



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

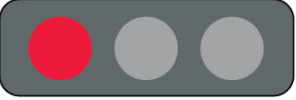



October 5th, 2022

This Session will be recorded.

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➤ Intelligence Highlights
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Kristie Pfosi, Executive Director of Product Security, Aptiv- ETSC Chair➤ Christine Pelione, Cybersecurity Strategic Risk Manager, GM- ETSC Vice Chair➤ Tamara Shoemaker, ACT Program Manager, Auto-ISAC- ETSC Staff Lead➤ Title: "Auto-ISAC Education and Training Standing Committee (ETSC) 2022 Cybersecurity Awareness Project"
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!

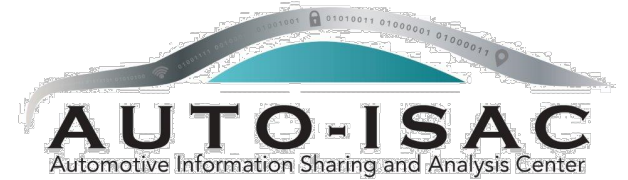
(sharmilakhadka@automotiveisac.com)



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

48 *Supplier & Commercial Vehicle Members*

19
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



Allen Houck
Chair of the SAG
NXP



Larry Hilkene
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF OCTOBER 2022

Highlight = Change

70 Members, 7 in Progress

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

Seven Pending: Thyssenkrupp; AAM, Ferrari, ChargePoint; Nuspire, KTM, Micron

UPCOMING EVENTS

Upcoming Meetings

- **Community Call:**
 - Wednesday, November 2nd – **Speaker:** TBA **Title:** “TBA” **Time:** 11 – 12:00 p.m. **TLP:WHITE**
- **European Workshop:**
 - Tuesday, October 11th, Working with Partners (Open to partners)
 - Wednesday, October 12th, Automotive Scoring of Vulnerabilities and Vulnerability Monitoring **(Members Only)**
- **Members Teaching Members:**
 - Wednesday, October 19th – **Speaker:** Christine Pelione, Cybersecurity Strategic Risk Manager, GM **Title:** Awareness: It’s More Than an Annual Check-Up **Time:** 10 – 11:30 a.m. **TLP:AMBER (Members Only)**

Announcements:

- **ACT Program Advanced Courses** – Beta Advanced registration is open. Beta Advanced classes started September 19th. Contact [Tamara Shoemaker](#). **(Members Only)**
- **Uptane Virtual Industry Conference: Securing Software Updates and Supply Chains on Connected Vehicles.** Thursday, October 13, and target a global audience (13-17 CEST, 7-11 EST, 20-24 JST). If you want to learn more about the security pitfalls of SOTA and how to transition your existing system to Uptane, please join this escar pre-event for free: <https://lnkd.in/eVniWsS8>



AUTO-ISAC INTELLIGENCE HIGHLIGHT

TLP:WHITE



AUTO-ISAC INTELLIGENCE HIGHLIGHT

- 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**
 - September 15, Uber suffered a cyberattack to its internal systems but did not affect operations. The attacker allegedly used a combination of social engineering and MFA fatigue attacks to access the company's VPN. Most notably, the cybercriminal downloaded the HackerOne vulnerability reports. ([Bleeping Computer](#)).
 - September, industrial cybersecurity firm Otorio reported that hacktivist group, GhostSec, repeatedly compromised poorly secured industrial devices ([Security Week](#)).
 - September 28, security researcher BushidoToken reported popular red-teaming tool Brute Ratel C4 (BRC4) was cracked and shared on cybercrime forums ([Bushido Token](#)).
 - **Notable Tactics, Techniques, Procedures and Tools:**
 - Domain Shadowing ([Unit 42](#)).
 - Customized Facebook forms for credential harvesting ([Avanan](#)).
 - LinkedIn Smart Links used in phishing campaign ([Cofense](#)).
 - Chaos malware botnet of devices ([Recorded Future](#)).

CISA RESOURCE HIGHLIGHTS



Stop Ransomware: Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting

Regardless of industry, service providers need to monitor threats.

