



# **WELCOME TO AUTO-ISAC!**

## ***MONTHLY VIRTUAL COMMUNITY CALL***






January 11, 2023

**This Session will be recorded.**

TLP:WHITE



# DHS TRAFFIC LIGHT PROTOCOL (TLP) 2.0 CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p><b>TLP:RED</b></p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.</p>	<p>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.</p>
<p><b>TLP:AMBER+STRICT</b></p>  <p>Limited disclosure, restricted to participants' and its organization.</p>	<p>Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.</p>	<p>Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.</p>
<p><b>TLP:AMBER</b></p>  <p>Limited disclosure, restricted to participants' organization and its clients.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.</p>	<p>Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.</p>
<p><b>TLP:GREEN</b></p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.</p>
<p><b>TLP:CLEAR</b></p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Recipients may share this information without restriction. Information is subject to standard copyright rules.</p>

# AGENDA

Time (ET)	Topic
11:00	<b>Welcome</b> <ul style="list-style-type: none"><li>➤ Why We're Here</li><li>➤ Expectations for This Community</li></ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"><li>➤ Auto-ISAC Activities</li><li>➤ Heard Around the Community</li><li>➤ Intelligence Highlights</li></ul>
11:15	<b>DHS CISA Community Update</b> <ul style="list-style-type: none"><li>➤ Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)</li></ul>
11:20	<b>Featured Speaker:</b> <ul style="list-style-type: none"><li>➤ Tamara Shoemaker- Cybersecurity Training Leader - Title: <i>“Auto-ISAC Automotive Cybersecurity Training (ACT) Program”</i></li></ul>
11:45	<b>Around the Room</b> <ul style="list-style-type: none"><li>➤ Sharing Around the Virtual Room</li></ul>
11:55	<b>Closing Remarks</b>

# 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!

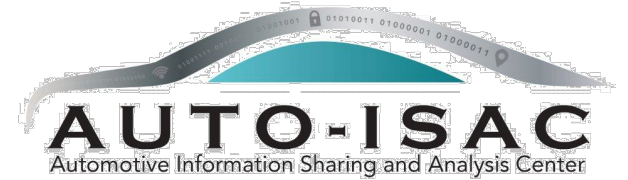
([sharmilakhadka@automotiveisac.com](mailto:sharmilakhadka@automotiveisac.com) )



# 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 (1<sup>st</sup> Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

**27**  
OEM Members

**21**  
Navigator  
Partners

## ❖ 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

**47** Supplier &  
Commercial  
Vehicle Members

**18**  
Innovator  
Partners

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)



# 2023 BOARD OF DIRECTORS

*Thank you for your Leadership!*



**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**



**Andreas Ebert**  
*Chair of the EuSC*  
**Volkswagen**



**Larry Hilkene**  
*Chair of the CAG*  
**Cummins**



**Ravi Puvvala**  
*Chair of the SAG*  
**Harman**



**Monica Mitchell**  
*Member of the Board of the Directors*  
**Polaris**



**Bob Kaster**  
*Member of the Board of the Directors*  
**Bosch**



**Brian Witten**  
*Member of the Board of the Directors*  
**Aptiv**

# AUTO-ISAC MEMBER ROSTER

AS OF JANUARY 1, 2023

74 MEMBERS + 4 PENDING

Aisin	Flex	Magna	Renesas Electronics
Allison Transmission	Ford	MARELLI	Stellantis
American Axle & Manufacturing	Garrett	Mazda	Subaru
Aptiv	General Motors (Cruise-Affiliate)	Mercedes-Benz	Sumitomo Electric
AT&T	Geotab	Mitsubishi Electric	ThyssenKrupp
AVL List GmbH	Harman	Mitsubishi Motors	Tokai Rika
Blackberry Limited	Hitachi	Mobis	Toyota (Woven Planet-Affiliate)
BMW Group	Honda	Motional	TuSimple
BorgWarner	Hyundai	Navistar	Valeo
Bosch (Ecrypt-Affiliate)	Infineon	Nexteer Automotive Corp	Veoneer
Canoo	Intel	Nissan	Vitesco
ChargePoint	John Deere Electronic	Nuro	Volkswagen
Continental (Argus-Affiliate)	Kia America, Inc.	Nuspire	Volvo Cars
Cummins (Meritor-Affiliate)	Knorr Bremse	NXP	Volvo Group
Cymotive	KTM	Oshkosh Corp	Waymo
Denso	Lear	PACCAR	Yamaha Motors
e:fs TechHub GmbH	LG Electronics	Panasonic (Ficosa-Affiliate)	ZF
Faurecia	Lucid Motors	Polaris	
Ferrari	Luminar	Qualcomm	

