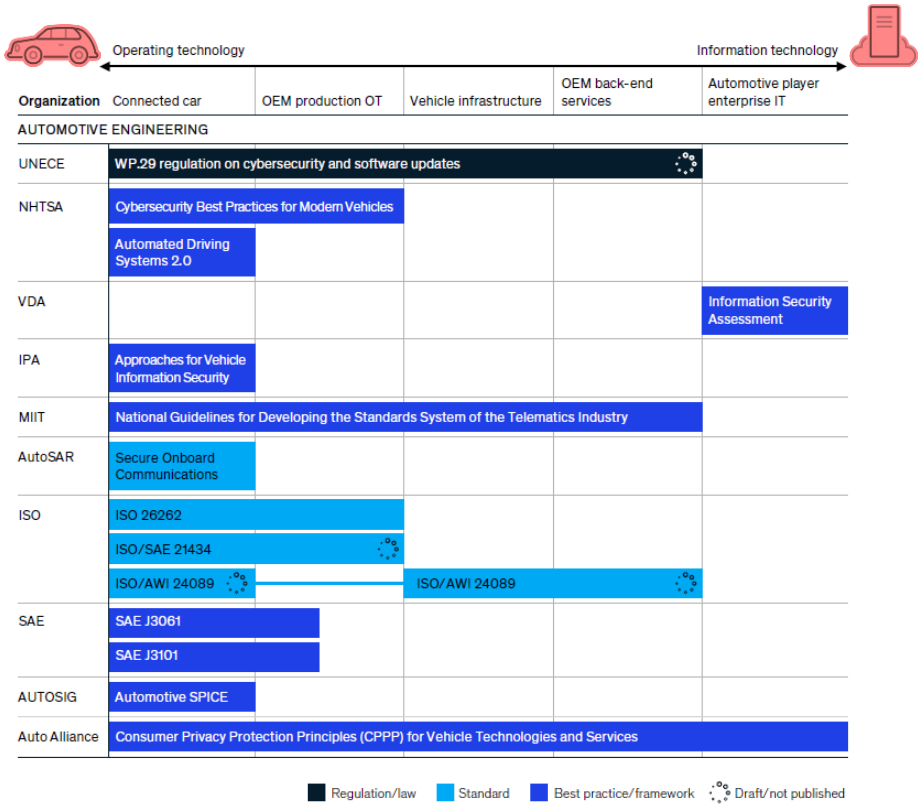
- Cybercriminals could install a botnet in a connected car and use network and CPU resources while the car is idle at home for the night, or they could use the ***car as an initial access point to hack the power grid (infra/ cooperate backend)***.



Protecting CASE Eco System

Regulation & Standard

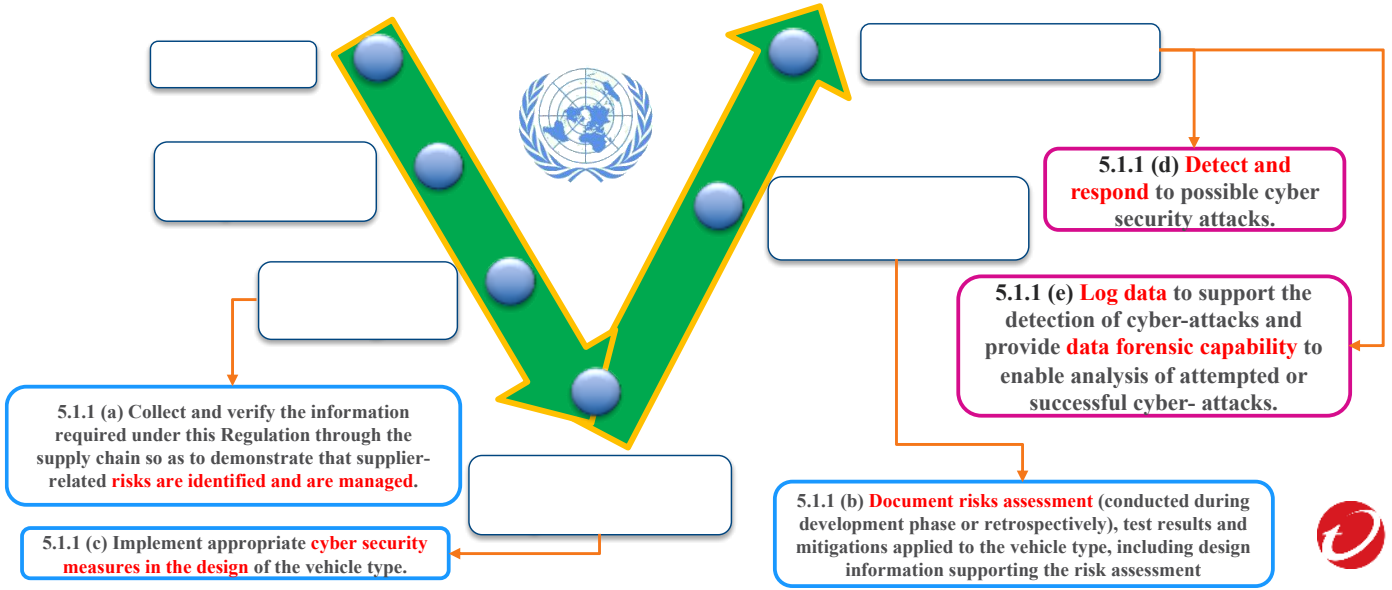
Regulation, Standard and Best Practices



https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge

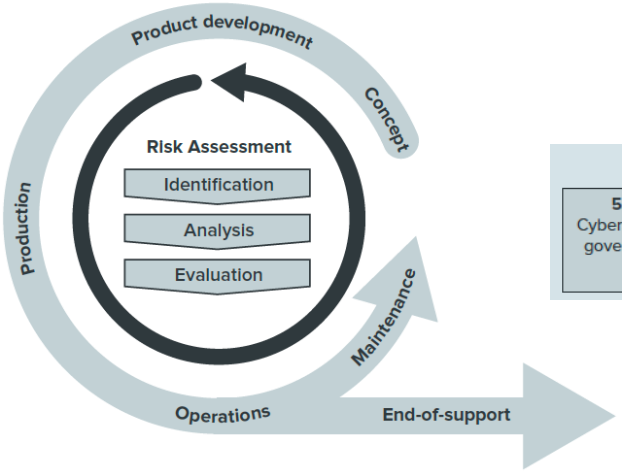
UNECE WP.29

- UNECE WP.29 regulations focus on **cybersecurity** and **software updates**.
- OEMs will need to show evidence of sufficient cyber-risk management practices **end to end**.
- This includes the demonstrated ability to deploy OTA software security fixes even after the sale of the vehicle.



