Welcome to Auto-ISAC!

Monthly Virtual Community Call

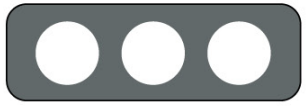
November 2nd, 2022

This Session will be recorded.

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

DHS Traffic Light Protocol (TLP) Chart

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
TLP:RED Not for disclosure, restricted to participants only.	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.	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.
TLP:AMBER Limited disclosure, restricted to participants organizations.	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.	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.
TLP:GREEN Limited disclosure, restricted to the community.	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.	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.
TLP:WHITE  Disclosure is not limited.	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.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

From: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ➢ **Brandon Barry, *CEO, Block Harbor Cybersecurity*** ➢ **Title: "*A Global Grassroots Community of 10,000+ Automotive Security Folks: The ASRG*"**
11:45	**Around the Room** ➢ 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!

26 *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

49 *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)*

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

2022-2023 Advisory Board (AB) Leadership

Todd Lawless
Chair *of the*
Advisory Board
Continental

Bob Kaster
Vice Chair *of the*
Advisory Board
Bosch

TBA
Chair *of the SAG*
TBA

Larry Hilkene
Chair *of the CAG*
Cummins

Member Roster
As of November 2022

Highlight = Change

75 Members, 3 in Progress

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

Pending: KTM, Micron, Rivian

Upcoming Events

Upcoming Meetings:

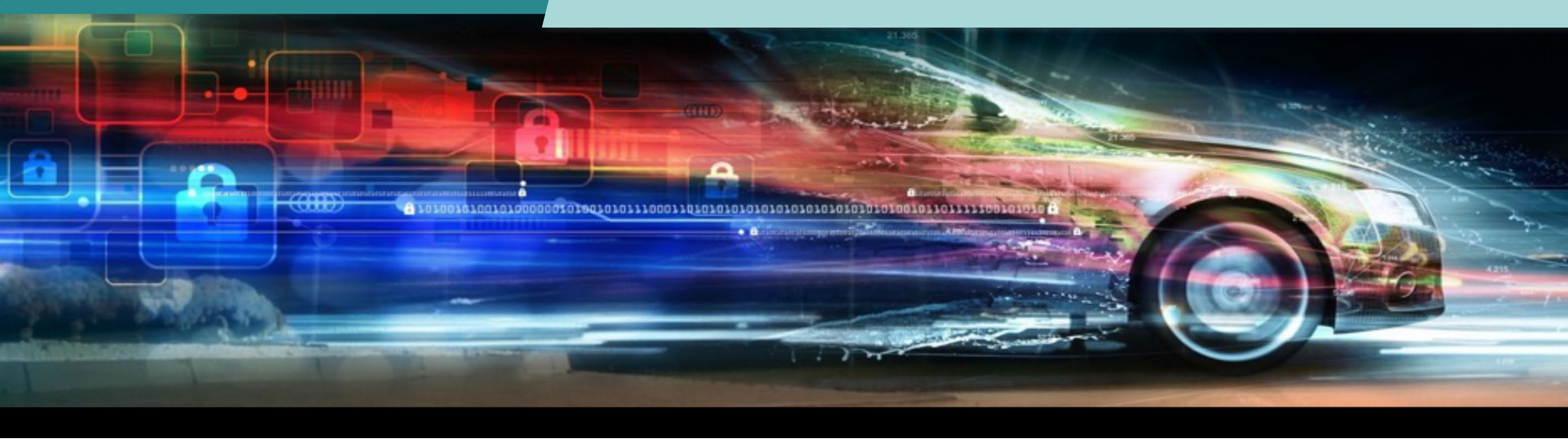
- **Community Call: Wednesday, December 7th Time: *11 – 12:00 p.m.* TLP:WHITE**
  - **Title: "CISCP to JCDC Transition"**
  - **Speaker:**
    - **James Murphy- Section Chief, Industry Partnerships | Joint Cyber Defense Collaborative (JCDC)**
    - **Dan Strachan- Senior Engagement Lead, Industry Partnerships | Joint Cyber Defense Collaborative (JCDC)**
    - **Pranav Julakanti- Consultant, Industry Partnerships | Joint Cyber Defense Collaborative (JCDC)**

- **Members Teaching Members:**
  - **Wednesday, November 16th – Speaker: Michael Schneider, ETAS GmbH, Senior Security Consultant**
    Title: *"Securing Modern Vehicles with AUTOSAR"* Time: 10 – 11:30 a.m. TLP:AMBER (Members Only)

Announcements:

- **ACT Program Advanced Courses –** Beta Advanced registration is open. Concepts and Compliance (Nov 1-4) is still open for registration. Contact Tamara Shoemaker. **(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
Automotive Information Sharing and Analysis Center

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 in key regions show no signs of abating:**
    - **Russia-Ukraine: In Crisis (The Hill, BBC)**
    - **China-Taiwan: High (Taiwan News, Eurasian Times)**
    - **North Korea-South Korea: High (Reuters, Aljazeera)**
    - **Iran: High (CNN, Reuters)**

    Russia, China, North Korea, and Iran have significant cyberattack capabilities which could manifest without warning and impact business and industrial operations (Russia, China, North Korea, Iran;

    CISA-Technical Approaches to Uncovering and Remediating Malicious Activity*).
  - **Ransomware Groups Targeting Automotive: RansomEXX, Vice Society, Black Basta.**
  - **Multiple incidents of threat actors selling access to automotive organizations' networks and selling or leaking sensitive information.***
  - **Notable Incidents, TTPs, and Tools: BlueBleed (Microsoft, Socradar); Unidentified Fraudulent Diagnostic Tool Used for Vehicle Theft (BleepingComputer); Targeting Shadow APIs (Cequence); Qbot Malware Deployment (Trend Micro); Azov Data Wiper (BleepingComputer); Mark-of-the-Web Bypass (BleepingComputer).**

CISA Resource Highlights

Joint Cyber Defense Collaborative

JOINT CYBER DEFENSE COLLABORATIVE

Pranav Julakanti
11/8/2022

JOINT CYBER DEFENSE COLLABORATIVE

Sunsetting CISCP

Guide on Responding to DDoS Attacks and DDoS Guidance for Federal Agencies

- CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have released a publication: Understanding and Responding to Distributed Denial-of-Service Attacks to provide organizations with proactive steps to reduce the likelihood and impact of distributed denial-of-service (DDoS) attacks. The guidance is for both network defenders and leaders to help them understand and respond to DDoS attacks, which can cost an organization time, money, and reputational damage.

- A PDF of the guidance can be found here: https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

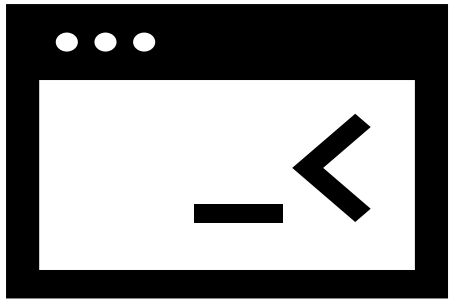
- The announcement can be found here: Joint CISA FBI MS-ISAC Guide on Responding to DDoS Attacks and DDoS Guidance for Federal Agencies | CISA

CISA Releases Four Industrial Control Systems Advisories

ICS news October

CISA has released four (4) Industrial Control Systems (ICS) advisories on October 27, 2022. 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 advisory for technical details and mitigations:

- ICSA-22-300-01 Rockwell Automation FactoryTalk Alarm and Events Server Rockwell Automation FactoryTalk Alarm and Events Server | CISA
- ICSA-22-300-02 SAUTER Controls moduWeb | CISA
- ICSA-22-300-03 Rockwell Automation Stratix Devices Containing Cisco IOS | CISA
- ICSA-22-300-04 VTScada | CISA



Pranav Julakanti
11/8/2022

KEVs Catalogue

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 has added 11 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of October. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Pranav Julakanti

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
- 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

