



WELCOME TO AUTO-ISAC!





MONTHLY VIRTUAL COMMUNITY CALL

December 1, 2021

TLP:WHITE



DHS TRAFFIC LIGHT PROTOCOL (TLP) 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 by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</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</p>  <p>Limited disclosure, restricted to participants organizations.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>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.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

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

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➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ Michael Daniel, <i>President and CEO, Cyber Threat Alliance</i>
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!

22
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

43 *Supplier & Commercial Vehicle Members*

15
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)*



2020 - 2021 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)

2022-2023 Leadership
Coming Soon



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



Todd Lawless
*Chair of the
Advisory Board*
Continental



Michael Feiri
*Vice Chair of the
Advisory Board*
ZF



Chris Lupini
Chair of the SAG
Aptiv



Larry Hilkene
Chair of the CAG
Cummins

2020 - 2021 ADVISORY BOARD (AB) LEADERSHIP

MEMBER ROSTER

AS OF DECEMBER 1, 2021

63 Members

Aisin	Hyundai	NXP
Allison Transmission	Infineon	Oshkosh Corp
Aptiv	Intel	PACCAR
Argo AI, LLC	John Deere Electronic	Panasonic
AT&T	Kia	Polaris
Blackberry Limited	Knorr Bremse	Qualcomm
BMW Group	Lear	Renesas Electronics
BorgWarner	LGE	Stellantis
Bosch (Ecrypt-Affiliate)	Luminar	Subaru
Continental (Argus-Affiliate)	Magna	Sumitomo Electric
Cummins	MARELLI	Tokai Rika
Denso	Mazda	Toyota
Faurecia	Mercedes-Benz	TuSimple
Ford	Meritor	Valeo
Garrett	Mitsubishi Motors	Veoneer
General Motors (Cruise-Affiliate)	Mitsubishi Electric	Volkswagen
Geotab	Mobis	Volvo Cars
Google	Motional	Volvo Group
Harman	Navistar	Waymo
Hitachi	Nexteer Automotive Corp	Yamaha Motors
Honda	Nissan	ZF

BUSINESS ADMINISTRATION

➤ Upcoming Key Events:

- **Members Teaching Members – December 15** **Speaker:** Jenny Gilger, Honda **Title:** Corporate Impact and Lessons Learned from a Global Ransomware Attack **TLP:AMBER**
- **Integrated Preparedness Program TTX #2 For Executives – Dec 16**

➤ Community Call:

- **Wednesday, January 5th -** **Speaker:** Paul Eisler, US Telecom **Title:** “IoT Standards, Policy Harmonization & Multi-Stakeholder Cyber Crisis Response” **Time:** 11 – 12:00 p.m. **TLP:WHITE**

➤ Announcements:

- **Call for CC Speakers** – Might you want to speak? Please send your ideas to **Sharmila Khadka**. We are working to build a list of speakers in advance of presentations for MBSC approval.

➤ Upcoming Surveys:

- **Community Call Year-End Survey** to be sent Dec 1st/due Dec. 15th
- **Member Access Portal (MAP) Year-End User Experience Survey** to be sent Dec 13th



AUTO-ISAC INTELLIGENCE

TLP:WHITE



AUTO-ISAC INTELLIGENCE

- Know what we track daily by subscribing to the DRIVEN
 - Send feedback, contributions or questions to analyst@automotiveisac.com
- The Auto-ISAC 2021 Threat Assessment is nearly complete. Expect it in Q1 2022.
- Intelligence Notes
 - Tesla used its over-the-air (OTA) update capability to fix an issue that **caused some Tesla vehicles to stop themselves without warning**. Tesla started receiving complaints about the issue within hours of a previous OTA update that was sent to the vehicles ([Bloomberg](#)).
 - There is no indication that the issue was caused by a malicious actor. However, the vehicle impacts that occurred highlight what is at stake in terms of vehicle and public safety. Auto-ISAC Members collaborate to prevent threat actors from causing such impacts.
 - The two main vectors for compromising Operational Technology are **through the network** or through **removable media and devices** ([DarkReading](#)). Study the vulnerabilities in Data Distribution Service (DDS) implementations ([ZDNet](#), [CISA](#)).
 - Although there were no reports of a major cyberattack being launched during the week of the US Thanksgiving holiday, IT, OT, and product cybersecurity personnel should keep their guard up and maintain heightened vigilance for signs of malicious activity, including **outside normal business hours** ([CISA-FBI](#), [CISA-FBI](#)).

