



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL






March 1, 2023

This Session will be recorded.

TLP: CLEAR



DHS TRAFFIC LIGHT PROTOCOL (TLP) 2.0 CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</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>TLP:AMBER+STRICT</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>TLP:AMBER</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>TLP:GREEN</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>TLP:CLEAR</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	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ Intelligence Highlights
11:15	DHS CISA Community Update <ul style="list-style-type: none">➤ Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Karl Heimer, Principal, Heimer & Associates LLC➤ Title: : Introducing the CyberAuto Challenge – a Tool for Talent Development and Engaging the Next Generation Workforce
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

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!

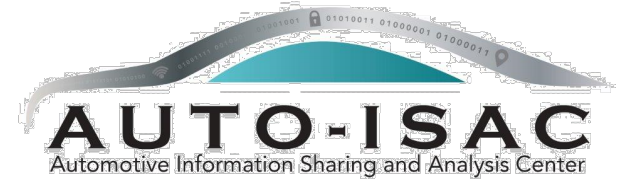
(sharmilakhadka@automotiveisac.com)



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!

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)



TLP: CLEAR

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

Retiring! Thank you for your service.



Tim Geiger
Treasurer of the Board of the Directors
Ford



Andreas Ebert
Chair of the EuSC
Volkswagen



Larry Hilkene
Chair of the CAG
Cummins

Thank you for your service.



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 MARCH 1, 2023

Highlight = New Active Member

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 (ETAS-Affiliate)	Infineon	Nexteer Automotive Corp	Veoneer
Bose Automotive	Intel	Nissan	Vitesco
Canoo	John Deere Electronic	Nuro	Volkswagen
ChargePoint	Kia America, Inc.	Nuspire	Volvo Cars
Continental (Argus-Affiliate)	Knorr Bremse	NXP	Volvo Group
Cummins (Meritor-Affiliate)	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: Fleet Defender, JTEKT, Micron, Rivian

AUTO-ISAC BUSINESS UPDATES AND EVENTS

**All times are in ET

Upcoming Meetings:

➤ Community Call:

- Wednesday, April 5th – Time: 11:00am – 12:00 p.m. **TLP:GREEN**; Speaker: Suzzanne Lightman, NIST Title: “TBA”

Announcements:

- ACT Program Advanced Courses – Certifications for “CASE” and both Alpha and Beta phases have been issued. Working to plan for sustainment. Contact Tamara Shoemaker for more details **(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’s first European Summit will be **June 13th-14th, 2023**. More information will be available soon!
- Auto-ISAC Summit will be, **October 17th-18th, 2023** in Redondo Beach, California. Registration information and complementary passes will be coming soon.
- Join an immersive deep dive into threat hunting, where KELA will provide live threat indicators and real-time analysis to help you enhance your threat hunting skills. <https://ke-la.com/advanced-threat-hunting-workshop> This workshop is eligible for 1 CPE Credit from ISC2. Requests for CPE credits can be submitted via email to training@ke-la.com after the session.



AUTO-ISAC INTELLIGENCE HIGHLIGHT

TLP: CLEAR



AUTO-ISAC INTELLIGENCE

➤ Know what we track daily: [subscribe](#) to the **DRIVEN**; **TLP:GREEN** Auto-ISAC 2022 Threat Assessment – Likely March release; Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) – Likely March release.

- **Send feedback**, contributions, or questions to analyst@automotiveisac.com

➤ Intelligence Notes

- Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia and Ukraine in crisis. Monitor for cyber-related spillover ([Russia-Ukraine](#) ¹, [China](#), [North Korea](#) ², [Iran](#) ³).
- Ransomware⁴ Groups Targeting Automotive: [Phobos](#), [BianLian](#), [Play](#), [BlackByte](#), [LockBit 3.0](#) ⁵ [Royal](#).
- Multiple incidents of threat actors selling access to automotive organizations' stolen data. Notable Dark Web Marketplaces: [OMG!OMG! Market](#), [Blacksprut](#), [Mega Darknet Market](#)⁶
- Notable TTPs and Tools: Sandbox Evasion ([Minerva](#)); Unenrolling Devices from Admin Control ([The Hacker News](#)); Exploitation of CCTV system ([Rescurity](#)); LockBit Disguised as Resumes ([AhnLab](#)); Multilingual Executive Impersonation ([Abnormal](#)); Old Vulnerabilities in Ransomware Attacks ([TechTarget](#)); sshd backdoor ([GitHub](#)); M2RAT Mobile Device Scanner/Scraper ([Bleeping Computer](#)); Automated Injection of Malicious NPM/PyPI Packages ([CheckMarx](#), [Phylum](#)); SwiftSlicer Wiper ([ESET](#)); LockBit Green ([GitHub](#)); MyloBot Botnet ([The Hacker News](#)); Medusa Botnet ([BleepingComputer](#)).

