AUTO-ISAC

2023 ANNUAL REPORT

ENHANCING AUTOMOTIVE CYBERSECURITY

TABLE OF CONTENTS

INTRODUCTION ►

MEMBERSHIP ►

KEY ACTIVITIES ►

AUTO-ISAC EUROPE ►

ANNUAL CYBERSECURITY SUMMITS ►

AUTOMOTIVE CYBERSECURITY TRAINING ►

2024 THREAT ASSESSMENT ►

APPENDIX ►

JOSH DAVIS
GROUP VICE PRESIDENT,
CHIEF CYBERSECURITY
OFFICER AT TMNA
AUTO-ISAC CHAIRPERSON,
AUTO-ISAC CISO XWG CHAIR

Josh Davis

CHAIRPERSON'S LETTER

Welcome to the Auto-ISAC 2023 Annual Report. I am pleased to report another successful year of growth and accomplishments for the Auto-ISAC. Our success affects not only our Auto-ISAC Members but also the entire automotive industry. The strides we made in 2023 set us up for continued success moving into our eighth year of operations.

As the automotive industry continues to drive forward with new initiatives in EV and AI, the need for protection against cybersecurity threats moves into third gear. Throughout 2023, we implemented many initiatives to increase information sharing between our Members, including continued efforts across our 14 working groups and best practices discussions in our monthly Members Teaching Members meetings. We highlighted several of our yearly key activities during our October 2023 summit, with presentations on the Automotive Cybersecurity Training (ACT) program; Automotive Threat Matrix (ATM) progress; Software Bill of Materials (SBOM) activities; and growth in our European operations, including remarks from our European Director and European Steering Committee (EuSC) and Working Group leader.

It has been satisfying watching our European office grow and mature in its operations with its first, very successful summit, held in Sochaux, France, in June. We were thrilled to announce at our annual summit in Torrance, California, that a Memorandum of Understanding (MoU) with Japan Auto-ISAC (J-Auto-ISAC) was signed that week. This solidifies our ability to provide enhanced collaboration and information sharing with J-Auto-ISAC.

Next year I will transition to the vice chair of the Auto-ISAC, and I look forward to continuing to lead and shape the direction of our operations and add value to our Members. And I will remain in my role as the chair of the CISO Executive Working Group. We still have a lot of work to do to secure our industry as "an attack on one is an attack on all!"

In addition, I am delighted to share that our membership has continued to grow, and we are closing in on a record high of 80 Members.

I continue to look forward to all the collaboration and information sharing among our Auto-ISAC Members, which is the root of our mission.

FAYE FRANCY
EXECUTIVE DIRECTOR,
AUTO-ISAC

Faye Francy

EXECUTIVE DIRECTOR'S LETTER

Dear Members and Partners,

As we reflect on the accomplishments of 2023, I am deeply grateful for the unwavering support and dedication of our Members and partners. It is through your collaborative efforts and commitment that Auto-ISAC has achieved another successful year. Your contributions have propelled our organization forward, driving growth in both membership and operational capabilities. Together, we have navigated challenges, celebrated milestones, and advanced the automotive industry's cybersecurity mission. Thank you for your dedication in building resiliency for the auto industry!

Membership Growth: We're on the brink of reaching a record high of 80 Members, supported by a team of 18 full-time employees contributing to our maturing operations.

Board Evolution: Our Board, streamlined from 24 to 10 dedicated leaders, has been actively supporting our evolving operations and made strides in updating membership criteria, enhancing information sharing, and strategic investments, achieving all set goals.

Leadership and Collaboration: Under the guidance of Chair Josh Davis of Toyota, our progress-to-plan has thrived in key areas in CISO Executive Working Group and European stand up.

Events: We successfully launched our first European Summit in Sochaux, France, sponsored by Stellantis. We had an impressive turnout at our 7th annual Cybersecurity Summit in Torrance, California, kindly sponsored by American Honda.

Initiatives: Working groups are advancing crucial initiatives like Software Bill of Materials (SBOM) and Automotive Threat Matrix (ATM). Signing a Memorandum of Understanding (MoU) with the Japan Auto-ISAC was a significant achievement in strengthening collaboration across the globe.

Training: Thanks to NHTSA and our Cooperative Agreement, the Automotive Cybersecurity Training (ACT) program has made significant progress in the design of a Common Body of Knowledge (CBK) in the automotive cybersecurity. Fundamental and advanced courses are available to enhance cybersecurity awareness and skills across the entire industry.

Welcoming New Chair: Join me in welcoming Kevin Tierney of GM as our 2024-25 Board Chair. With his prior experience, we anticipate continued success and growth in the coming year.

In closing, I express profound gratitude for the steadfast dedication of our Board Directors, Members, partners, and staff. Together, let's anticipate and strive for an exceptional 2024 filled with even greater achievements and impact.

Thank you!

OUR MISSION

The Auto-ISAC collaborates with global partners to identify and assess cybersecurity threats, provide best practices for auto manufacturers, and ensure a safe user experience for consumers.

The early 21st century has seen a transformative movement in digitization and technological innovation. Connected vehicles are now the norm. In this modern vehicle ecosystem, cybersecurity is a collective responsibility. To combat ongoing risks and forecast future ones, Auto-ISAC facilitates discussion and analysis of issues facing vehicles during the entire life cycle. Manufacturing is now considered critical infrastructure and has become a target for cyber criminals. To build a secure environment in manufacturing, we need to keep our systems up to date, secure our devices, and be aware of social engineering scams. As threats continually evolve, automotive over the air (OTA) updates and vehicle security operations centers (VSOC) will help protect the vehicles of today and tomorrow, driving towards a safe and secure future for all.

