Hitachi, Trend Micro, Microsoft Japan
Agreed to Develop Security Solutions for Connected Cars Jointly

Tokyo, October 19, 2021 – Hitachi, Ltd. (TSE:6501, "Hitachi"), Trend Micro Incorporated (TYO: 4704; TSE: 4704. “Trend Micro”), and Microsoft Japan Co., Ltd. have agreed to develop a security solution for connected cars jointly.

Specifically, the three companies will combine Hitachi's automotive and IT solutions, Trend Micro automotive and cloud security solutions, threat intelligence, and Microsoft's cloud platform will be jointly developed for connected cars, including security solutions inside connected vehicles that detect, analyze, and manage cyberattacks on automobiles and peripheral systems. The solutions will be rolled out to automotive manufacturers and suppliers in Japan by the end of 2022 and followed by global markets.

<The points of solutions provided through collaboration>

1. Detecting and preventing cyberattacks and risks on vehicles
   - For information systems*[1] in the cars connected to the Internet, such as car navigation systems, cyberattacks are detected and blocked using Trend Micro's automotive security solution "Trend Micro IoT Security for Automotive."

   - For the security of control systems*[2], such as gas pedals and brakes, and systems that communicate between control and information systems, Hitachi's original in-vehicle Intrusion Detection System is used to reduce the operational load of monitoring with fewer false positives and over-detections.

   - Using the security solutions provided by Trend Micro and Hitachi for vehicles, the security sensor logs, such as attacks and communication abnormalities that exploit vulnerabilities, are collected and sent to the cloud.

2. Providing a highly functional and secure cloud platform
   - Build a platform for detecting, analyzing, and managing cyberattacks related to automobiles on Microsoft Azure. With a streamlined data processing capability that captures millions of events per second and the storage database, security logs, and alerts will be separated into analytical data for threat detection and data needed as evidence.

   - In this initiative, security and compliance support is provided by Azure. Leverage Microsoft Intelligent Security Graph, which consists of approximately 8.2 trillion security signals per day, to help you detect the latest security threats.

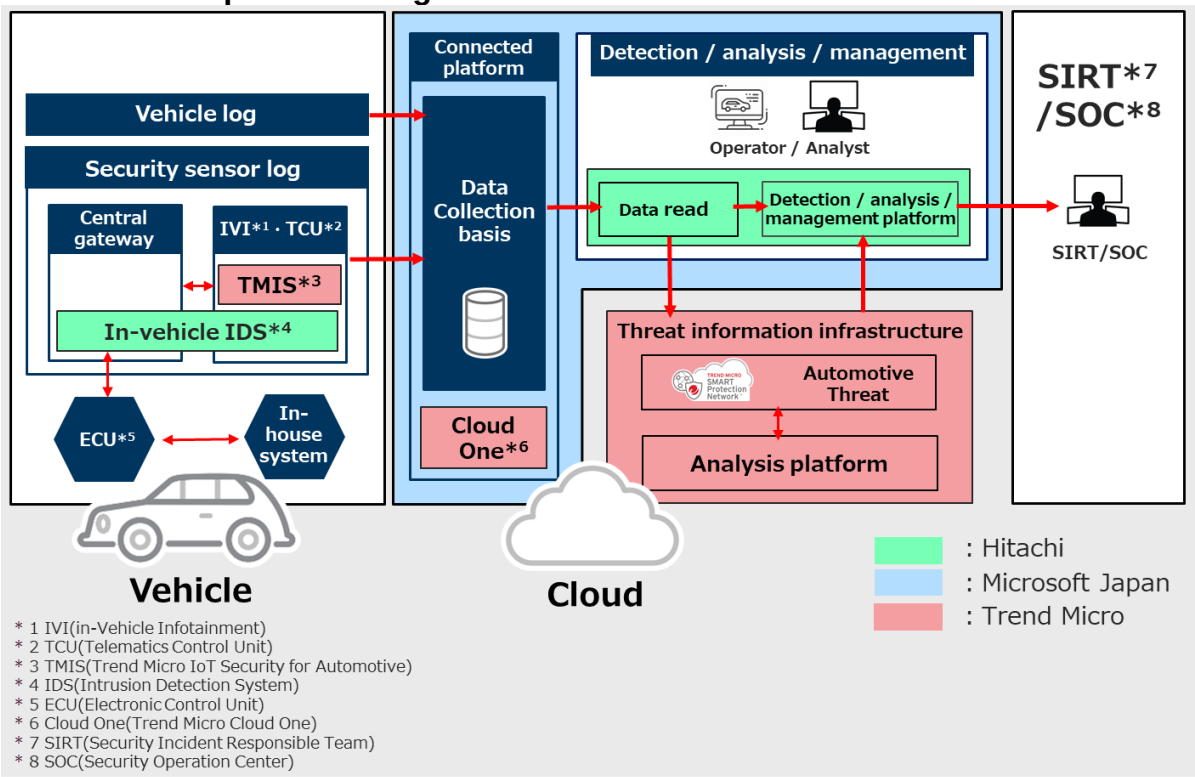
   - The cloud platform where various automotive data is stored is protected by Trend Micro's cloud security solution, "Trend Micro Cloud One."

[1] Information systems refer to in-vehicle infotainment devices (IVI: in-Vehicle Infotainment) such as car navigation systems.
[2] Control system refers to devices that control the running of automobiles, such as accelerators and brakes.

- more -

3. Visualizing the overall picture of cyberattacks in collaboration with vehicle data
   - The solution consolidates security sensor logs for attacks and communication abnormalities that exploit vulnerabilities in vehicles. These include the activation status of information systems, such as car navigation systems, and operating status of control systems, such as accelerators and brakes, and vehicle logs, such as driving information in the cloud. By utilizing Trend Micro's comprehensive threat intelligence, linking security sensors, vehicle log information, detection mechanism, data, and threat analysis, connected cars benefit from enhanced protection. In addition, the threat monitoring platform provides necessary log data for incident response and countermeasures, enabling early detection and the prompt initial response by Security Incident Response Team and Security Operation Center.

<Solution composition image>



<Background of collaboration>

The connected cars market is growing along with the expansion of digital technology, which enables external networks to collect and analyze various data on automobiles and surrounding road conditions to improve safety and convenience. However, smart cars are exposed to the threat of cyberattacks because of their connection to the Internet. Continuous security and threat monitoring are required inside the connected cars and the platform to reliably detect and respond to incidents and signs of cyberattacks.

In addition, automobile manufacturers that sell passenger vehicles, including but not limited to trucks, buses, trailers, that operate on public roads must comply with local laws and regulations to ensure safety. For example, the United Nations World Forum for Harmonization of Automotive Standards (WP.29) established international standards for cybersecurity. New models sold in Japan and Europe are required to comply beginning July 2022.

A comprehensive view of vehicle data is essential to protect connected cars from cyberattacks effectively. In addition to the mechanisms that protect the cloud where data transmitted from the vehicle is stored, data correlation logic that assesses transmitted data from each component is required to identify signs of cyberattacks and provide effective mitigation.

In such a situation, a solution that can monitor and secure many vehicles operating globally against the ever-evolving attack requires a highly coordinated cloud security, IT system, and automobile infrastructure.

Related websites
Hitachi Connected Car Security
https://www.hitachi.com/products/life/portal/index.html

Trend Micro Connected Car Security
https://www.trendmicro.com/en_us/business/solutions/iot/connected-car.html

Microsoft Japan Automotive
https://www.microsoft.com/en-us/industry/automotive

# # #

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.