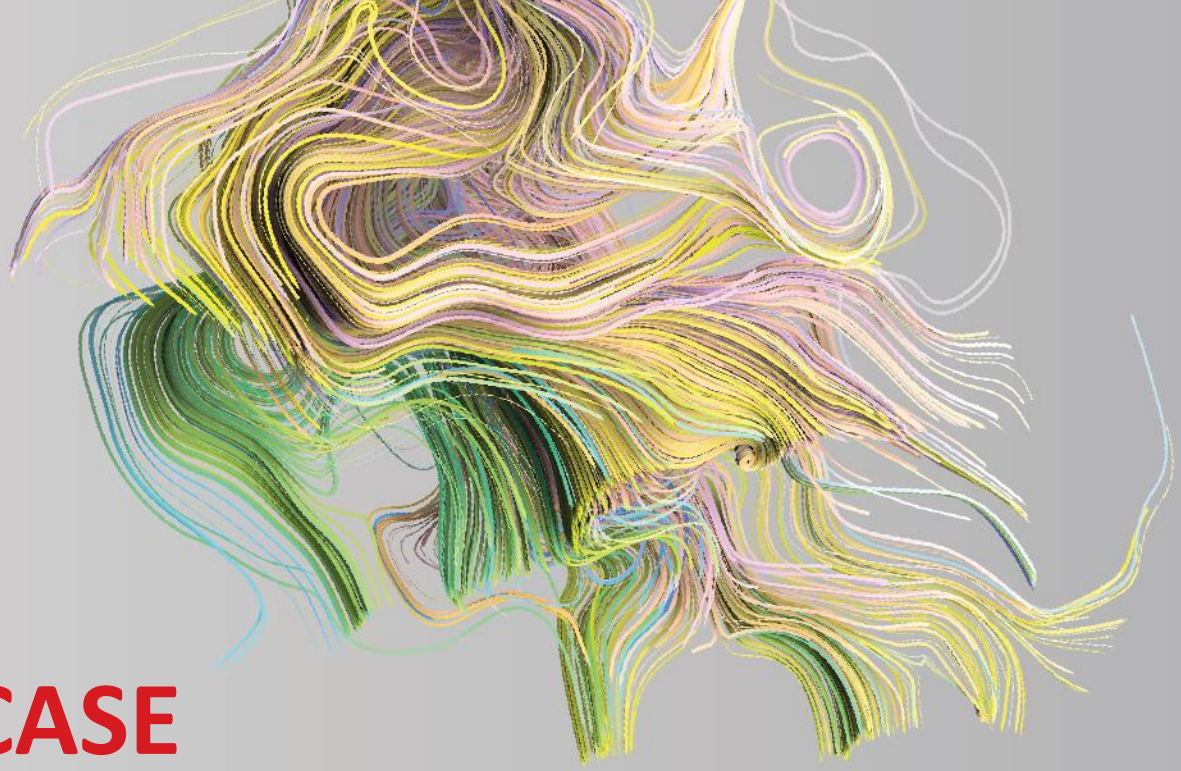
ISO/SAE 21434

- Currently, ISO 26262 “Road vehicles – Functional safety” is not focused on software development or detailing the cybersecurity infrastructure of car subsystems.
- **ISO/SAE 21434** “Road vehicles – **Cybersecurity engineering**” sets standards specific to items for identification such as the use of embedded controllers, the long lifecycle of vehicles, and the safety implications of these technologies in cars.
  - The first standard that lays out clear organizational, procedural, and technical requirements throughout the vehicle lifecycle.



5. Overall cybersecurity management							
5.4.1 Cybersecurity governance	5.4.2 Cybersecurity culture	5.4.3 Cybersecurity risk management	5.4.4 Organizational cybersecurity	5.4.5 Information sharing	5.4.6 Management systems	5.4.7 Tool management	5.4.8 Information security management

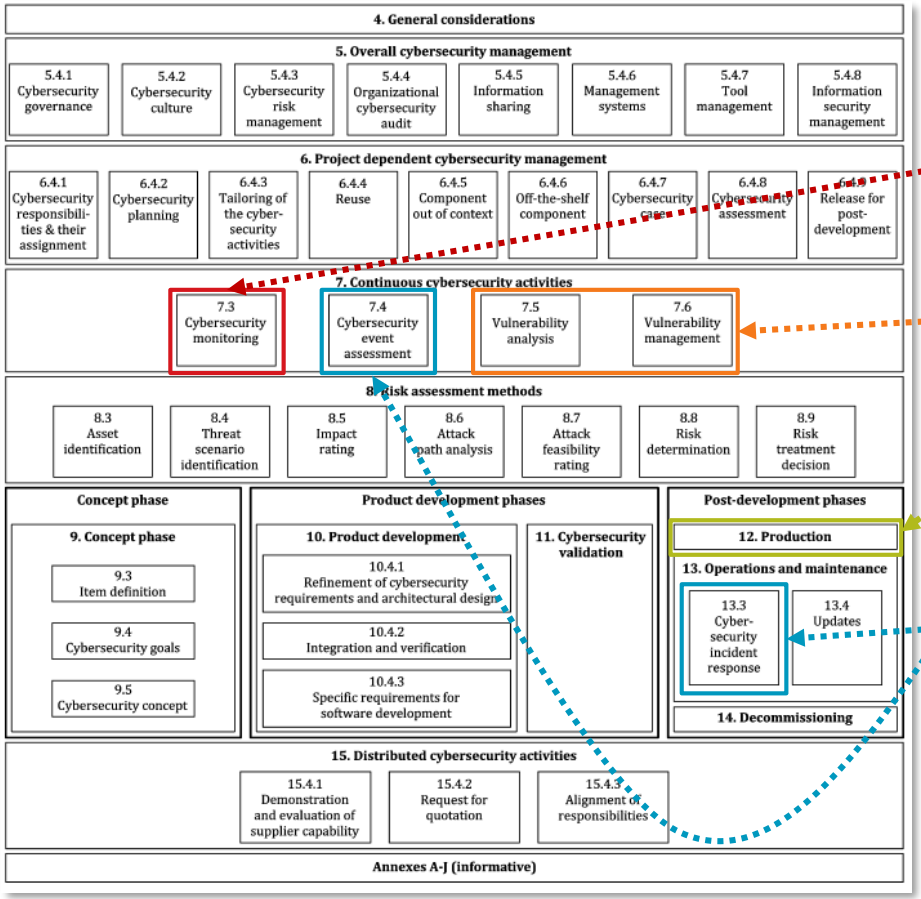
ISO/ SAE 21434: Overall Cybersecurity Management chapter structure



