Welcome to Auto-ISAC!

Monthly Virtual Community Call

August 3, 2022
This Session will be recorded.
## DHS Traffic Light Protocol (TLP) Chart

<table>
<thead>
<tr>
<th>COLOR</th>
<th>WHEN SHOULD IT BE USED?</th>
<th>HOW MAY IT BE SHARED?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLP:RED</strong></td>
<td>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party’s privacy, reputation, or operations if misused.</td>
<td>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</td>
</tr>
<tr>
<td></td>
<td>Not for disclosure, restricted to participants only.</td>
<td></td>
</tr>
<tr>
<td><strong>TLP:AMBER</strong></td>
<td>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</td>
<td>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</td>
</tr>
<tr>
<td></td>
<td>Limited disclosure, restricted to participants organizations.</td>
<td></td>
</tr>
<tr>
<td><strong>TLP:GREEN</strong></td>
<td>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</td>
<td>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</td>
</tr>
<tr>
<td></td>
<td>Limited disclosure, restricted to the community.</td>
<td></td>
</tr>
<tr>
<td><strong>TLP:WHITE</strong></td>
<td>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</td>
</tr>
<tr>
<td></td>
<td>Disclosure is not limited.</td>
<td></td>
</tr>
</tbody>
</table>

*From: https://www.us-cert.gov/tlp*
## Agenda

<table>
<thead>
<tr>
<th>Time (ET)</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td><strong>Welcome</strong></td>
</tr>
<tr>
<td></td>
<td>Why We’re Here</td>
</tr>
<tr>
<td></td>
<td>Expectations for This Community</td>
</tr>
<tr>
<td>11:05</td>
<td><strong>Auto-ISAC Update</strong></td>
</tr>
<tr>
<td></td>
<td>Auto-ISAC Activities</td>
</tr>
<tr>
<td></td>
<td>Heard Around the Community</td>
</tr>
<tr>
<td></td>
<td>What’s Trending</td>
</tr>
<tr>
<td>11:15</td>
<td><strong>DHS CISA Community Update</strong></td>
</tr>
<tr>
<td>11:20</td>
<td><strong>Featured Speaker:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Title:</strong> “Continuously automated vulnerability management for safer cars and regulatory compliance”</td>
</tr>
<tr>
<td>11:45</td>
<td><strong>Around the Room</strong></td>
</tr>
<tr>
<td></td>
<td>Sharing Around the Virtual Room</td>
</tr>
<tr>
<td>11:55</td>
<td><strong>Closing Remarks</strong></td>
</tr>
</tbody>
</table>
Welcome - Auto-ISAC Community Call!

**Purpose:** These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- Stay informed of Auto-ISAC activities
- Share information on key vehicle cybersecurity topics
- Learn about exciting initiatives within the automotive community from our featured speakers

**Participants:** Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

**Classification Level:** TLP:GREEN - May be shared within the Auto-ISAC Community and “off the record”

**How to Connect:** For further info, questions or to add other POCs to the invite, please contact us!

(sharmilakhadka@automotiveisac.com)
Engaging in the Auto-ISAC Community

❖ Join
❖ If your organization is eligible, apply for Auto-ISAC Membership
❖ If you aren’t eligible for Membership, connect with us as a Partner
❖ Get engaged – “Cybersecurity is everyone’s responsibility!”

❖ Participate
❖ Participate in monthly virtual conference calls (1st Wednesday of month)
❖ If you have a topic of interest, let us know!
❖ Engage & ask questions!

