



# **WELCOME TO AUTO-ISAC!**

## *MONTHLY VIRTUAL COMMUNITY CALL*





May 4, 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><b>TLP:RED</b></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><b>TLP:AMBER</b></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><b>TLP:GREEN</b></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><b>TLP:WHITE</b></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	<b>Welcome</b> <ul style="list-style-type: none"><li>➤ Why We're Here</li><li>➤ Expectations for This Community</li></ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"><li>➤ Auto-ISAC Activities</li><li>➤ Heard Around the Community</li><li>➤ What's Trending</li></ul>
11:15	<b><i>DHS CISA Community Update</i></b>
11:20	<b>Featured Speaker:</b> <ul style="list-style-type: none"><li>▪ <b><i>Kenneth J. Peterson, CTPRP, Founder and CEO, Churchill &amp; Harriman, Inc.</i></b></li></ul>
11:45	<b>Around the Room</b> <ul style="list-style-type: none"><li>➤ Sharing Around the Virtual Room</li></ul>
11:55	<b>Closing Remarks</b>



# 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](mailto: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 (1<sup>st</sup> 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*

**13**  
*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 Hilken**  
*Chair of the CAG*  
Cummins

# MEMBER ROSTER

## AS OF MAY 1, 2022

Highlight = Change

68 Members, 3 in Progress

Aisin	Honda	Nissan	Yamaha Motors
Allison Transmission	Hyundai	Nuro	ZF
Aptiv	Infineon	NXP	
Argo AI, LLC	Intel	Oshkosh Corp	
AT&T	John Deere Electronic	PACCAR	
AVL List GmbH	Kia	Panasonic	
Blackberry Limited	Knorr Bremse	Polaris	
BMW Group	Lear	Qualcomm	
BorgWarner	LGE	Renesas Electronics	
Bosch (Ecrypt-Affiliate)	Lucid Motors	Stellantis	
Canoo	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	Vitesco	
Geotab	Mobis	Volkswagen	
Google	Motional	Volvo Cars	
Harman	Navistar	Volvo Group	
Hitachi	Nexteer Automotive Corp	Waymo	

# UPCOMING EVENTS

## ➤ Upcoming Meetings:

### ➤ Community Call:

- Wednesday, June 1 – **Speaker:** François-Frédéric Ozog, Linaro **Title:** *Automotive Firmware, Hypervisor and OS Cybersecurity Made Simpler* **Time:** 11 – 12:00 p.m. **TLP:WHITE**

### ➤ Partners Teaching Members:

- Wednesday, May 18 **Speaker:** Suzanne Lightman & Cheri Pasco, NIST **Title:** *NIST Cybersecurity Framework (CSF)* **Time:** 10 – 11:30 a.m. **TLP:AMBER**

- **Registration is open for the first Auto-ISAC Partner Day.** Virtual presentations are May 23-27 from 11:00a-1:00p each day. [Register here.](#) **TLP:AMBER**

## ➤ Announcements:

- **\*\*\*New Auto-ISAC Website launched.** Contact [Michael Shokouhi](#) if you have any feedback.
- Board approved the **SAG's SBOM's** material as an **Information Report for release to Members only** at this time. **SAG's SBoM WG targeting a broader release in 3Q2022.**
- **2021 Auto-ISAC Annual Report:** ExCom approved **TLP: GREEN report** for dissemination.
- **ACT Program Advanced Courses** begin on April 11<sup>th</sup>. Beta signup is open for **Members only now**. Contact [Tamara Shoemaker](#).
- **Auto-ISAC Cybersecurity Summit – Registration is Open!** Both in-person and virtual venue. Dates: September 7-8, 2022, in Dearborn, MI at The Henry Hotel.



2022 Auto-ISAC

# Partner Day

May 23-27 • 11AM-1PM EST



2022 AUTO-ISAC CYBERSECURITY SUMMIT

# DRIVING A SECURE FUTURE

Hybrid Event • Dearborn, MI and Virtual • September 7-8, 2022



[More information here](#)