Protecting CASE Eco System

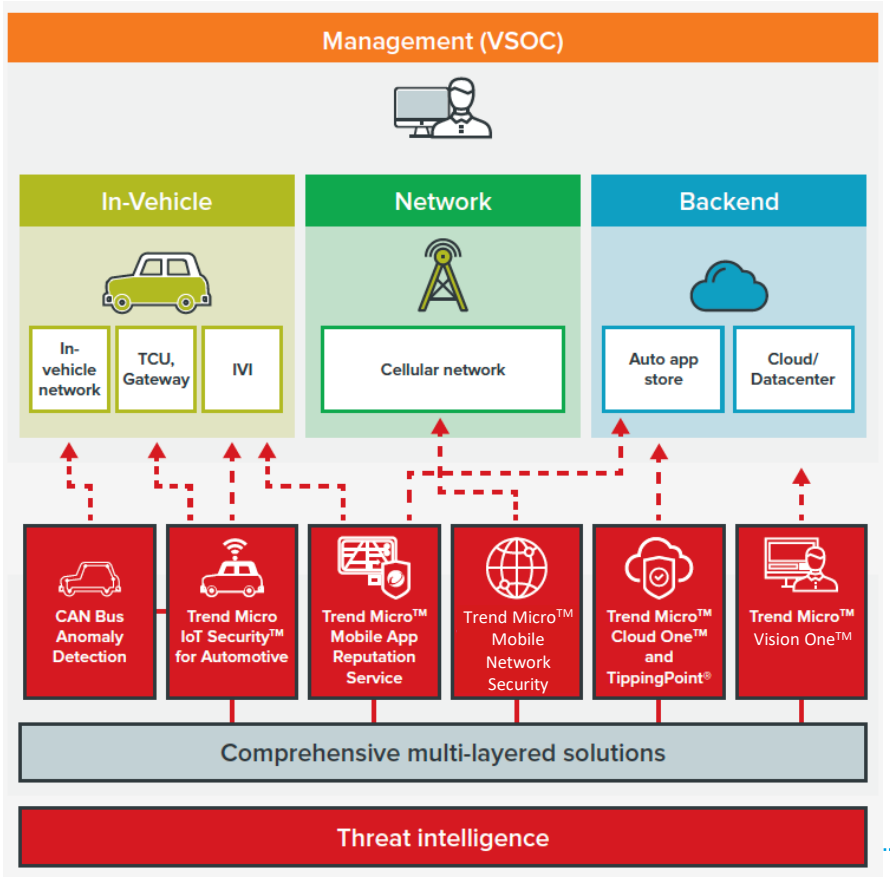
Technical Implementations

NO Out-of-Shelf Security Product/ Service



ISO/SAE 21434 and Trend Micro's solution map

Solutions & Strength for Automotive

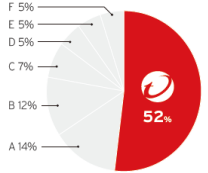


SMART PROTECTION NETWORK

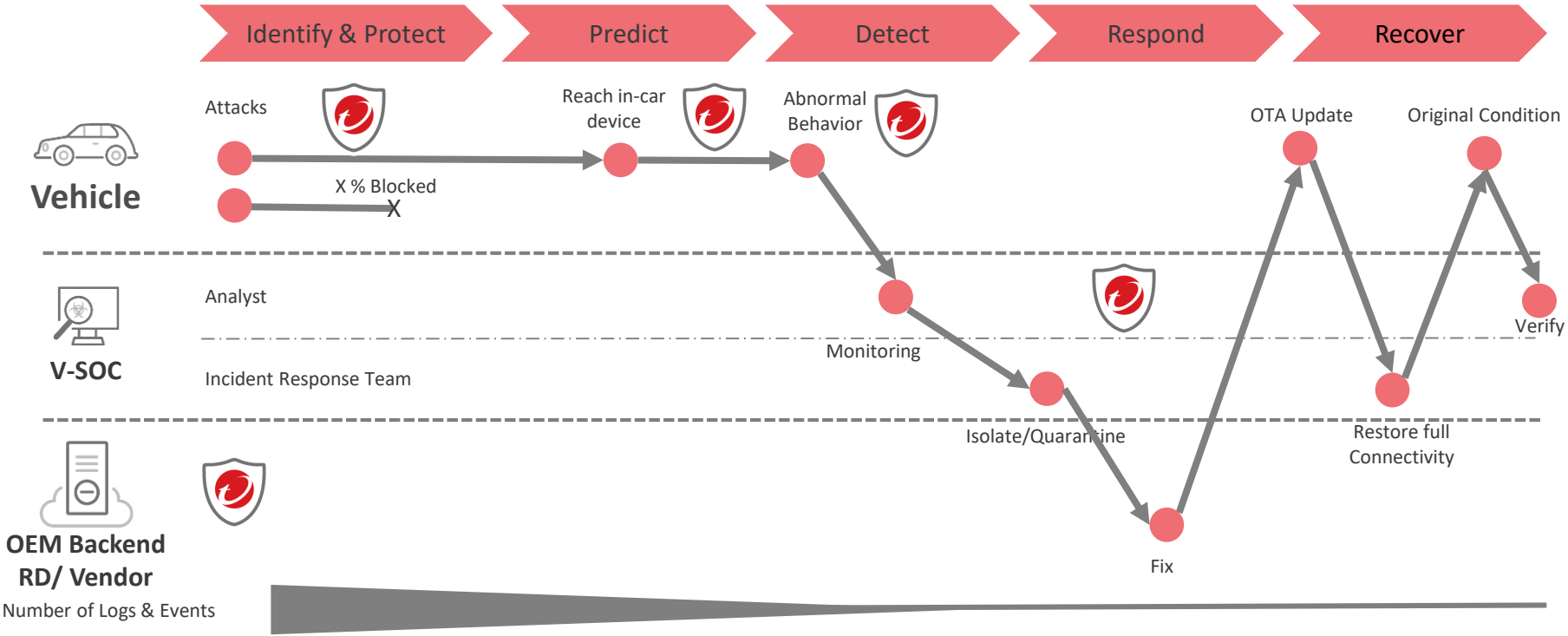
250M+	2.5T+	65B+
sensors	threat queries yearly	threats blocked yearly

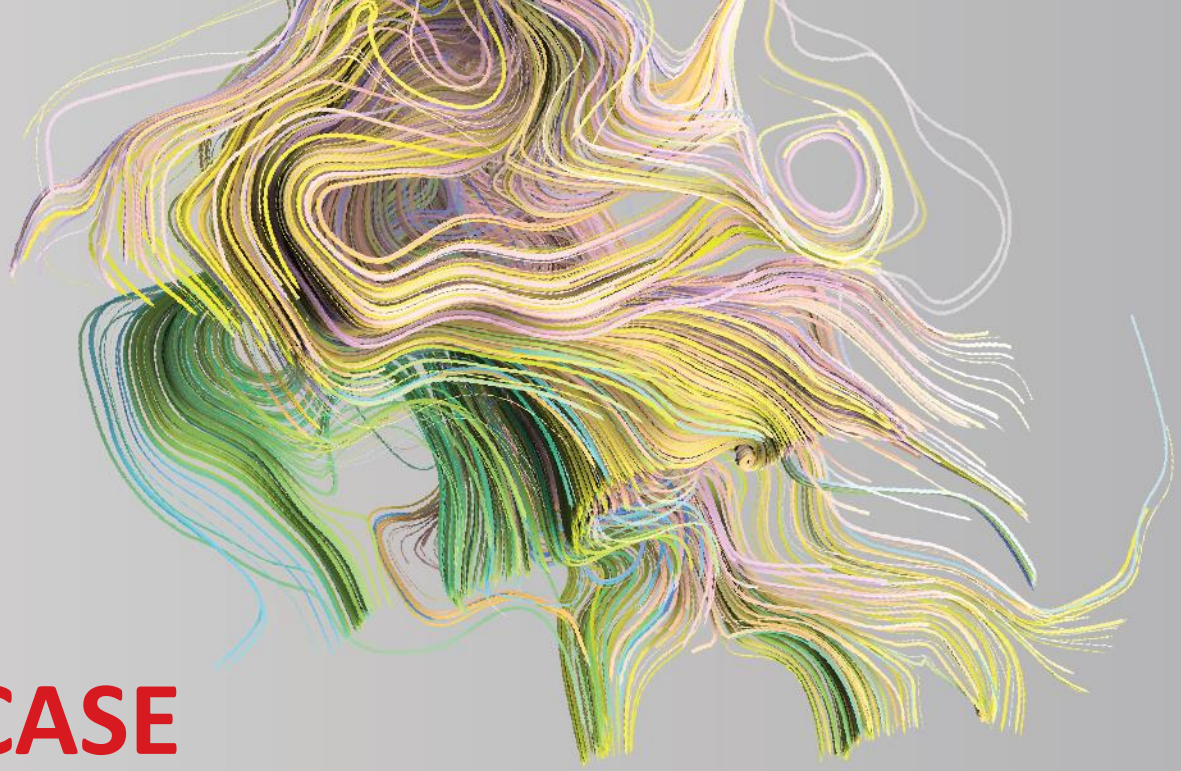
ZERO DAY INITIATIVE

- **Founded in 2005, Trend Micro's bug bounty**
- Powered **by over 10,000 independent researchers**
- Contributing research from many different areas including **Automotive and IoT**
- Disclosed the most vulnerabilities in 2018/ 2019



