REALIZING CYBERSECURITY

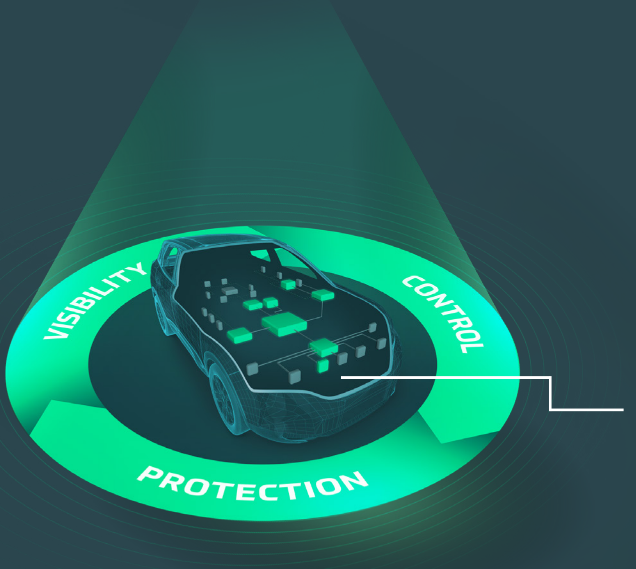
ACROSS VEHICLE LIFECYCLE

C2A security

An evolving industry, new standards and complex supply chain make cybersecurity challenging.

The automotive industry is rapidly evolving. Modern vehicles operate on increasingly complex hardware and software systems that are more vulnerable to cyber attack. WP.29 and ISO/SAE 21434 require OEMs and suppliers to scale cybersecurity capabilities across the supply chain, and ensure compliance in all new vehicle models. This is making coordination and communication more critical than ever before: cybersecurity teams must abandon outdated practices and implement a more methodical, systematic approach to cybersecurity across all organizations.

AutoSec



CYBERSECURITY LIFECYCLE MANAGEMENT

Designed to meet automotive-relevant, industry-specific needs, AutoSec is a Cyber Security Management System (CSMS) that empowers industry stakeholders to identify and mitigate cyber risks in today's challenging environment. Emboldened by visibility, control and protection, OEMs and suppliers can seamlessly scale cybersecurity across vehicle programs in a way not possible before.

ANALYSIS **NETWORK** **ENDPOINT**

Streamlining cybersecurity needs into one centralized location mitigates risk throughout the entire vehicle lifecycle. Threat Analysis and Risk Assessment (TARA), in-vehicle protection and vulnerability analysis are easily managed through the AutoSec platform. Armed with AutoSec, cybersecurity teams can collaborate, delegate security work across the entire supply chain and design in-vehicle protection.

AWARD WINNING SOLUTION 2021

CES 2022 INNOVATION AWARDS HONOREE

AUTOMOTIVE CYBERSECURITY SOLUTIONS OF THE YEAR

SECURITY ORCHESTRATION SOLUTION OF THE YEAR

AUTOMOTIVE SECURITY SOLUTION

CYBERSECURITY INDUSTRY SOLUTION

All C2A's products are production ready and available directly from C2A Security or via a Tier-1 partnership

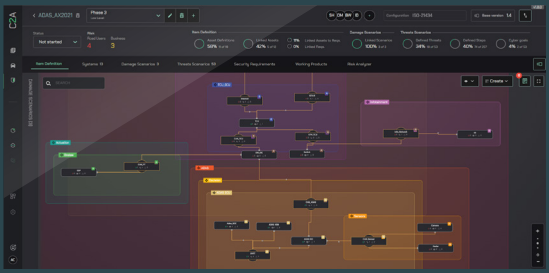
C2A

c2a-sec.com

info@c2a-sec.com

AutoSec ANALYSIS

SCALE UP SECURITY AND WP.29 COMPLIANCE ACROSS THE ENTIRE ORGANIZATION



SCALABLE

Intuitive UI, automation and reuse abilities mean seamless scalability of WP.29 and ISO 21434 compliance across the entire organization.

SYNCHRONIZED

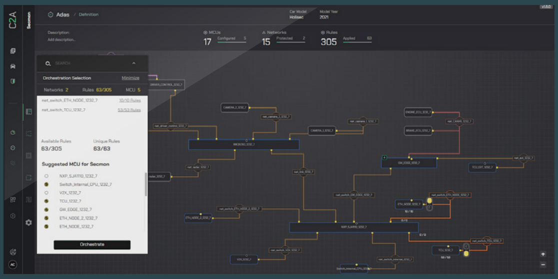
Delegate security work to internal and external stakeholders across the supply chain, enabling teams to deliver faster and more efficiently.

SOPHISTICATED ANALYTICS

AutoSec's cutting-edge proprietary Risk Analyzer tool allows balanced, secure, and automated policy enforcement.

AutoSec NETWORK

DISTRIBUTE IDPS ACROSS MULTIPLE COMPONENTS AND NETWORKS FOR OPTIMAL PROTECTION



VISIBILITY

Advanced UI allows simulation, control and security insight based on target E/E architecture. Intelligent software automatically identifies cybersecurity priorities for user attention.

ORCHESTRATION

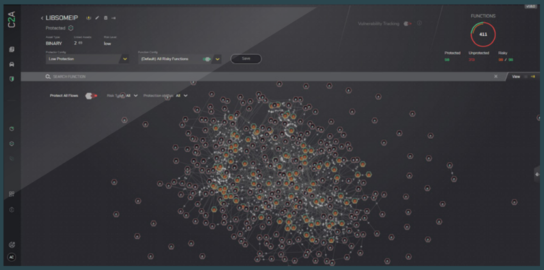
AutoSec Network leverages proprietary deep learning algorithms across multiple networks and components to ensure optimal network protection.

TRANSPARENCY

IDPS source code and switch configuration files as deliverables for each component.

AutoSec ENDPOINT

SEAMLESSLY PROTECT THE VEHICLE FROM SUPPLY CHAIN ATTACKS



DETECTION

SBOM analysis identifies weaknesses before they're exploited.

PROTECTION

Protect against zero-day vulnerabilities across the entire supply chain, eliminating the need for frequent, unplanned OTA campaigns.

COMPATIBILITY

Support stripped and non-stripped binaries, available for common automotive operating systems and chipsets.

C2A

c2a-sec.com

info@c2a-sec.com