Pending: Bose Automotive, JTEKT, Micron, Rivian

# AUTO-ISAC BUSINESS UPDATES AND EVENTS

**\*\*All times are in ET**

## Upcoming Meetings:

- **Auto-ISAC Strategic Partner Irdeto Membership Offering Call**
  - **Thursday, January 12<sup>th</sup> – Time: 10 – 11:00 a.m. TLP:AMBER; Speaker: TBA, Irdeto; Title: “Security Vulnerability Metrics”**
- **SAE/NHTSA Cybersecurity Workshop: In Person: Washington, DC**
  - **Tuesday, January 17<sup>th</sup> - Time: 12 pm – 3 pm**
- **Members Teaching Members:**
  - **Wednesday, January 18<sup>th</sup> – Time: 10 – 11:30 a.m. TLP:AMBER; Speaker: Assaf Harel, Karamba; Title: “EV and SDV Cyber Compliance Risks and How to Avoid Them”**

## Announcements:

- **ACT Program Advanced Courses** – Beta Completed. Working to plan for sustainment and certification. Contact [Tamara Shoemaker](#) for more detail. **(Members Only)**
- **Best Practice Guide Updates** – ETSC is kicking off a “Light Touch” Best Practice Guide update to bring the existing guides up to current references and standards.





# AUTO-ISAC INTELLIGENCE HIGHLIGHT

TLP:WHITE



# AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; Auto-ISAC 2022 Threat Assessment complete (TLP:GREEN version pending); Auto-ISAC Automotive Cyber Threat Ecosystem (1<sup>st</sup> Iteration) complete (TLP downgrade pending).
  - **Send feedback**, contributions, or questions to [analyst@automotiveisac.com](mailto:analyst@automotiveisac.com)
- Intelligence Notes
  - Geopolitical tensions involving Russia, China, North Korea, and Iran remain elevated with Russia-Ukraine in crisis. Monitor for cyber-related spillover ([Russia-Ukraine](#), [China](#), [North Korea](#), [Iran](#)).
  - Do not expect a reprieve from cyberattacks if there is an economic downturn regardless of severity ([Securityweek](#)).
  - Ransomware<sup>1</sup> Groups Targeting Automotive: [Zeppelin](#), [Quantum](#), [BianLian](#), [Royal](#), [LockBit 3.0](#) <sup>2</sup>, [AlphV/BlackCat](#), [Hive](#).
  - Multiple incidents of threat actors selling access to automotive organizations' networks and specific email accounts, and selling stolen sensitive information.
  - Notable TTPs and Tools: Exploitation of Vulnerabilities Telematics and Automotive API Infrastructure ([Sam Curry](#)); Exploitation of Vehicle Product Supply Chain ([inews](#) <sup>3</sup>); Insider Threat ([Reuters](#)); Microsoft Distributed Transaction Coordinator Service DLL Hijacking ([Minerva](#)); Google Ad-Words Abuse ([Guardio](#)); Employing OpenAI Maliciously ([Checkpoint](#)); Highly-Targeted Social Engineering ([PCmag](#)).

# CISA Resource Highlights

Joint Cyber Defense Collaborative



JOINT CYBER DEFENSE  
COLLABORATIVE

Jeff Terra  
1/11/2023



# FBI, FDA OCI, and USDA Release Joint Cybersecurity Advisory Regarding Business Email Compromise Schemes Used to Steal Food

12

- The Federal Bureau of Investigation (FBI), the Food and Drug Administration Office of Criminal Investigations (FDA OCI), and the U.S. Department of Agriculture (USDA) have released a joint Cybersecurity Advisory (CSA) detailing recently observed incidents of criminal actors using business email compromise (BEC) to steal shipments of food products and ingredients valued at hundreds of thousands of dollars.
  - The joint CSA analyzes the common tactics, techniques, and procedures (TTPs) utilized by criminal actors to spoof emails and domains to impersonate legitimate employees and order goods that went unpaid and were possibly resold at devalued prices with labeling that lacked industry standard “need-to-knows” (i.e., necessary information about ingredients, allergens, or expiration dates).
- Please note all information provided is TLP Amber

## Cuba Ransomware

The Federal Bureau of Investigation (FBI) and CISA have updated joint Cybersecurity Advisory AA22-335A: #StopRansomware: Cuba Ransomware, originally released on December 01, 2022.