With membership and partnerships growing each year, we are able to collectively enhance vehicle cybersecurity capabilities across the globe. Currently, Auto-ISAC Members account for more than 99% of light-duty vehicles in North America, with over 75 global OEM and supplier Members representing the commercial vehicle sector, including fleets and carriers.

MAJOR ACCOMPLISHMENTS

The Auto-ISAC's consistent efforts to establish and enhance cybersecurity standards for the automotive sector ensured a consistent, robust approach to cybersecurity across manufacturers.

First Annual European Cybersecurity Summit

The inaugural Auto-ISAC European Cybersecurity Summit was held at the Peugeot Adventure Museum in Sochaux, France, in June of 2023. The 2nd European Summit in 2024 will bring together manufacturers, suppliers, industry leaders, experts, and other stakeholders for two full days of engaging discussions and insights.

EUROPEAN CYBERSECURITY SUMMIT ▸

Auto-ISAC ACT Training Program Available to General Public

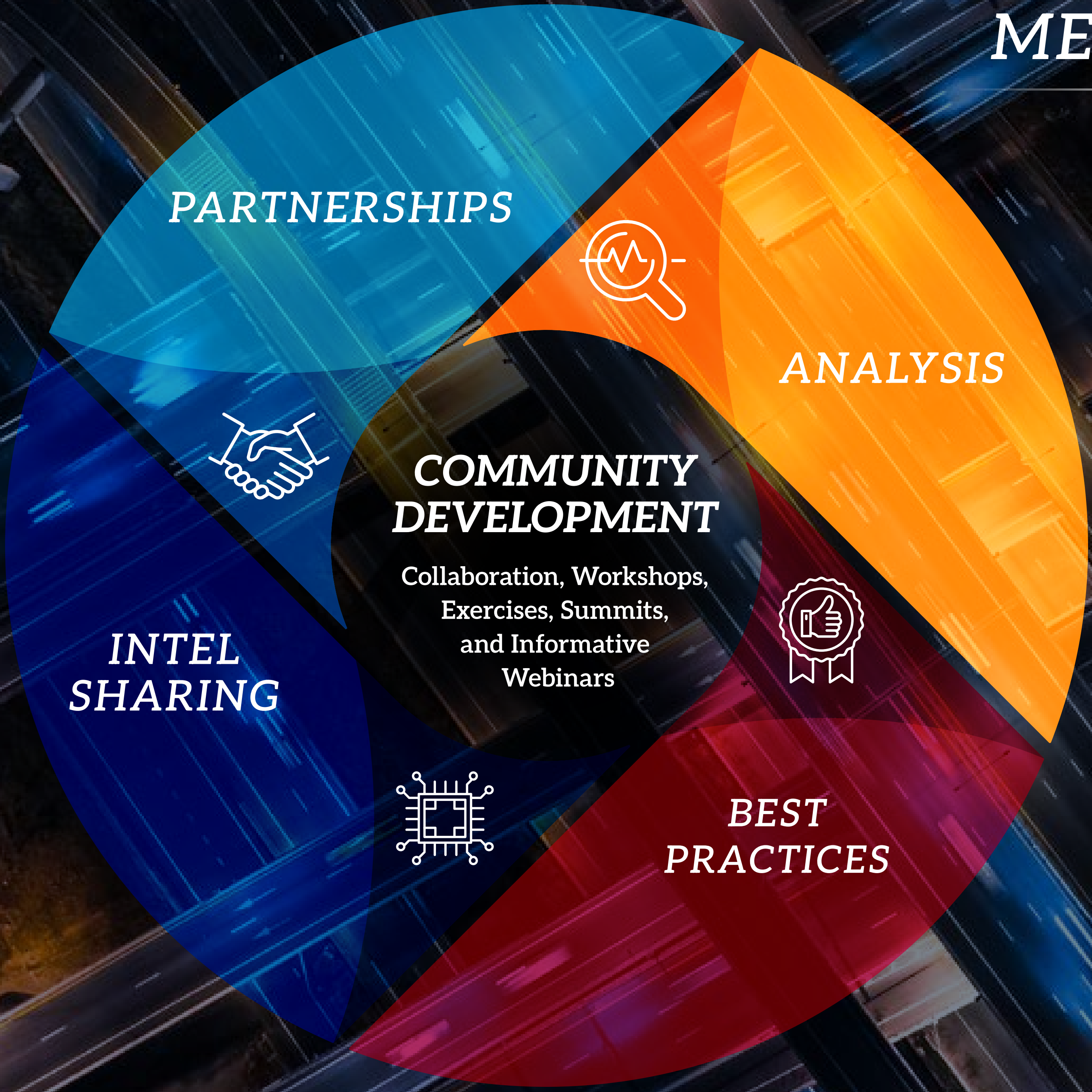
Auto-ISAC's cybersecurity training program, originally supported by NHTSA, has evolved into an officially recognized program as of 2023. Foundational courses were introduced in August 2023, paving the way for advanced courses slated for release in 2024.

AUTO-ISAC ACT TRAINING PROGRAM ▸

Japanese Auto-ISAC and Auto-ISAC Formalized an Agreement to Enhance Vehicle Cybersecurity

In October of 2023, the Auto-ISAC and J-Auto-ISAC signed a Memorandum of Understanding that outlined priorities for working together and coordinating activities and information. Some of the activities will include the two groups collaborating in cyber education and awareness events. In addition, Members of both groups will meet to share the status of emerging cybersecurity issues of interest.

