FOR IMMEDIATE RELEASE

Hitachi Astemo, Trend Micro, and VicOne Expand Collaboration on Security Solutions for Connected Cars, Targeting 2025 Commercialization

Tokyo, January 24, 2023 – Hitachi Astemo, Ltd. ("Hitachi Astemo"), Trend Micro Inc. ("Trend Micro") and its subsidiary VicOne Inc. ("VicOne") have expanded their collaboration to provide security solutions for connected cars, aiming for commercialization by 2025.

Hitachi Astemo's division that develops in-vehicle components for connected cars has been working with Trend Micro on the joint development of security solutions for connected cars*1 since October 2021*2. Now, Hitachi Astemo,Trend Micro and VicOne, will expand collaboration on security solutions for the in-vehicle side of the business. The collaboration will combine Hitachi Astemo's Edge-SIEM*3 security solution for automobiles with Trend Micro and VicOne's xCarbon*4 embedded security solution for in-vehicles, and will provide security solutions to detect and mitigate cyber attacks and their risks to connected cars on the in-vehicle side by 2025.

*1 October 19, 2021 announcement regarding the joint development of security solutions for connected cars.(https://www.hitachi.com/New/cnews/month/2021/10/211019.html)
*2 During this period, the Division in question had been temporarily transferred to Hitachi, Ltd.
*3 SIEM (Security Information and Event Management) centrally manages and analyzes IT equipment logs to detect problematic threats. Edge-SIEM plays the role of SIEM at the periphery (Edge) of the in-vehicle network. At the time of the October 19, 2021 announcement, this intrusion detection system was called an "IDS (Intrusion Detection System)and it had been further enhanced as the Edge-SIEM.
*4 xCarbon is a solution that detects and prevents abnormal communication and unauthorized access.

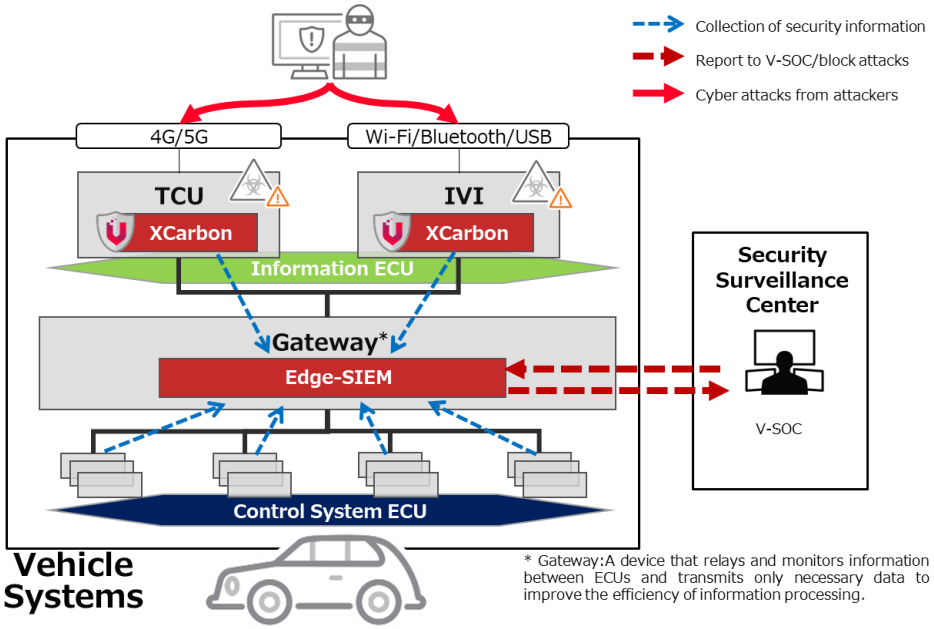
Specifically, xCarbon protects information-related ECUs*5 from cyber attacks, including devices that communicate over the Internet (TCU*6) installed in vehicles and information systems (IVI*7) with embedded high-performance OS such as car navigation systems. xCarbon detects and blocks, in real time, attacks that exploit vulnerabilities, communications with command and control (C&C) servers*8 that are remotely controlled by cyber attackers, communications used by malware, and unauthorized file rewriting.

*5 ECU (Electronic Control Unit) is a generic name for a computer that controls the systems built into automobiles using electronic circuits.
*6 TCU (Telematics Control Unit) is a communication module that can be connected to mobile communication networks.
*7 IVI (In-Vehicle Infotainment) is a device that provides information and entertainment needed by the driver and passengers.
*8 Command and control (C&C) servers are command servers that control bot networks for cyber attackers to issue commands to malware and receive stolen information.

