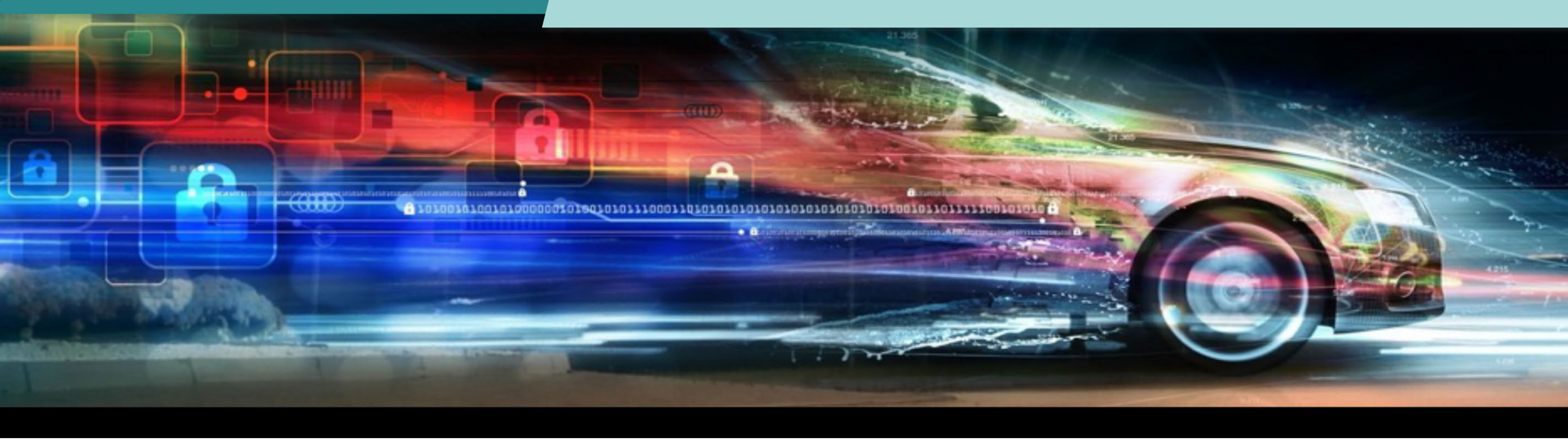


Welcome to Auto-ISAC!

Monthly Virtual Community Call

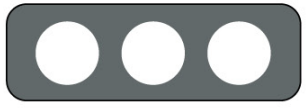
December 7th, 2022

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*** ➢ **Pranav Julakanti- Consultant, Industry Partnerships, Joint Cyber Defense Collaborative (JCDC)**
11:20	**Featured Speaker:** ➢ **Dan Strachan - Senior Engagement Lead, Joint Cyber Defense Collaborative (JCDC)** ➢ **Title: *"CISCP to JCDC Transition"***
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!"*

AUTO-ISAC
Automotive Information Sharing and Analysis Center

❖ 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

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) / Senior Leadership

Josh Davis
Chair *of the*
Board of the Directors
Toyota

Kevin Tierney
Vice Chair *of the*
Board of the Directors
GM

Jenny Gilger
Secretary *of the*
Board of the Directors
Honda

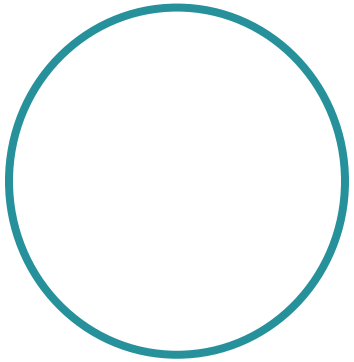
Tim Geiger
Treasurer *of the*
Board of the Directors
Ford