MEMBERSHIP



PARTNERSHIPS

ANALYSIS

COMMUNITY DEVELOPMENT

Collaboration, Workshops, Exercises, Summits, and Informative Webinars

INTEL SHARING

BEST PRACTICES

THE AUTO-ISAC MEMBER ADVANTAGE

Welcome to the heart of our community! The Membership and Benefits Standing Committee (MBSC) serves as the driving force behind the growth, engagement, and prosperity of our Auto-ISAC family. Our mission is to cultivate a thriving ecosystem where every Member and strategic partner finds immense value, support, and opportunities for collaboration.

In addition, Members can participate in standing committees, affinity groups, working groups, workshops, task forces, and global summits. The more we remain immersed and invested in cybersecurity, the better we're able to protect the technology we need in a connected world.

Foster collaboration that creates a safe, efficient, secure, and resilient connected vehicle ecosystem.

Facilitate collaboration and engagement across the broader vehicle cybersecurity ecosystem in the United States, Europe, and Asia.

Inclusive approach to knowledge and information sharing with our community and strategic partners from government, security innovators, research institutions, academia, and industry associations.

NEW MEMBERS IN 2023

amazon

BOSE

CNH

Daimler Truck AG

FLEET DEFENDER

JTEKT

PHINIA

Rivian

INTELLIGENCE & INFORMATION SHARING

- Analysts deliver pre-filtered, focused, and curated information
- Member-only Reporting Exchange and Discussion (RED) Platform enables secure sharing of intelligence and vulnerabilities
- Requests for Information (RFIs) enabling Member-requested and Member-driven intelligence on events or best practices
- Conference calls on selected topics
- Daily Research, Incident, Vulnerability & Executive News (DRIVEN) Report provides open-source intelligence and analysis to Members and community
- Weekly Cyber & Automotive Report (CAR) provides highlights of open-source and Member-only intelligence and analysis curated throughout the week
- Receive threat intelligence from Members and external sources
- Share intel and incident information within a secure environment
- Assist in identifying and mitigating industry vulnerabilities
- Aggregate data to identify and discuss emerging trends

MEMBER COLLABORATION

- Best practice collaboration
- Monthly community calls
- Standing Committees, Affinity Groups, Working Groups, and Task Forces
- Cyber event-response exercise programs that enhance collective and individual Member readiness
- Implementing cybersecurity best practices
- Exchanging experiences with cybersecurity program development
- Participating in exercises and workshops to test readiness
- Member Teaching Members and Partner Teaching Members forums
- Ask and tell, building a trusted crowd sourced cybersecurity ecosystem

CYBERSECURITY CULTURE

- Building a collaborative environment around cybersecurity
- Creating trusted relationships within vehicle cybersecurity industry
- External outreach and networking
- Non-prescriptive, aspirational best practice guides that do not limit technological innovation
- Helping grow the future work force
- Offering a good opportunity for Members to reflect on and build internal processes
- Working together to build resiliency for the whole of the automotive industry
- Seasoned Auto-ISAC Members mentor new Members with similar industry exposure to quickly maximize the value of membership

BOARD OF DIRECTORS

The Auto-ISAC started 2023 with a new streamlined Board of Director's structure that was consolidated to a 10 Member company Board consisting of:

JOSH DAVIS
CHAIR, TOYOTA

KEVIN TIERNEY
VICE CHAIR, GM

TIM GEIGER
TREASURER, FORD

STEPHEN ROBERTS
SECRETARY, HONDA

ANDREAS EBERT
EUSC, VW

ANDREW HILLERY
CAG CHAIR, CUMMINS

RAVI PUVVALA
SAG CHAIR, HARMAN

BRIAN WITTEN
FLEX SEAT, APTIV

BOB KASTER
FLEX SEAT, BOSCH

MONICA MITCHELL
FLEX SEAT, POLARIS

SOME OF THE TOPICS THE BOARD FOCUSED ON FOR 2023 INCLUDED:

"WHITE GLOVE" SHARING OF THREAT RELATED INTELLIGENCE

The "White Glove" approach emphasizes personalized and tailored intelligence sharing, providing Members with insights that are specifically relevant to their organization. We designed a threat intel dashboard to share with the Directors for their awareness. This initiative underscores the Auto-ISAC's commitment to fostering a culture of collaboration and information sharing within the automotive industry, ultimately enhancing the resilience and security of the ecosystem as a whole.

REVIEW OF MEMBERSHIP CRITERIA

In response to the evolving landscape of cybersecurity threats and the changing needs of the automotive industry, the Auto-ISAC conducted a comprehensive review of its current membership criteria in 2023. This review aimed to ensure that membership criteria align with what the industry needs today. The criteria updates to ensure Members are able to contribute meaningfully to the collective cybersecurity efforts of the automotive industry, fostering a stronger and more resilient ecosystem for all stakeholders.

INVESTMENT TO INCREASE MEMBERSHIP VALUE

Recognizing the importance of continuously enhancing the value proposition for its Members, the Auto-ISAC made strategic investments in projects aimed at increasing membership value in 2023. These investments encompassed a range of initiatives, including the development of innovative cybersecurity tools and resources, the expansion of collaborative platforms and information sharing networks, and the provision of targeted training and educational programs. Through these investments, the Auto-ISAC reaffirms its commitment to delivering tangible value and benefits to its Members.

OUR MEMBER ADVISORY FORUM (MAF)

Held bi-annually, provides for open discussion on progress-to-plan against organizational goals and objectives and allows for Member ideas, questions, and concerns. Board Directors and the ED provide awareness of Auto-ISAC strategic decisions and business operations updates. The forum provides an opportunity for Standing Committee and Affinity Group chairs and vice chairs to report on current activities, metrics, and deliverables.