❖ Share – “If you see something, say something!”
❖ Submit threat intelligence or other relevant information
❖ Send us information on potential vulnerabilities
❖ Contribute incident reports and lessons learned
❖ Provide best practices around mitigation techniques

OEM Members
22
Navigator Partners
21
Supplier & Commercial Vehicle Members
46
Innovator Partners
17
Membership represents 99% of cars and trucks on the road in North America
Coordination with 26 critical infrastructure ISACs through the National Council of ISACs (NCI)
2022 - 2023 Board of Directors
Executive Committee (ExCom)

Josh Davis
Chair of the Board of the Directors
Toyota

Kevin Tierney
Vice Chair of the Board of the Directors
GM

Jenny Gilger
Secretary of the Board of the Directors
Honda

Tim Geiger
Treasurer of the Board of the Directors
Ford

Todd Lawless
Chair of the Advisory Board
Continental

Bob Kaster
Vice Chair of the Advisory Board
Bosch

Allen Houck
Chair of the SAG
NXP

Larry Hilkene
Chair of the CAG
Cummins

2022-2023 Advisory Board (AB) Leadership
# Member Roster
## As of August 1, 2022

<table>
<thead>
<tr>
<th>Highlight = Change</th>
<th>68 Members, 8 in Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eight Pending: Thyssenkrupp; Cymotive; AAM, Flex, Ferrari, ChargePoint; Nuspire, KTM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Member Name</th>
<th>Company 1</th>
<th>Company 2</th>
<th>Company 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aisin</td>
<td>Garrett</td>
<td>MARELLI</td>
<td>Qualcomm</td>
</tr>
<tr>
<td>Allison Transmission</td>
<td>General Motors <em>(Cruise-Affiliate)</em></td>
<td>Mazda</td>
<td>Renesas Electronics</td>
</tr>
<tr>
<td>Aptiv</td>
<td>Geotab</td>
<td>Mercedes-Benz</td>
<td>Stellantis</td>
</tr>
<tr>
<td>Argo AI, LLC</td>
<td>Harman</td>
<td>Meritor</td>
<td>Subaru</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Hitachi</td>
<td>Mitsubishi Motors</td>
<td>Sumitomo Electric</td>
</tr>
<tr>
<td>AVL List GmbH</td>
<td>Honda</td>
<td>Mitsubishi Electric</td>
<td>Tokai Rika</td>
</tr>
<tr>
<td>Blackberry Limited</td>
<td>Hyundai</td>
<td>Mobis</td>
<td>Toyota <em>(Woven Planet-Affiliate)</em></td>
</tr>
<tr>
<td>BMW Group</td>
<td>Infineon</td>
<td>Motional</td>
<td>TuSimple</td>
</tr>
<tr>
<td>BorgWarner</td>
<td>Intel</td>
<td>Navistar</td>
<td>Valeo</td>
</tr>
<tr>
<td>Bosch <em>(Escripaffiliate)</em></td>
<td>John Deere Electronic</td>
<td>Nexteer Automotive Corp</td>
<td>Veoneer</td>
</tr>
<tr>
<td>Canoo</td>
<td>Kia</td>
<td>Nissan</td>
<td>Vitesco</td>
</tr>
<tr>
<td>Continental <em>(Argus-Affiliate)</em></td>
<td>Knorr Bremse</td>
<td>Nuro</td>
<td>Volkswagen</td>
</tr>
<tr>
<td>Cummins</td>
<td>Lear</td>
<td>NXP</td>
<td>Volvo Cars</td>
</tr>
<tr>
<td>Denso</td>
<td>LGE</td>
<td>Oshkosh Corp</td>
<td>Volvo Group</td>
</tr>
<tr>
<td>EFS</td>
<td>Lucid Motors</td>
<td>PACCAR</td>
<td>Waymo</td>
</tr>
<tr>
<td>Faurecia</td>
<td>Luminar</td>
<td>Panasonic <em>(Ficosa-Affiliate)</em></td>
<td>Yamaha Motors</td>
</tr>
<tr>
<td>Ford</td>
<td>Magna</td>
<td>Polaris</td>
<td>ZF</td>
</tr>
</tbody>
</table>
Upcoming Events

- **Upcoming Meetings**
  - **Community Call:**
    - Wednesday, **September 14** – Speaker: Tim Weisenberger, SAE International **Title:** “SAE EV Charging Public Key Infrastructure Program” **Time:** 11 – 12:00 p.m. **TLP:WHITE**
  - **Joint AWG & IT/OT Workshop:** Tuesday, September 6th 9 a.m. - 4 p.m. at the Henry in Dearborn, MI. [Click here for registration.](#) **TLP:AMBER/ Members Only**
  - **Members Teaching Members:**
    - Wednesday, August 17 Speaker: Moritz Minzlaff, Es crypt **Title:** “Benefits of an automotive security maturity model” **Time:** 10 – 11:30 a.m. **TLP:AMBER**

