Auto-ISAC

Monthly Community Call

May 2020

COVID-19

Our thoughts and prayers go out to all those affected by COVID-19. We are very grateful to our Members and Partners for their continued support and engagement during these unprecedented times. If we can assist in any manner, please let us know how we might help.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why we're here ➢ Expectations for this community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC overview ➢ Heard around the community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ***SBOM – Dr. Allan Friedman***
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**

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 Auto-ISAC Staff** (staff@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!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, connect with Auto-ISAC Staff– staff@automotiveisac.com
- ❖ Engage & ask questions!

20 *OEM Members*

❖ 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

35 *Supplier & Commercial Vehicle Members*

Membership represents 99% *of cars on the road in North America*

Coordination with 23 *critical infrastructure ISACs through the National ISAC Council*

TLP WHITE: Disclosure and distribution is not limited

AUTO ISAC – *2020 WAY FORWARD*

[redacted]

RE-EVALUATION OF STRATEGY & MISSION → ***Who We Are & Why We Are Here***

MISSION: *To strengthen the global automotive industry against cyber threats and enhance cyber attack resilience and response.* ***An attack on one is an attack on all.***

Timely Sharing of Threat & Vulnerability Information	**Building Strong Relationships**	**Developing Effective Response Plans**	**Ensuring & Maturing Consistent Cyber Capability**

Each Member is expected to: Trust, Share, Teach, Learn, Act

We are a **technical organization**, serving membership by enabling **cyber learning and capability development**. As members, we are expected to both **share and learn**, and continue to strengthen capabilities to protect our customers.

We will hold ourselves accountable.