STANDING COMMITTEES

Education and Training Standing Committee (ETSC)

The ETSC is dedicated to enhancing Member capabilities and fostering overall resilience through comprehensive training and education programs grounded in Auto-ISAC's best practices, enriched by Member experiences, and informed by lessons learned.

In 2023, the ETSC continued to support the updating of the Auto-ISAC Best Practice Guides to better align with the current state of automotive security, in addition to the roll out of the ACT Program to the general public.

Finance and Audit Standing Committee (FASC)

The FASC is an advisory body to the board of directors and executive director in overseeing and planning the budget to ensure the organization's financial stability.

Implemented enhanced budget review procedures to facilitate adherence to budgeted parameters. Additionally, endorsed an initiative to broaden and integrate the utilization of budgeting support software.

Information Sharing Standing Committee (ISSC)

The ISSC is the organization within the Auto-ISAC focused on driving effective and efficient methods of proactive information sharing to and between Members to enhance the awareness of security intelligence.

ISSC evaluated Member intelligence needs and recommended changes and updates to current intelligence offerings of the Auto-ISAC. Additionally, the ISSC evaluated Auto-ISAC internal intelligence-sharing metrics and developed recommendations for improving participation and tracking of Member activity. Finally, committee Members concluded the year by electing a new chair and vice chair for the 2024–2025 term.

Membership and Benefits Standing Committee (MBSC)

MBSC serves as the voice of our community, advocating for the industry's needs and priorities. Through active communication and collaboration, MBSC informs the evolution of Auto-ISAC Member and partner programs, ensuring that they remain responsive to our Member's feedback and aligned with the automotive interests.

In 2023, the MBSC reviewed, updated, and simplified the Member application template based on the committee's experience. A one-page document highlighting the benefits of membership was created and an annual survey identifying Members' key priorities was conducted. The new Member mentor program continued to be fine tuned and expanded. Overall membership grew by 10% for the year.

AFFINITY GROUPS

Commercial Vehicle Affinity Group (CAG)

The purpose of the CAG is to collaborate across the industry to understand the commercial vehicle threat landscape and proactively work together to mitigate cyber risks.

In 2023, the CAG celebrated a standout year with monthly meetings that explored a wide range of topics, from intrusion detection to the complexities of SAE J1939-91C. The CAG engaged with speakers from the commercial vehicle sector to contribute insights. Additionally, the CAG started the process of creating a detailed, peer-reviewed document dedicated to intrusion detection inclusive to commercial vehicles.

Supplier Affinity Group (SAG)

Automotive suppliers play an integral role in supporting automotive security, but suppliers have different challenges than original equipment manufacturers. The SAG provides a venue for automotive suppliers to voice concerns applicable to suppliers to the Auto-ISAC and to work on topics that are different from OEM-level issues.

SAG Members worked collaboratively to develop Auto-ISAC internal documents intended to facilitate broader discussion on areas of increasing interest to automotive suppliers: auto supplier compliance with business infrastructure (IT), manufacturing (OT), and product-related cybersecurity regulations and standards; and vehicle lifecycle cybersecurity support. Additionally, SAG Members provided input and recommendations for various initiatives of the Auto-ISAC Board of Directors, including perspectives on membership criteria.

WORKING GROUPS

Chief Information Security Officer Executive Working Group (CISO XWG)

The CISO XWG provides a forum for Auto-ISAC Member CISOs, deputy CISOs, and executive personnel to deliberate on sensitive cybersecurity topics facing their organizations and the automotive industry. The purpose of the CISO XWG is to discuss threats and attacks experienced within Member company environments and across groups examines security concerns as the automotive industry expands vehicle connectivity, autonomy, and electrification in their monthly discussion.

In 2023, we had a total of 31 Member companies whose respective CISO executives actively participated in the monthly discussions, which was an 18% increase from 2022. Several Member companies led discussions and shared their experience in a Ransomware CISO Roundtable shared across the organization. Some of the key topics discussed in 2023:

- *Building an Integrated Cybersecurity Org (IT / OT / Product)*
- *Incident Chronological Review, Supplier Portal Issues*
- *Understanding UNECE Type Approval and Role of OEM*
- *CISO Current Challenges and Opportunities*
- *MOVEit Ransomware Attack, New Privacy Law, Cyber Resiliency in the Supply Chain*
- *How do we Leverage and Protect our Companies from AI?*
- *Generative AI Part 2*
- *EV Threat Intel Brief / IT*

Japan Working Group (JWG)

The JWG works toward fostering communication and cooperation on topics of specific interest to Japanese companies and their US-based operations that support the global goals of the Auto-ISAC. This is achieved by leading, contributing to, and advocating for Auto-ISAC programs that benefit Japanese Member companies and Japanese operations of Auto-ISAC Member companies. In addition, the JWG liaisons with the J-Auto-ISAC to support activities of mutual interest.

In October of 2023, the Auto-ISAC and J-Auto-ISAC signed a MoU that outlined priorities for working together and coordinating activities and information. The formal collaboration fosters information sharing on automotive vehicle cybersecurity and opened the way to begin coordinating their sharing of sensitive and other information.

WORKING GROUPS

Product Working Group (PWG)

The PWG provides a forum for product cybersecurity technical experts, cyber intelligence analysts, and other professionals in the vehicle cybersecurity industry to share and collaboratively analyze actionable intelligence and information about vulnerabilities; emerging research; current, emerging, and future challenges; and other product-related topics of interest.