Cybersecurity Framework for CASE



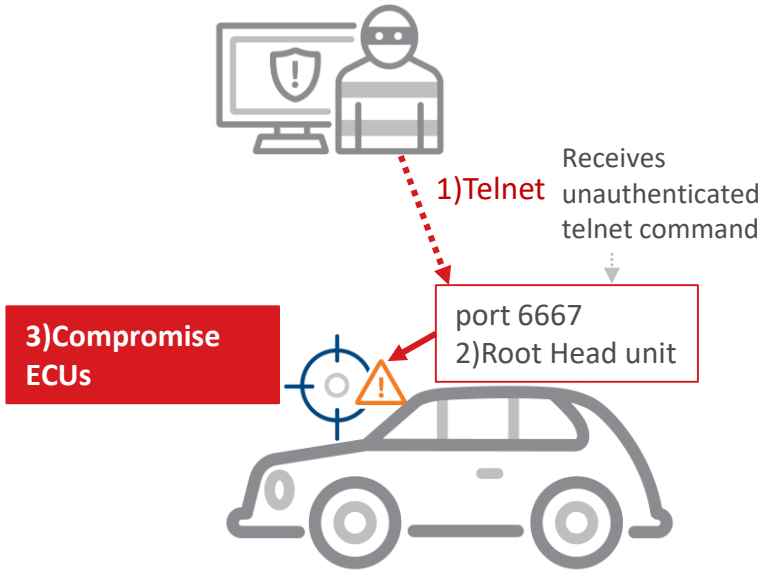


Protecting CASE Eco System

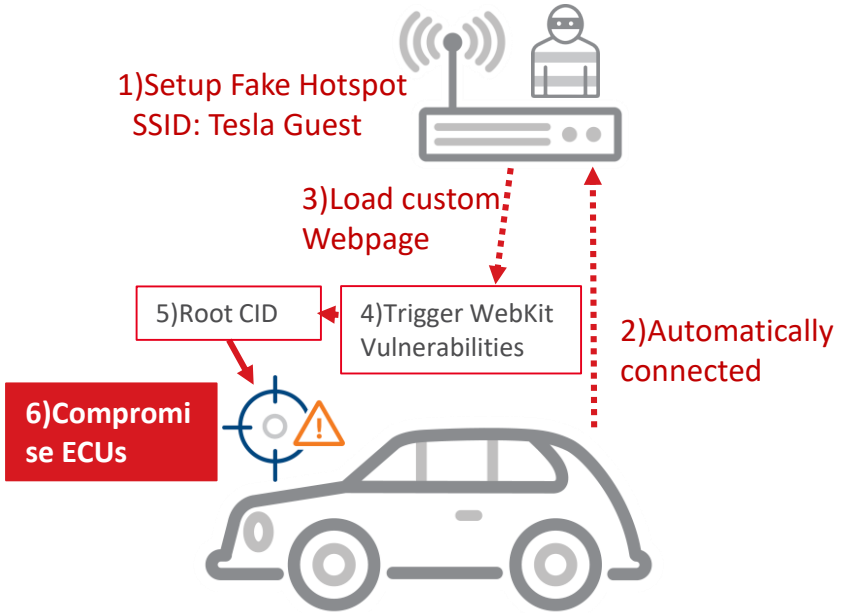
Behind the Scenes

Jeep Cherokee & Tesla Remote Hacking

Jeep Hack 2015

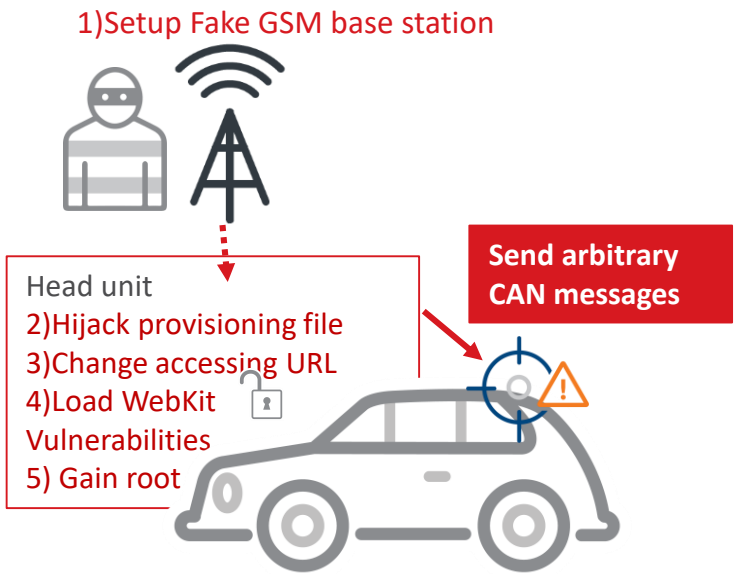


Tesla Hack 2016 & 2017

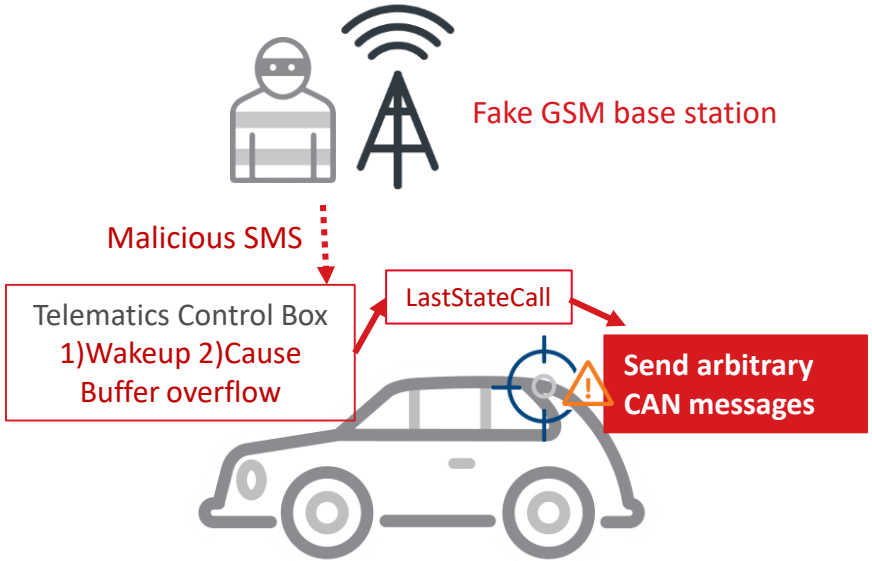


BMW Remote Hacking

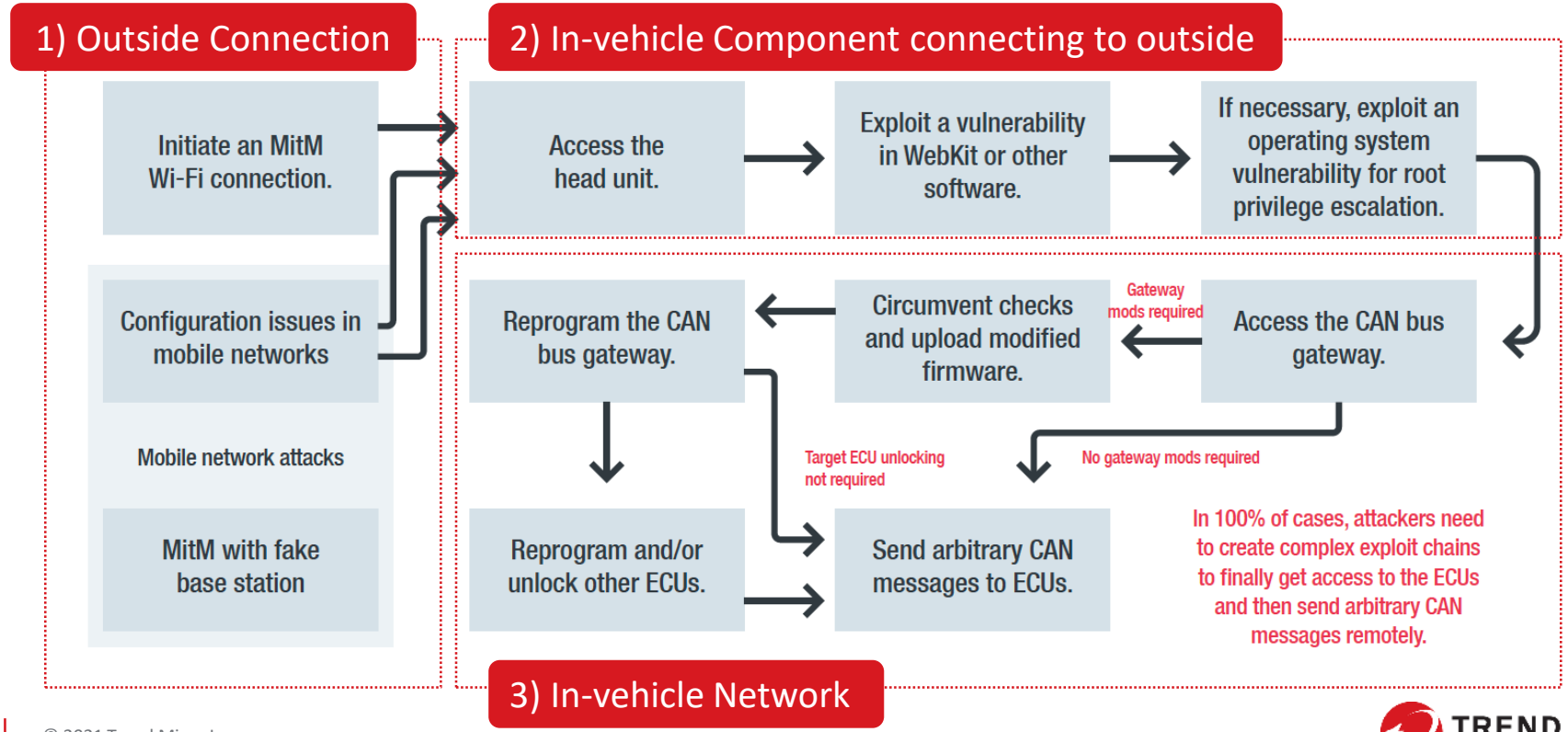
BMW Hack 2018 A



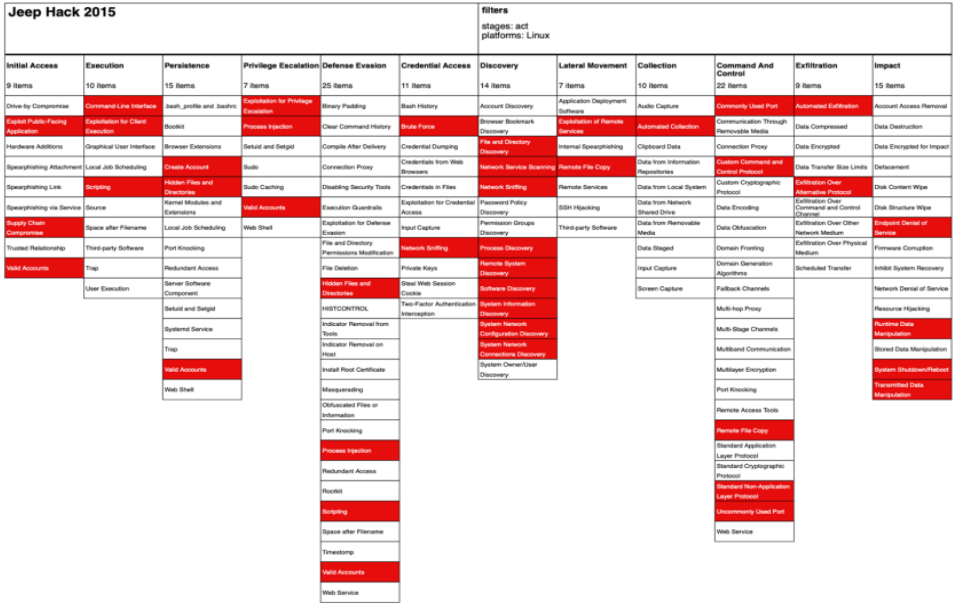
BMW Hack 2018 B



Generalized Remote Hacking Techniques



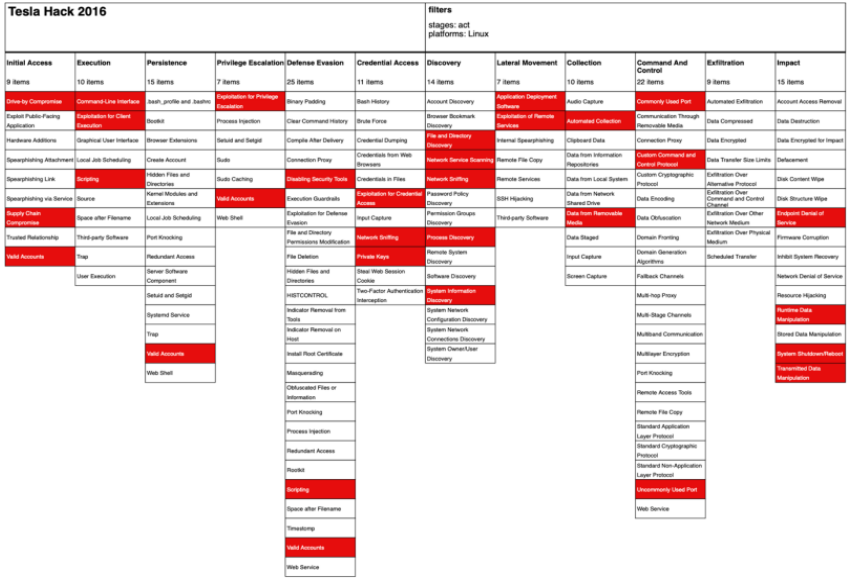
The Jeep/ Tesla Hack MITRE ATT&CK Matrix



Jeep Hack 2015

filters
stages: act
platforms: Linux

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
9 items	10 items	15 items	7 items	25 items	11 items	14 items	7 items	10 items	22 items	9 items	15 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Booktit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Sniffing	Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Password Policy Discovery	Remote Services	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Permission Groups Discovery	SSH Hijacking	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Trusted Relationship	Third-party Software	Port Knocking		File and Directory Permissions Modification	Network Sniffing	Process Discovery	Third-party Software	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Valid Accounts	Trap	Redundant Access		File Deletion	Private Keys	Remote System Discovery		Input Capture	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
	User Execution	Server Software Component		Hidden Files and Directories	Steal Web Session Cookie	Software Discovery		Screen Capture	Fallback Channels		Network Denial of Service
		Setuid and Setgid		HISTCONTROL	Two-Factor Authentication Interception	System Information Discovery			Multi-hop Proxy		Resource Hijacking
		Systemd Service		Indicator Removal from Tools		System Network Configuration Discovery			Multi-Stage Channels		Runtime Data Manipulation
		Trap		Indicator Removal on Host		System Network Connections Discovery			Multiband Communication		Stored Data Manipulation
		Valid Accounts		Install Root Certificate		System Owner/User Discovery			Multilayer Encryption		System Shutdown/Reboot
		Web Shell		Masquerading					Port Knocking		Transmitted Data Manipulation
				Obfuscated Files or Information					Remote Access Tools		
				Port Knocking					Remote File Copy		
				Process Injection					Standard Application Layer Protocol		