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*



CISA Resource Highlights

- Joint Cyber Defense Collaborative



JOINT CYBER DEFENSE
COLLABORATIVE

Jeff Terra
3/1/2023



#StopRansomware - Ransomware Attacks on Critical Infrastructure Fund DPRK Espionage Activities

13

- CISA, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), and Republic of Korea's Defense Security Agency and National Intelligence Service have released a joint Cybersecurity Advisory (CSA).
- The authoring agencies urge network defenders 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 phishing-resistant multifactor authentication.
 - Install and regularly update antivirus and antimalware software on all hosts.

- Please note all information provided is TLP Amber

CISA Releases ESXiArgs Ransomware Recovery Script

14

- CISA has released a recovery script for organizations that have fallen victim to ESXiArgs ransomware. The ESXiArgs ransomware encrypts configuration files on vulnerable ESXi servers, potentially rendering virtual machines (VMs) unusable.
 - CISA recommends organizations impacted by ESXiArgs evaluate the script and guidance provided in the accompanying README file to determine if it is fit for attempting to recover access to files in their environment.
 - Organizations can access the recovery script here: <https://github.com/cisagov/ESXiArgs-Recover>
-
- Please note all information provided is TLP Amber

CISA and FBI Release ESXiArgs Ransomware Recovery Guidance

15

- CISA and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory, ESXiArgs Ransomware Virtual Machine Recovery Guidance.
- This advisory describes the ongoing ransomware campaign known as “ESXiArgs.”
- Malicious cyber actors may be exploiting known vulnerabilities in unpatched and out-of-service or out-of-date versions of VMware ESXi software to gain access to ESXi servers and deploy ESXiArgs ransomware.
- The ransomware encrypts configuration files on ESXi servers, potentially rendering virtual machines unusable.

- Please note all information provided is TLP Amber

As of February 1, 2023:

- VMware Releases Security Update: vRealize and Carbon Black
- Drupal Releases Security Update: Apigee vulnerability
- CISCO Releases Security Advisories: Multiple products
- OpenSSL Releases Security Advisory
- Apple Releases Security Updates: Multiple products
- Microsoft Releases Security Updates: Multiple products
- Citrix Releases Security Updates: Workspace Apps, Virtual Apps, Desktops
- Mozilla Releases Security Updates: Firefox 110 and ESR
- Adobe Releases Security Updates: Multiple products
- Fortinet Releases Security Updates: Multiple products
- **Best practices:**
 - Leverage automatic updates for all operating systems and third-party software
 - Implement security configurations for all hardware and software assets
 - Remove unsupported or unauthorized hardware and software from systems



Please note all information provided is TLP Amber

JOINT CYBER DEFENSE
COLLABORATIVE

Jeff Terra
3/1/2023



- 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 2/1/23 approximately 28 advisories have been issued
- The advisories span the following sectors: Information Technology, Critical Manufacturing, Energy and Multiple Sectors
- [Cybersecurity Alerts & Advisories | 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 13 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of February. 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/>
- ❑ CISA NCAS – <https://cisa.gov/resources-tools/all-resources-tools>
- ❑ CISA Shields Up - <https://www.cisa.gov/shields-up>
- ❑ Free Cybersecurity Services and Tools - <https://www.cisa.gov/free-cybersecurity-services-and-tools>
- ❑ CISA News Room - <https://www.cisa.gov/cisa/newsroom>
- ❑ CISA Blog - <https://www.cisa.gov/blog-list>
- ❑ CISA Publications Library - <https://www.cisa.gov/publications-library>
- ❑ CISA Cyber Resource Hub - <https://www.cisa.gov/cyber-resource-hub>
- ❑ CISA Cybersecurity 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
3/1/2023





FEATURED SPEAKER

TLP: CLEAR



KARL HEIMER, PRINCIPAL, HEIMER & ASSOCIATES LLC



Current Position

- Owner of Heimer & Associates (consultant)
- Founder of CyberAuto Challenge & CyberBoat Challenge
- Co-Founder of CyberTruck Challenge
- Assisted John Deere in creating CyberTractor Challenge
- Cybersecurity advisor to State of Michigan (MEDC)

Past Positions

- Sr. Research Director, Battelle
- Division Manager, Sparta
- Sr. Program Manager, Lockheed Martin
- US Army

AGENDA FOR PRESENTATION

TOPICS TO BE COVERED

1. **Mission & Purpose** (how we can help you and our industry)?
2. **Students** – who comes, what they learn, what they think?
3. **Professionals** – who teaches, who mentors, how industry engages?
4. **Support** – who sponsors?
5. **What** – outcomes?