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – CISA Current Activity (CA) - CISA BOD 22-01 and Catalog of Known Exploited Vulnerabilities

- **Binding Operational Directive (BOD) 22-01 “Reducing the Significant Risk of Known Exploited Vulnerabilities”** establishes specific timeframes for Federal civilian agencies to remediate vulnerabilities that are being actively exploited by known adversaries
- The catalog of Known Exploited Vulnerabilities (KEVs) was created by CISA to support the Directive, and will be updated regularly
- Organizations can sign up for alerts when updates to the catalog are made
- **See:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/11/03/cisa-issues-bod-22-01-reducing-significant-risk-known-exploited](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/11/03/cisa-issues-bod-22-01-reducing-significant-risk-known-exploited)
 - [https://www\[.\]cisa\[.\]gov/known-exploited-vulnerabilities](https://www[.]cisa[.]gov/known-exploited-vulnerabilities)



TLP: WHITE – CISA Capacity Enhancement Guides (CEGs) to Enhance Mobile Device Cybersecurity

- **Two (2) actionable CEGs to help users and organizations improve mobile device cybersecurity:**
 - CEG checklist for consumers which covers using strong authentication and enabling automatic operating system updates
 - CEG checklist for organizations that provides steps to help them secure mobile access to enterprise resources
- **Available at:**
 - **Consumers:**
[https://www\[.\]cisa\[.\]gov/sites/default/files/publications/CEG_Mobile%20Device%20Cybersecurity%20Checklist%20for%20Consumers.pdf](https://www[.]cisa[.]gov/sites/default/files/publications/CEG_Mobile%20Device%20Cybersecurity%20Checklist%20for%20Consumers.pdf)
 - **Organizations:**
[https://www\[.\]cisa\[.\]gov/sites/default/files/publications/CEG_Mobile%20Device%20Cybersecurity%20Checklist%20for%20Organizations.pdf](https://www[.]cisa[.]gov/sites/default/files/publications/CEG_Mobile%20Device%20Cybersecurity%20Checklist%20for%20Organizations.pdf)



TLP: WHITE – CISA Current Activity (CA) - Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends

- CISA and the FBI strongly urge all entities—especially critical infrastructure partners—to examine their current cybersecurity posture and implement best practices and mitigations to manage the risk posed by cyber threats
- Best practices and mitigations are included in Activity Alert AA21-243
- List of actions recommended by CISA and the FBI for users and organizations to protect themselves are included in the CA
- See:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-243a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-243a)



TLP: WHITE – CISA Current Activity (CA) – Joint Cybersecurity Advisory Update - APT Exploitation of ManageEngine ADSelfService Plus Vulnerability

- Update to the FBI, CISA and CGCYBER Joint Cybersecurity Advisory AA21-259A on November 19, 2021.
- Update includes a list of tools Advanced Persistent Threat (APT) actors are known to be using to enable the campaign (list also included in the CA)
- URLs to relevant vendor blogposts included in the CA and update
- See:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/11/19/updated-apt-exploitation-manageengine-adservice-plus](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/11/19/updated-apt-exploitation-manageengine-adservice-plus)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-259a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-259a)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA NCAS – [https://us-cert\[.\]cisa\[.\]gov/](https://us-cert[.]cisa[.]gov/)
- 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/)
- CISA COVID-19 Response – [https://www\[.\]cisa\[.\]gov/coronavirus](https://www[.]cisa[.]gov/coronavirus)
- CISA Webinar Series on YouTube: [https://www\[.\]youtube\[.\]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy](https://www[.]youtube[.]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy)





For more information:
[cisa.gov](https://www.cisa.gov)

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870



AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

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

How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

30+
*Featured
Speakers to
date*

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

TLP:WHITE



MICHAEL DANIEL, CYBER THREAT ALLIANCE (CTA)

PRESIDENT & CEO



Michael Daniel serves as the President & CEO of the Cyber Threat Alliance (CTA), a not-for-profit that enables high-quality cyber threat information sharing among cybersecurity organizations.

Prior to CTA, Michael served for four years as US Cybersecurity Coordinator, leading US cybersecurity policy development, facilitating US government partnerships with the private sector and other nations, and coordinating significant incident response activities. From 1995 to 2012, Michael worked for the Office of Management and Budget, overseeing funding for the U.S. Intelligence Community. Michael also works with the Aspen Cybersecurity Group, the World Economic Forum's Partnership Against Cybercrime, and other organizations improving cybersecurity in the digital ecosystem.