- *Held two PWG Analyst workshops and two joint Analyst workshops with the IT/OT WG.*
- *Participated in the development, review and production of the 2024 Auto-ISAC Threat Assessment.*
- *Reviewed and updated Auto-ISAC's Priority Intelligence Requirements (PIRs) to identify emerging intelligence needs based on evolving threats to automotive product security.*

Supplier Bill of Materials Working Group (SBOM WG)

The Auto-ISAC SBOM WG was officially chartered during 2023 to support the automotive industry's SBOM operations efforts and gain experience in SBOM implementation.

In an effort to identify industry-specific needs in developing and operationalizing SBOMs for vehicle systems, the group performed several workshops and exercises that facilitated hands-on SBOM development and testing activities. These activities will inform the development of an automotive SBOM informational report intended to be finalized for Auto-ISAC Members in 2024.

IT/OT Working Group

The IT/OT WG provides a forum for and of IT and OT cybersecurity personnel supporting the security of the automotive ecosystem to confer on information about challenges, threats, intelligence, methods, topics of related interest, and emerging research related to the security of the automotive ecosystem and its supporting infrastructure.

- *Held one IT/OT WG Analyst workshop and two joint Analyst workshops with the PWG.*
- *In collaboration with the PWG, developed and finalized an Automotive Cyber Threat Ecosystem outlining the holistic cyber threat landscape and identifying overlapping aspects of concern between the IT, OT, and Product environments.*

PARTNERSHIP PROGRAM

Enriching the Fabric of the Automotive Community

Through partnership with Auto-ISAC, a diverse set of organizations and individuals can support our mission — because an attack on one is ***an attack on all***. Strategic partners have a vested interest in helping build industry resiliency. Community partners raise awareness with consumers and local organizations.

STRATEGIC PARTNERS

These partners are for-profit companies, such as “solutions providers,” that provide connected vehicle cybersecurity products and services — as well as develop value-added projects — that support, educate, and engage the Auto-ISAC and its community.

COMMUNITY PARTNERS

These partners include companies, individuals, or organizations interested in engaging with the automotive cybersecurity ecosystem by supporting and educating Auto-ISAC Members and its community. These partners include industry associations, government entities, academia, research institutions, standards organizations, non-profits, technical experts, and Auto-ISAC sponsors.

In 2023, Auto-ISAC welcomed four new strategic partners:

accenture

Block Harbor. Cybersecurity

IOActive.

VicOne A Trend Micro Subsidiary

PARTNER WEEK

Our second Partner Week was held May 22–26. Two hundred and fifty-three Members registered, with an average of 40 attendees per 30-minute session. Twenty organizations that included strategic and community partners and summit sponsors provided an ***overview of their services and offerings***. The event was provided at no cost to the partners and Members.

253

REGISTRANTS

23% ↑

INCREASE FROM 2022

A GLIMPSE INTO THE SESSIONS:

- Bosch—Bosch Engineering Group Cybersecurity Products and Services
- Cybellum—Revving Up Your Software Supply Chain Security: The Role of BOM in the Automotive Industry
- Vultara—Break the Cybersecurity Silo: Involve Non-Security Engineers in the Cybersecurity Engineering Early
- Upstream—API Security in the Automotive Ecosystem Requires a Fresh Approach
- itemis—itemis SECURE: Automotive Cybersecurity Threat Analysis and Risk Assessment Tool

OCTOBER 2023 CYBERSECURITY AWARENESS MONTH

Auto-ISAC Members put together some common scenarios and best practices to follow to be cyber safe and to ***Break the Chain!***

October 2023 marked the observation of the 20th Cybersecurity Awareness Month. Cyber incidents have become very common these days. Data theft and privacy intrusion are common cyber threats, but these risks can be reduced. Automobile companies take measures to protect their vehicles, but it is still important for customers and drivers to be aware of the various cyber threats and how to mitigate them to prevent threats from cascading to their personal and professional networks. Employees of automobile companies can also take simple steps to prevent cyber threats from affecting their company's networks, equipment, and customers.

The scenarios provided:

- Physical connections to the vehicle
- Device and data connections to the vehicle
- Patching systems and devices
- How to support by following safe cybersecurity behaviors

A listing of free cybersecurity awareness resources was also provided.

CYBER CHALLENGES

At the request of Members, the Auto-ISAC sponsored the ***CyberAuto*** and ***CyberTruck Challenges*** in 2023.

www.CyberAuto-Challenge.org **www.CyberTruckChallenge.org**

These exciting events combine professional development and practicum-based training in a high-energy format that captures the imagination and raises awareness of participating students from around the globe.

The goal of Cyber Challenges is to reach across disciplines, companies, and organizations in the automotive and heavy-vehicle domain to establish a community of interest for automotive cybersecurity and help create a more universal and experienced base of engineers and managers.

15
SCHOOLS REPRESENTED

52%
MASTERS

40%
UNDERGRAD

KEY ACTIVITIES

MEMBERS TEACHING MEMBERS (MTM)

The Auto-ISAC's MTM program is founded upon the power of information exchange, or what we call "sharing lessons." We tap into the experience and expertise of both Members and partners for innovative solutions to complex cybersecurity issues. Through this sharing of lessons, Members can take advantage of industry-wide best practices, in turn building resilience and ensuring zero safety impact from vulnerabilities.

Partners Teaching Members (PTM)

In addition, our strategic partners are encouraged to participate in PTM by providing value-added presentations specific to automotive cybersecurity that provides value to our Members and the industry.

6 MEMBERS TEACHING MEMBERS

3 PARTNERS TEACHING MEMBERS

9 TOTAL SESSIONS IN 2023

2023 TOPICS

Karamba Security

EV and SDV Cyber Compliance Risks and How to Avoid Them

escrypt SECURITY. TRUST. SUCCESS.

