ESET THREAT INTELLIGENCE

Threat Intelligence for the Automotive Industry

The automotive sector remains a key target for cyberattacks and hacking incidents. As vehicles become more connected and software-driven, the opportunities for attackers are increasing. Modern infotainment systems, telematics, over-the-air updates, and autonomous features also make vehicles more vulnerable to cyber threats.

Automotive-specific threat intelligence and reports allow manufacturers and suppliers to stay informed about novel exploits, providing paths to mitigate these threats. Given the need for enhanced supply chain security, threat intelligence also offers the insights needed to monitor third-party software and hardware components for indicators of potential compromise, a critical concern.

On the regulatory side, threat intelligence plays a key part in compliance support for automotive manufacturers by helping to meet cybersecurity standards like ISO/SAE 21434 and UNECE WP.29.

THE MAIN CONCERNS OF AUTOMOTIVE FIRMS

- ✓ Connected vehicle and automotive infrastructure vulnerabilities
- ✓ Software and firmware vulnerabilities, including potential compromises
- ✓ Supply chain weaknesses and pain points
- ✓ Ransomware and malware

THEIR CRITICAL NEEDS

- ✓ Protection against cyber threats targeting connected vehicles and infrastructure
- ✓ Real-time threat detection and incident response
- ✓ Compliance with automotive cybersecurity regulations

HOW CAN ESET THREAT INTELLIGENCE HELP?

ESET is a trusted provider of cyber threat intelligence to the automotive sector, with 38 years of experience in cybersecurity. Our global presence, built up over decades, provides us with a rich and diverse intelligence library drawn from more than 100 million nodes.

By leveraging ESET's Data Feeds and APT Reports, you gain access to high-quality, actionable insights that enhance your threat detection and response capabilities. ESET goes well beyond just collecting indicators—we employ advanced AI technology and expertise to provide your organization with real added value.

We deliver actionable intelligence that leads to faster, better decisions

We provide unique insights that enable a profound understanding of the threat landscape

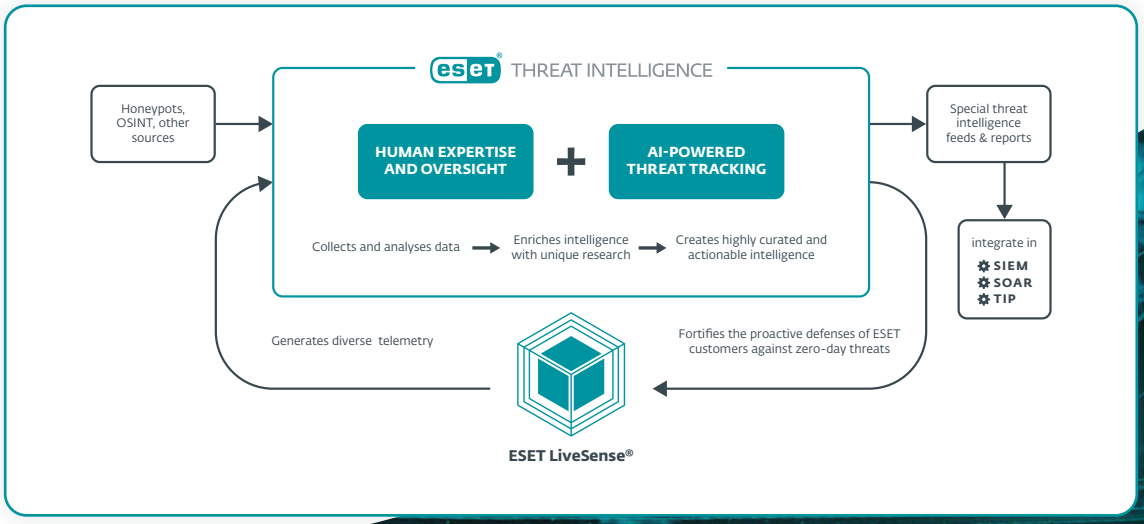
We allow you to proactively zoom in on new and emerging threats

We enable you to prioritize threat investigation, and thus minimize impact

Unique, Enriched Intel for Actionable Insights

Threat intelligence is not just about collecting indicators and wrapping them up—ESET goes well beyond that. We employ advanced technology and extensive expertise to process and enrich our intelligence, ensuring it provides real value to your business.

1. **Comprehensive Telemetry:** ESET LiveSense, integrated within the ESET PROTECT Platform, delivers broad and deep collection of data from a hugely diverse range of telemetry.
2. **Diverse Collection Methods:** We also utilize diverse collection and monitoring methods, including honeypots, sensors, OSINT, and more, to gather large volumes of quality data.
3. **Advanced Processing:** All data is processed through our robust backend systems, which leverage AI to classify and analyze intel so that only the most relevant and actionable is surfaced.
4. **Expert Analysis:** Beyond automated processing, our skilled threat intelligence analysts and researchers play a crucial role, going beyond what machine learning and automation alone can achieve.



Threat Intelligence, Tailored by ESET for the Automotive Sector

ESET delivers cutting-edge cyber threat intelligence for the automotive sector, leveraging 38 years of cybersecurity expertise. Our Data Feeds and APT Reports are tailored to protect connected vehicles and automotive infrastructure from sophisticated cyber threats. ESET's comprehensive telemetry and expert analysis provide real-time threat detection and actionable insights, helping you comply with automotive cybersecurity regulations and enhance your threat detection and response capabilities. Organizations in the automotive sector can benefit from our Malicious Data Feed, Ransomware Feed, Botnet Feed, and APT IOC Feed to protect connected vehicles and infrastructure.

MALICIOUS DATA FEED

Gain valuable insights from this real-time feed, which provides information on newly discovered malware samples, their characteristics, and IoCs. The feed includes details such as file hashes, timestamps, and identified threat types.

RANSOMWARE FEED

Combat ransomware with real-time data on prevalent samples. Our feed provides insights into active ransomware families, enabling proactive blocking. Stay ahead of threats and protect your organization from data breaches and costly disruptions.

BOTNET FEED

Leverage insights from ESET's proprietary botnet tracker network with our Botnet Feed. This feed comprises three sub-feeds: botnet, command and control (C&C), and targets. It provides crucial data, including detection details, file hashes, IP addresses, and more.

APT IOC

Benefit from valuable information from ESET's proprietary APT Feed, which provides insights into advanced persistent threats (APTs) based on ESET's meticulous research and long experience of APT detection and remediation.