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*

Larry Hilkene
Chair *of the CAG*
Cummins

Member Roster
As of December 2022

Highlight = Change

76 Members, 4 in Progress

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

Pending: Micron, Rivian, JTEKT, Bose

Upcoming Events

Upcoming Meetings

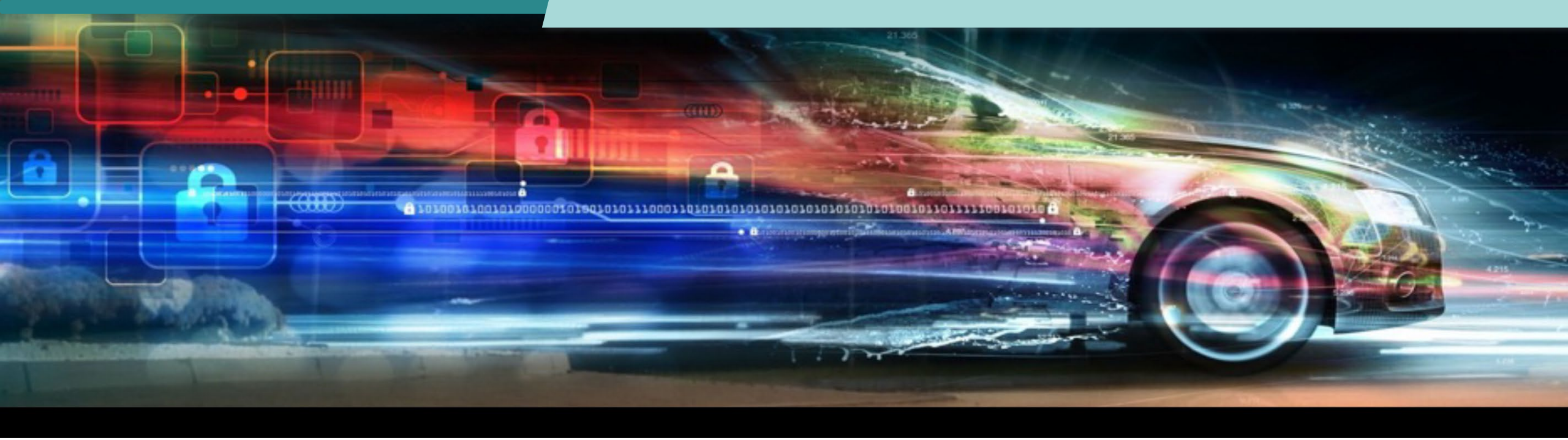
- **Community Call:**
  - **Wednesday, January 4th – Time: *11 – 12:00 p.m.* TLP:GREEN**
  - **Speakers: Tamara Shoemaker, Auto-ISAC**
  - **Title: "*Auto-ISAC Automotive Cybersecurity Training (ACT) Program*"**

- **Members Teaching Members:**
  - **Wednesday, January 18th – Speaker: Nir Hasson, Karamba Title: "*TBA*" (Members Only)**
  - **Wednesday, February 15th – Time: 10 – 11:30 a.m. TLP:AMBER (Members Only) Rescheduled from November Speaker: Michael Schneider, ETAS GmbH, Senior Security Consultant**
  - **Title: *"Securing Modern Vehicles with AUTOSAR"***

Announcements:

- **ACT Program Advanced Courses –** Beta Completed. Working to plan for sustainment and certification. Contact **Tamara Shoemaker** for more detail. **(Members Only)**

- **Best Practice Guide Updates** – ETSC is kicking off a "Light Touch" Best Practice Guide update to bring the existing guides up to current references and standards.



Auto-ISAC Intelligence Highlight

TLP:WHITE

AUTO-ISAC
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**
  - **Continue to monitor geopolitical tensions involving Russia, China, North Korea, and Iran as all have significant cyberattack capabilities which could manifest without warning and impact business and industrial operations if tensions get out of control (Russia-Ukraine, China, North Korea, Iran).**
  - **Reminder: The holidays attract even more malicious cyber activity than normal as threat actors assume security teams will be minimally staffed and off guard (Cybereason).**
  - **Ransomware Groups Targeting Automotive: LockBit 3.0 [1]; Karakurt, Project Relic [2], Cl0p, Black Basta, Lorenz, Vice Society, Daixin, LV, AlphV/BlackCat, Hive.**
  - **Multiple incidents of threat actors selling access to automotive organizations' networks and specific email accounts, and selling stolen sensitive information.**
  - **Notable TTPs and Tools: SiriusXM and Mobile App Research (The Hacker News); Use of Steganography to Evade Defenses (Unit 42); Malicious Apps in Trusted App Stores (BleepingComputer); Malicious Proxy Services Providers (DomainTools); DuckLogs Malware (BleepingComputer); CryWiper (Kaspersky); Invisible nmp Malware (JFrog).**

CISA Resource Highlights

Joint Cyber Defense Collaborative

JOINT CYBER DEFENSE COLLABORATIVE

Pranav Julakanti
12/12/2022

CISA, ODNI, NSA Release Guidance for Customers on Securing the Software Supply Chain

- CISA published the third of a three-part series on securing the software supply chain: Securing Software Supply Chain Series - Recommended Practices Guide for Customers. This publication follows the August 2022 release of guidance for developers and October 2022 release of guidance for suppliers.

- The Securing Software Supply Chain Series is an output of the Enduring Security Framework (ESF), a public-private cross-sector working group led by NSA and CISA. This series complements other U.S. government efforts underway to help the software ecosystem secure the supply chain, such as the software bill of materials (SBOM) community.