Furthermore, by placing Edge-SIEM in the central gateway, which is responsible for the central communication control of the vehicle network, log information such as gas and brake pedal operation and car navigation system manipulation is collected from each control ECU and information ECU to monitor the behavior of the entire vehicle system. Edge-SIEM monitors and determines suspicious behavior in the vehicle, including braking and accelerating, and immediately notifies V-SOC*9, the automaker's security monitoring center, if there is a

possibility of a cyber attack. At this time, xCarbon functions as a security sensor for Edge-SIEM and provides the security logs of information ECUs such as TCU and IVI to Edge-SIEM. By collecting information, making decisions, and notifying in the vehicle, xCarbon reduces the monitoring burden on the V-SOC, blocks attacks in real time, and supports early response to cyber-attacks.

*9 V-SOC (Vehicle Security Operation Center): An organization that detects and analyzes cyber attacks on vehicles and takes countermeasures.



Solution Construction Image

In August 2022, a verification experiment was conducted using Hitachi Astemo's central gateway equipped with Edge-SIEM and a pseudo-IVI equipped with xCarbon in an environment simulating an actual vehicle. In the experimental environment, cyber attacks that attempted to steal a vehicle by exploiting a vulnerability in the IVI, entering the vehicle network, and use of unauthorized commands was detected by xCarbon at the intrusion stage and transmitted to Edge-SIEM. The solution was confirmed to be effective in preventing the attack by blocking the transmission of unauthorized commands from the IVI. The three companies aim to commercialize the solution for connected car by 2025.

A technical demonstration using the same attack scenario as the demonstration test conducted in August 2022 will be presented at the Trend Micro exhibit booth*10 at the 15th Connected Car Expo, Automotive World, to be held at Tokyo Big Sight from January 25 (Wednesday) to 27 (Friday), 2023.

*10 Comprehensive exhibition of Automotive. Trend Micro will be exhibiting and demonstrating its security products for automobiles at the Trend Micro booth in booth #48-7.
https://www.nepconjapan.jp/tokyo/en-gb/search/2023/directory/directory-details.org-5fdb8642-5554-48a6-937f-592f5612f00e.html#/

■Background of Collaboration

The importance of cyber security in connected vehicles is growing, as any breach or tampering with vehicle systems can seriously affect vehicle functionality. From UN-R155, an international regulation on cyber security for automobiles established by the World Forum for Harmonization of Vehicle Regulations (WP.29), automobile manufacturers are required to conduct security monitoring for connected cars to detect and respond to cyber attacks. As a result, in Japan, from July 2022, when selling vehicles that support firmware updates via wireless communication, it will be necessary to comply with the law in order to obtain formal certification, and security measures are now mandatory. In addition, it is necessary to reduce the risk of cyber threats entering the connected car by implementing cyber attack countermeasures against points that could be exploited as the starting point of a cyber attack on the connected car or as an attack surface (attack target area) to expand the intrusion.

■Related Links

Hitachi Astemo Connected Car Security
https://www.hitachiastemo.com/en/products/connected/vsoc.html

Trend Micro Connected Car Security
https://www.vicone.com/

VicOne　VicOne Leads the Way Toward Automotive Cybersecurity
https://www.vicone.com/company#about-us

■About Hitachi Astemo

Hitachi Astemo is committed to strengthening its business and delivering technological innovation through a strategic business portfolio that includes a Powertrain & Safety Systems business, Chassis business, Motorcycle business, Software business and Aftermarket business. Aiming for growth driven by "green," "digital," and "innovation," Hitachi Astemo will contribute to a better global environment with highly efficient internal combustion engine systems that reduce emissions; electric systems, and also enhance safety and comfort with autonomous driving systems; advanced driver assistance systems; and advanced chassis systems. Through such advanced mobility solutions, Hitachi Astemo will contribute to realizing a sustainable society and provide enhanced corporate value for its customers.

■About Trend Micro

Trend Micro has been consistently engaged in the cyber security field for more than 30 years since its establishment with the vision of "creating a world where digital information can be exchanged securely. As a leader in cyber security, we contribute to the safety of society by continuously providing security solutions that respond quickly to constantly evolving digital technologies and markets. We also make security information obtained through our own research, analysis, and studies widely available to the public, and work with law enforcement agencies such as the FBI and Interpol, as well as international organizations, to promote the elimination of cyber crimes that lurk in society. Trend Micro will continue its efforts to realize a safe and secure society.

■About VicOne

With a vision to secure the vehicles of tomorrow, VicOne delivers a broad portfolio of cybersecurity software and services for the automotive industry. Purpose-built to address the rigorous needs of automotive manufacturers, VicOne solutions are designed to secure and scale with the specialized demands of the modern vehicle. As a Trend Micro subsidiary, VicOne is powered by a solid foundation in cybersecurity drawn from Trend Micro's 30+ years in the industry, delivering unparalleled automotive protection and deep security insights that enable our customers to build secure as well as smart vehicles. For more information, visit https://www.vicone.com/

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