On September 14th CISA released a joint cybersecurity advisory with several other government agencies which provides information on Iranian government-sponsored APT actors exploiting known Fortinet and Microsoft Exchange vulnerabilities to gain initial access to a broad range of targeted entities in furtherance of malicious activities, including ransom operations. The authoring agencies in the advisory now judge these actors are an APT group affiliated with the IIRGC.

1010
1010



Threat Actors Exploiting Multiple CVEs Against Microsoft Exchange

On September 30th Microsoft confirmed that threat actors are exploiting two unpatched zero-day vulnerabilities in Microsoft Exchange servers. The first one, identified as CVE-2022-41040, is a Server-Side Request Forgery (SSRF) vulnerability, and the second one, identified as CVE-2022-41082, allows Remote Code Execution (RCE) when PowerShell is accessible to the attacker.

Currently, Microsoft is aware of limited targeted attacks using these two vulnerabilities. Attackers need access to user credentials in order to exploit this vulnerability.



For customers who have the Exchange Emergency Mitigation Service (EEMS) enabled, Microsoft released the URL Rewrite mitigation for Exchange Server 2016 and 2019



Microsoft created the following script for the URL Rewrite mitigation steps.

<https://aka.ms/EOMTv2>



Another current Exchange Server mitigation is to add a blocking rule in “IIS Manager -> Default Web Site -> URL Rewrite -> Actions” to block the known attack patterns.

[Microsoft Releases Guidance on Zero-Day Vulnerabilities in Microsoft Exchange Server | CISA](#)



CNMF Discloses Malware in Ukraine

The current geopolitical conflict has affected organizations all over the world, regardless of industry. Some of the greatest exploitations have resulted in financial, human resource, and other losses.



CNMF has issued warnings.

U.S. Cyber Command's Cyber National Mission Force (CNMF), in close coordination with the Security Service of Ukraine, has released a list of indicators of compromise (IOCs) of malware seen in Ukraine. According to CNMF, "Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cyber security, just as we are sharing with them."



We want to help you fight this vulnerability.

CISA encourages users and administrators to review U.S. Cyber Command's press release, Cyber National Mission Force discloses IOCs from Ukrainian networks, as well as their VirusTotal and GitHub pages for more information. See Mandiant's report, Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities, for additional information.



Read more here: [CNMF Discloses Malware in Ukraine | CISA](#)

Pranav Julakanti
October 5, 2022

KEVs Catalog

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



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 Shields Up - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
- ❑ Free Cybersecurity Services and Tools - [https://www\[.\]cisa\[.\]gov/free-cybersecurity-services-and-tools](https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools)
- ❑ 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/)





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

Questions?
Central@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



MEET THE SPEAKER



Christine Pelione
General Motors

Current Positions

- Vice Chair of Auto-ISAC Education & Training Standing Committee
- General Motors, Cybersecurity Strategic Risk Manager

Past Cyber Positions

- Integration Leader, GM Cybersecurity
- Business Manager, GM Product Cybersecurity

Education

- BA, Business Administration – Baker College
- Advanced Computer Science Certificate – Stanford University
- MSIT, Information Security & Assurance – Carnegie Mellon (*expected graduation 2024*)



MEET THE SPEAKER



Kristie Pfosi
Aptiv



Current Positions

- Aptiv Executive Director of Product Cybersecurity
- Auto-ISAC Education & Training Standing Committee Chair

Past Positions

- Auto-ISAC Chair Positions
 - Education & Training Standing Committee Chair 2021+
 - Best Practice Standing Committee Chair 2019- 2020
 - Summit Chair 2018
 - Best Practice Task Force Lead 2018
- Sr Manager Automotive Cybersecurity, Mitsubishi Electric Automotive
- Program Manager Cybersecurity, FCA
- Sr Program Manager, MAHLE Powertrain
- Technical Intelligence Officer, CIA
- Engineer, Magna Intier Seating