Pranav Julakanti
11/8/2022

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*

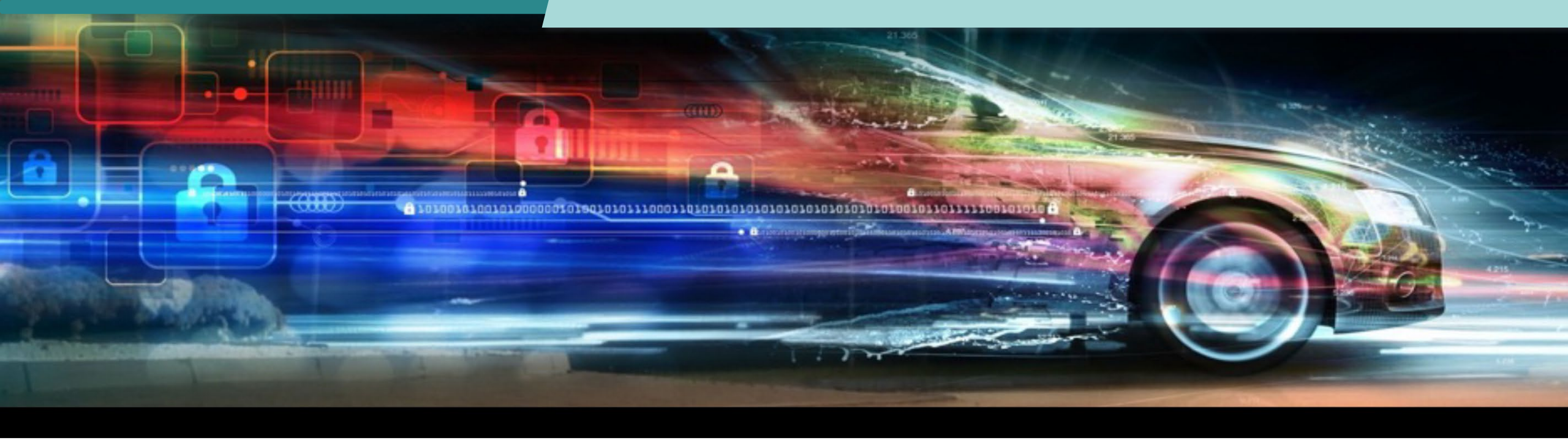
30+
Featured Speakers to date

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!

7 ***Best Practice Guides available on website***

2000+
Community Participants



Featured Speaker

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Meet the Speaker

Brandon Barry

Block Harbor Cybersecurity

Brandon Barry studied Computer Engineering with a research focus on vehicle cybersecurity at Brown University. He founded Block Harbor Cybersecurity in 2014 to support automakers and tier ones with solutions in vehicle cybersecurity where his role is CEO. His team placed first place at the DEF CON Car Hacking Village Capture the Flag in 2019 and second place in 2022. He has been invited to several private bug bounty events with automakers.

Brandon leads the Americas chapters of the ASRG with a focus on the Detroit chapter. Outside of the day job at Block Harbor and the ASRG, he's passionate about cars with a focus on drift racing.

Community Driven Automotive Security

A Global Grassroots Community of 10,000+ Automotive Security Folks: the ASRG

Agenda

01 My story

02 About the ASRG

03 What the ASRG’s up to

04 Get involved

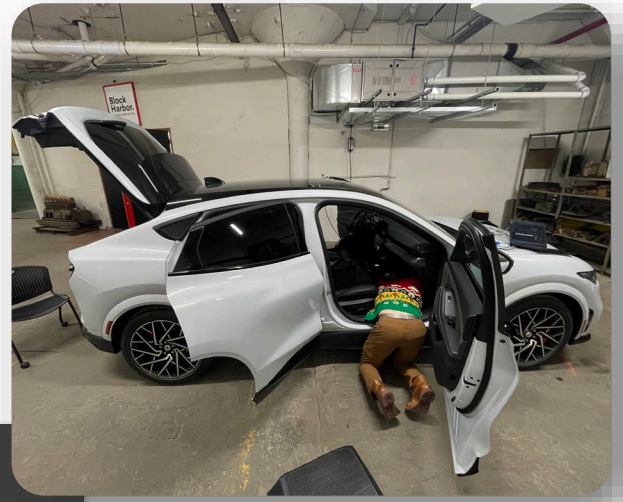
05 ASRG-Detroit: Toy Drive & Shop Talk

3PM-8PM on December 8, 2022 #FILLTHEFRUNK

ASRG Toy Drive & Shop Talk

December 8th, 2022
@Block Harbor: 1111 Bellevue Street, Detroit, MI 48207
3-8pm

Topic: I'm a Vehicle Cybersecurity Expert, Change My Mind



#FILLTHEFRUNK

bit.ly/3Ue8lzM

ASRG

Food & Drink provided w/ a special guest visit
Admission: Free, but bring a toy or donate if you can

Brandon Barry

About Me

Founder
Block Harbor Cybersecurity

Americas Lead
Automotive Security Research Group (NPO)

Self-Proclaimed Professional Drift Racer

My Story

How I got into Vehicle Cybersecurity

- 2014: Internship in cybersecurity, FCA
- Late 2014: Founded Block Harbor as an Undergrad at Brown University
    - Computer Engineering, research focus on Vehicle Cybersecurity
    - Early projects in:
        - VSOC
        - Vehicle System Risk Assessment
        - Vehicle System Penetration Testing
        - Vehicle Cybersecurity Automated Testing
- 2015: Vehicle Cybersecurity, front and center in the media
- Tinkered with my own car
- 2016: J3061, Car Hacker's Handbook
- 2018: Graduated, came back to Detroit to really tackle problems in Vehicle Cybersecurity full time
- 2019: DEF CON Car Hacking Village CTF 1st Place, CANucks
- 2020: The standard and regulatory landscape started to shape up.