The advisory has been updated to include additional indicators of compromise (IOCs).

Please note all information provided is TLP Amber



# Mozilla Releases Security Updates for Thunderbird and Firefox

14

- Mozilla has released security updates to address vulnerabilities in Thunderbird, Firefox ESR, and Firefox. An attacker could exploit these vulnerabilities to take control of an affected system.
- CISA encourages users and administrators to review Mozilla's security advisories for Thunderbird 102.6, Firefox ESR 102.6, and Firefox 108 for more information and apply the necessary updates.

Please note all information provided is TLP Amber

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations
- Since 12/1/22 approximately 68 advisories have been issued
- The advisories span the following sectors: Information Technology, Critical Manufacturing, Energy and Multiple Sectors
- [Current Activity | CISA](#)

Please note all information provided is TLP Amber

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.



CISA added 9 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of December. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber





- ❑ CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- ❑ CISA NCAS – [https://us-cert\[.\]cisa\[.\]gov/](https://us-cert[.]cisa[.]gov/)
- ❑ CISA Shields Up - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
- ❑ Free Cybersecurity Services and Tools - [https://www\[.\]cisa\[.\]gov/free-cybersecurity-services-and-tools](https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools)
- ❑ CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- ❑ CISA Blog - [https://www\[.\]cisa\[.\]gov/blog-list](https://www[.]cisa[.]gov/blog-list)
- ❑ CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- ❑ CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- ❑ CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)



**JOINT CYBER DEFENSE  
COLLABORATIVE**

For more information:

**cisa.gov**

Questions?

**Central@cisa.dhs.gov**

**1-888-282-0870**

**Jeff Terra**  
1/11/2023



# 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

TLP:WHITE



# ABOUT THE SPEAKER



**Tamara Shoemaker**  
**Auto-ISAC**  
**Cybersecurity Training Lead**

## Current Positions

- Auto-ISAC Automotive Cybersecurity Training Program Lead - (ACT)
- ETSC Staff Lead

## Past Positions

- Director, University of Detroit Mercy's Center for Cybersecurity & Intelligence Studies
  - **Designating a Center of Academic Excellence in Cyber Defense with Dept of Homeland Security and the National Security Agency since 2004**
- Founder of the Michigan CyberPatriot K-12 Program
- Program Coordinator, Michigan Member Alliance InfraGard
- Co-Founder of the MCISSE Coalition of Michigan CAEs
- Licensed Private Investigator for 12 years

## Education

- BS, Criminal Justice/Legal Administration, University of Detroit Mercy

## Drive

- 2019 Ford Taurus Sho and 2004 Ford T-Bird

# ACT PROGRAM - DEVELOPMENT OF CURRICULUM & COURSES

## DESIGN OF THE ACT PROGRAM



- Performed global research on existing vehicle cybersecurity training and education
- Membership review and validation
- Alignment with industry needs



Dedicated **Tiger Team** to support the review development and oversight:

- Curriculum
- Courseware
- Training Staff



- Conducted **Alpha and Beta pilots** to determine any course corrections
- Selected both novice and experienced cybersecurity trainees
- Program will be sustained and updated as needed

# ACT PROGRAM

## *COURSE DELIVERY*



### Fundamental courses

Delivered online using University's learning system, offered both synchronously and asynchronously, as defined tracks:

1. **Basic Cybersecurity (36 Hours)**
2. **Security Engineering (36 Hours)**
3. **Security Operations, Government, & Management (36 Hours)**



### Advanced courses

Delivered hands-on at the **American Center for Mobility** in Ypsilanti, Michigan:

1. **Advanced Engineering (36 Hours)**
2. **Advanced Wireless (40 Hours)**
3. **Guided Attacks (38 Hours)**
4. **EV and EV Infrastructure (36-40 Hours)**