Education

- Kettering University
 - BS Electrical Engineering
 - BS Mechanical Engineering



Powertrain



MEET THE PANELISTS



Tamara Shoemaker
Auto-ISAC

Current Positions

- Auto-ISAC Cybersecurity Training Lead
- Auto-ISAC Education and Training Standing Committee Staff Lead
- ACT Program Manager

Past Positions

- Director, University of Detroit Mercy's Center for Cybersecurity & Intelligence Studies
 - Designating a Center of Academic Excellence in Cyber Defense with Dept of Homeland Security and the National Security Agency since 2004
- Founder of the Michigan CyberPatriot Program 2015-current
- Program Coordinator, Michigan Member Alliance InfraGard
- Co-Founder of the MCISSE Coalition of Michigan CAEs
- Licensed Private Investigator for 12 years

Education

- BS, Criminal Justice/Legal Administration, University of Detroit Mercy

AGENDA FOR PRESENTATION







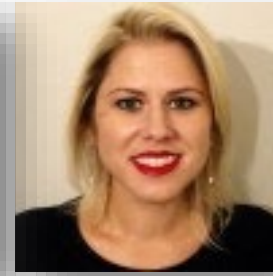

TOPICS TO BE COVERED

AGENDA

- Introductions & **Contributing Members**
- Itching our Curiosity
- **What Made the Difference**
- Plan Development
- Video Series Storyboard
- Awareness Release **Timing**
- **YOUR Call-to-Action**

CONTRIBUTING MEMBERS



							
Adam Brackman	Oliver Creighton	Lidia Constantin	Benjamin Hill	Ellen Lu	Kevin Leonard	Monica Mitchell	Maeve Nichols
ZF	BMW	Aptiv	Cummins	Harman	ESCRYPT	Polaris	GM

TIMELINE

May	June	July	August	September	October
Kickoff, theme decision, format decision	Storyboard & initial concepts complete OVERVIEW AVAILABLE	First drafts complete	Auto-ISAC BoD approvals on content / final drafts	Finalized content available to all Members the 1st week of September	Start of Awareness Campaign

ITCHING OUR CURIOSITY

THE WHO, WHAT, WHEN, WHERE AND WHY

What is our **THEME**??

- Cybersecurity Mindset – what can YOU do?
- See something, Say something

What is the **EXPECTATION**? Is there a **CALL TO ACTION**?

- Education themselves, learn what is available out there
- Should we have a quiz? **Internal Quiz**? ID their own gaps in thinking and knowledge

Who is our **Target Audience**

- All member companies (OEM, Suppliers, etc.)
- Do we know what our target audience wants?
- Why does cybersecurity mean something to them (shop floor)?
- Consequence to not follow?

How do we **MESSAGE**?

- **Real Life stories** MEAN A LOT (do we have real examples? Experiences? How does it impact the company / individual / customer? What happens on the production line / to the parts their working on – engineering? Jeep hack video (overused? Older...)
- **Wash DC executive order** impact. Perspective on critical infrastructure, level of awareness at all levels.

How will we **DELIVER** the Message?

- Videos? Length target?
- Budget available?
- Interactive Game, adventure?
- Google Doodle (interactive)
- Trivia Game challenge?
- Can we give out prizes?
- Can we publish to the AutoISAC website and public?
- Make the links available / direct content for downloading / process

WHAT MADE THE DIFFERENCE?

WE MET IN PERSON!

RISK/IMPACT → STORY → ACTION → RESOURCES

11/14/22

Purpose: Raise Awareness, "So what"

- dispel myths of cyber
- Importance of cyber (culture) ROI
- "unknowns"
- call to action - what's my part
- recruiting

Tag Line: Cyber: Product Life-cycle (Sustainability)

Kit | L&L | Poll | Quiz | Video | TipSheet | Poster | Game | Social Media Post

3	a							
	b							
	c							
10	a							
	b							
	c							
17	a							
	b							
	c							
24	a							
	b							
	c							