- **Announcements**
  - **Auto-ISAC Cybersecurity Summit** – *Registration is Open!* Both in-person and virtual venue. Dates: September 7-8, 2022 in Dearborn, MI at The Henry Hotel. Your Company PoC has the “free passes” please check with them!
2022 AUTO-ISAC CYBERSECURITY SUMMIT

DRIVING A SECURE FUTURE

Hybrid Event • Dearborn, MI and Virtual • September 7-8, 2022

More information here
Auto-ISAC Intelligence
Auto-ISAC Intelligence

- Know what we track daily: subscribe to the DRIVEN; know our strategic view of the cyber threat environment: read the TLP:GREEN Threat Assessment in our 2021 Annual Report
  - Send feedback, contributions, or questions to analyst@automotiveisac.com

- Intelligence Notes
  - Geopolitical tensions are: extremely high in and around Ukraine (PBS) and between Russia and the West (The Telegraph); high around the Taiwan Strait (The Hill); and appear to be building around the Korean Peninsula (The Associated Press) and the Middle East (The Times of Israel). Such developments could add to an already heightened cyber threat environment. Organizations within the automotive community should be routinely looking for indications that their business networks, industrial systems, or products may be compromised (CISA-Technical Approaches to Uncovering and Remediating Malicious Activity, CISA Shields Up).

  - We continue to see ransomware groups attacking automotive companies’ business networks (Active Groups: Cuba, Hive, Lockbit 3.0, Black Basta).

  - We continue to see and internally discuss technology-enabled vehicle theft research and incidents. Notable open-source reports are included in the Auto-ISAC DRIVEN.

  - Notable Tactics Techniques and Procedures: Deploying Malware via ISO Container Files (Proofpoint); Follina-Based Phishing (Security Affairs); Bug Bounties Offered by Threat Actors (BleepingComputer); Threat Actor Use of Pen Testing Tools (Trend Micro).
CISA RESOURCE HIGHLIGHTS
Case Study: Apple Releases Security Updates for Multiple Products

Regardless of industry, service providers need to monitor threats.

Apple has released security updates to address vulnerabilities in multiple products. These updates address vulnerabilities attackers could exploit to take control of affected systems.

CISA encourages users and administrators to review the Apple security updates and apply necessary releases.

Read more here: Apple Releases Security Updates for Multiple Products | CISA

Think about it: What are potential cyber threats to your organization today?
CISA, the Federal Bureau of Investigation (FBI), and the Department of the Treasury (Treasury) have released a joint Cybersecurity Advisory (CSA), North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector, to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

CISA, FBI and Treasury urge network defenders, regardless of industry, to examine their current cybersecurity posture and apply the recommended mitigations in this joint CSA, which include:

- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.
- Install and regularly update antivirus and antimalware software on all hosts.

North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA
Case Study: Atlassian Releases Security Advisory for Questions for Confluence App, CVE-2022-26138

Atlassian has released a security advisory to address a vulnerability (CVE-2022-26138) affecting Questions for Confluence App. An attacker could exploit this vulnerability to obtain sensitive information. Atlassian reports that the vulnerability is likely to be exploited in the wild.

CISA encourages users and administrators to review Atlassian’s security advisory, Questions For Confluence Security Advisory 2022-07-20, and apply the necessary updates immediately.

Regardless of industry, service providers need to monitor threats.

Think about it: What are potential cyber threats to your organization today?

Read more here: Atlassian Releases Security Advisory for Questions for Confluence App, CVE-2022-26138 | CISA
The current geopolitical conflict has affected organizations all over the world, regardless of industry. Some of the greatest exploitations have resulted in financial, human resource, and other losses.

**CNMF has issued warnings.**

U.S. Cyber Command’s Cyber National Mission Force (CNMF), in close coordination with the Security Service of Ukraine, has released a list of indicators of compromise (IOCs) of malware seen in Ukraine. According to CNMF, “Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cyber security, just as we are sharing with them.”