Mission & Purpose



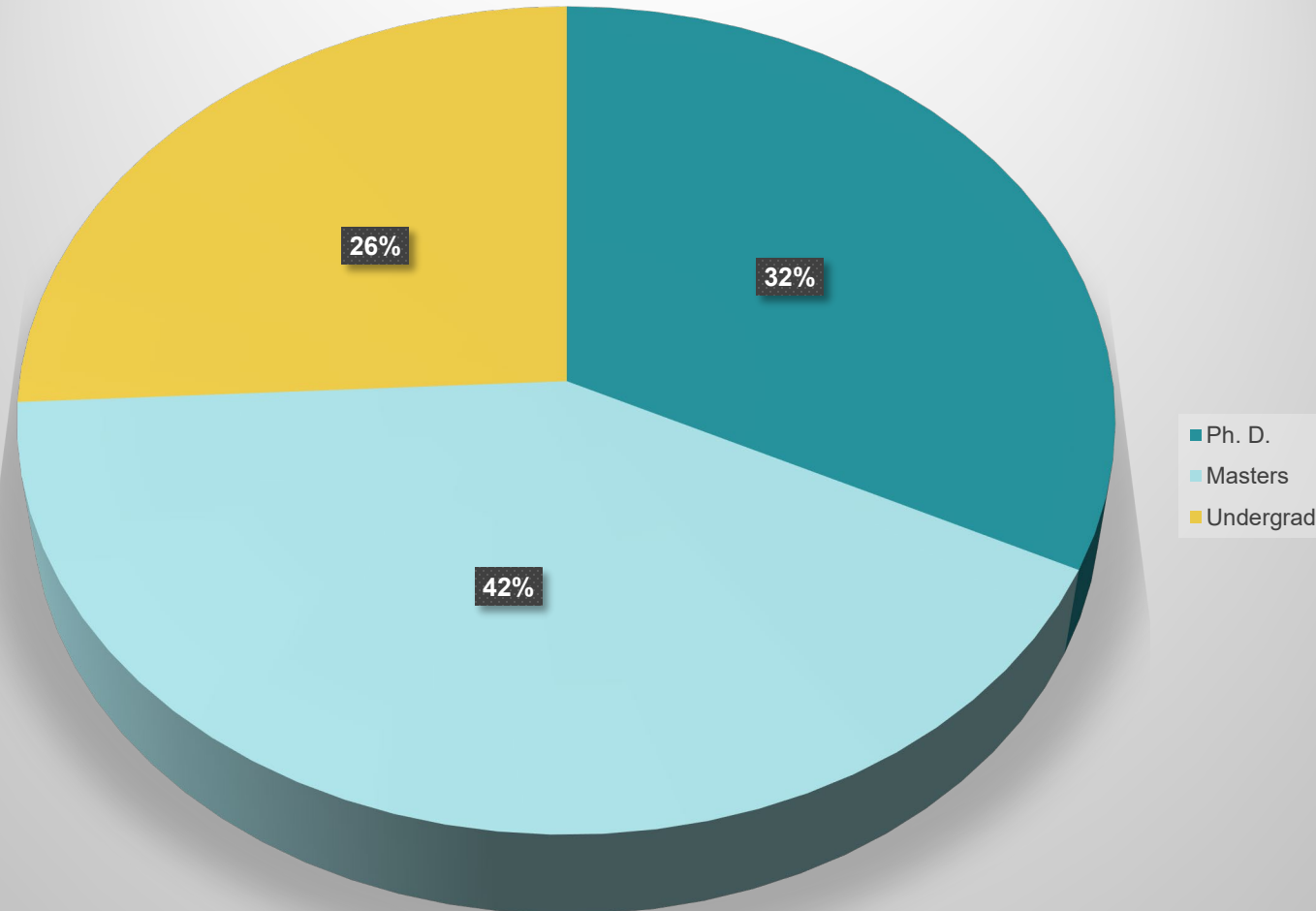
- Help **develop the next generation workforce** by bringing awareness, excitement, professional involvement, and practicum-based training to the automotive, heavy vehicle, & maritime cyber domain.
- Help **establish community of interest for automotive cybersecurity** that transcends individual companies or departments and reaches across disciplines and organizations to make a more universal and experienced base of engineers and managers.