Securing Modern Vehicles with AUTOSAR

BOSCH
PACCAR Inc
POLARIS
gm
AUTO-ISAC

Panel: Mitigating Cyber Risks Through Awareness and Training

AUTO-ISAC

Tools, Tips, and Tricks to Maximize Your Membership: Insight from Auto-ISAC I&A and Membership Operations

itemis

Key Technologies for Performing TARAs Efficiently

ARGUS CYBER SECURITY

Tales From a Penetration Testing Team

ETAS

Automotive Cyber Maturity Survey 2023: an Industry on the Move

NXP
infineon
RENESAS
STELLANTIS
BOSCH

Panel: What Should We Do About Physical Attacks?

Block Harbor

Knowledge Transfer and Retention in Automotive Cybersecurity, What Happens When an Automotive Cybersecurity Professional Leaves Your Organization and What to Do About It

COMMUNITY CALLS

The Auto-ISAC holds monthly virtual community meetings for Members and connected vehicle ecosystem stakeholders to stay informed of Auto-ISAC activities and share information on key vehicle cybersecurity topics, technologies, and regulation. The calls are held on the first Wednesday of every month at 11 am ET and are open to the public.

Participants include Auto-ISAC OEM and non-OEM Members, strategic, community, and government partners, academia and research institutions, and key global automotive stakeholders. During the sessions, the Auto-ISAC provides key business operation updates and intelligence highlights, CISA's Joint Cyber Defense Collaborative (JCDC) partner provides CISA Resources Highlights, and a featured speaker provides a presentation relevant to the automotive cybersecurity ecosystem.

These speakers are subject-matter experts in a variety of public and private sectors presenting key topics of interest, providing learning experiences and question and answer opportunities for participants.

Interested participants are encouraged to submit recommendations on various speakers or topics of interest for future community calls. The presentations are made available on the Auto-ISAC website.

250 **AVERAGE ATTENDEES**

12 **SESSIONS**

JANUARY
Auto-ISAC ACT Program Overview

FEBRUARY
Cross-Sector Cybersecurity Performance Goals for Critical Infrastructure

MARCH
Introducing the CyberAuto Challenge – A Tool for Talent Development and Engaging the Next-Generation Workforce

APRIL
NIST Auto Cybersecurity Community of Interest

MAY
Cybersecurity Challenges in the Electric Vehicle Market

JUNE
What is the Car Hacking Village (CHV)?

JULY
Driving a Cyber-Secure Culture in Auto Manufacturing: The Essential Role of the Human Factor

AUGUST
Towards Deployment of a Zero-Trust Architecture (ZTA) For Automated Vehicles (AV)

SEPTEMBER
Cyber Policy Developments Affecting the Auto Industry

OCTOBER
Pwn2Own for Automotive @ Automotive World Tokyo, January 2024

NOVEMBER
The Game of IT / OT Security: Unveiling New Critical Developments in Our Critical Infrastructure Threat Landscape

DECEMBER
API Security Risks for Connected Cars

AUTO-ISAC EUROPE

EUROPEAN STEERING COMMITTEE

The European Steering Committee (EuSC) consists of five designated representatives from our European Members, along with the European director and the EuSC chair, who will also hold a seat on the Auto-ISAC Board of Directors. The primary role of the EuSC is to define strategic goals and general policies for Europe.

European Steering Members 2023

EUROPEAN CHAIR

VW

BMW GROUP

Continental

STELLANTIS

AUTO-ISAC EUROPE

By promoting ongoing collaboration on a global level, we aim to maximize the impact of our mission. Throughout 2023, we enhanced our footprint in Europe by hiring our own Product Intel Analyst for Europe and through ongoing partnerships with authorities, lawmakers and automotive organizations supporting the automotive industry.

EUROPEAN WORKSHOPS

The 2023 first quarter European Working Group Workshop featured Threat Intelligence as the main theme and included the following highlights:

- A presentation summarizing the Current Threat Landscape.
- A Case Study on Information Sharing using Social Media sources.
- How Machine Learning and Artificial Intelligence can be deployed for boosting Automotive Threat Intelligence.

The 2023 second quarter European Working Group Workshop featured the following topics:

- A Quarterly Threat Review & Intel Report.
- A discussion regarding VSOC – Challenges and Experiences and insights into Virtual Security Operations Centers.
- An experiment exploring Automotive Security using ChatGPT.
- An introduction to an Automotive Cybersecurity Maturity Level Assessment Programme.

The 2023 fourth quarter European Working Group Workshop revolved around the theme "Cybersecurity Lifecycle and Regulation" and included presentations regarding:

- Automotive Software Maintenance: Challenges Learned – A Security Perspective. Focusing on insights gained from challenges in automotive software maintenance from a security standpoint.
- An overview about Cybersecurity Regulations and a discussion regarding what lies beyond UN Regulation No. 155.

ANNUAL CYBERSECURITY SUMMITS

30 SPONSORS

485 REGISTRANTS

191 ORGANIZATIONS ATTENDED

366 IN-PERSON

119 VIRTUAL

7TH ANNUAL CYBERSECURITY SUMMIT

The 2023 Auto-ISAC Cybersecurity Summit was a hybrid event that took place October 17–18 in Torrance, California, as well as virtually. Focusing on *"Accelerating CASE Security,"* this year's summit highlighted the drive towards **Connected, Autonomous, Shared, and Electrified (CASE)** security as its main themes. There is a connective bond across the industry as the relationship between people and vehicles becomes more complex and integrated. **CASE** is no longer a future concept; it is here now, and we need to ensure that security is at the core of all related people, processes, and technologies.

This year's summit showcased insights on the implementation of CASE security from manufacturers, suppliers, thought leaders, lawmakers, practitioners, and other stakeholders. Collaborative events such as our cybersecurity summits encourage a collective commitment to Trust, Share, Teach, Learn, and Act to make the industry more resilient.