In his spare time, he enjoys running and martial arts.



Combating Ransomware:
Creating a Ransomware Incident Response Network



**CYBER
THREAT**
ALLIANCE

THE Rise OF RANSOMWARE



Ransomware has evolved from an economic nuisance to a national security and public health and safety threat.

In 2020, nearly
2,400

U.S.-based governments,
healthcare facilities, and schools
were victims of ransomware



The Ransomware Task Force

- 60+ experts from industry, government, law enforcement, civil society, and international organizations
- Met from January through April 2021
- Drew on expertise from different sectors to create a comprehensive suite of recommendations

Represented Sectors Included:

- Incident Responders
- Cyber Insurance Providers
- Healthcare Entities
- Cryptocurrency Analysis Firms
- International Law Enforcement
- Financial Regulators
- Platform Providers

TASK FORCE recommendations SUMMARY

The Task Force:

- Created a four-part framework for combating ransomware
- Developed 48 recommendations across the framework that:
 - Specify both short- and medium-term actions.
 - Address primarily policy and process, rather than technology.
 - Focus on the US government, due to the Task Force's composition.
- Did not reach consensus on whether to recommend banning ransom payments.
- Report: <https://securityandtechnology.org/ransomwaretaskforce/report/>

TASK FORCE Recommendations FRAMEWORK

RTF Framework

1. *Deter Ransomware Attacks*



2. *Disrupt the ransomware business model*



3. *Help organizations prepare*



4. *Respond to ransomware attacks more effectively*



WE ARE FIGHTING PARTIALLY BLIND

Two information problems hinder efforts to combat ransomware:

- We lack reliable, representative data about ransomware's scope, scale, distribution, and frequency.
- Information about ransomware threats does not reach enough people or organizations.

The RTF made several recommendations to address these two problems. One would directly involve ISACs:

- Establish a Ransomware Incident Response Network (RIRN)

Ransomware incident response network (RIRN)

- The RIRN would serve several functions
 - Sharing anonymized incident reports across the ecosystem
 - Connecting victim organizations to ransomware incident response services
 - Aggregating incident data
 - Distributing alerts about on-going threats
- To carry out these functions, the RIRN would:
 - Use a standard reporting format
 - Adopt a system of unique identifiers to avoid double-counting while maintaining anonymity
 - Share the resulting anonymized information with other cyber intelligence organizations and national governments in the network

Creating the RIRN: Next Steps

- CTA is working with the Institute for Security and Technology, the Global Cyber Alliance, the Cybercrime Support Network, and other organizations to stand up the RIRN.
- Key steps include:
 - **Creating a charter**
 - **Establishing core business rules**
 - **Recruiting participants, focusing on key information sharing nodes**
- ISACs can play a key role in the RIRN.
 - **Bring sector knowledge and reach**
 - **Have experience in sharing information**

QUESTIONS?

Backup

RANSOMWARE TASK FORCE LEADERSHIP

RTF Co-Chairs

Megan Stifel, *Global Cyber Alliance* **John**

Davis, *Palo Alto Networks*

Michael Phillips, *Resilience*

Executive Director

Philip Reiner, *Institute for Security and
Technology*

RTF Working Group Co-Chairs

John Davis, *Palo Alto Networks*

Megan Stifel, *Global Cyber Alliance*

Michael Phillips, *Resilience*

Kemba Walden, *Microsoft*

Jen Ellis, *Rapid7*

Chris Painter, *The Global Forum on Cyber Expertise*

Michael Daniel, *Cyber Threat Alliance*

Philip Reiner, *Institute for Security and Technology*

RANSOMWARE TASK FORCE Membership

Joel de la Garza, a16z

Temi Adebambo, Amazon Web Services

David Forcsey, Aspen Digital

Jeff Troy, Aviation ISAC

Rich Friedburg, Blackbaud

Austin Berglas, BlueVoyant

Lewis Robinson, Center for Internet Security

Roger Francis, CFC Underwriting

Don Spies, Chainalysis

Pamela Clegg, CipherTrace

Brad Garnett, Cisco

Matt Olney, Cisco

Peter Lefkowitz, Citrix

Bill Siegal, Coveware

James Perry, CrowdStrike

Stéphane Duguin, The CyberPeace Institute

Yonatan Striem-Amit, Cybereason

Neil Jenkins, Cyber Threat Alliance

Andy Thompson, CyberArk

Ari Schwartz, Cybersecurity Coalition

John Banghart, Cybersecurity Coalition

Ryan Weeks, Datto

Patrice Drake, Deloitte

Keith Mularski, Ernst & Young

Stacy O'Mara, FireEye

Nick Bennett, FireEye

Jill Fraser, Jefferson County, CO

Mark Orsi, K12 SIX

RANSOMWARE TASK FORCE Membership

Kent Landfield, McAfee

Ginny Badanes, Microsoft

Kaja Ciglic, Microsoft

Ping Look, Microsoft

John Guerriero, National Governors Association

Justin Herring, New York Department of Financial Services (NYDFS)