**We want to help you fight this vulnerability.**

CISA encourages users and administrators to review U.S. Cyber Command’s press release, Cyber National Mission Force discloses IOCs from Ukrainian networks, as well as their VirusTotal and GitHub pages for more information. See Mandiant’s report, Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities, for additional information.

Read more here: [CNMF Discloses Malware in Ukraine | CISA](https://www.cisa.gov/)
CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.
Additional Resources from CISA

- CISA Homepage - https://www.cisa.gov/
- CISA NCAS – https://us-cert.cisa.gov/
- CISA Shields Up - https://www.cisa.gov/shields-up
- CISA News Room - https://www.cisa.gov/cisa/newsroom
- CISA Blog - https://www.cisa.gov/blog-list
- CISA Cybersecurity Directives - https://cyber.dhs.gov/directives/
For more information:
cisa.gov

Questions?
Central@cisa.dhs.gov
1-888-282-0870
**Auto-ISAC Community Meeting**

**Why Do We Feature Speakers?**
- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the **connected vehicle**

**What Does it Mean to Be Featured?**
- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- **Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC**

**How Can I Be Featured?**
- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

- 30+ **Featured Speakers to date**
- 7 **Best Practice Guides available on website**
- 2000+ **Community Participants**
Featured Speaker
Gilad Bandel, Cymotive
Business Development and Marketing

Gilad drives CYMOTIVE’s automotive cybersecurity business development and product marketing. His focus is on delivering to the market state-of-the-art, unique and innovative solutions - automotive for cyber-security protection.

Gilad is an accomplished executive with over 30 years of experience in the cyber-security and networking industries. Having covered markets in Europe, America and the APAC region, Gilad is a renowned expert in conceptualizing and developing go-to-market strategies. He specializes in business development for cyber-security solutions for automotive, IoT, critical infrastructure and homeland security markets.

Prior to joining Cymotive, Gilad served as VP of Product and Marketing at Arilou Automotive Cybersecurity, as VP of Product at Radiflow and as Director of Product Management at CyberSeal (a Magal Security company). Earlier positions held include VP of R&D, and CTO at leading networking, telecommunication and homeland security companies.
Continuously automated vulnerability management for safer cars and regulatory compliance

Gilad Bandel
Cymotive Technologies
About

CYMOTIVE

TRUSTED SMART MOBILITY

Founded in 2016 by leaders of Israel’s National Security Services

Selected cyber partner of the Volkswagen Group

Financially Strong & Profitable

A full lifecycle smart mobility platform

A growing workforce
~200 employees
85% cyber experts

A global footprint
Israel, North America, Europe & Asia

Industry certifications
ISO 9001, ISO/IEC 90003, TISAX, A-SPICE® Level 2
Automotive vulnerability management – why?

OEMs, Fleet owners/operation and Tier 1/2s must address and manage risks emerging from embedded software running in the vehicle

1. Comply with the process regulation required for homologation

2. Perform a documented intrinsic secured development
## Challenges and motivation

<table>
<thead>
<tr>
<th>Development</th>
<th>Type approval</th>
<th>Postproduction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OEM/Feet owner/operator</strong></td>
<td>Provide evidence for cybersecurity type approval certification</td>
<td>Continuously monitor cybersecurity risks during fleet lifespan</td>
</tr>
<tr>
<td>Identify and manage cybersecurity risks during software development</td>
<td>Provide OEM with evidence necessary for cybersecurity type approval</td>
<td>Continuously monitor cybersecurity risks during the ECU lifespan</td>
</tr>
<tr>
<td><strong>Tier 1/2</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Brand Damage

Researchers Used a Drone and a WiFi Dongle to Break Into a Tesla
A hardcoded password was just the start.

By Eduard Kovacs on May 3, 2021

THE BYTE.

HACKERS BROKE INTO TESLA USING A DRONE
A ZERO-C Click EXPLOITS LET HACKERS UNLOCK AND PARTIALLY CONTROL A NEARBY TESLA.