Your Story

How’d you find your way into Vehicle Cybersecurity?

01 Existing automotive professional – career pivot

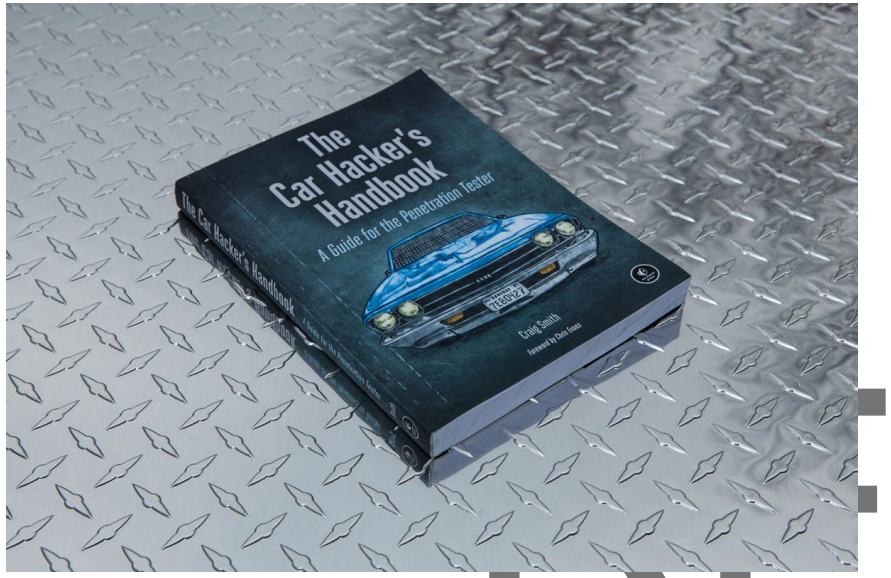
02 IT security folks lured into vehicle security

03 Government (FBI, CIA, etc.) pivot to industry

04 Car hacker/hobbyist turned professional

05 Academic

Getting Started in Vehicle Cybersecurity

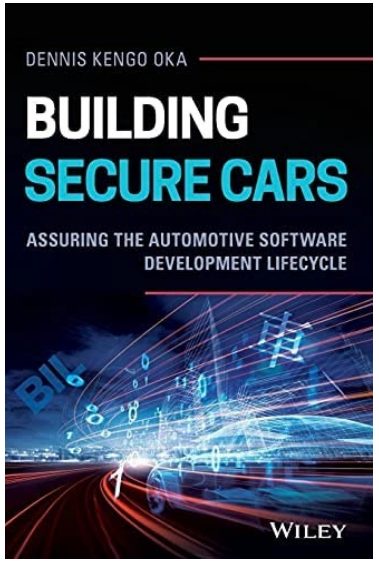


Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS

READ ME



Licensed to Block Harbor Cybersecurity / Brandon Barry (brandon@blockharbor.io)
ISO Store Order: OP-545230 / Downloaded: 2021-08-31
Single user licence only, copying and networking prohibited.

INTERNATIONAL STANDARD

ISO/SAE 21434

First edition
2021-08

Road vehicles — Cybersecurity engineering

Véhicules routiers — Ingénierie de la cybersécurité

Automotive Security Research Group

The Origin

John Heldreth

- Master's Thesis
- August 2017: ASRG-Stuttgart First Meetup

October 2018: ASRG-Detroit First Meetup - Sean McKeever

ASRG-D First Meetup

ASRG

Why?

When you entered vehicle cybersecurity, don't you wish…

- you had a community?
- you had resources?