- The announcement can be found here: CISA, NSA, and ODNI Release Guidance for Customers on Securing the Software Supply Chain | CISA

Stop Ransomware: Cuba

Cuba Ransomware

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint CSA to disseminate known Cuba ransomware IOCs and TTPs associated with Cuba ransomware actors identified through FBI investigations, third-party reporting, and open-source reporting. Since the release of the December 2021 FBI Flash, the number of U.S. entities compromised by Cuba ransomware has doubled, with ransoms demanded and paid on the increase. This year, Cuba ransomware actors have added to their TTPs, and third-party and open-source reports have identified a possible link between Cuba ransomware actors, RomCom Remote Access Trojan (RAT) actors, and Industrial Spy ransomware actors.

#StopRansomware: Cuba Ransomware | CISA

CISA Releases Stakeholder-Specific Vulnerability Categorization Methodology to Prioritize Vulnerabilities

- The SVCC is a vulnerability management methodology that assesses vulnerabilities and prioritizes remediation efforts based on exploitation status, impacts to safety, automatability, and prevalence of the affected product in a singular system.
- The aim is to increase vulnerability management capabilities and reduce the window threat actors have to exploit networks.
- Organizations whose mission spaces need to evaluate the effect of vulnerabilities in at least one external organization may find the CISA SSVC decision tree model helpful.
- CISA Releases SSVC Methodology to Prioritize Vulnerabilities | CISA

Iranian State Sponsored APT Activity

- From Mid June- Mid July CISA conducted an incident response engagement at a Federal Civilian Executive Branch (FCEB) where APT activity was observed. In the course of incident response activities, CISA determined that cyber threat actors exploited the Log4Shell vulnerability in an unpatched VMware Horizon server, deployed crypto mining software, compromised credentials, and implanted reverse proxies to maintain persistence.
- CISA and FBI encourage all organizations with affected VMware systems that did not immediately apply available patches or workarounds to assume compromise and initiate threat hunting activities.
- Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester | CISA

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 10 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of November. 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:

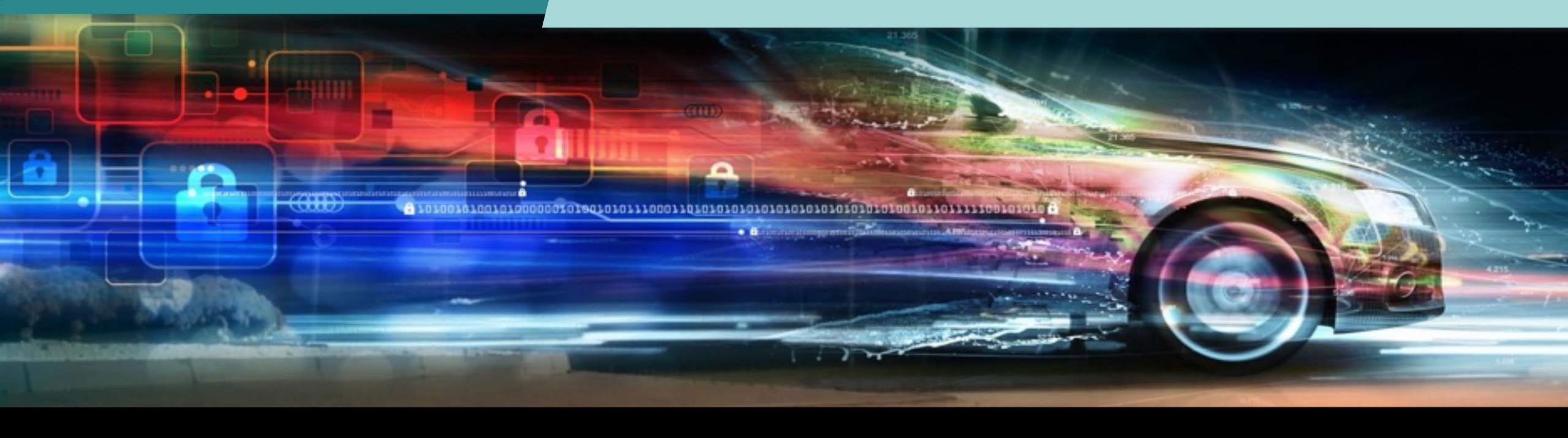
cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Pranav Julakanti
12/12/2022



Featured Speaker

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

About the Speaker

Dan Strachan
Senior Industry Engagement Lead

Current Positions

- Senior Industry Engagement Lead- CISA JCDC
- Maryland Sector Chief (Energy) -InfraGard

Past Positions

- Director, Industrial Relations & Programs- American Fuel and Petrochemical Manufacturers (AFPM)
- Program Manager – National Electrical Manufacturers Association (NEMA)

Education

- Bachelor's of Arts, Political Science, UCF
- MBA, Marketing, The Johns Hopkins University

Drive

- 2017 Lexus GX 460

CISCP 〉〉〉JCDC INTEGRATION

CYBER INFORMATION SHARING AND COLLABORATION PROGRAM

JOINT CYBER DEFENSE COLLABORATIVE

JOINT CYBER DEFENSE COLLABORATIVE

What is the JCDC?