Technologie / #Drone #IA #Intelligenceartificielle #AirForce

Comment cette Tesla a été piratée par un drone en quelques minutes ! Démonstration
Vulnerability management overview

Asset management

Threat intelligence

Vulnerability management

Vulnerabilities
Risks
Mitigations
Reports
Gained values of proper vulnerability management

- Reduced costs of development, certification and maintenance while strengthening the vehicle’s security protection
- Fulfills regulation requirements - UNR 155 following ISO/SAE 21434
- Manages the risks and provides recommended mitigation
- Provides ongoing visibility and insight of the critical vulnerabilities
Automated vulnerability management process

**Assets**
- ECU INFO

**In-Vehicle Network Architecture**
- ECU Details
- Partitions
- Functions
- Software Packages
- Risk Tags

**Review by Business Owner**
- CVE Scores
- Attack Types
- Exploits

**Profiling**
- ECU Details

**Analyzing**
- CVE Scores
- Attack Types

**Assessment**
- Damage Potential
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor classification

**Reporting**
- Lateral Movement
- Heat map
- Top Risks
- Recommendations
- Compliance
- Interface to systems
Automated vulnerability management process

**Assets**
- ECU INFO

**In-Vehicle Network Architecture**
- User

**Review by Business Owner**
- Risk Severities
  - Safety
  - Law
  - Financial
  - Quality

**Threat Intelligence**
- User

**Profiling**
- ECU Details
  - Partitions
- Functions
- Software Packages
- Risk Tags

**Analyzing**
- CVE Scores
  - Attack Types
- Exploits

**Assessment**
- Damage Potential
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor classification

**Reporting**
- Lateral Movement
- Heat map
- Top Risks
- Recommendations
- Compliance
- Interface to systems

**Security**
- ATT&CK
- EOL
- GNX

**Compliance**
- ISO

**Risk Severities**
- Safety
- Law
- Financial
- Quality

**Damage Potential**
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor classification

**Vendor**
- Classification

**EOL**
- End of Life
Automated vulnerability management process

**Assets**
- ECU Details
- Partitions
- Functions
- Software Packages
- Risk Tags

**In-Vehicle Network Architecture**
- CVE Scores
- Attack Types
- Exploits

**Review by Business Owner**
- Risk Severities
- Safety, Law, Financial, Quality

**Threat Intelligence**

**Profiling**
- ECU Details
- Partitions
- Functions
- Software Packages
- Risk Tags

**Analyzing**
- CVE Scores
- Attack Types
- Exploits

**Assessment**
- Damage Potential
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor classification

**Reporting**
- Lateral Movement
- Heat map
- Top Risks
- Recommendations
- Compliance
- Interface to systems
Automated vulnerability management process

**Assets**
- ECU INFO

**In-Vehicle Network Architecture**
- ECU Details
- Partitions
- Functions
- Software Packages
- Risk Tags

**Profiling**

**Analyzing**
- CVE Scores
- Attack Types
- Exploits

**Review by Business Owner**
- Risk Severities
- Safety, Law, Financial, Quality

**Assessment**
- Damage Potential
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor Classification

**Reporting**
- Lateral Movement
- Heat map
- Top Risks
- Recommendations
- Compliance
- Interface to systems

**Threat Intelligence**
- User

**User**
Automated vulnerability management process

**Assets**
- ECU INFO
- Risk Severities
- Safety, Law, Financial, Quality

**In-Vehicle Network Architecture**
- ECU Details
- Partitions
- Functions
- Software Packages
- Risk Tags
- CVE Scores
- Attack Types
- Exploits
- Damage Potential
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor Classification

**Review by Business Owner**

**Threat Intelligence**
- User
- Threat Intelligence
- Business Owner

**Profiling**
- ECU Details
- Partitions
- Functions
- Software Packages
- Risk Tags

**Analyzing**
- CVE Scores
- Attack Types
- Exploits

**Assessment**
- Damage Potential
- Attack Feasibility
- Vehicle Impact
- Risk Level
- Vendor Classification

**Reporting**
- Lateral Movement
- Heat map
- Top Risks
- Recommendations
- Compliance
- Interface to systems
Mitigation plan for risk minimization

Once a vulnerability has been discovered, the ideal solution is to fix or remediate it, before it can become a security threat. For this, we must always check a few different parameters.