				Redundant Access					Standard Cryptographic Protocol		
				Rootkit					Standard Non-Application Layer Protocol		
				Scripting					Uncommonly Used Port		
				Space after Filename					Web Service		
				Timestomp							
				Valid Accounts							
				Web Service							

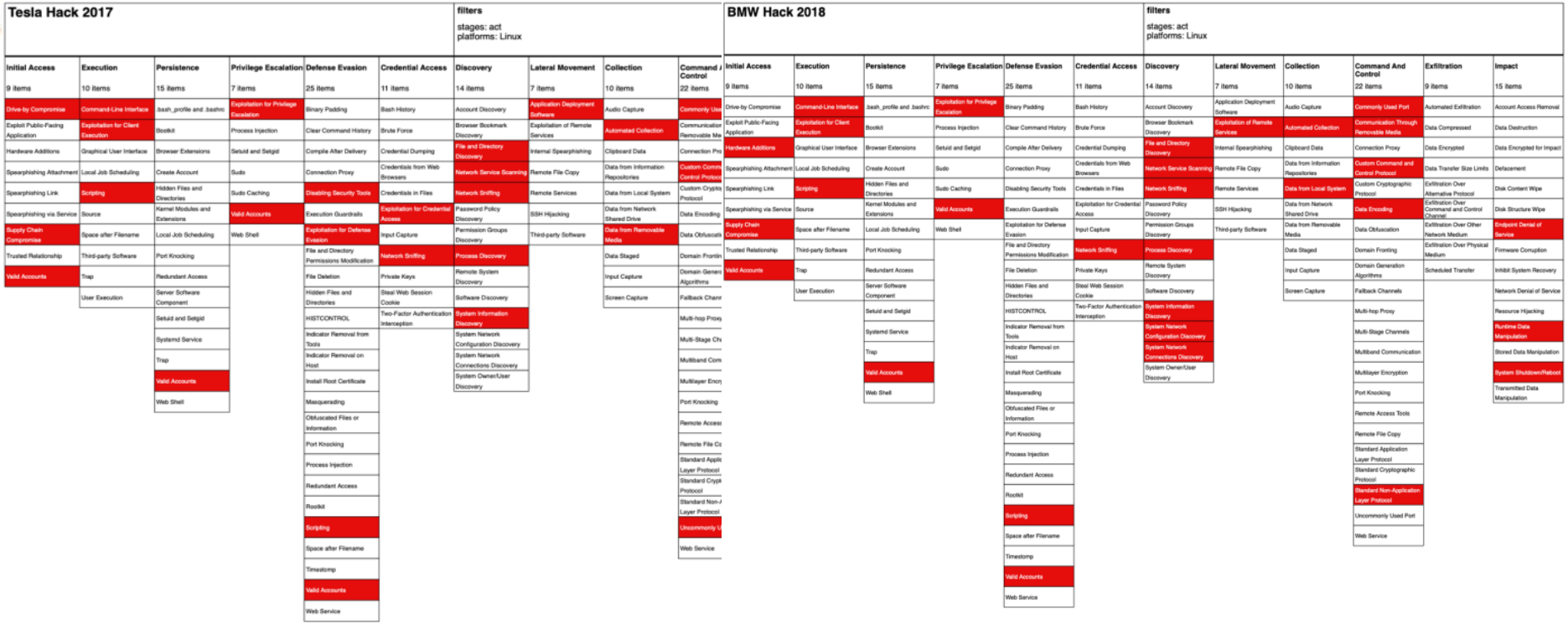


Tesla Hack 2016

filters
stages: act
platforms: Linux

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
9 items	10 items	15 items	7 items	25 items	11 items	14 items	7 items	10 items	22 items	9 items	15 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Booktit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Sniffing	Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Password Policy Discovery	Remote Services	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Permission Groups Discovery	SSH Hijacking	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Trusted Relationship	Third-party Software	Port Knocking		File and Directory Permissions Modification	Network Sniffing	Process Discovery	Third-party Software	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Valid Accounts	Trap	Redundant Access		File Deletion	Private Keys	Remote System Discovery		Input Capture	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
	User Execution	Server Software Component		Hidden Files and Directories	Steal Web Session Cookie	Software Discovery		Screen Capture	Fallback Channels		Network Denial of Service
		Setuid and Setgid		HISTCONTROL	Two-Factor Authentication Interception	System Information Discovery			Multi-hop Proxy		Resource Hijacking
		Systemd Service		Indicator Removal from Tools		System Network Configuration Discovery			Multi-Stage Channels		Runtime Data Manipulation
		Trap		Indicator Removal on Host		System Network Connections Discovery			Multiband Communication		Stored Data Manipulation
		Valid Accounts		Install Root Certificate		System Owner/User Discovery			Multilayer Encryption		System Shutdown/Reboot
		Web Shell		Masquerading					Port Knocking		Transmitted Data Manipulation
				Obfuscated Files or Information					Remote Access Tools		
				Port Knocking					Remote File Copy		
				Process Injection					Standard Application Layer Protocol		
				Redundant Access					Standard Cryptographic Protocol		
				Rootkit					Standard Non-Application Layer Protocol		
				Scripting					Uncommonly Used Port		
				Space after Filename					Web Service		
				Timestomp							
				Valid Accounts							
				Web Service							