*These courses lead to certificates of completion.*

# AUTOMOTIVE CYBERSECURITY TRAINING (ACT) PROGRAM UPDATE

- **Beta Advanced in-person training completed on November 4, 2022**
- **Metrics for the ACT program:**
  - **224** Individual members signed up for courses from **53** Member companies
  - **134** Trainees attended the Fundamentals Alpha and Beta Courses
  - **105** Trainees attended Advanced Alpha and Beta Courses
- **Certificates of completion will be issued in January**
  - Setting up certification application to track certificates of completion and CASE Certification.
  - Compiled criteria for certificates of completion on current trainees.
  - **CAPEX** is a Capability Exercise required to qualify for the **Certified Automotive cyberSecurity Engineer Certification (CASE)**. To take the CAPEX: You must be an experienced Cybersecurity Engineer or a trainee that has completed the ACT course blocks.
  - This virtual scenario-based one-day test will be administered on **January 24th** and February TBD.
- **ACT Training will be scheduled for the Fall of 2023 – be on the lookout for more details.**



# SUSTAINMENT OF THE ACT PROGRAM

## ➤ Goal:

- ACT Fundamental Courses available through University Partners, and
- ACT Fundamental Courses available through Auto-ISAC via a *Learning Management System*
- ACT Advance Course scheduled in-person for the Fall of 2023
- Certifications awarded for Course completion
- CASE Certification awarded after passing the CAPEX

## ➤ Fundamentals will be shared with Partnering Universities

- University Partners supply their Cybersecurity curriculum (prerequisites)
- Audit of curriculum, unless certified as an NSA/DHS Center of Academic Excellence (CAE)
- Auto-ISAC supplies Fundamentals Courses from the ACT Program
- Periodic Follow-ups will be required to ensure the integrity of the Program

## ➤ Assembling of Courses to fit the University model

- Mapping to standards, regulations, and best practices
- Adjusting to Tiger Team, Trainee reviews, and Expert advice
- Membership requesting online on-demand training (LMS)
- Standardizing of curriculum for partnering universities

## ➤ Advance Courses

- Negotiate contracts with 20+ instructors
- Choose venues and LMS
- Purchase Equipment

# ACT BETA RE-ALIGNED CURRICULUM

## ➤ Fundamentals – Online instructor led training

### ▪ Basics – 30-36 Hours

- Cybersecurity Basics (NIST Workforce Framework, CSEC 2017, NIST800)
- Automotive Threat Management (Clause 15)
- Risk Management (RMF)
- UNECE Regulatory Compliance (R155-21434, R156-24089)
- Security Operations
- Data Privacy and Protection (GDPR, PCI . . )