EVENT HOST & TITANIUM SPONSOR



**BOSCH**

**escrypt**





# 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](mailto:analyst@automotiveisac.com)
- Know our strategic view of the cyber threat environment by reviewing the **TLP:GREEN** Threat Assessment in the Auto-ISAC 2021 Annual Report
- Intelligence Notes
  - We continue to advise the automotive community to maintain heightened vigilance for indications of malicious activity or compromise. **The continuing Russia threat merely adds to an already heightened threat environment** ([CISA Shields Up](#), [CISA-Known Exploited Vulnerabilities Catalog](#), [CISA-Technical Approaches to Uncovering and Remediating Malicious Activity](#)).
  - We continue to see periodic reports of threat actors selling **internal data/files or access to networks** of various types of automotive companies. Automotive companies should routinely look for indications that their information or access to their network is being sold on the open, deep, and dark webs.
  - Notable TTPs: Browser-in-the-Browser ([Safeguard Cyber](#), [Google](#)); reflection/amplification distributed denial-of-service attack (DDoS)([Akamai](#)); Obfuscation ([SentinelOne](#), [BleepingComputer](#), [BlackBerry](#))



# CISA RESOURCE HIGHLIGHTS



## TLP: WHITE – Virtual Corporate Engagement Series

- Conducted by DHS Intelligence & Analysis (I&A) Private Sector Engagement
- Contributors to the events include leaders from both the public and private sector
- Topics include:
  - key trends and lessons learned that are shaping security
  - best practices through discussion of real-life case studies
  - Current physical and digital security challenges
- Event overview at [https://www.dhs.gov/sites/default/files/publications/20210615\\_virtual\\_cses\\_overview.pdf](https://www.dhs.gov/sites/default/files/publications/20210615_virtual_cses_overview.pdf)
- Contact email for more information at [I&APrivateSector@hq.dhs.gov](mailto:I&APrivateSector@hq.dhs.gov)



# TLP: WHITE – CISA Current Activities – Joint Products

- **Updated Advisory on Destructive Malware Targeting Organizations in Ukraine – CISA, FBI**
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/28/cisa-and-fbi-update-advisory-destructive-malware-targeting](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/28/cisa-and-fbi-update-advisory-destructive-malware-targeting)
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-057a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-057a)
  - [https://www\[.\]cisa\[.\]gov/uscert/sites/default/files/publications/AA22-057A.stix.xml](https://www[.]cisa[.]gov/uscert/sites/default/files/publications/AA22-057A.stix.xml)
- **2021 Top Routinely Exploited Vulnerabilities - CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK**
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/27/2021-top-routinely-exploited-vulnerabilities](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/27/2021-top-routinely-exploited-vulnerabilities)
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-117a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-117a)



## TLP: WHITE – CISA Current Activities – Joint Products - continued

- **Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure – CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK, NCA-UK**
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/20/russian-state-sponsored-and-criminal-cyber-threats-critical](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/20/russian-state-sponsored-and-criminal-cyber-threats-critical)
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-110a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-110a)
- **North Korean State-Sponsored APT Targets Blockchain Companies – CISA, FBI, U.S. Department of Treasury**
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/18/north-korean-state-sponsored-apt-targets-blockchain-companies](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/18/north-korean-state-sponsored-apt-targets-blockchain-companies)
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-108a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-108a)
  - [https://www\[.\]cisa\[.\]gov/uscert/sites/default/files/A22-108A.stix.xml](https://www[.]cisa[.]gov/uscert/sites/default/files/A22-108A.stix.xml)





# TLP: WHITE – CISA Current Activities – Joint Products - continued

- **APT Actors Target ICS/SCADA Devices – CISA, DOE, NSA, FBI**
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/13/apt-actors-target-icsscada-devices](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/13/apt-actors-target-icsscada-devices)
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-103a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-103a)



# TLP: WHITE – CISA NCAS CA – Guidance on Sharing Cyber Incident Information

- Information provided by CISA partners to build a common understanding of how adversaries are targeting U.S. networks and critical infrastructure sectors
- Provides stakeholders with clear guidance and information about what to share, who should share, and how to share information about unusual cyber incidents or activity
- Resources:
  - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/07/guidance-sharing-cyber-incident-information](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/07/guidance-sharing-cyber-incident-information)
  - [https://cisa\[.\]gov/sites/default/files/publications/Sharing\\_Cyber\\_Event\\_Information\\_Fact\\_Sheet\\_FINAL\\_v4.pdf](https://cisa[.]gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf)