When you were solving hard problems in vehicle cybersecurity, don't you wish…

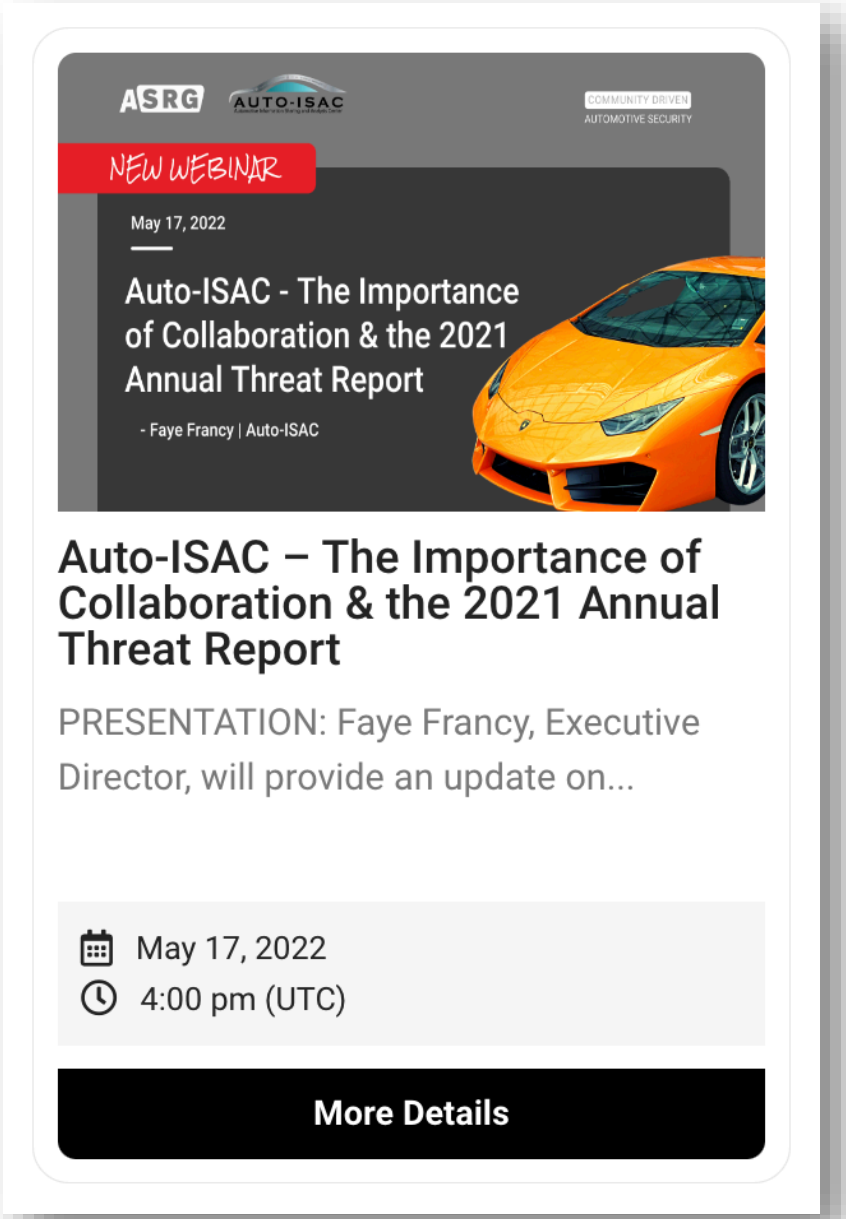
- you could refer to talks that might support you in solving it?
- you could talk to others from around the world to see how their perspective might shape your own?
- you could draw insight from people from completely different backgrounds - car hacker, academic, professional, etc.?

ASRG

Why?

Sounds kind of like the Auto ISAC…

but it's a focus on a different audience.



ASRG

Why?

Industry Groups
ACIC
VOLPE/NHTSA
Auto ISAC

Conferences/Events
DEFCON/Black Hat/RSA
ESCAR
CyberTruck/CyberAuto

Company Leadership
Automakers
Suppliers
Vendors

Vehicle Cybersecurity Community

?

Anyone and Everyone Else
Vehicle Cybersecurity Professionals
Interested Automotive Professionals
Students
Car Hackers
Other people with Interest

Academia/Researchers

ASRG

Casting a much wider net

ASRG at glance

12181	50	194
Members	Locations	Events

Losing people? Trying desperately to hire? Welcome to the club. If only there was a global pool of people that went out of their way to sign up with a non-profit in automotive security.

Passion and interest go a long way.