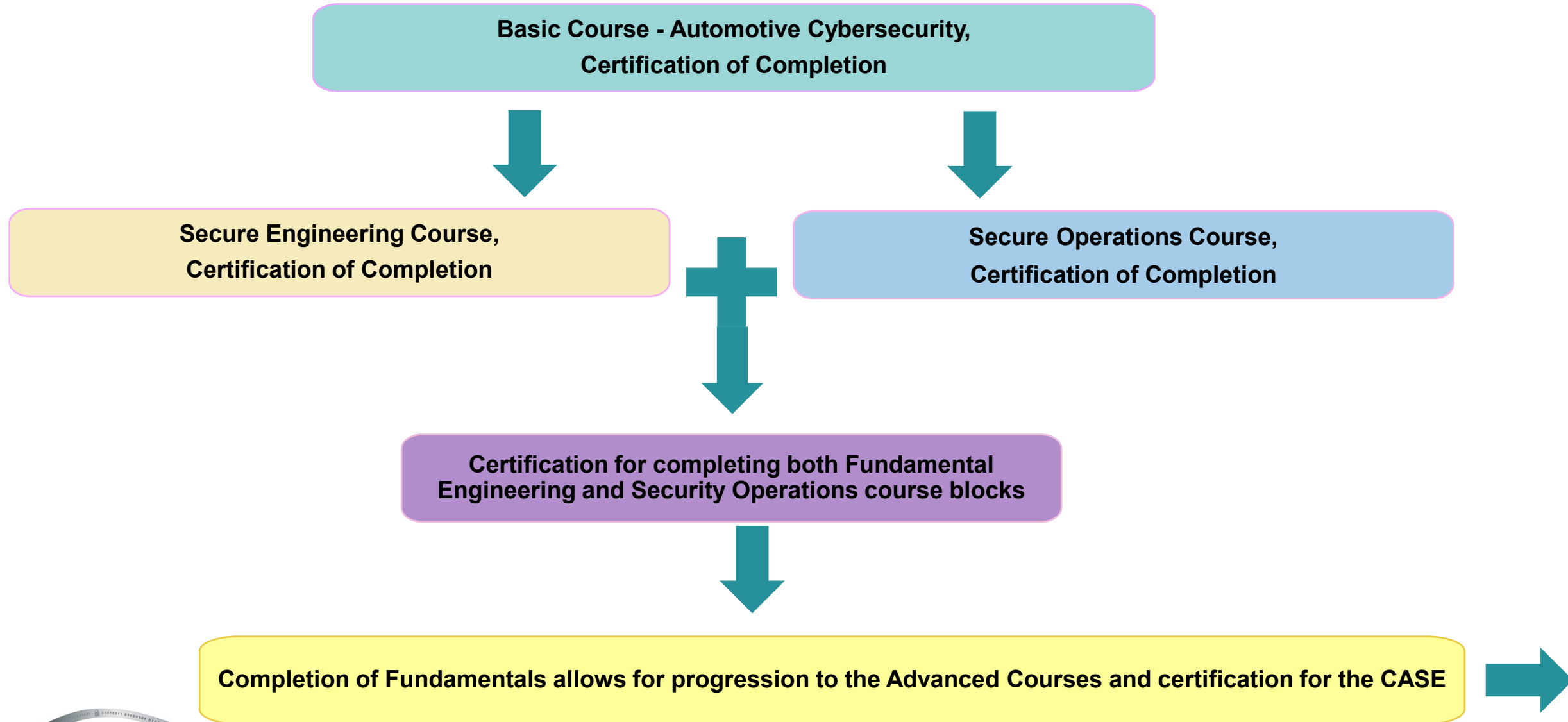
### ▪ Security Engineering – 36 Hours

- System Security Engineering Process (24089)
- CANBus and Protocols
- Crypto Applications
- Intro to Communication Security/OSI
- Metrics & Measurements Process
- Operating Systems Security

### ▪ Security Operations, Government, & Management – 36 Hours

- Cybersecurity Policies (Clause 5)
- Cybersecurity Policy Implementation (clause 8)
- Cybersecurity Control Models (Clause8)
- Product Vulnerability Management/CM (Clause 7)
  - Build IR Playbook
  - Incident Response Process
  - Supply Chain Woes
- Other, Fleets, Off Road, Military . . .

# CERTIFICATION STACKABLE PATHWAY FOR FUNDAMENTALS



# ACT BETA CURRICULUM

## ➤ Advanced – Collaborative in-person hands-on training

### ▪ Advanced Engineering – 36 Hours

- Approaches to Secure Design Thinking
- CAN Tools & Low-Level Interactions
- Overview of Sec Hardware Design Principals
- ISO-TP Details
- Interactive UDS
- Software Updates

- Infotainment Flaws and Remedies
- Forensics
- Automotive Risk Assessment
- Intro to Hardware Reverse Engineering
- Intro to Software Reverse Engineering

### ▪ Advanced Intelligence Analyst – 36 Hours

- Bluetooth
- WiFi
- Nearfield
- Cellular & Telematics

- Protocols & Diagnostics
- SDR & GPS
- V2X
- Ultra Wide Band

### ▪ Guided Attacks – 40 Hours

- Remote Keyless Entry
- Side Chanel Analysis and Fault Injection
- Relay Hardware Attacks
- RF Attacks
- Phone App Attacks

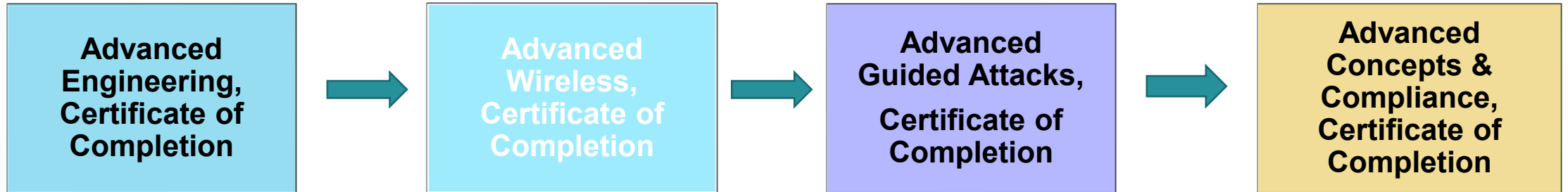
- ARM/Intel/etc. Exploitation
- ISO 21434 – Advanced Attacks
- Sensor Fusion, Adversarial AI
- TMPS