Auto ISAC – 2020 Way Forward

Roles, Responsibilities & Metrics

Measuring Success

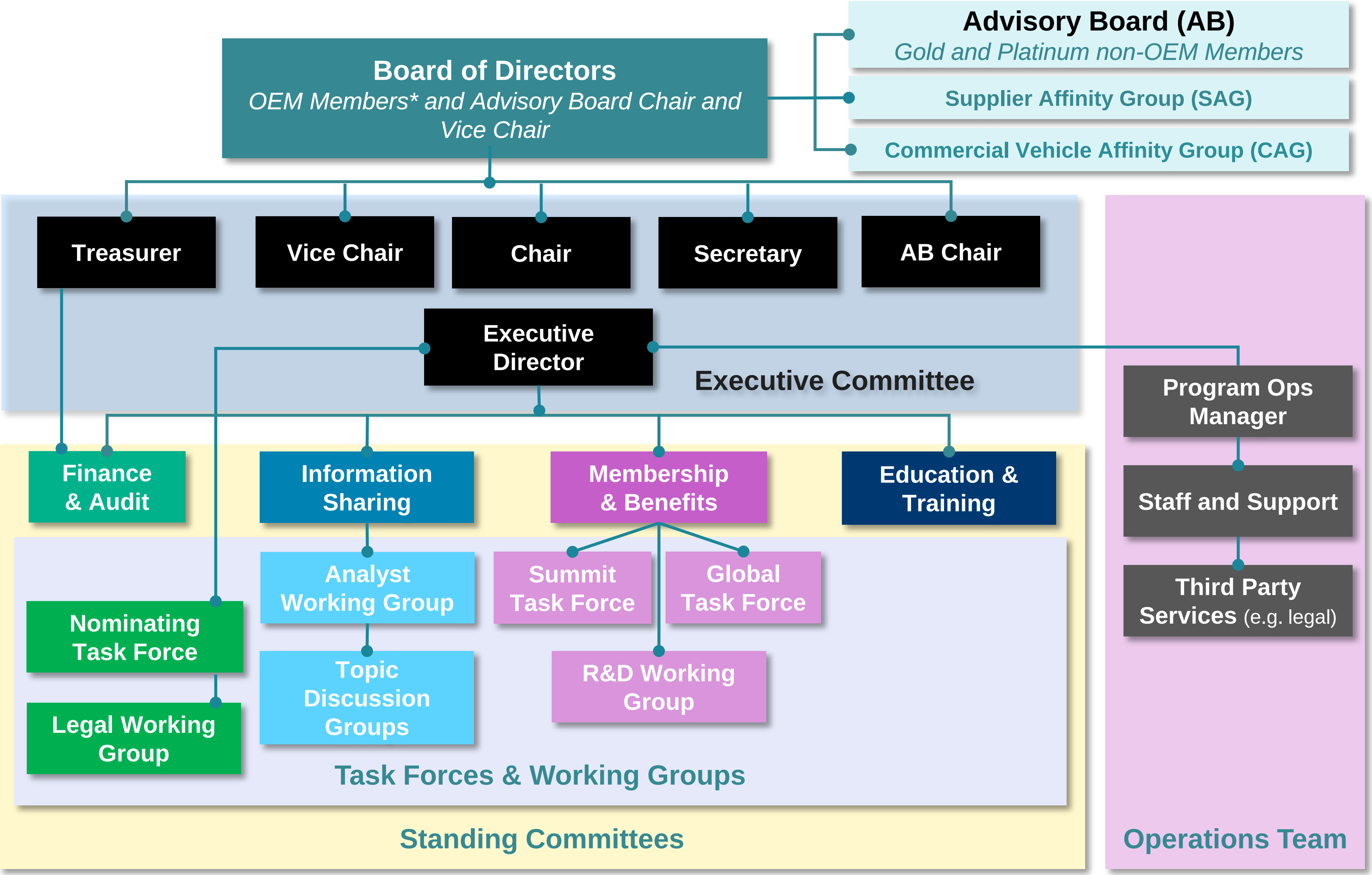
VALUE STREAMS & PERFORMANCE INDICATORS

Top Line Goal: Zero safety related cyber events in the industry

INFO SHARING & AWARENESS	EDUCATION	RELATIONSHIPS
% Participation Sharing / Platform / Attendance	% Taking Educational Offerings Maturity Surveys	% Member Satisfaction with value added relationships

Bottom Line Goal: ***Automotive Cybersecure & Resilient Across Industry!***

Auto-ISAC Operating Model



TLP WHITE: Disclosure and distribution is not limited

2020 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

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

2020 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Kevin Walker
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster
as of April 20, 2020

Highlighted = Change

Aisin	Honda	PACCAR
Allison Transmission	Hyundai	Panasonic
Aptiv	Infineon	Qualcomm
AT&T	Intel	Renesas Electronics
Blackberry Limited	Kia	Subaru
BMW Group	Knorr Bremse	Sumitomo Electric
Bosch	Lear	Tokai Rika
Continental	LGE	Toyota
Cummins	Magna	TuSimple
Denso	~~Magneti~~ MARELLI	Valeo
Delphi Technologies	Mazda	Veoneer
FCA	Mercedes-Benz	Volkswagen
Ford	Mitsubishi Motors	Volvo Cars
Garrett	Mitsubishi Electric	Volvo Group
General Motors	Mobis	Waymo
Geotab	Navistar	Yamaha Motors
Google	Nissan	ZF
Harman	NXP	
Hitachi	Oshkosk Corp	TOTAL: 55

2020 Auto-ISAC Staff

Staff Positions OPEN
Membership Engagement Lead
Organization Coordinator

Faye Francy
Executive Director
fayefrancy@
automotiveisac.com

Josh Poster
Program Operations Manager
joshposter@
automotiveisac.com

Ricky Brooks, II
Intelligence Officer
rickybrooks@automotiveisac.com

Jake Walker
Cyber Intel Analyst
jacobwalker@
automotiveisac.com

Lisa D. Scheffenacker
Business Administrator
lisascheffenacker@
automotiveisac.com