The JCDC is a platform to unify public and private entities across the global cyber community in the collective defense of cyberspace. JCDC members gather, analyze, and share actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response.

How is JCDC different from other public-private partnerships?

JCDC offers a more intimate and collaborative technical exchange among public and private stakeholders in critical infrastructure sectors and maintains a focus on actionable engagement and planning to mitigate risk in advance of cyber incidents.

JOINT CYBER DEFENSE COLLABORATIVE

CISA Private Industry Partnerships: CISCP & JCDC

CISCP & JCDC's public and private sector partnerships drive collective action across the cybersecurity community.

Together, we have:

- Strong strategic and operational alliances within the cybersecurity community
- Increased visibility and insight into the cyber threat landscape
- Diverse resources and expertise to fuel creative cybersecurity solutions
- Vastly amplified capacity to gather, analyze, and share information to defend against cyber threats

JOINT CYBER DEFENSE COLLABORATIVE

Why integrate CISCP into JCDC?

Representing such similar objectives and capabilities,
the JCDC seeks to transition CISCP Partners into JCDC Members.

- Eliminate confusion around the difference between CISCP and JCDC Membership
- Align all collaborative efforts under the JCDC brand
- Streamline member outreach, cyber defense planning, and information sharing.

JOINT CYBER DEFENSE COLLABORATIVE

What will change for CISCP Members?

- Rebranding of CISCP facing titles, assets and collaborations
- Intimate analysis and threat exchange
- Outlined information sharing expectations

- Sector-Specific communications
- Public-Partner media releases

**Detailed instructions regarding process changes will be communicated to Members directly*

JOINT CYBER DEFENSE COLLABORATIVE

Transition Timeline

September 2022

Announcement to current CISCP Partners will communicate JCDC's intention to integrate. Establish the timelines and expectations regarding the current membership structure and logistics.

October 2022

JCDC outreach will begin to socialize CISCP members into current JCDC Membership, informing partners of the detailed change in processes and collaboration vehicles.

January 2023

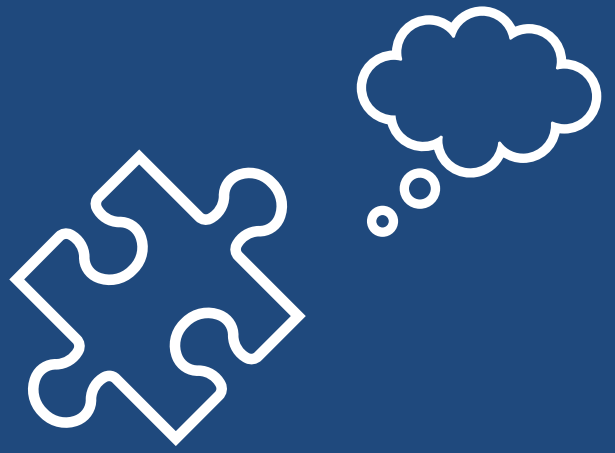
Official sunset of the Cyber Information Sharing and Collaboration Program. A public announcement of official program sunset will be made, as well as a communication to all JCDC members notifying a conclusion of the CISCP brand.

JOINT CYBER DEFENSE COLLABORATIVE

Frequently Asked Questions

Q. How will this change affect my organization's day-to-day participation/operations?
A. Full CISCP capabilities will remain. Additional JCDC venues and initiatives will be added.