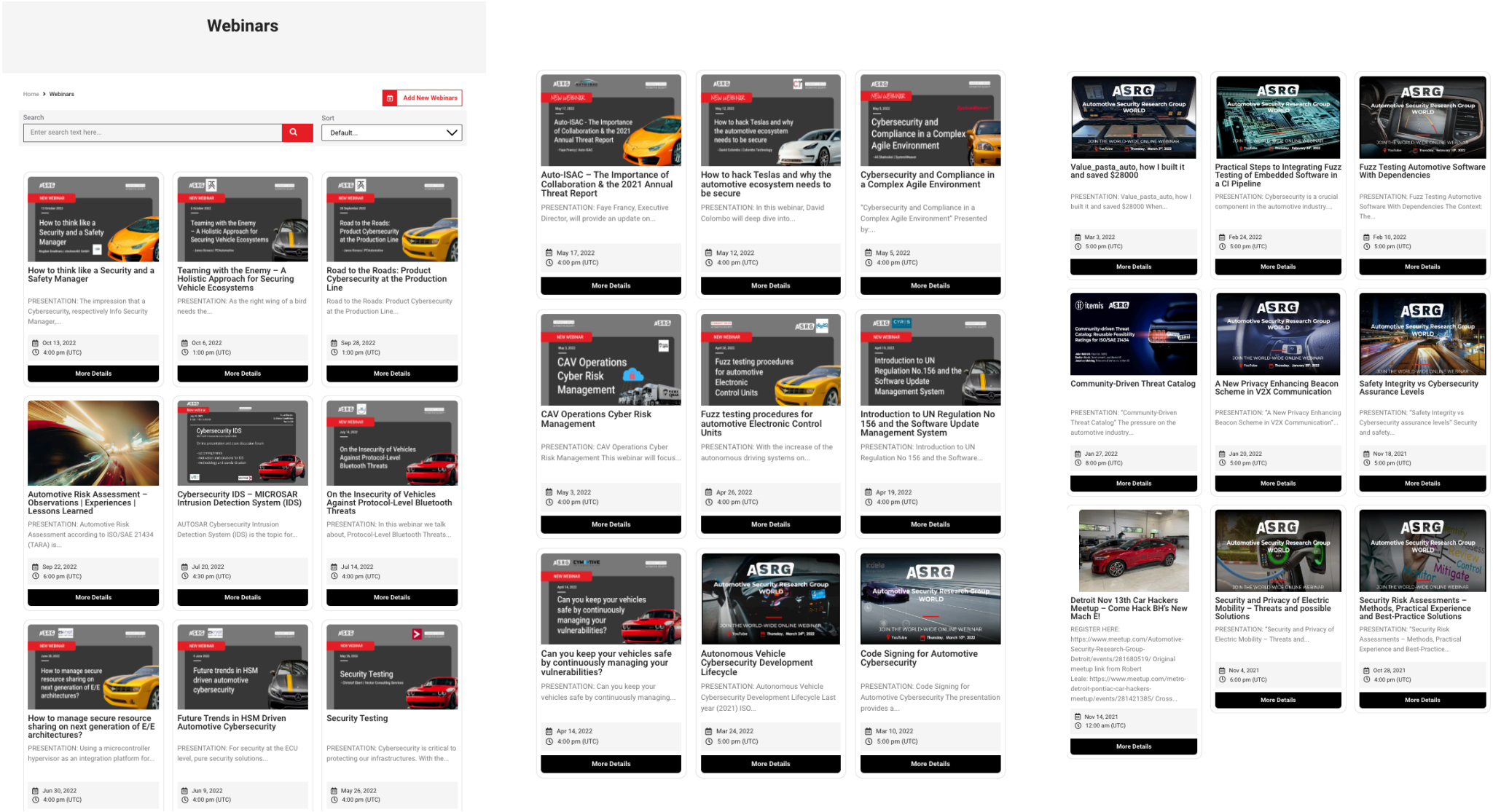
ASRG at glance

12181	50	194
Members	Locations	Events

So, what’s the ASRG up to?

ASRG

So what are we up to?: ASRG WORLD Webinars



ASRG

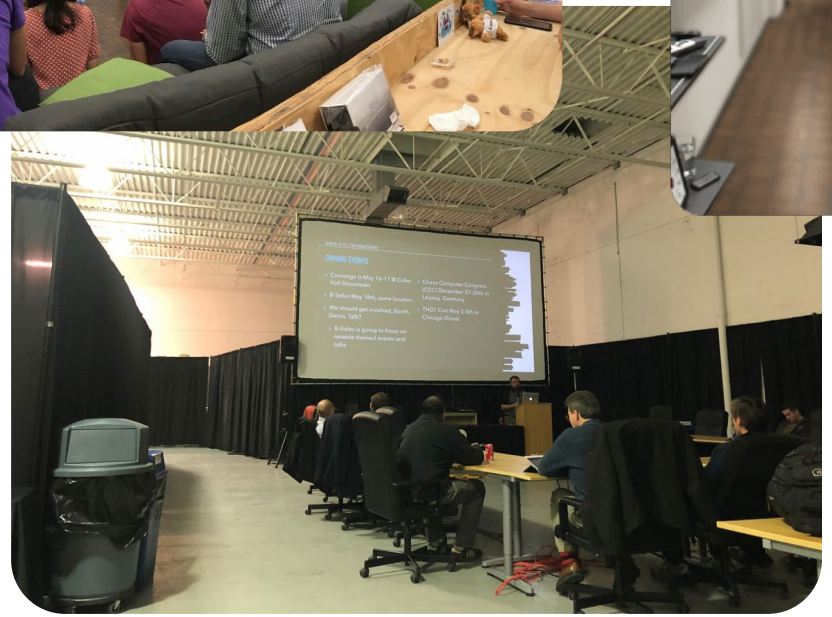
So what are we up to?: ASRG Chapters

- Ideally, monthly in-person meetups led by a local chapter lead.
- Still trying to recover chapter events post-COVID
- Check out a chapter near you – they might be hosting an event. If not – ask them when the next one will be!