External Support Staff

Julie Kirk
Finance
juliekirk@
automotiveisac.com

Linda Rhodes
Legal Counsel,
Mayer Brown
lrhodes@mayerbrown.com

Callen Mackey
CPA,
RSM US LLP
Callen.mackey@rsmus.com

Auto-ISAC Activities

Auto-ISAC

- **Automotive industry retooling for critical COVID19 work – *Thank you!***
- **Advisory Board & Board of Directors Meeting To Be Held Virtually June 23**
- **Auto-ISAC Incident Response Plan (IRP) *Completed!***
- **Auto-ISAC TTX *going virtual***
- **CyberStorm 2020 postponed**
- **Other events cancelled or postponed: IQPC, TU-Auto, escar**
- **We are *cautiously optimistic* we'll hold Auto-ISAC Summit – registration, call for papers, and sponsorships on website – www.automotiveisac.com**

Stay safe, secure and well!

Auto-ISAC Summit – Oct 14-15

AUTO-ISAC
SUMMIT

Oct. 14-15,
2020
Detroit, MI

2 days

400 attendees

ABOUT THE AUTO-ISAC SUMMIT: The 2020 Auto-ISAC Summit hosted by General Motors connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.

WHAT'S TRENDING?

From a TCU to Corporate Domain Admin [Pentest Partners] took a telematics unit from a vehicle, pulled the SIM card from it, put it in a USB modem connected to a laptop, connected to [an] internal network and compromised the entire domain it from the outside.

Connected Cars Are Just Computers on Wheels, Warns Context A report published by leading independent consumer body Which?, reveals serious questions about the cyber security of 'connected cars' and the need for more regulations. Research was carried out on behalf of Which? by Context Information Security and identified [potential] security, data privacy and safety concerns in two of the most popular European car brands.

Israel Says Hackers Targeted SCADA Systems at Water Facilities According to an alert published by Israel's National Cyber Directorate, the attacks targeted supervisory control and data acquisition (SCADA) systems at wastewater treatment plants, pumping stations and sewage facilities. Organizations in the water and energy sectors have been advised to immediately change the passwords of internet-accessible control systems, reduce internet exposure, and ensure that all control system software is up to date.

Intelligence Gathering on Critical Infrastructure in Southeast Asia Currently, you can come across hundreds of thousands publicly accessible SCADA devices from different vendors and variety of models. So how can you find [SCADA] devices operating in one of the mentioned 16 sectors of critical infrastructure? The main point of this research is to find any device or management panel exposed directly to the Internet counted as a critical infrastructure.

Is Automotive CyberSecurity A National Defense Issue? At the industrial, infrastructure and utility level, computer-controlled physical resources are increasingly common. Since bad actors have the potential to cause real damage with these systems, great care is taken to protect these systems from external attacks. In many of the most critical situations, the Department of Homeland Security is directly involved. However, the modern automobile is the rare entity which is large enough to cause damage (especially when viewed as a fleet), yet managed like a consumer device.

CISA RESOURCE HIGHLIGHTS

Version 3.0 - Guidance on Essential Critical Infrastructure Workers During COVID-19 (TLP: WHITE)

- Released on April 17, 2020 and is intended to help state and local jurisdictions and the private sector identify and manage their essential workforce while responding to COVID-19.
- Clarifies and expands critical infrastructure workers in several categories and provides additional information as considerations for both government and business
- Guidance provided in the document is intended to support decision makers in communities and jurisdictions across the country during the COVID-19 emergency and it is non-binding
- Available at https://www[.]cisa[.]gov/publication/guidance-essential-critical-infrastructure-workforce

Current Activity - FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing

- Highlights FBI guidance resource at https://www[.]fbi[.]gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

- Includes reference to CISA Security Tip ST04-006 for patching and software update guidance at https://www[.]us-cert[.]gov/ncas/tips/ST04-006

- Includes reference to additional FBI and vendor resources with safeguards for operating in virtual environments

AA20-107A - Continued Threat Actor Exploitation Post Pulse Secure VPN Patching (TLP: WHITE)