## TLP: WHITE – Forty-five (45) Known Exploited Vulnerabilities (KEV) added to the catalog in April 2022:

- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/25/cisa-adds-seven-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/25/cisa-adds-seven-known-exploited-vulnerabilities-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/19/cisa-adds-three-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/19/cisa-adds-three-known-exploited-vulnerabilities-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/15/cisa-adds-nine-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/15/cisa-adds-nine-known-exploited-vulnerabilities-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/14/cisa-adds-one-known-exploited-vulnerability-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/14/cisa-adds-one-known-exploited-vulnerability-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/13/cisa-adds-10-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/13/cisa-adds-10-known-exploited-vulnerabilities-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/11/cisa-adds-eight-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/11/cisa-adds-eight-known-exploited-vulnerabilities-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/06/cisa-adds-three-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/06/cisa-adds-three-known-exploited-vulnerabilities-catalog)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/04/04/cisa-adds-four-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/04/04/cisa-adds-four-known-exploited-vulnerabilities-catalog)
- **KEV Catalog:**
  - [https://www\[.\]cisa\[.\]gov/known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/known-exploited-vulnerabilities-catalog)



## 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 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](mailto: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



# KENNETH J. PETERSON, CHURCHILL & HARRIMAN, INC.

## *FOUNDER AND CEO*



**Kenneth** is the Founder and Chief Executive Officer of Churchill & Harriman (C&H), based in Princeton, NJ. C&H is a strategic consulting company specializing in the development and implementation of risk management strategies across critical infrastructure clientele in several industries and government.

He is an active leader in the international standards community, maintaining a strong relationship with The National Institute of Standards and Technology (NIST).

Kenneth has been an Enterprise Risk Governance, Crisis Management, and Third-Party Vendor Risk Management keynote speaker/panelist for The Risk Management Association, The Bank Policy Institute, The MITRE Corporation, The Automotive Information Sharing and Analysis Center, The Health Information Sharing and Analysis Center, The American Society for Quality, Depository Trust & Clearing Corporation, CVS Health, The Shared Assessments Program, and The CMMC Center of Excellence.





**Protecting and Enabling Existing and New Revenue Streams**

**Presentation to The Automotive ISAC**

**May 4, 2022**



## The Challenge

In this increasingly volatile global business climate, more than ever it is imperative that you protect and enable existing and new revenue streams.

## The Challenge (continued)

There is currently a particular global confluence of High-Level risks across industries that increasingly threaten existing and new revenue streams and pose systemic risk. These risks include those inherent in technical continuity, cyber resilience, and the potential for a ransomware attack.

# Protecting and Enabling Current and New Revenue Streams

**These risks are ever-increasing based on two factors:**

- 1) Increased dependence on working remotely.
- 2) Ransomware Attacks and Phishing Attacks.

Boards of Directors and Risk Committees require evidence to inform their funding decisions. Ever increasing scrutiny is being placed on technology investments and on security investments. Current, irrefutable evidence is increasingly required to inform these decisions.

## Understanding Ransomware – from CISA

**Ransomware** is a sub-category of malware, a class of software designed to cause harm to a computer or computer network. CISA defines ransomware as “an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.”

# Ransomware — Executive Summary

**Ransomware** is a high-profile threat that demands immediate attention:

- Organizations large and small hit by ransomware make the news every week; everyone is a target.
- Executives want reassurance but aren't ready to write a blank check. Improvements must be targeted and justified.
- No one is bulletproof, so the ability to recover (not just prevent) a ransomware attack is critical, yet existing backup and DR capabilities are often lacking.

**Ransomware** impact and recovery is more complicated than other security breaches:

- Ransomware attackers use multiple attack vectors. They can even have ransomware lay dormant, so it infiltrates your backups, disaster recovery (DR) site, and even more endpoints before it's activated.
- Data loss is bad; data loss plus the inability to restore from backups is devastating.
- Ransomware is constantly evolving; traditional security and DR practices may not be enough.



# Recent High Visibility Attacks



**Car manufacturer Toyota** has suspended production at 14 plants in Japan for at least a day in response to a “system failure” at components supplier Kojima Industries. In a brief statement issued on Monday (February 28, 2022), Toyota confirmed the temporary shutdown, which auto industry experts estimate might lead to a 5% drop in Toyota’s monthly production or the loss of about 13,000 units: “Due to a system failure at a domestic supplier (KOJIMA INDUSTRIES CORPORATION), we have decided to suspend the operation of 28 lines at 14 plants in Japan on Tuesday, March 1st (both 1st and 2nd shifts).