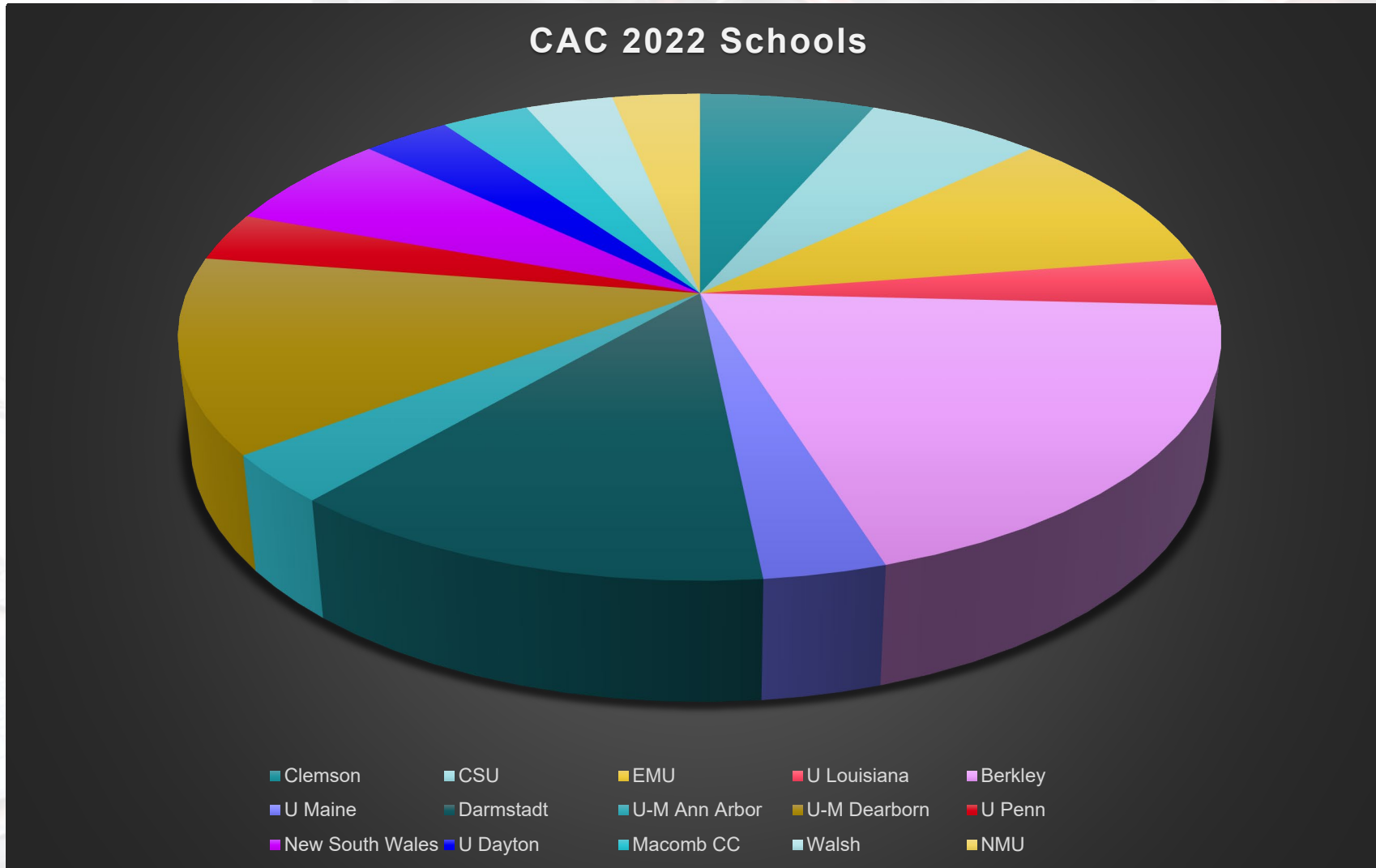
Student Composition (2022)



CAC 2022 Student Level



Universities represented (2022)



Partial List of Universities (2012-2022)



Michigan Universities

Eastern Michigan University
Macomb Community College
Michigan State
Michigan Tech
Northern Michigan University
UD - Mercy
University of Michigan –
Dearborn
University of Michigan – Ann
Arbor
Walsh College