### ▪ Future EV Session 36 Hours

- EV Security & GRID Interactions
- Courses for this section TBD

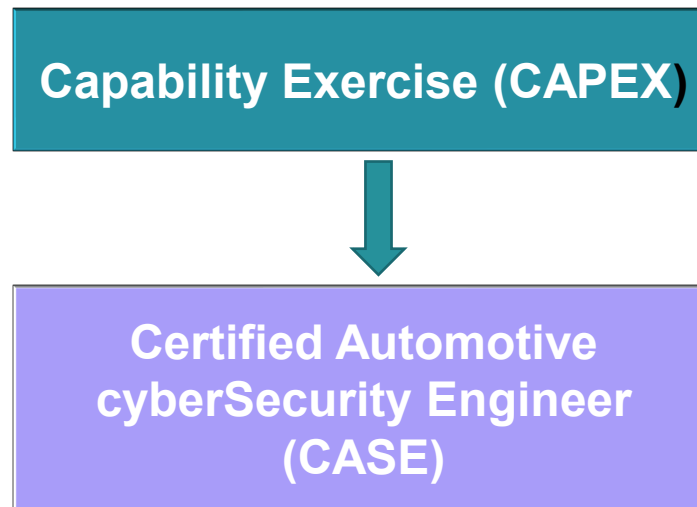
# ADVANCED COURSES & CERTIFICATION FOR CASE

Those without experience should take the courses in this order.



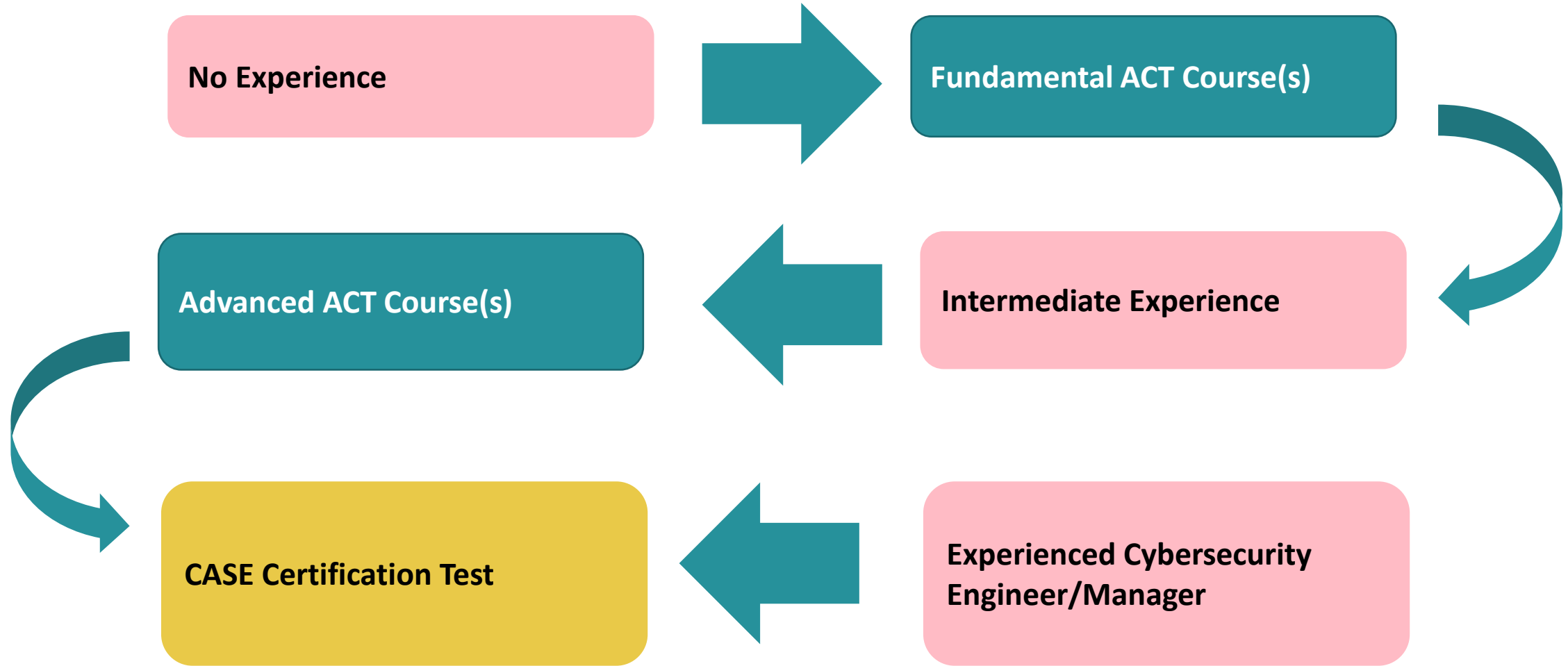
Intermediate experienced may take courses that fulfill their needs.