**In February 2021, Kia Motors America was hit with a ransomware attack** that caused a nationwide IT outage affecting internal, dealer and customer-facing systems<sup>3</sup>. The attackers, the DoppelPaymer ransomware gang, left a ransom note stating that a “huge amount” of data was stolen and would be released in 2–3 weeks if Kia Motors America **did not pay the ransom**.



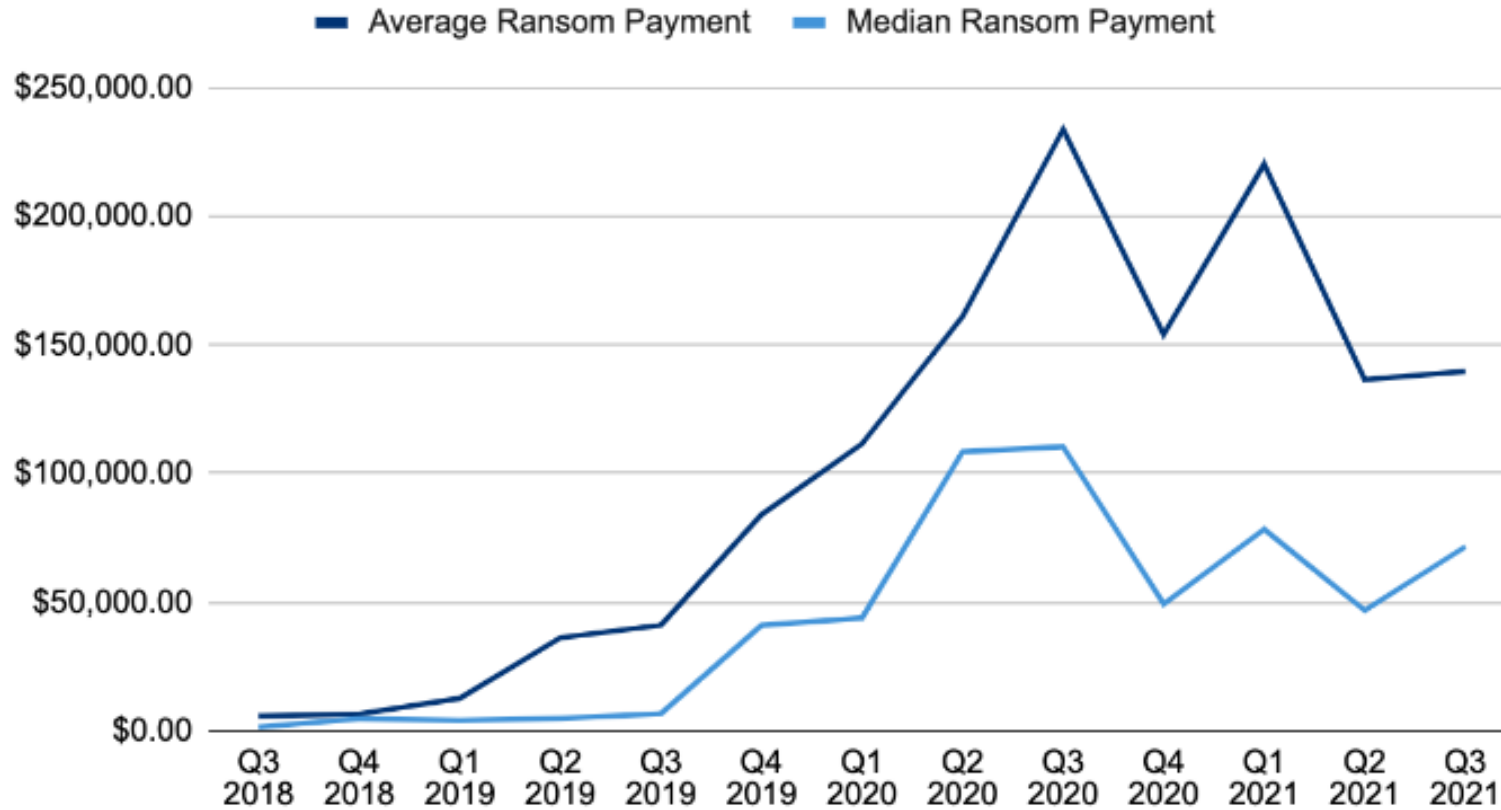
**Bridgestone Americas** has reportedly “disconnected” many of its manufacturing and retreading facilities after suffering a possible cyber-attack yesterday morning (February 27, 2022). According to reports, the automotive giant has said it is so far unable to “determine with certainty the scope or nature of any potential incident.” In a statement sent to several media outlets, Bridgestone Americas said: “Bridgestone Americas is currently investigating a potential information security incident. Since learning of the potential incident in the early morning hours of February 27, we have launched a comprehensive investigation to quickly gather facts while working to ensure the security of our IT systems.”