The Tesla/ BMW Hack MITRE ATT&CK Matrix



Tesla Hack 2017

filters
stages: act
platforms: Linux

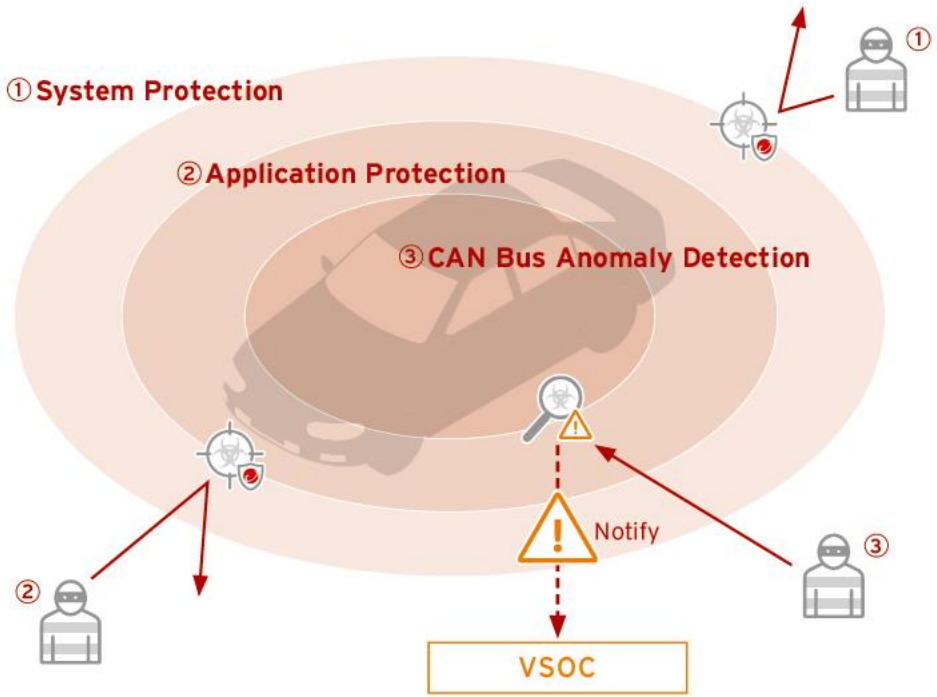
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control
9 items	10 items	15 items	7 items	25 items	11 items	14 items	7 items	10 items	22 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Sniffing	Remote Services	Data from Local System	Custom Cryptographic Protocol
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Password Policy Discovery	SSH Hijacking	Data from Network Shared Drive	Data Encoding
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Permission Groups Discovery	Third-party Software	Data from Removable Media	Data Obfuscation
Trusted Relationship	Third-party Software	Port Knocking		File and Directory Permissions Modification	Network Sniffing	Process Discovery		Data Staged	Domain Fronting
Valid Accounts	Trap	Redundant Access		File Deletion	Private Keys	Remote System Discovery		Input Capture	Domain Generation Algorithms
	User Execution	Server Software Component		Hidden Files and Directories	Steal Web Session Cookie	Software Discovery		Screen Capture	Fallback Channels
		Setuid and Setgid		HISTCONTROL	Two-Factor Authentication Interception	System Information Discovery			Multi-hop Proxy
		Systemd Service		Indicator Removal from Tools		System Network Configuration Discovery			Multi-Stage Channels
		Trap		Indicator Removal on Host		System Network Connections Discovery			Multiband Communication
		Valid Accounts		Install Root Certificate		System Owner/User Discovery			Multilayer Encryption
		Web Shell		Masquerading					Port Knocking
				Obfuscated Files or Information					Remote Access Tools
				Port Knocking					Remote File Copy
				Process Injection					Standard Application Layer Protocol
				Redundant Access					Standard Cryptographic Protocol
				Rootkit					Standard Non-Application Layer Protocol
				Scripting					Uncommonly Used Port
				Space after Filename					Web Service
				Timestomp					
				Valid Accounts					
				Web Service					

BMW Hack 2018

filters
stages: act
platforms: Linux

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
9 items	10 items	15 items	7 items	25 items	11 items	14 items	7 items	10 items	22 items	9 items	15 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Sniffing	Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Password Policy Discovery	SSH Hijacking	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Permission Groups Discovery	Third-party Software	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Trusted Relationship	Third-party Software	Port Knocking		File and Directory Permissions Modification	Network Sniffing	Process Discovery		Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Valid Accounts	Trap	Redundant Access		File Deletion	Private Keys	Remote System Discovery		Input Capture	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
	User Execution	Server Software Component		Hidden Files and Directories	Steal Web Session Cookie	Software Discovery		Screen Capture	Fallback Channels		Network Denial of Service
		Setuid and Setgid		HISTCONTROL	Two-Factor Authentication Interception	System Information Discovery			Multi-hop Proxy		Resource Hijacking
		Systemd Service		Indicator Removal from Tools		System Network Configuration Discovery			Multi-Stage Channels		Runtime Data Manipulation
		Trap		Indicator Removal on Host		System Network Connections Discovery			Multiband Communication		Stored Data Manipulation
		Valid Accounts		Install Root Certificate		System Owner/User Discovery			Multilayer Encryption		System Shutdown/Reboot
		Web Shell		Masquerading					Port Knocking		Transmitted Data Manipulation
				Obfuscated Files or Information					Remote Access Tools		
				Port Knocking					Remote File Copy		
				Process Injection					Standard Application Layer Protocol		
				Redundant Access					Standard Cryptographic Protocol		
				Rootkit					Standard Non-Application Layer Protocol		
				Scripting					Uncommonly Used Port		
				Space after Filename					Web Service		
				Timestomp							
				Valid Accounts							
				Web Service							

Trend Micro IoT Security for Automotive



①System Protection

- Vulnerability Scan
- Host Based IPS(Virtual Patch)
- Safelist
- Hypervisor Protection
- IoT Reputation Service etc.

②Application Protection

- Web Reputation Service
- Android App Security etc.

③CAN Bus Anomaly Detection

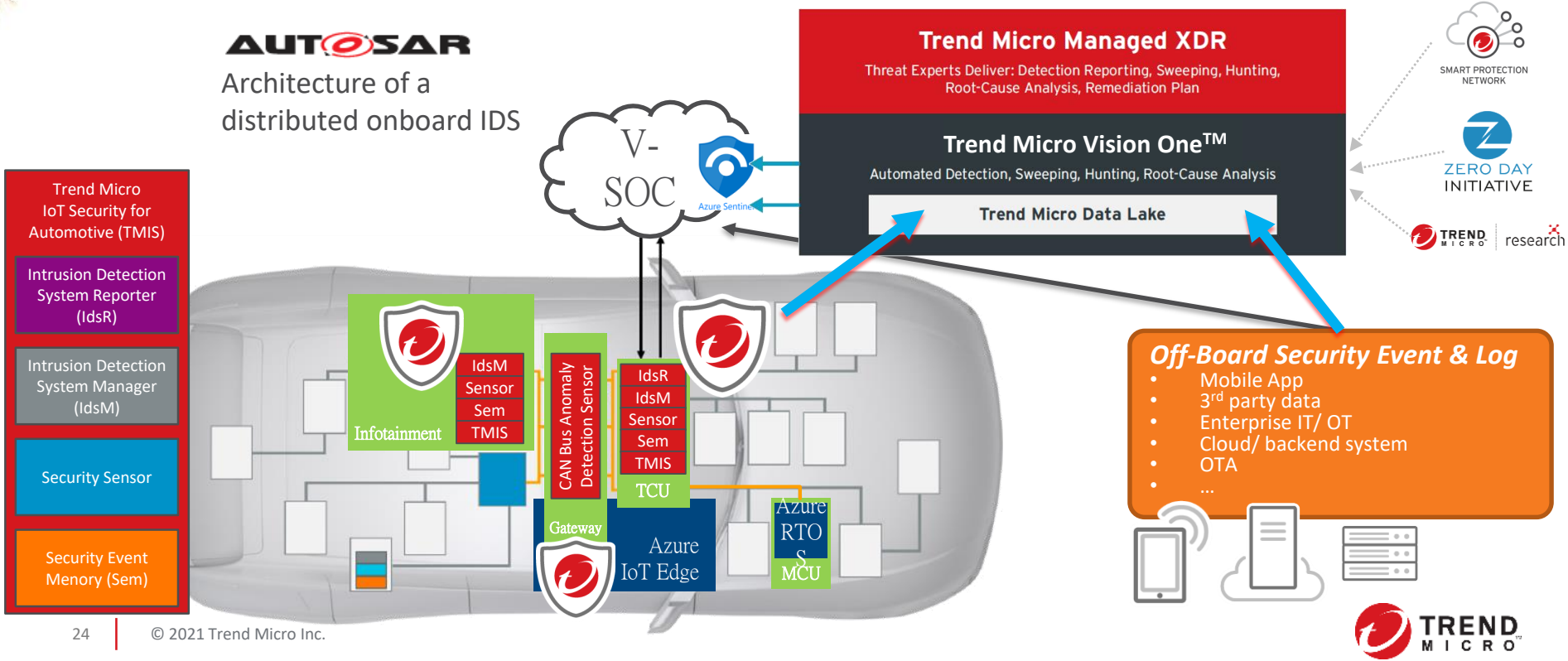
- CAN Bus ID validation
- Frequency check
- Payload structure check
- Payload sequence check etc.