Q. Will I have to sign a new agreement?
A. No.



Q. Will I still have access to CISCP resources?
A. Yes.

Q. Are QTTE and ATTE going away?
A. No.

JOINT CYBER DEFENSE COLLABORATIVE

Resources and Communication Channels

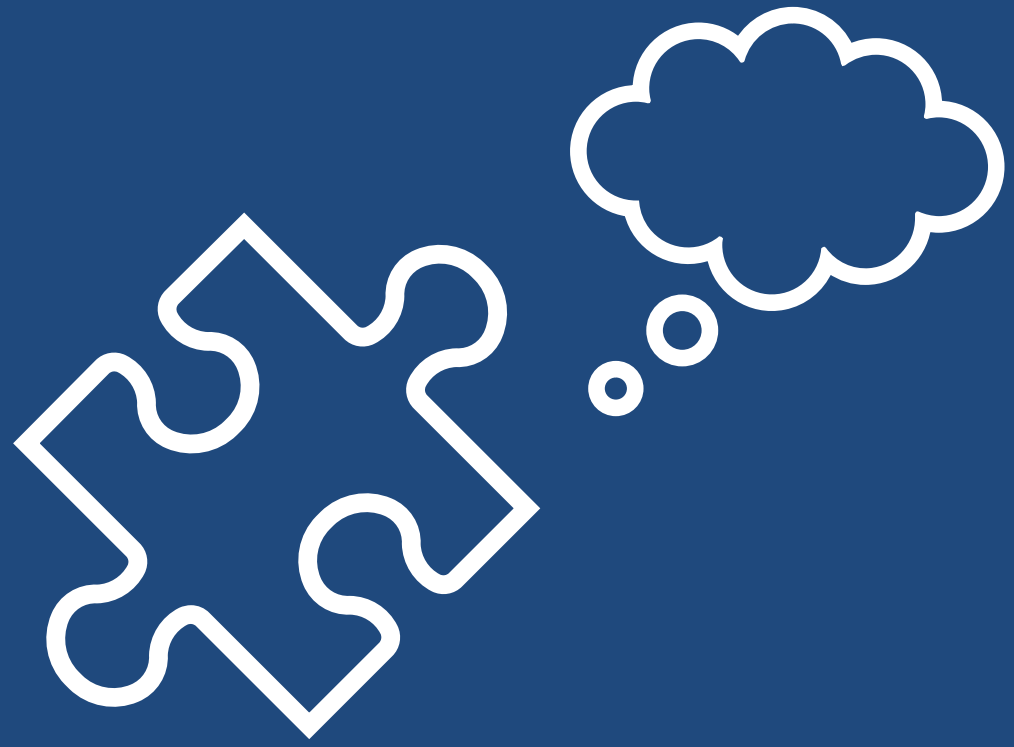
- JCDC Website: Joint Cyber Defense Collaborative | CISA
- CISCP Transition Fact Sheet: [PLACEHOLDER]
- JCDC FAQ: JCDC FAQs | CISA
- Success Stories: JCDC Success Stories | CISA
- News & Resources: JCDC News and Resources | CISA

Direct Administrative Communications:

- CISA.JCDC@cisa.dhs.gov [PLACEHOLDER]
- CISCP_Coordination@hq.dhs.gov [PLACEHOLDER]

JOINT CYBER DEFENSE COLLABORATIVE

Additional Questions?



CISCP 〉〉〉 JCDC INTEGRATION

CYBER INFORMATION SHARING AND COLLABORATION PROGRAM

JOINT CYBER DEFENSE COLLABORATIVE

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-

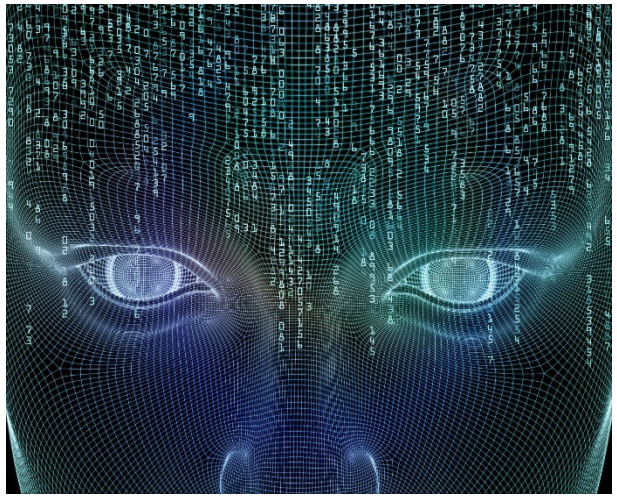
Argus
BGNetworks
Bosch
Blackberry
Block Harbor
BlueVoyant
Booz Allen Hamilton
C2A
Cybellum
CyberGRX
Cyware
Deloitte
Denso
Finite State
Fortress
Itemis
Keysight Technologies
Micron
NXP
Okta
Sandia
Securonix
Tanium
UL
Upstream
VicOne

AUTO-ISAC
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
OBRIGADO
MOCHCHAKKERAM
SPASIBO
WELALIN
SPASIBO
MAAKE
OBRIGADO
SPASIBO
DANK JE
RAIBH MAITH AGAT
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