- Update to CISA Activity Alert AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability - https://www[.]us-cert[.]gov/ncas/alerts/aa20-010a
- Alerts administrators that threat actors who successfully exploited CVE-2019-11510 and stole a victim organization’s credentials will still be able to access—and move laterally through—that organization’s network after the organization has patched this vulnerability if the organization did not change those stolen credentials.
- Includes reference to CISA Github resource for detection of IOCs associated with exploitation of CVE-2019-11510 – see https://github[.]com/cisagov/check-your-pulse
- AA20-107A available at https://www[.]us-cert[.]gov/ncas/alerts/aa20-107a

CISA Resources for Secure Video Conferencing and Teleworking (TLP: WHITE)

- Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
  - https://www[.]cisa[.]gov/publication/cybersecurity-recommendations-critical-infrastructure-using-video-conferencing
- Cybersecurity Recommendations for Federal Agencies Using Video Conferencing
  - https://www[.]cisa.gov/publication/cybersecurity-recommendations-federal-agencies-using-video-conferencing
- Guidance for Securing Video Conferencing
  - https://www[.]cisa[.]gov/publication/guidance-securing-video-conferencing

CISA Resources for Secure Video Conferencing and Teleworking (TLP: WHITE) (continued)

- Video Conferencing Tips
  - https://www[.]cisa[.]gov/publication/video-conferencing-tips
- Telework Best Practices
  - https://www[.]cisa[.]gov/publication/telework-best-practices
- For a complete listing of the CISA Publications Library resources, visit https://www[.]cisa[.]gov/publications-library

Activity Alert AA20-099A - COVID-19 Exploited by Malicious Cyber Actors (TLP: WHITE)

- Joint alert from DHS CISA and the UK NCSC available at https://www[.]us-cert[.]gov/ncas/alerts/aa20-099a
- Highlight's CISA's and NCSC's observance of growing use of COVID-19-related themes by malicious cyber actors.
- Provides summaries of the types of attacks observed, to include phishing, malware distribution, COVID-19-related domain registration, and attacks against remote access and teleworking infrastructure
- Includes a non-exhaustive list of COVID-19-related IOCs in STIX- and CSV-format

Activity Alert AA20-126A - APT Groups Target Healthcare and Essential Services (TLP: WHITE)

- Joint alert from DHS CISA and the UK NCSC available at https://www[.]us-cert[.]gov/ncas/alerts/AA20126A
- Highlight’s ongoing APT activity against organizations involved in national and international COVID-19 responses. Includes healthcare bodies, pharmaceutical companies, academia, medical research organizations, and local governments.
- Highlights CISA and NCSC active efforts to investigate large-scale password spraying campaigns conducted by APT groups
- Includes links to CISA and NCSC password spraying attack mitigation resources.
- Also see https://www[.]cisa[.]gov/publication/joint-cisa-and-uk-tip-covid-19-cyber-threat-exploitation

DHS and FEMA COVID-19 Resources

- https://www[.]dhs[.]gov/coronavirus
- https://www[.]cisa[.]gov/coronavirus
- https://www[.]fema[.]gov/coronavirus
- https://www[.]fema[.]gov/news-release/2020/03/13/covid-19-emergency-declaration

For more information:

cisa.gov

Questions?

CISAServiceDesk@cisa.dhs.gov

1-888-282-0870

Community Speaker Series

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 our Auto-ISAC (staff@automotiveisac.com)**

7 *Best Practice Guides available on website*

2000+ *Community Participants*

30 *Featured Speakers to date*

Example of Previous Community Speakers

- Urban Jonson, NMFTA, Heavy Vehicle Cybersecurity Working Group (April 2018)
- Ross Froat, American Trucking Association, ATA Cyberwatch Program (Oct 2018)
- Katherine Hartman, Chief – Research, Evaluation and Program Management, ITS Joint Program Office, US DOT (August 2019)
- Joe Fabbre, Global Technology Director, Green Hills Software (October 2019)
- Oscar Marcia, CISSP, Eonti, Device Authentication in Auto-ISAC as a Foundation to Secure Communications (November 2019)
- Amy Smith, the Manager of Pre-College Educational Programming at SAE International (January 2020)