SMART PROTECTION NETWORK

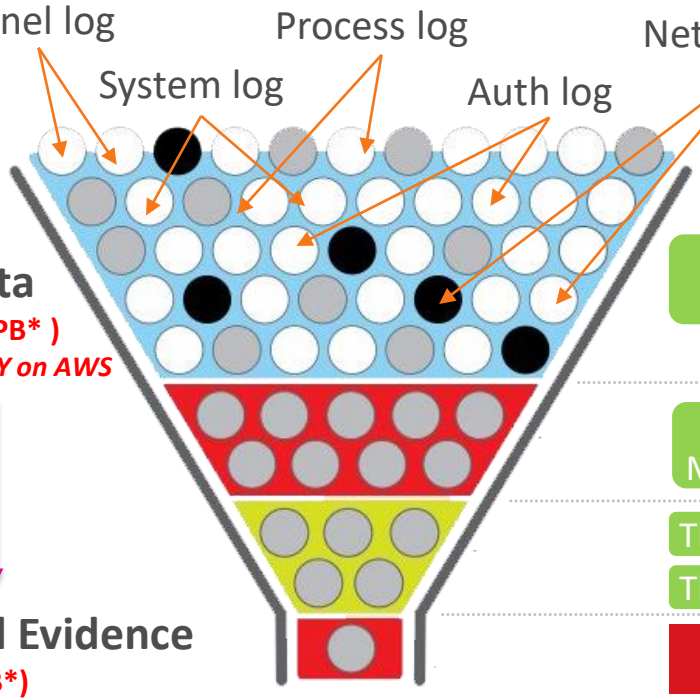
TMIS + XDR Deployment (Reduce SOC Effort)

AUTOSAR

Architecture of a distributed onboard IDS



On-Board Inteligent Sensor (Reduce Data Volume)



Big Data
(≥ 40.52PB*)
~1M USD/Y on AWS

-99.35%

Critical Evidence
(267.42TB*)

*1M cars on the road/ year in U.S

HIDPS

ML Model

ML Model

Threat Expert Rule

Threat Expert Rule

TMIS Sensor

SMART PROTECTION NETWORK

TREND MICRO research

ZERO DAY INITIATIVE

Delivery:
Detection Reporting, Sweeping, Hunting, Behavior Analysis, Root-Cause Analysis, Remediation Plan