Block
Harbor

connectory

connectory


COMING EVENTS

RIGHT TURN
MUST YIELD
TO PEDESTRIANS

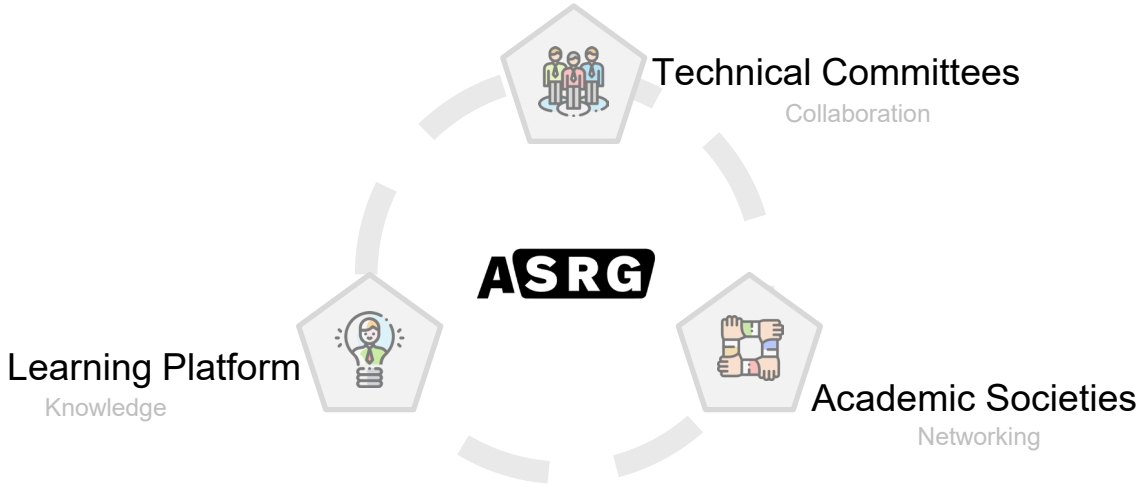
ASRG

So what are we up to?: ASRG Academic Network

.edu

- Missing University Curriculums
- Inadequate Relationship to Industry
- Non-Applied Research
- No Certification Program
- High Barrier of Entry

Solution



ASRG

So what are we up to?: ASRG Projects & Technical Committees

- Automotive Security Intelligence Platform (ASIP)
  - garage.asrg.io/intelligence/
- Threat Catalog
  - garage.asrg.io/threat-catalog/
- Open Exchange for Security Analysis Models
  - openxsam.io
- Vulnerability Management
  - ASRG is a CVE Numbering Authority for automotive-applicable vulnerabilities
  - ASRG receives vulnerability disclosures
- EU Vehicle Security Operations Center

ASRG

So what are we up to?: ASRG Secure Our Streets (SOS)

SECURE OUR STREETS
VEHICLE CYBER SECURITY

#SecureOurStreets

TOTAL REGISTERED

850

MAXIMUM PARTICIPANTS PER SESSION

282

AVERAGE PARTICIPANTS PER SESSION

116

TOP 10 DEMOGRAPHICS

33% | GERMANY
13% | INDIA
8% | UNITED STATES
8% | UNITED KINGDOM
7% | ISRAEL
3% | ROMANIA
2% | SPAIN
2% | SINGAPORE
2% | ITALY
2% | AUSTRIA

ROLES

63% | PROFESSIONAL
17% | RESEARCHER
7% | STUDENT
5% | STILL LOOKING FOR MYSELF...
2% | HOBBYIST / HACKER

ASRG

Individuals: So how can you get involved?

Sign up at garage.asrg.io

- Join/start a local chapter.
- Contribute to an ASRG effort:
  - Lead a WORLD Webinar
  - Support a Project/Technical Committee
  - Support SOS
  - Support the Academic Network
- Join slack & stir up the conversation
  - https://join.slack.com/t/asrg/shared_invite/zt-83ivvj85-Nny_0n8DN7HB1ws6w1u89g

Slack:

ASRG

Companies: So how can you get involved?

