ARGUS
CYBER SECURITY

Product Overview

Argus Vehicle Vulnerability Management

Understand your vehicle vulnerability risk exposure, respond fast, and manage cyber security processes across the organization.

AUTOMOTIVE VULNERABILITIES ON THE RISE

Software vulnerabilities that may compromise vehicles are being discovered at an alarming rate—putting your brand, drivers, and public safety at risk. To address this threat, cyber security regulations and standards such as UNR 155 and ISO/SAE 21434 require vehicle manufacturers to continually monitor, manage, and mitigate vulnerabilities.

KEY BENEFITS

- Understand your vehicle cyber risk exposure
- Know what issues matter most
- Reduce time from detection to response
- Discover vulnerabilities, even without a software bill of materials (SBOM)
- Streamline vulnerability & cyber security management and comply with regulations and standards (UNR 155 and ISO/SAE 21434)
- Leverage unmatched expertise based on 200 person-years of automotive cyber security research

UNDERSTAND YOUR EXPOSURE WITH A TOOL BUILT FOR AUTOMOTIVE

Argus Vehicle Vulnerability Management (VVM) solution continually monitors your vehicle assets for vulnerabilities, identifies and prioritizes your highest points of risk, and provides an immediate plan for mitigation.

Designed specifically for vehicle vulnerability management, the tool enables vehicle manufacturers to gain immediate insights into what software packages are affected, on which ECUs, and in which vehicles, together with a precise impact analysis of each vulnerability. Argus VVM reduces your vulnerability risk exposure and helps you comply with automotive standards and best practices.

KEY FEATURES

- Automotive-oriented asset management
- Automatic vulnerability search across all assets
- Impact analysis & automatic prioritization
- Mitigation recommendations
- Cyber security knowledge management
- Evidence and reports for type approval process

EXPAND YOUR INTELLIGENCE PICTURE

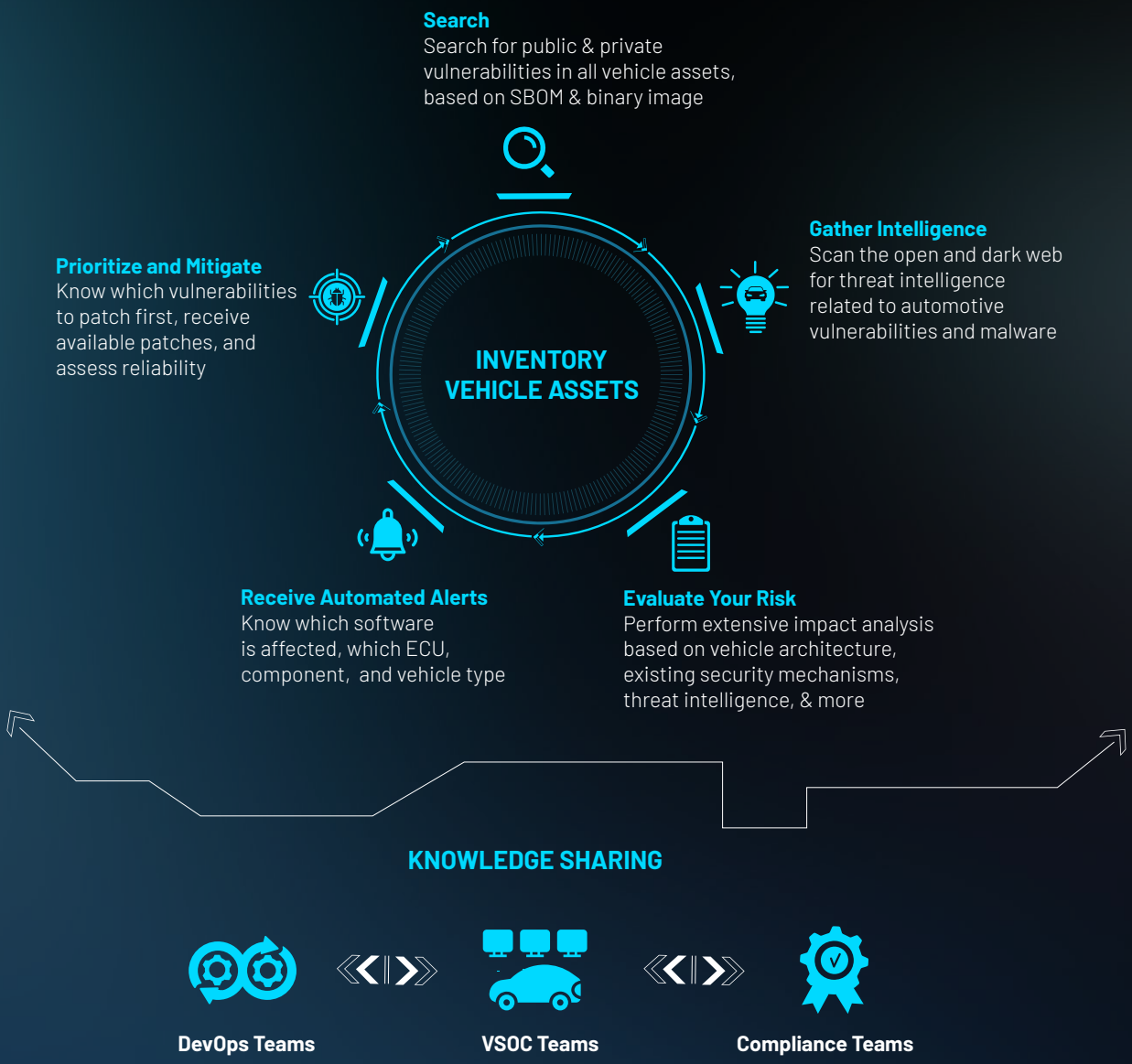
Argus VVM delivers detailed impact analysis reports that consider the vehicle architecture, surrounding cyber security mechanisms, and existing service agreements. This information is fused with automated threat intelligence feeds from the open and dark web, such as hacker forums, to provide a broad and up-to-date view of today's dynamic threat landscape.