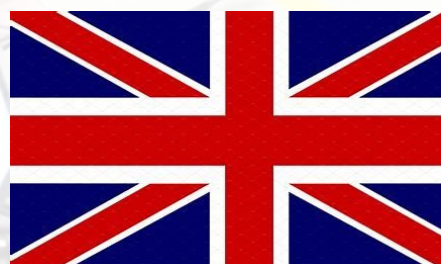
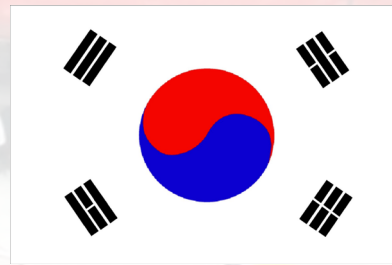
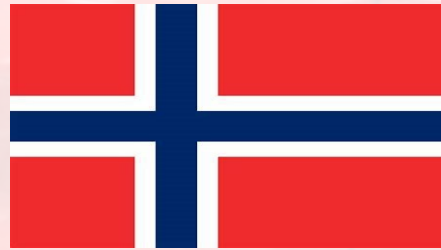
International Universities

Queens College
University of Darmstadt
University of New South Wales

Other US Universities (partial)

Berkeley	Carnegie Mellon
Clemson	Colorado State University
DePaul University	Draper
Drexel	Georgetown
Howard	Johns Hopkins
MIT	Ohio State University
Purdue	Tennessee Tech
University of Arizona	University of Dayton
University of Delaware	University of Louisiana
University of Maryland	University of Pennsylvania
University of Texas (Arlington)	University of Washington
University of Virginia	West Point
Virginia Tech	

Participation is International



Schedule (2022)



	Welcome & Inprocessing	Training Days						Assessment Day	Report & Release
24-hour	Sunday 24 July 2022	Monday 25 July 2022 ICE	Monday 25 July 2022 EV	Tuesday 26 July 2022 ICE	Tuesday 26 July 2022 EV	Wednesday 27 July 2022 ICE	Wednesday 27 July 2022 EV	Thursday 28 July 2022	Friday 29 July 2022
0700-0730	Site Opens & Breakfast								0700-0730
0730-0800	Welcome								Sleep / Recover / Clear Hotel
0800-0830	Lab Orientation		WIFI & Bluetooth	CANBUS	Forensics	Electrical Vehicles	ASSESSMENT	0800-0830	
0830-0900	Legal								Team Intros / Integration
0900-0930	CANBUS		Software Reverse Engineering	Hardware Reverse Engineering	Ghidra	Forensics		Hearty Brunch	
0930-1000	CANBUS		Software Reverse Engineering					SocketCAN	Ghidra
1000-1030	CANBUS		Software Reverse Engineering	SocketCAN	Ghidra	Forensics			
1030-1100	CANBUS		Software Reverse Engineering					SocketCAN	Ghidra
1100-1130	CANBUS		Software Reverse Engineering	SocketCAN	Ghidra	Forensics	Outbrief		
1130-1200	CANBUS		Software Reverse Engineering					SocketCAN	Ghidra
1200-1230	Lunch								
1230-1300	Lunch								RELEASE
1300-1330	CANBUS	Software Reverse Engineering		SDR & GPS	SocketCAN	Electrical Vehicles	Ghidra	ASSESSMENT	1300-1330
1330-1400		SDR & GPS							
1400-1430	SDR & GPS		WIFI & Bluetooth	Ghidra	Forensics	1430-1500			
1430-1500	SDR & GPS						WIFI & Bluetooth		Ghidra
1500-1530	SDR & GPS		WIFI & Bluetooth	Ghidra	Forensics	1530-1600			
1530-1600	SDR & GPS						WIFI & Bluetooth		Ghidra
1630-1660	SDR & GPS		WIFI & Bluetooth	Ghidra	Forensics	1630-1700			
1660-1700	SDR & GPS						WIFI & Bluetooth	Ghidra	Forensics
1700-1730	SDR & GPS		WIFI & Bluetooth	Ghidra	Forensics	1730-1800			
1730-1800	SDR & GPS						WIFI & Bluetooth	Ghidra	Forensics
1800-1830	Dinner								
1830-1900	Dinner								1900-1930
1900-1930	Dinner								1930-2000
1930-2000	Dinner								2000-2030
2000-2030	Dinner								2030-2100
2030-2100	Dinner								2100-2130
2100-2130	Dinner								2130-2200
2130-2200	Dinner								2200-2230
2200-2230	Dinner								2230-2400
2230-2400	Dinner								2230-2400
0000-0630 next day	Dinner								0000-0630 next day

Schedule (2022)