Supporter

Supporters are individuals, corporations, or organizations contributing existing organizational resources to ASRG without risk. There is **no official agreement/contract**.

Example: Meeting Rooms, Tools, Garages, Educational Content, Presentations, etc.

Sponsor

A Sponsor is a **formal agreement** between an organization or corporation and ASRG. This formal agreement details the relationship, services and fixed donations.

Example: ASRG Marketing opportunities.

Defined Levels (see Slide)

Partnership

A Partnership is a **formal agreement** between a **non-profit organization** and ASRG to work together towards a common goal. Risks and benefits are shared based on the formal agreement.

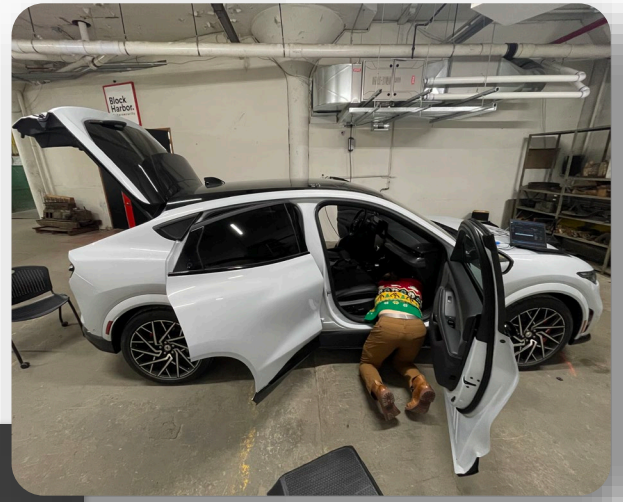
Example: Other non-Profit organizations

Sponsorships index is changed every year because of new offerings from ASRG, and potential increase in donation requirements.

ASRG Toy Drive & Shop Talk

December 8th, 2022
@Block Harbor: 1111 Bellevue Street, Detroit, MI 48207
3-8pm

Topic: I'm a Vehicle Cybersecurity Expert, Change My Mind



#FILLTHEFRUNK

bit.ly/3Ue8lzM

ASRG

Food & Drink provided w/ a special guest visit
Admission: Free, but bring a toy or donate if you can

Questions / Comments

(Anwsers are also acceptable)

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

BENEFACTOR
Sponsorship Partnership

2022 Summit Sponsors-

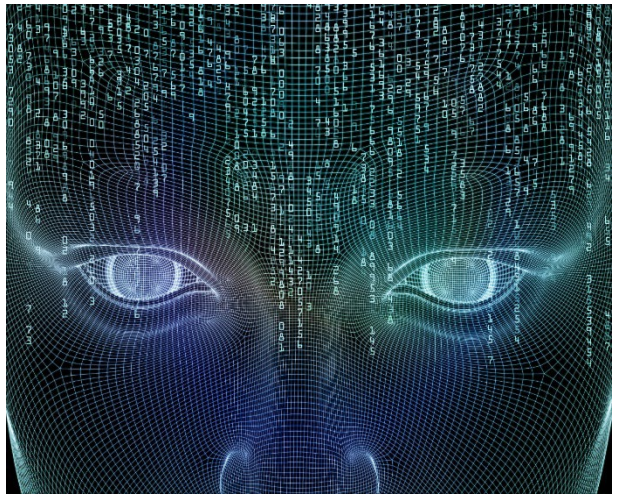
Argus
BGNetworks
Bosch
Blackberry
Block Harbor
BlueVoyant
Booz Allen Hamilton
C2A
Cybellum
CyberGRX
Cyware
Deloitte
Denso
Finite State
Fortress
Itemis
Keysight Technologies
Micron
NXP
Okta
Sandia
Securonix
Tanium
UL
Upstream
VicOne

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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!

THANK
YOU
GRAZIE
MERCI
MULTUMESC
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
JUSPAXAR
OBRIGADO
MATONDO
KIITOS
SALAMAT
MOCHCHAKKERAM
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
KIITOS
OBRIGADO
DANK JE
VINAKA
NIRRINGRAZZJAK
MAMANA
MULTUMESC
ARIGATO
KIITOS
DANKON
NIRRINGRAZZJAK
MOCHCHAKKERAM
MOCHCHAKKERAM
OBRIGADO
SPASIBO
WELALIN
SPASIBO
MAAKE
OBRIGADO
DANK JE
RAIBH MAITH AGAT
SPASIBO
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
MATUR NUWUN
CHOKRANE
GRAZIE
MERCI
MOCHCHAKKERAM

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