Customers receive a scored, prioritized list of critical vulnerabilities that require mitigation.
Automated Process Vulnerability Management

User
- Assets
- ECU INFO

In-Vehicle Network Architecture

Owner Review

Recommendations & Reports

- Threat Intelligence
- ECU Profiling
- Analyzing CVEs, Attacks, Exploits
- Assessment of Risk & Impact
- Evaluation

UNECE

UNECE

UNECE
Continuous vulnerability management is a major cornerstone of the cybersecurity management system, required for regulation compliance and vehicle safety

Proper asset acquisition and supply chain management is a real challenge

All software development organizations should perform risk minimization as early as possible in the secured software development lifecycle by applying proper controls to mitigate vulnerabilities in a prioritized fashion

Product based vulnerability management such as Cymotive Car Alert increases the security while reducing the associated costs and shortens the development schedule

The process can be done internally by cybersecurity experts if available or outsourced to a professional service company

Things to remember
Thank You   |   cymotive.com

gilad.bandel@cymotive.com
Any questions about the Auto-ISAC or future topics for discussion?
If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- Real-time Intelligence Sharing
- Intelligence Summaries
- Regular Intelligence Meetings
- Crisis Notifications
- Member Contact Directory
- Development of Best Practice Guides
- Exchanges and Workshops
- Tabletop exercises
- Webinars and Presentations
- Annual Auto-ISAC Summit Event

To learn more about Auto-ISAC Membership, please contact michaelshokouhi@automotiveisac.com. For Partnership, please contact sharmilakhadka@automotiveisac.com.
## Auto-ISAC Partnership Programs

### Strategic Partnership

- **For-profit** companies such as “Solutions Providers” that sell connected vehicle cybersecurity products & services.
- **Examples:** Hacker ONE, Upstream, IOActive, Karamba, Grimm

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently **no fee**.
4. **Does not overtly sell or promote** product or service.
5. Commits to **support the Auto-ISAC’s mission**.
6. Engages with the automotive ecosystem, **supporting & educating** Auto-ISAC Members and its Community.
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
9. Engagement must provide **Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
11. Supports our mission through **educational webinars and sharing of information**.

### Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- **Includes** **Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non-Profit, Technical Experts, Auto-ISAC Sponsors**.
- **Examples:** Autos Innovate, ATA, ACEA, JAMA, MEMA, CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.

1. No formal agreement required.
2. **No approval** required.
3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
4. Participate in **Auto-ISAC Monthly Community Calls**.
5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
6. Added to **Auto-ISAC DRIVEN** list to receive our daily cyber automotive newsletter.
7. Part of the Network with **Automotive Community and the extended automotive ecosystem**.
8. Invitation to **attend and support** our yearly Summit.
Current Partnerships
Many organizations engaging

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR
Strategic Partnership
(17)
ArmorText
Cybellum
Deloitte
FEV
GRIMM
HackerOne
Irdeto
Itemis
Karamba Security
KELA
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trustonic
Upstream

NAVIGATOR
Support Partnership
AA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR
Coordination Partnership
AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVi
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTORS
Sponsorship Partnership
2021 Summit Sponsors-
Celerium
Cyware
Denso
NDIAS
I.OActive
Clarotoy
Deloitte
Finite State
Tanium
Recorded Future
Palo Alto Networks
Upstream
Securicor
Zimperium
Micron
Block Harbor
SecurityScorecard
Booz Allen
CybelAngel
ATT
Ford
Cybellum

2020 Summit Sponsors-
Clarotoy
Upstream
Escrypt
Blackberry
Cybellum
Block Harbor
C2A
Synopsis
Intsighs
ValiMail

TLP:WHITE
**Auto-ISAC Benefits**

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency

**Building Resiliency Across the Auto Industry**
Thank You!
Our Contact Info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology Executive Coordinator

20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com

www.automotiveisac.com
@auto-ISAC