CyberTruck Challenge 2022 Schedule

Version:20220619

	Sunday, 19 June	Monday, 20 June		Tuesday, 21 June		Wednesday, 22 June	Thursday, 23 June	Friday, 24 June	Time						
		Group A	Group B	Group A	Group B										
Before 0700	Site Closed	Site Closed							Before 0700						
0700-0730		Breakfast							Breakfast	0700-0730					
0730-0800		Welcome // NDA							Student Team Briefs (30 minutes each group)	0730-0800					
0800-0830		Safety and Orientation								0800-0830					
0830-0900				Vehicle Network Security	<u>Ghidra</u>	Legal Briefing	Assessment	Assessment		0830-0900					
0900-0930		<u>Software RE</u>	Truck Systems and J1939	Vehicle Network Security	<u>Ghidra</u>	Assessment				Assessment	0900-0930				
0930-1000											<u>Cryptography</u>	Vehicle Network Security	Assessment	Assessment	0930-1000
1000-1030															Assessment
1030-1100		Assessment	Assessment	Assessment	Assessment	1030-1100									
1100-1130						Assessment				Assessment	Assessment	Assessment	1100-1130		
1130-1200		Assessment	Assessment	Assessment	Assessment								Awards	1130-1200	
1200-1230						Assessment			Assessment	Assessment	Assessment	Assessment	Lunch	1200-1230	
1230-1300		Assessment	Assessment	Assessment	Assessment								Assessment	Assessment	1230-1300
1300-1330						Assessment	Assessment	Assessment	Assessment	Assessment	Assessment	1300-1330			
1330-1400		Assessment	Assessment	Assessment	Assessment							Assessment	Assessment	1330-1400	
1400-1430						Assessment	Assessment	Assessment	Assessment	Assessment	Assessment			1400-1430	
1430-1500		Assessment	Assessment	Assessment	Assessment							Assessment	Assessment	1430-1500	
1500-1530						Assessment	Assessment	Assessment	Assessment	Assessment	Assessment			1500-1530	
1530-1600		Assessment	Assessment	Assessment	Assessment							Assessment	Assessment	1530-1600	
1600-1630	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment	1600-1630				
1630-1700		Assessment	Assessment	Assessment	Assessment						Assessment	Assessment	1630-1700		
1700-1730	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment			1700-1730		
1730-1800		Assessment	Assessment	Assessment	Assessment						Assessment	Assessment	1730-1800		
1800-1830	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment			1800-1830		
1830-1900		Assessment	Assessment	Assessment	Assessment						Assessment	Assessment	1830-1900		
1900-1930	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment			1900-1930		
1930-2000		Assessment	Assessment	Assessment	Assessment						Assessment	Assessment	1930-2000		
2000-2030	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment			2000-2030		
2030-2100		Assessment	Assessment	Assessment	Assessment						Assessment	Assessment	2030-2100		
2100-2130	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment			2100-2130		
2130-2200		Assessment	Assessment	Assessment	Assessment						Assessment	Assessment	2130-2200		
After 2200	Assessment					Assessment	Assessment	Assessment	Assessment	Assessment			After 2200		

Snacks will be served each afternoon.

*Survey

*Survey



Outcomes – Student Comments



“This experience is amazing. I would never get an opportunity to work with an actual vehicle if it wasn’t for the CyberTruck Challenge.”

-- Subhojeet Mukherjee, Ph.D. Candidate (CS)

“The biggest benefit for me was probably talking with all the professionals in industry. Talking to them about what they did just affirmed that I want to work in the same field.”

-- John Maag, Class of 2019 (EE)



“In one short week I came together with a range of professionals, students, and hobbyists. We spent two days getting a broad crash course in reverse engineering. Then with teams and a mentor, we chose a project or two from a range of levels that make up the various truck systems. It was intense; I was totally engaged; it was one of the most fantastic weeks of my life.”

-- Zach Aubin, Graduate Student in Computer Science, Class of 2022.

This is a fantastic opportunity to learn and explore as it covers every aspect of the car related to security. Well-designed schedule to learn all about computers in the car. A chance to learn and explore many technologies and standards.