Sensor Improvement:
Machine Learning Model, Threat Expert Rules, HIDPS

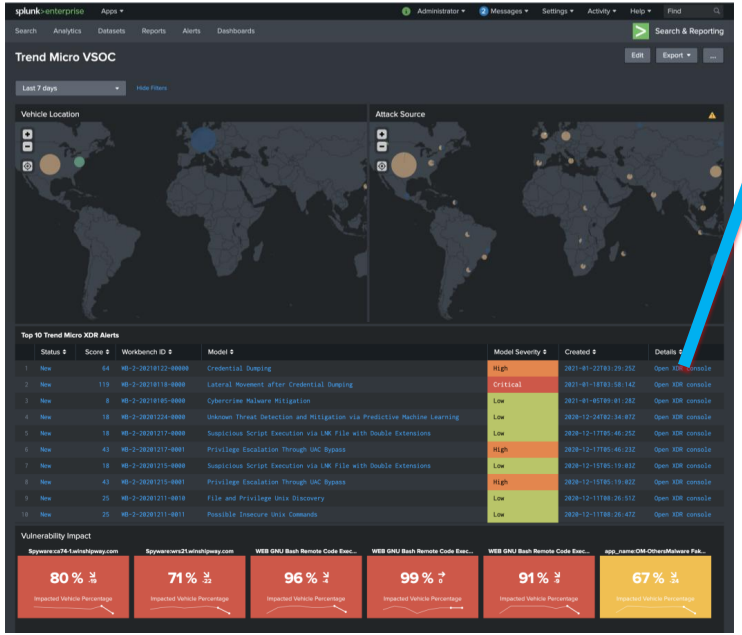
Trend Micro Vision One™

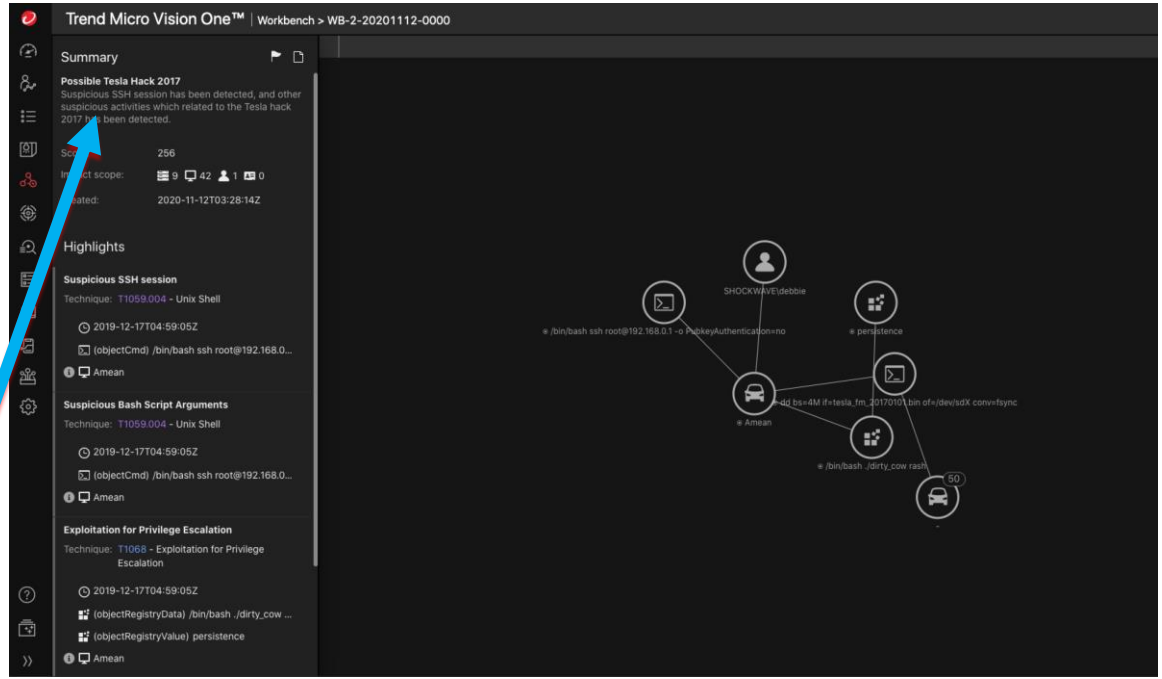
Critical Logs

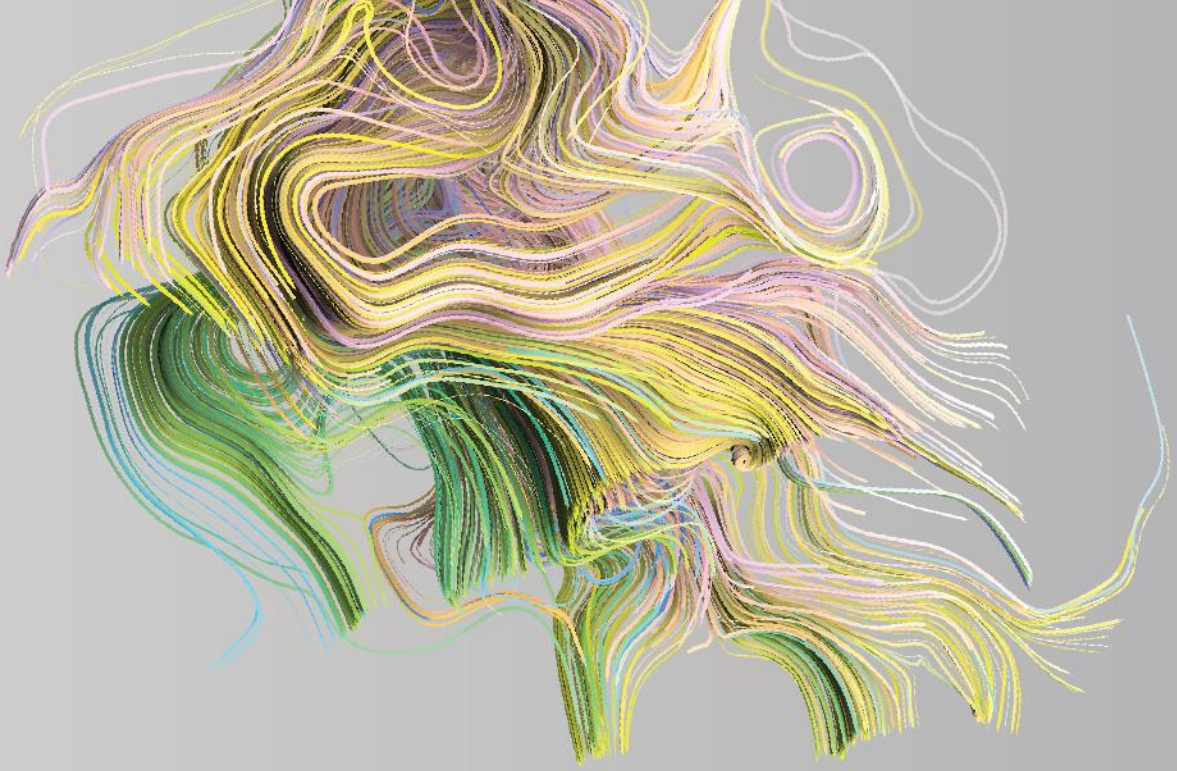
TREND MICRO

Vehicle-SOC/ SIEM

Trend Micro Vision One for Vehicle-SOC







Better Together

Industry Partner & Contribution

Mindset Shift – OPEN – Better Together

- CASE Vehicle
  - is a massive system of systems
  - is transforming into super high spec mobile PC with wheels and high-speed connection

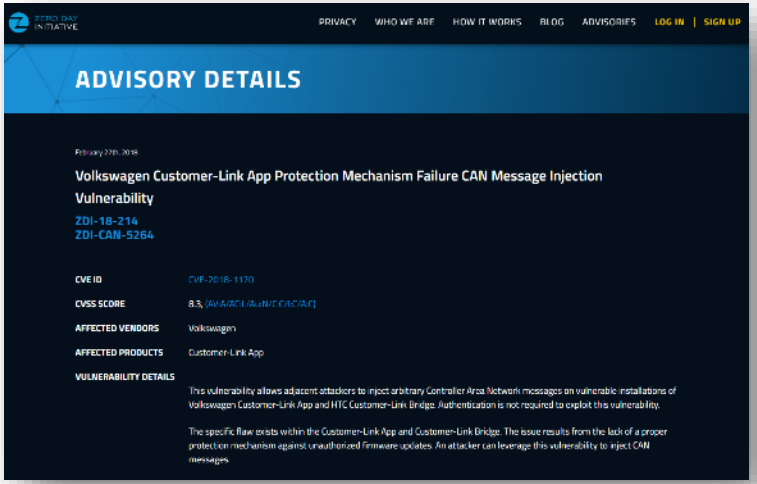
  => Transforming to system with vulnerabilities remote attacks are possible

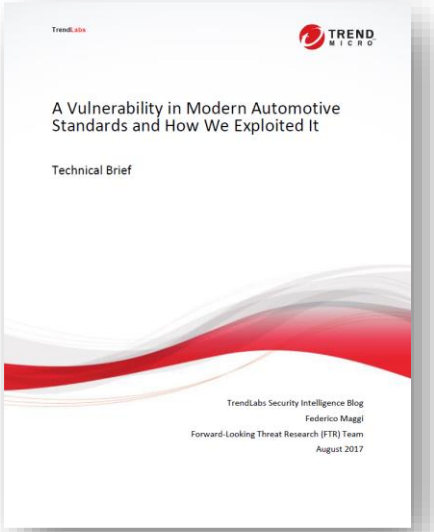
- Plan with “CYBER security” mindset
  - Exclusivity Will Not Provide Protection
    - Work across industries to learn how incidents can affect decisions
  - Develop Automotive/IT Security Industry Partnerships
    - Leverage lessons learned, implement best practices and share intelligence on the research space

Auto Vulnerability Reported by Trend Micro

Research reports and vulnerabilities by Forward-Looking Threat Research (FTR) Team

- Volkswagen Customer-Link App Protection Mechanism Failure CAN Message Injection Vulnerability
  - https://www.zerodayinitiative.com/advisories/ZDI-18-214/
- Connected Car Vulnerabilities Affect the CAN Standard
  - https://www.trendmicro.com/en_us/research/17/h/connected-car-hack.html



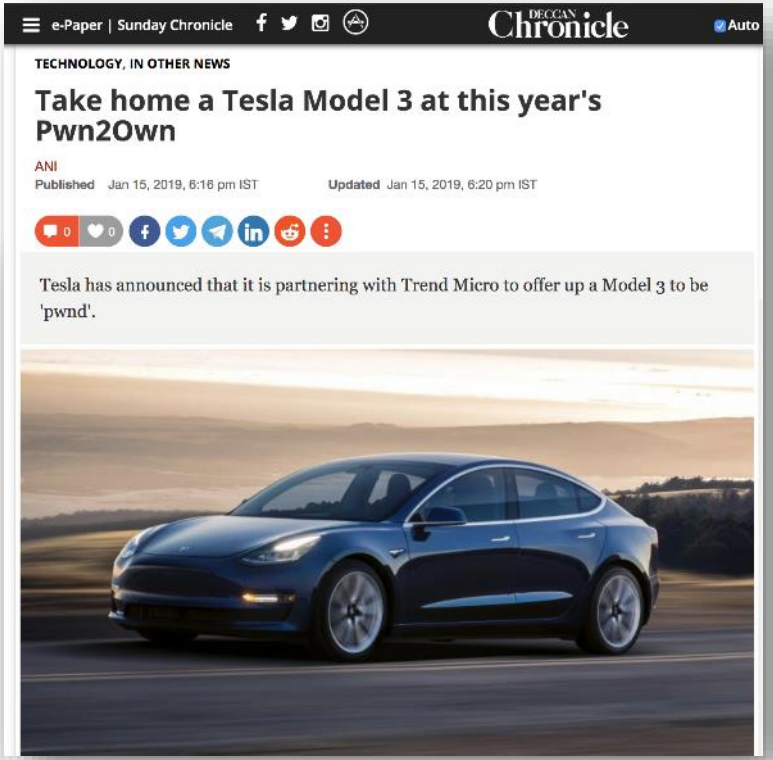


TREND MICRO | research

Tesla Vulnerability Reported by Trend Micro's ZDI

- The Zero Day Initiative (ZDI) was created to encourage the reporting of 0-day vulnerabilities privately to the affected vendors by financially rewarding researchers.
- Pwn2Own 2019 wraps up with the first successful entries in the automotive category. In all, we awarded $545,000 USD for 19 unique bug reports - and, of course, the car itself.

https://www.cyberscoop.com/tesla-hacked-pwn-2-own-2019/



https://www.deccanchronicle.com/technology/in-other-news/150119/take-home-a-tesla-model-3-at-this-years-pwn2own.html

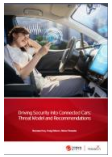
Trend Micro's Automotive Expertise

2017 — Vulnerabilities Affect the CAN

2017 — Cyberattack against ITS

2020 — ISO/SAE 21434

2020 — Threat Modeling &recommendation



and so on

Automotive Research

Research Community Engagement

PoC Record & customer

Contribution to Industrial Consortium

ZERO DAY INITIATIVE

Automotive Hacking contest with Tesla

Invited talk about automotive specific vulnerability management at escar 2020

Top Japanese and Chinese OEMs and Tier1s (names are confidential)

Panasonic

Luxoft A DXC Technology Company

GENIVI

Automotive Grade Linux

Mentor A Siemens Business

GENIVI

JasPar

Automotive Grade Linux

The Linux Foundation

MONET Consortium

CRANTS

Landlog

浜松市 Hamamatsu City

OCCI The Osaka Chamber of Commerce and Industry

and so on

TREND MICRO

TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**