AUTOMATIC PRIORITIZATION & MITIGATION RECOMMENDATION

Leveraging a wide intelligence picture and focused on reducing remediation efforts, Argus VVM automatically white lists and filters information to minimize false positives and prioritize the vulnerabilities that matter most. Security DevOps and analysts receive comprehensive mitigation recommendations that include information regarding available patches and their reliability, enabling immediate and effective action.

GAIN VISIBILITY WITHOUT A SOFTWARE BILL OF MATERIALS (SBOM)

We realize that it isn't always possible to attain a detailed software bill of materials (SBOM). Accordingly, in addition to supporting automatic alerts of vulnerabilities based on your SBOM, Argus VVM provide alerts based on binary images, enabling maximum visibility across vehicle assets.



STREAMLINE VULNERABILITY MANAGEMENT ACROSS THE ORGANIZATION

Sharing knowledge across vehicle development teams, vehicle SOC analysts, and compliance teams is critical. Argus VVM integrates into existing databases and tools, such as JIRA, as well as vehicle security incident management systems, giving stakeholders easy access to related documentation and ongoing visibility into vehicle risk exposure, compliance status, and mitigation activities.

FACILITATE UNR 155 VEHICLE TYPE APPROVAL & KNOWLEDGE SHARING

Argus VVM facilitates vehicle type approval, by providing a fully customizable cyber security knowledge management tool to help you meet new regulatory requirements and industry best practices, such as UNR 155 and ISO/SAE 21434.

With Argus VVM, you can store all cyber risk-related documents in a single location, share insights from alert investigations and mitigations, map your security progress, identify gaps, and deliver detailed reports for type approval authorities.

SUPPORTED BY ARGUS WORLD-CLASS SERVICES TEAM

Potentially high-impact vulnerabilities that don't have simple mitigation recommendations may require further in-depth analysis by automotive cyber security experts. Highly-skilled in identifying and mitigating automotive vulnerabilities, Argus' world-class researchers team are available to provide further in-depth investigations and incident response.

Prioritize the Vulnerabilities that Matter Most

LEVERAGE 200 PERSON YEARS OF AUTOMOTIVE CYBER SECURITY RESEARCH

Built from scratch by seasoned automotive cyber security researchers, Argus VVM is based on first-hand knowledge gained in dozens of automotive cyber security research projects. Argus VVM vulnerability search capabilities, impact analysis, prioritization and mitigation recommendations reflect insights collected from detecting and analyzing a broad range of vulnerabilities, including 0-days and logical errors, across varying vehicle architectures and protocols.

ABOUT ARGUS CYBER SECURITY

Argus is a global leader in cyber security for connected mobility, providing advanced solutions and lifecycle services for protecting connected and autonomous vehicles against cyber threats, vulnerabilities and attacks. Founded in 2014, and offering onboard and offboard cyber security solutions, Argus will be securing over 65 million vehicles over the next few years. Argus is headquartered in Tel Aviv, Israel, with offices in Detroit, Seoul, Stuttgart, Shanghai and Tokyo.

Visit Argus Cyber Security for more information at www.argus-sec.com