A recent research conducted by **Future of Automotive Security Technology Research (FASTR)** has concluded that connected cars could be the next targets for ransomware hackers/developers. FASTR which technically acts as a consortium of automotive manufacturers, software makers for automotive industry and suppliers, discovered in its research that as soon as a connected car connects to the internet, the entire vehicle gets exposed to threat surface.

# The Rising Cost of Ransomware

## Ransom Payments By Quarter



### Ransomware Targets:

- Large & Mid-sized Corporations
- Small businesses
- Local Governments
- Local Police
- Schools
- Hospitals



## Protecting and Enabling Current and New Revenue Streams — A Solution

**A Solution to this challenge is Exercises — conducted through open, safe, focused discussion of organizational strengths and areas for opportunity and improvement**

The outputs of your exercises will reveal “Findings” whereby the risks revealed through the execution of the exercise are identified and should be risk-ranked. Then you are positioned with irrefutable, current evidence to recommend to your Board for their approval so that your global revenue streams are protected and enabled, and you are mitigating reputational risk.

## Protecting and Enabling Current and New Revenue Streams — A Solution

*Ransomware is topical **NOW**. You can construct ransomware-specific exercise Scenarios and Injects to prove out specific business processes, technical processes, and business applications, ensuring they are properly vetted. Gaps are identified, actionable findings are produced, the Objectives of the Exercise are met, and the efficacy of your revenue streams is further ensured.*

### You collaborate with your relevant stakeholders to:

- Select the technical process(es), business process(es), or business application(s) you choose to focus the Tabletop, War Game or Critical Infrastructure exercise on.
- Ensure that representatives of all relevant internal and external functions participate in or Observe the exercise.
- Ensure you are including all relevant stakeholders in the planning process to optimally drive Ownership and interest. If a stakeholder is being measured on a certain element of the output of the exercise, all the better.

**For more information, please contact:**

**Questions?**

**Thank You**

Kenneth J. Peterson, CTPRP

CEO and Founder

[kpeterson@chus.com](mailto:kpeterson@chus.com)

908-581-8405



## 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](mailto:andreaschunn@automotiveisac.com).  
For Partnership, please contact [sharmilakhadka@automotiveisac.com](mailto: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  
(13)**

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

**2021 Summit Sponsors-**

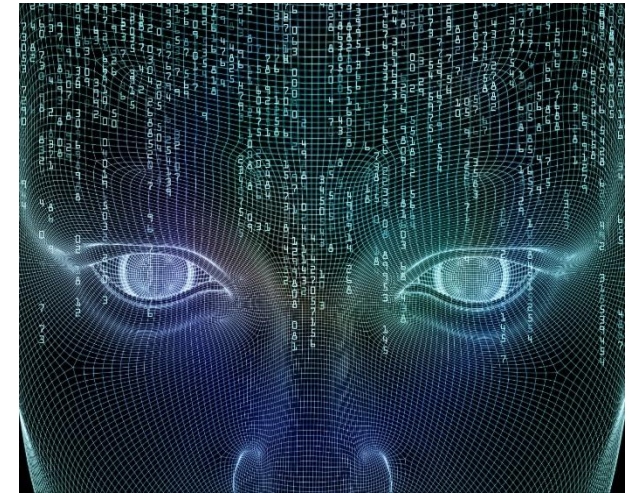
Celerium  
Cyware  
Denso  
NDIAS  
IOActive  
Claroty  
Deloitte  
Finite State  
Tanium  
Recorded Future  
PaloAlto Networks  
Upstream  
Securonix  
Zimperium  
Micron  
Block Harbor  
SecurityScorecard  
Booz Allen  
CybelAngel  
ATT  
Ford  
Cybellum

**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](http://www.automotiveisac.com)  
[@auto-ISAC](https://twitter.com/auto-ISAC)