KEYNOTE SPEAKERS

Noriya Kaihara, President & CEO, American Honda Motor Co., Inc.

Jay Joseph, Vice President – Sustainability & Business Development, Honda

Ann Carlson, Acting Administrator, NHTSA

Eric Goldstein, Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency

Donald Alway, Assistant Director in Charge, Los Angeles Field Office, FBI

Tom Osborne, Deputy Director of California Office of Emergency Services (CalOES), Homeland Security Division

Koos Lodewijkx, CISO, IBM

SAMPLING OF PRESENTATIONS

Auto Threat Matrix

Karl Leboeuf, Product Cybersecurity Technical Fellow, General Motors;
Josh Poster, Intelligence & Analysis Operations Manager, Auto-ISAC

SBOMs for Automotive: A Overview of the Auto-ISAC SBOM Working Group's Activities

Oliver Creighton, Vehicle Cybersecurity Specialist, BMW of North America and Auto-ISAC SBOM Working Group Vice Chair

Making the CASE for Accelerating!

Noriya Kaihara, President & CEO, American Honda Motor Co., Inc.

NHTSA's Apparoach to Vehicle Cybersecurity Safety Risks

Ann Carlson, Acting Administrator, NHTSA

Automotive Autonomous AI Security: Updates on the Latest Findings and Technologies

Dr. Alfred Chen, Assistant Professor of Computer Science, UC Irvine – Autonomous Security

96% FOUND THE INFORMATION RELEVANT

12 SPONSORS

128 ATTENDEES

96% WOULD ATTEND THE SUMMIT AGAIN

EUROPEAN CYBERSECURITY SUMMIT

THE FUTURE OF CONNECTED SECURITY

The inaugural Auto-ISAC European Cybersecurity Summit was held at the Peugeot Adventure Museum in Sochaux, France, from June 13–14. The theme of the event was targeted to advance the conversation regarding "***The Future of Connected Security.***" The Summit brought together manufacturers, suppliers, industry leaders, experts, and other stakeholders for two full days of engaging discussions and insights. The event was kicked off by Titanium Sponsor, Stellantis, whose keynote speech on the digital revolution and software-defined vehicles set the stage for future challenges and helped set the stage for the event to create enthusiasm about the role of Auto-ISAC in shaping the automotive cybersecurity landscape.

Throughout the summit, four sub-themes—**Securing Software Defined Vehicles**, **The Importance of Collaboration, Risk Management & Compliance**, and **Maturing Our Industry**—were explored in depth, providing attendees with a comprehensive understanding of the evolving cybersecurity landscape. Government engagement throughout the event was particularly insightful for attendees.

Overall, the event exceeded expectations, fostered rich discussions, and provided valuable networking opportunities and a collective commitment to advancing automotive cybersecurity in Europe.

AUTO-ISAC

ACT

AUTOMOTIVE
CYBERSECURITY
TRAINING

AUTO-ISAC ACT

The Auto-ISAC ACT Program's Fundamental-level online course transitioned from a pilot to an official program in **August 2023**, making it available to everyone across the globe.

ACT closes the educational gap by:

- Defining a comprehensive training program for vehicle cybersecurity training to improve safety and security.
- Bridging the skill gap between cybersecurity enterprise and vehicle embedded systems training.
- Providing guidance to academia to align with government / industry priorities in automotive cybersecurity.

What is it?

Cybersecurity is an essential component of automotive safety due to the increased connectivity of automobiles. The automotive industry faces growing challenges in managing cybersecurity threats and enhancing cybersecurity resiliency to ensure automotive safety. Addressing these challenges requires specialized skills and training different from traditional enterprise / information systems-focused cybersecurity educational programs.

The Auto-ISAC recognized the need for a common automotive cybersecurity educational program. The ACT program was established because no comprehensive curriculum addressed cybersecurity in the automotive segment. NHTSA's "Cybersecurity Best Practices for the Safety of Modern Vehicles," September 2022, identified workforce development and continuous education as crucial steps to improve automotive cybersecurity.

Certified Automotive Cybersecurity Engineer (CASE)

The CASE attests to the holder's professional mastery of the field of automotive cybersecurity. The completed program certifies the holder's ability to develop and implement a comprehensive and practical response to cybersecurity threats and risks.

The CASE endorses the holder's ability to adapt and sustain a coherent set of systematic best practices acquired through the applied training sequences of the ACT Program. These practices ensure the integrity and security of vehicular system development, operation, and maintenance. This applies to every phase in the vehicle lifestyle. Visit our website to learn more.

AUTOMOTIVE CYBERSECURITY TRAINING

ACT FUNDAMENTAL PROGRAMS

(ALL PROGRAMS ONLINE AND ON-DEMAND)

Cybersecurity Basics

- Models for Cybersecurity (CSEC 2017, NICE, NIST)
- Automotive Threat Management (ISO/SAE 21434 Clause 15)
- Risk Management Models (Risk Management Framework)
- UNECE Reg Compliance
- Threat Modeling
- Access Control
- Intro to Networking Security Operations
- Personally Identifiable Information (PII)
- Intel Analytics

Secure Engineering

- Software Update Management R156
- CAN bus and Protocols
- Privacy
- Engineering Framework and Principles (Threat Analysis)
- Intro to Rev Engineering
- OSI Layers for Automotive
- Resilience
- Hardening and Pen Testing Kali Linux Pen Testing

Secure Operations / Management

- Global Regulations
- Risk Control Process (ISO / SAE 21434 Clause 6)
- Governmental Authorities and Programs
- Product Vulnerability (ISO / SAE 21434 Clause 7)
- Building IR Playbooks
- Incident Response Process
- Supply Chain Woes