-- Ruthvik K, Graduate Student in Computer Science

Instructors and Keynotes (partial)



- Len Lapadula (Bell/Lapadula Model)
- John J. Strauchs (Former CIA / former tech consultant to “Sneakers” movie)
- Jim Christy (Chief of Defense Cyber Crimes Center)
- Bruce Schneier (Crypto guru)
- Mudge (Hacker, DARPA, Researchers)
- David Strickland (NHTSA Administrator)
- Faye Francy (Executive Director for Auto-ISAC)
- David Columbo (Car hacker)
- Colin O’Flynn (Creator of Chip Whisperer)
- Craig Smith (Author of Car Hacker’s Handbook)
- Ollie Hartkopp (Creator of SocketCAN)
- Karl LeBouef (Technical Fellow for Cybersecurity at General Motors)
- Karl Kosher (Author of USENIX 2010 & 2011 papers that really moved vehicle cybersecurity to the forefront)

Community Building



CyberAuto Challenge Highlights Michigan's Leadership in Cybersecurity, Workforce Training



Now in its ninth year, CyberAuto Challenge has kicked off this week at Macomb Community College, with Lt. Governor Garlin Gilchrist II joining officials from Michigan State Police and the Michigan Economic Development Corporation yesterday to highlight the state's leadership in cybersecurity and workforce training.

Industry, Government, Academia, and the Research Community (& Hackers) meet and share information at the CyberAuto Challenge – this helps forge/foster Community.

The Michigan State Police have been a critical partner for the CyberAuto Challenge, providing outstanding training, equipment, and mentorship. Some students have sought employment with MSP/MC3 after the event.



Community Building - Federal



Industry and Government interactions to help provide common perceptions and operating environments

DOT (NHTSA & FHA)

DOD (uniformed)

NSA

DHS

FBI

Department of Energy & National Labs

Other US Government Orgs

GoC (Government of Canada)

What its like?



What its like?



CyberBoat Challenge – what its like?