Community Call Slides are located at: www.automotiveisac.com/communitycalls/

Welcome to Today's Speaker

Dr. Allan Friedman, Director Cybersecurity Initiatives

National Telecommunications and Information Administration (NTIA)

Department of Commerce

Dr. Allan Friedman is Director of Cybersecurity Initiatives at NTIA. He coordinates NTIA's multi-stakeholder processes on cybersecurity, focusing on addressing software vulnerabilities and resiliency across the software world.

Prior to joining the Federal Government, Friedman spent over 10 years as a noted cybersecurity and technology policy researcher at Harvard's Computer Science Department, the Brookings Institution, and George Washington University's Engineering School.

He is the coauthor of the popular text ***"Cybersecurity and Cyberwar: What Everyone Needs to Know"*** and has a degree in computer science from Swarthmore College and a Ph.D. in public policy from Harvard University.

SBOM – *Progress in Software Supply Chain Security*

The software we depend on has emerged as a primary risk in the supply chain, whether from active attempts to compromise key components, or ordinary vulnerabilities buried deep in our systems. Addressing software supply chain risk will require more transparency across the ecosystem, through the adoption of a "software bill of materials" (SBOM).

This presentation will offer a brief overview of the concept of an SBOM, and the progress being made by an open, cross-sector, and international initiative convened by NTIA in the US Department of Commerce. We will review lessons learned, remaining challenges, and expected progress. We will also touch on the path to adoption, including market forces and the ongoing role of regulators.

Dr. Allan Friedman Slides

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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 company, 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 or Partnership, please contact Auto-ISAC Staff (staff@automotiveisac.com).

Strategic Partnership Programs

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, SANS, IOActive, GRIMM

INNOVATOR

Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Alliance, ACEA, ATA, JAMA, CLEPA

NAVIGATOR

Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: DHS, NHTSA, Colorado State, Johns Hopkins, NCI

COLLABORATOR

Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges-coordination activities

Community

Companies interested in engaging the automotive ecosystem and supporting the community.

Examples: Summit sponsorship – key events

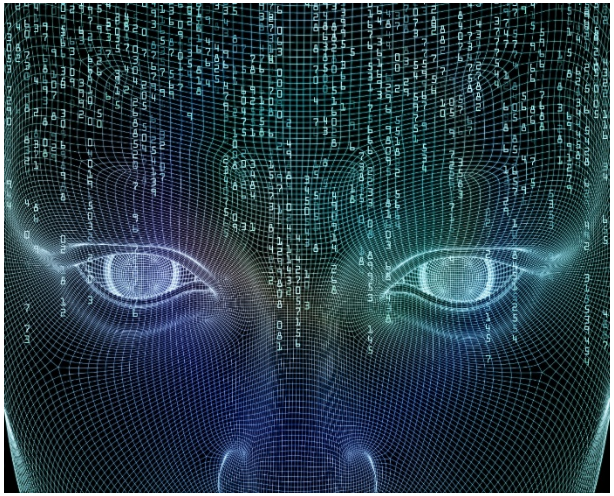
BENEFACTOR

Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

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!

рахмат
danke
謝謝
ngiyabonga
شكراً جزيلاً
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
thank you
gracias
хвала
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gràçie
hvala
köszönöm
enkosi
dankon
aciū
akun
djiere dieuf
tau
mochchakkeram
murakoze
dziękuję
дякую
mamnun
chokrane
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dēkuji
obrigado
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
rahmet
kam sah hamnida
rahmat
terima kasih
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercé
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

Our contact info

Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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

Josh Poster
Program Operations Manager

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street NW, Suite 700
Washington, DC 20001
joshposter@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

automotiveisac.com
@auto-ISAC