ACT ADVANCED HANDS-ON LIVE INSTRUCTION

(IN-PERSON COURSES AVAILABLE IN 2024)

Engineering

- Approaches to Secure Design
- CAN Tools
- Overview of Secure Hardware
- ISO-TP Details
- Interactive UDS
- Infotainment Flaws and Remedies
- Intro to Hardware Reverse Engineering
- Intro to Software Reverse Engineering
- Automotive Ethernet
- Software OTA Updates Forensics

Guided Attacks

- Exploitation using Software Defined Radios
- Side Channel Analysis
- Fault Injection
- Assisted Attack (Right-Seat Ride)
- Example Attack Categories
- RKE-PEPS Attack Tool Creation
- ARM / Intel Exploits
- TPMS Attack Tool Creation

Wireless

- Bluetooth
- Wi-Fi
- Nearfield
- Cellular and Telematics
- RF Vulnerabilities
- SDR and GPS
- V2X
- Phone App Attacks
- Automotive Risk Assessment

EV and EV Infrastructure

- ISO 15118 Security and Exploitation
- PnC Security and Exploitation
- OCPP 1.6 and 2.x Security and Exploitation
- Battery Management
- Battery Management System (BMS) — Penetration Testing
- Infrastructure
- Using CSS to Attack from EV to GRID Through EVSE

• COURSE LISTINGS ARE PERIODICALLY UPDATED

2024 THREAT ASSESSMENT

The Auto-ISAC completed its fourth annual Automotive Threat Report, which outlines the current global automotive cyber threat landscape as assessed by the Auto-ISAC's Intelligence & Analysis staff and Auto-ISAC Member subject matter experts from its Product Working Group and IT/OT Working Group. By analyzing automotive-related cybersecurity research, threats, and events occurring in 2023, the Auto-ISAC substantiates its key judgements and infers the 2024 threat outlook regarding threats to automotive products (vehicles), business networks, and manufacturing systems in 2024. A TLP:GREEN version is available to all Auto-ISAC community partners by requesting access through the Auto-ISAC website.

Threats to Automotive Business (IT) and Manufacturing (OT) Operations

- Ransomware groups and other cybercriminals will attack some automotive OEMs', suppliers', service providers', and fleet management companies' business infrastructure (IT) to steal or encrypt sensitive information for financial gain.
- State-sponsored APT groups may attack some automotive OEMs', suppliers', service providers', and fleet management companies' business infrastructure (IT) to steal intellectual property and other sensitive information in support of their sponsors' goals.
- State-sponsored APT groups will remain a potential destructive cyberattack threat to automotive OEMs', suppliers', service providers', and fleet management companies' business (IT) and manufacturing (OT) infrastructure.

Threats to Automotive Products (Vehicles)

- Criminals will continue to perpetrate technology-enabled vehicle thefts and fraud, and related tools will remain prevalent.
- Cyber threat actors may conduct disruptive attacks on electric vehicle charging systems.
- Cyber threat actors will remain a potential threat to in-vehicle control systems, telematics data, and road user personal data

TLP:CLEAR

AUTO-ISAC MEMBER ROSTER

(79-MEMBER ROSTER AS OF DECEMBER 31ST, 2023)

Aisin Seiki Co., Ltd.	Faurecia	Lucid Motors	Polaris
Allison Transmission, Inc.	Ferrari	Luminar	Qualcomm
Amazon.com ★	Fleet Defender ★	Magna	Renesas Electronics
American Axle & Manufacturing	Flex Ltd.	MARELLI	Rivian ★
Aptiv	Ford Motor Company	Mazda	Stellantis
AT&T	Garrett Motion	Mercedes-Benz	Subaru
AVL List GmbH	General Motors (Cruise-Affiliate)	Mitsubishi Electric	Sumitomo Electric
Blackberry Limited	Geotab	Mitsubishi Motors	thyssenkrupp
BMW Group	Harman International Industries, Inc.	Mobis	Tokai Rika
BorgWarner	Hitachi (Hitachi Astemo-Affiliate)	Motional	Toyota (Woven-Affiliate)
Bosch (ETAS-Affiliate)	Honda Motor Co., Inc.	Navistar	Valeo
Bose Automotive ★	Hyundai Motor America	Nexteer Automotive Corp	Veoneer
ChargePoint, LLC	Infineon	Nissan	Vitesco
CNH Industrial ★	Intel	Nuro	Volkswagen (CARIAD–Affiliate)
Continental	JTEKT Automotive North America Corporation ★	Nuspire	Volvo Cars
Cummins (Meritor-Affiliate)	Kia	NXP	Volvo Group
Daimler Truck AG ★	Knorr-Bremse	Oshkosh Corp	Waymo
Deere & Company	KTM AG	PACCAR	Yamaha Motors
Denso	Lear	Panasonic (Ficosa-Affiliate)	ZF
e:fs TechHub GmbH (EFS)	LG Electronics	Phinia Inc. ★	

★ New Member companies that joined in 2023

AUTO-ISAC STRATEGIC PARTNERS

(22 STRATEGIC PARTNERS AS OF DECEMBER 31ST, 2023)

Accenture ★	GRIMM	KELA	Trustonic
ArmorText	HackerOne	Pen Test Partners	Upstream
BlockHarbor ★	IOActive ★	Red Balloon Security	VicOne ★
Cybellum	Irdeto	Regulus Cyber	Vultara
Deloitte	itemis	Saferide	
FEV	Karamba Security	Security Scorecard	

★ New Member companies that joined in 2023