Digital Badge
 Puzzle piece each week

OCT
Overall: Threat Landscape / Emerging Threat Roadmap

3	CYBER 101	TLP WHITE
10	GPD / IT	GREEN/AMBER?
17	MFG / IT	
24	3P	

all
specific audience(s)
all

LIFE CYCLE
LIVE CYBER

Challenges

- Talent (recruit/retain)
- Communicating Risk / Appetite
- Cyber Hygiene (phishing... malware...)
- Cyber in dev-cycle

TLP

- Red
- Amber
- Green
- White

Sources

- NCSAM
- DHS/CISA
- CRI
- Industry Incidents
- BP

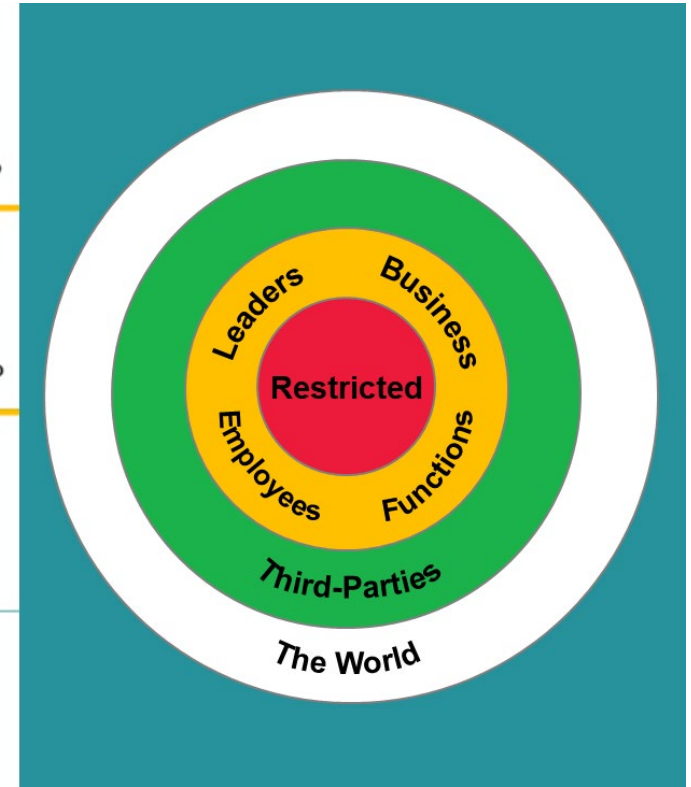
BP

- IR
- Govern
- 3P
- Risk Mgt
- ART
- Threat Act
- SPCC
- SBoM...

G Suite Business Users

OCTOBER CYBERSECURITY AWARENESS DEVELOPMENT

Together We Strive to	
Raise Awareness	Dispelling the myths of cyber
Make it Simple	Highlighting the “so what”
Promote Cyber’s Value	Driving a return on investment
Recruit Advocates	Arming with a call-to-action
Make it Accessible	Making public and shareable



Awareness Type	Channel
Video Shorts	YouTube, Red Platform
Print/Digital Content (<i>Tip Sheets, Posters, Kit etc.</i>)	Multiple
Survey (<i>poll / quiz</i>)	Web-based / online
Game	Web-based / online
Social Media Posts	LinkedIn
“Live” Event (lunch & learn)	Web-based

TLP:WHITE

OCTOBER CYBERSECURITY AWARENESS VIDEO SERIES STORYBOARD



Week	1	2	3	4
Theme	Cyber 101	Product & IT	MFG / 3P & IT	Lifecycle
Tag Line	<i>"We are all connected"</i>	<i>"Purpose Driven Security"</i>	<i>"Working together to securely Build & Deliver"</i>	<i>"Continuous Security"</i>
Mock-up Logo Build				

VIDEO SERIES DELIVERABLE TIMELINE

July	August	September	October
First Drafts Complete	Auto-ISAC BoD Approvals	Finalized Content Available	Start of Awareness Campaign

OCTOBER CYBERSECURITY AWARENESS RELEASE TIMING



Week 1

“We are all Connected”

Release Date: 10/03



AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

WE ARE ALL CONNECTED

Advanced connectivity across the variety of smart devices requires application of a **purpose-driven security** approach to ensure that our customers and their data are **safe**.