Adrian McCabe, Palo Alto Networks

Sam Rubin, Palo Alto Networks

Sean Morgan, Palo Alto Networks

Bob Rudis, Rapid7

Scott King, Rapid7

Tod Beardsley, Rapid7

Allan Liska, Recorded Future

Katie Nickels, Red Canary

Adam Flatley, Redacted

Davis Hake, Resilience

Michael Convertino, Resilience

Chris Lynam, Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)

Jeff Bonvie, Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)

Kevin Gronberg, SecurityScorecard

Richard Perlotto, The Shadowserver Foundation

Beau Woods, Stratigos Security

James Shank, Team Cymru

Michael Garcia, Third Way

RANSOMWARE TASK FORCE Membership CONTINUED

Ciaran Martin, *University of Oxford Blavatnik School of Government*

Eleanor Fairford, *U.K. National Cyber Security Centre (NCSC)*

U.K. National Crime Agency (NCA)

Bridgette Walsh, *U.S. Cybersecurity and Infrastructure Security Agency (CISA)*

U.S. Federal Bureau of Investigation (FBI)

Jonah Hill, *U.S. Secret Service (USSS)*

Bobby Chesney, *U.T. Austin Strauss Center*

RANSOMWARE TASK FORCE Staff

Sarah Powazek, RTF Program Manager, IST

Alexander Riabov, Communications Manager, IST

Leah Walker, Future Digital Security Leader Fellow, IST

Chuck Kapelke, Writing Support

Kathryn Pledger, Pledger Designs

Emma Hollingsworth, Global Cyber Alliance

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 andreaschunn@automotiveisac.com.
For Partnership, please contact sharmilakhadka@automotiveisac.com.**

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partner

Solutions Providers

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

Examples: Hacker ONE, IOActive, Karamba, Grimm

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed
- Must be educational provide awareness

Community Partners

Associations

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

Examples: Auto Alliance, ATA, ACEA, JAMA

NAVIGATOR
Support Partnership

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

Affiliations

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

Examples: NCI, DHS, NHTSA, Colorado State

COLLABORATOR
Coordination Partnership

- “See something, say something”
- May not require a formal agreement
- Information exchanges-coordination activities
- Information Sharing / research & development

Community

Companies or individuals interested in engaging the automotive ecosystem and supporting & educating the community.

Examples: Sponsors for key events, technical experts, etc.

BENEFACTOR
Sponsorship Partnership

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

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

INNOVATOR

**Strategic Partnership
(15)**

ArmorText
Celerium
Cybellum
Ernst and Young
FEV
GRIMM
HackerOne
Karamba Security
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trillium Secure
Upstream

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**

2020 Summit Sponsors-

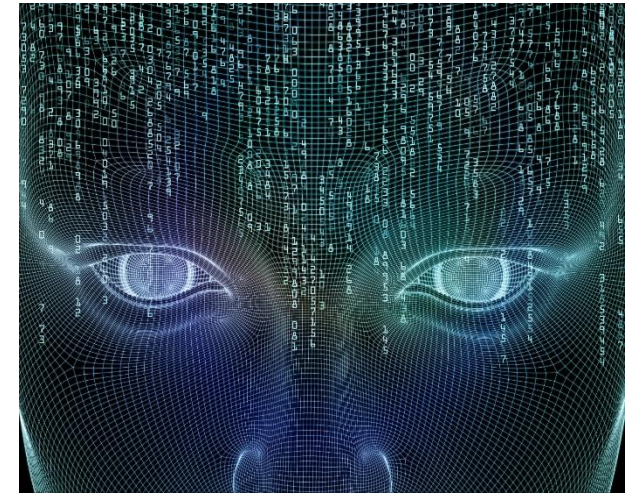
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

2019 Summit Sponsors-

Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
Valimail

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](https://twitter.com/auto-ISAC)