Thank you to the 2022 CyberAuto Challenge sponsors

CyberAuto Challenge Sponsors for 2022



SPONSORS are the reason we
can be here at all

We can be here because they
trust us – and trust you

We can be here because we
collectively provide value

Titanium
Platinum
Sponsors
Gold
Sponsors
Silver
Sponsors
Copper
Sponsors



SPONSORS are the reason we can be here at all

We can be here because they trust us – and trust you

We can be here because we collectively provide value

Premier Sponsor



Platinum Sponsors



Gold Sponsors



Silver Sponsors



Thank you to the CyberTruck Challenge sponsors



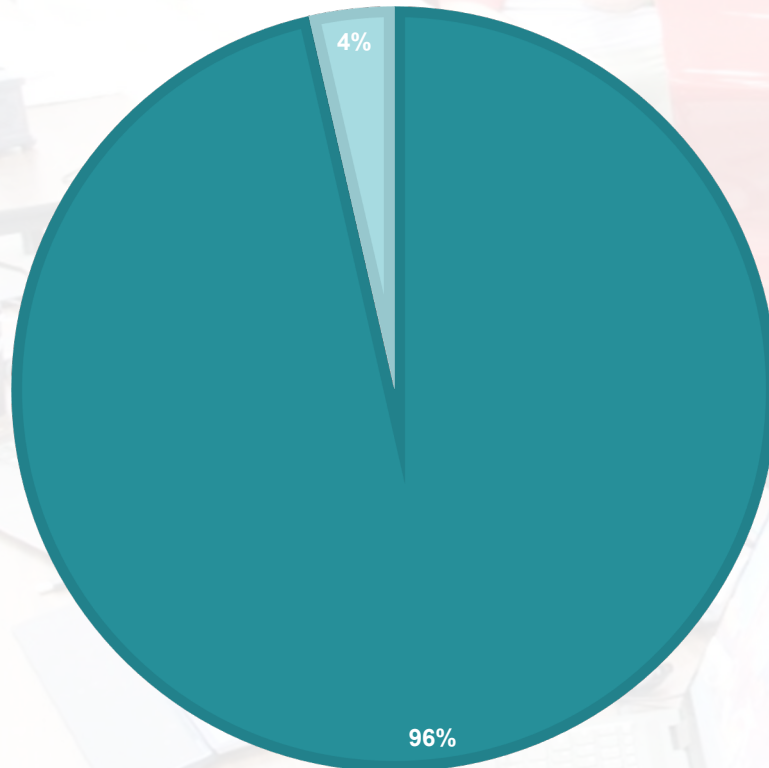


Outcomes – Student Intent & Connections



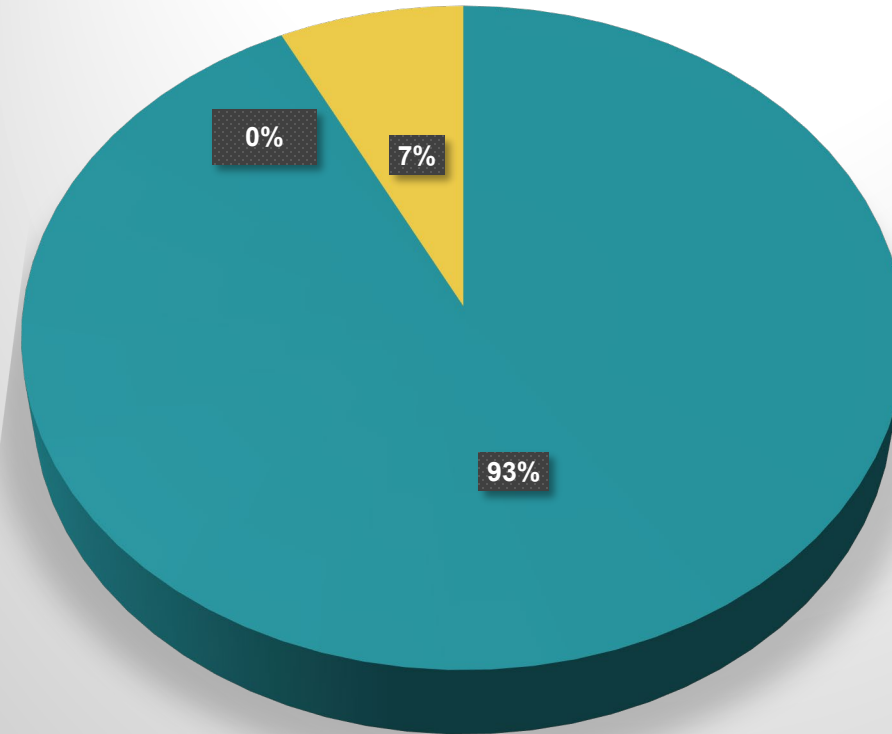
HAVE YOU FOUND A MENTOR?

■ [student] mentor yes ■ [student] mentor no



Has attending this event made you more likely to select this career?

■ [student] career more likely
■ [student] career less likely
■ [student] career no change





JOHN DEERE

CYBER TRACTOR CHALLENGE

UNLOCK THE POTENTIAL OF NEXT-GEN CYBERSECURITY TALENT BY EXPLORING AND SECURING JOHN DEERE'S AUTONOMOUS TECHNOLOGY STACKS

- Learn new skills and network with engineers
- Assess REAL equipment
- Explore ag-focused embedded technology stacks
- Create lasting employer relationships
- Bolster personal and professional growth

JUNE 26 - 30, 2023

WHAT: John Deere is hosting a week-long invitational event for students to take cybersecurity classes on & assess our embedded industrial control systems.*

WHEN: June 26 – 30, 2023

WHERE: Des Moines, Iowa

WHY APPLY?

- Grow skillsets in a highly competitive field
- Build resume for future opportunities
- Get hands-on experience with real embedded technology
- Learn about John Deere's student employment programs
- *All expenses paid: Free Travel, Free Stay, Free Food!*

* See application form for Eligibility Requirements

TIMELINE:



WHAT SKILLS YOU NEED:

- ▶ Must be enrolled as a full-time student pursuing a 2yr, 4yr, or advanced degree at an accredited college or university
- ▶ Experience with cybersecurity or embedded engineering technologies
- ▶ Background in networking, cloud, IoT, CANBUS, *nix or general security concepts
- ▶ Exposure to one or more programming languages: Python, C/C++, Bash
- ▶ Demonstrated ability to learn new technologies
- ▶ Strong analytical, communication and intrapersonal skills

WHAT MAKES YOU STAND-OUT

Pursuing Bachelor's degree (equivalent or higher) in Software/Computer Engineering, Cybersecurity, Computer Science

Have exposure to networking, cloud, IoT, CANBUS and *nix

Participation in cybersecurity competitions, such as CTF

Exposure to cloud concepts: AWS, Azure, etc.

Knowledge of security principles: ethical hacking, vulnerabilities, secure design

[Cyber Tractor Challenge Home-Page](#)

[Learn more about JD through our 2021 Sustainability Report](#)

[Contact Us: CyberTractorChallenge@JohnDeere.com](mailto:CyberTractorChallenge@JohnDeere.com)



CyberTruck Challenge 2023

- Macomb CC Sports & Expo Center
- June 12-16, 2023

CyberAuto Challenge 2023

- Macomb CC Sports & Expo Center
- July 24-28, 2023

Contact:

- Karl Heimer: karl.heimer@outlook.com
- [linkedin.com/in/karl-heimer](https://www.linkedin.com/in/karl-heimer)
- 248.270.0117
- (email is best)



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.
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
(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
[@auto-ISAC](#)