Application of key security principles such as **security-by-design** and **defense-in-depth** are vital for a robust, secure system.

Security-by-design ensures security controls and tools are built into devices from initial design phases and are incorporated in critical architecture.

- **Defense-In-Depth** ensures multi-layered security mechanisms are utilized for a holistic cybersecurity strategy.
- Incorporating **key defense principles** in security products and then ensuring successful implementation through **verification and validation** demonstrates a product with purpose-driven security is delivered to the customer.

Week 2

“Purpose Driven Security”

Release Date: 10/10



AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

PURPOSE DRIVEN SECURITY

Your vehicle contains a broad range of **sensitive information** like personal data and encryption keys, but also a significant quantity of **non-sensitive information**.

- A **security expert** can help analyze the needed security attributes based on the type of data, and a **risk assessment** can help evaluate if a security design is effective for the type of data it protects.
- **Purpose-driven security** is fundamental in the next era of automotive engineering. Ensuring that data is properly classified and properly protected is **critical to protect** the connected mobility ecosystem.

Week 3

“Build & Deliver Securely”

Release Date: 10/17



AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

BUILD & DELIVER SECURELY

TO BUILD A SECURE ENVIRONMENT IN MANUFACTURING, WE NEED TO:

- Keep our system **up-to-date**. Cyber criminals use vulnerabilities within systems, applications and devices. This is why it is important to **update or patch** them to ensure they are secure.
- Secure our **devices and accounts**, protect your devices with a lock screen, use strong **passphrases** for your online accounts and use **multi-factor authentication** for an extra layer of protection.
- **Be aware** of social engineering scams like phishing emails and malicious text messages. Watch for suspicious emails and text messages and **don't become a victim**.

Week 4

“Continuous Security”

Release Date: 10/24



AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

CONTINUOUS SECURITY

- As threats continually evolve, it is critical that we consider risk during the **entire vehicle lifecycle**. With vehicles becoming more **connected** and software-driven, attack vectors and vulnerabilities increase.
- **Over-the-air updates** will help to enable **cost effective and continuous** software and security maintenance. Vehicle Security Operations Center will continuously monitor, assess and correct these threats to help protect the vehicles of today and tomorrow, driving toward a safe and secure future for all.

These products are **TLP: WHITE** and are meant to be easily understandable and widely shared internally and externally, including **social media** platforms.

YOUR CALL-TO-ACTION

Cybersecurity Awareness Month is fast approaching!

To promote awareness and to issue an industry-wide call-to-action, please distribute the publicly shareable products throughout your network (for release each Monday in October).

Week	Theme	Sent to POCs	Release Date
1	We are all connected	09/29	10/03
2	Purpose Driven Security	10/06	10/10
3	Build & Deliver Securely	10/13	10/17
4	Continuous Security	10/20	10/24

These products are **TLP: WHITE** and are meant to be easily understandable and widely shared internally and externally, including social media platforms.

Please reach out to Tamara Shoemaker tamarashoemaker@automotiveisac.com with any questions

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 michaelshokouhi@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
(19)**

ArmorText
 Cybellum
 Deloitte
 FEV
 GRIMM
 HackerOne
 Irdeto
 Itemis
 Karamba Security
 KELA
 Pen Testing Partners
 Red Balloon Security
 Regulus Cyber
 Saferide
 Security Scorecard
 Tanium
 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**

2021 Summit Sponsors-

Celerium
 Cyware
 Denso
 NDIAS
 IOActive
 Claroty
 Deloitte
 Finite State
 Tanium
 Recorded Future
 PaloAlto Networks
 Upstream
 Securonix
 Zimperium
 Micron
 Block Harbor
 SecurityScorecard
 Booz Allen
 CybelAngel
 ATT
 Ford
 Cybellum

2020 Summit Sponsors-

Claroty
 Upstream
 Escrypt
 Blackberry
 Cybellum
 Blockharbor
 C2A
 Synopsis
 Intsignts
 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)