Experts may go straight to the CAPEX.



**Advanced EV in place of C&C coming soon!**

# ACT PROGRAM TARGET AUDIENCE



# CERTIFICATION SCHEME

- **Certifications of Completion**
  - **One certification per course block completed**
  - **One certification for completing all Fundamentals and Advance**
- **Certified Automotive Security Engineer (CASE)**
  - **Completion of Courses plus CAPEX for beginners**
  - **Completion of Advanced course plus CAPEX for intermediate level of experience**
  - **CAPEX for cybersecurity professionals**
  - **52 Registered for the CAPEX. Two sessions are scheduled, January 24<sup>th</sup> and Feb TBD**

## OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE  
TOPICS FOR DISCUSSION?*



# HOW TO GET INVOLVED: MEMBERSHIP

**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 [melissacromack@automotiveisac.com](mailto:melissacromack@automotiveisac.com).  
For Partnership, please contact [sharmilakhadka@automotiveisac.com](mailto: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  
(18)**

ArmorText  
Cybellum  
Deloitte  
FEV  
GRIMM  
HackerOne  
Irdeto  
Itemis  
Karamba Security  
KELA  
Pen Testing Partners  
Red Balloon Security  
Regulus Cyber  
Saferide  
Security Scorecard  
Trustonic  
Upstream  
Vultara

#### NAVIGATOR

**Support Partnership**

AAA  
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  
OASIS  
ODNI  
Ohio Turnpike & Infrastructure Commission  
SANS  
The University of Warwick  
TSA  
University of Tulsa  
USSC  
VOLPE  
W3C/MIT  
Walsh College

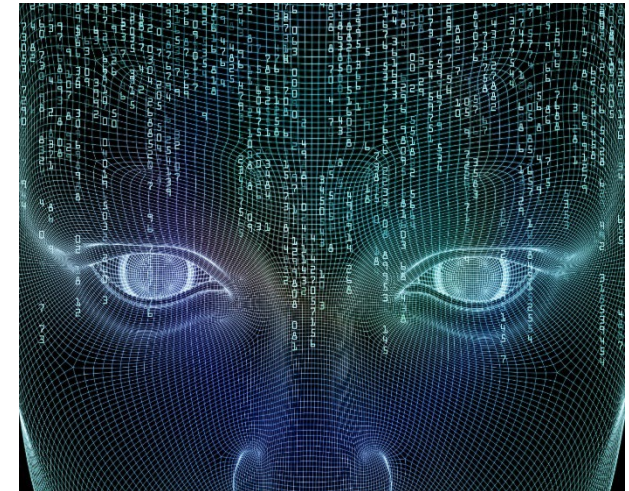
#### BENEFACTOR

**Sponsorship  
Partnership**  
2022 Summit Sponsors-

Argus  
BGNetworks  
Bosch  
Blackberry  
Block Harbor  
BlueVoyant  
Booz Allen Hamilton  
C2A  
Cybellum  
CyberGRX  
Cyware  
Deloitte  
Denso  
Finite State  
Fortress  
Itemis  
Keysight Technologies  
Micron  
NXP  
Okta  
Sandia  
Securonix  
Tanium  
UL  
Upstream  
VicOne

# 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](http://www.automotiveisac.com)  
[@auto-ISAC](https://twitter.com/auto-ISAC)