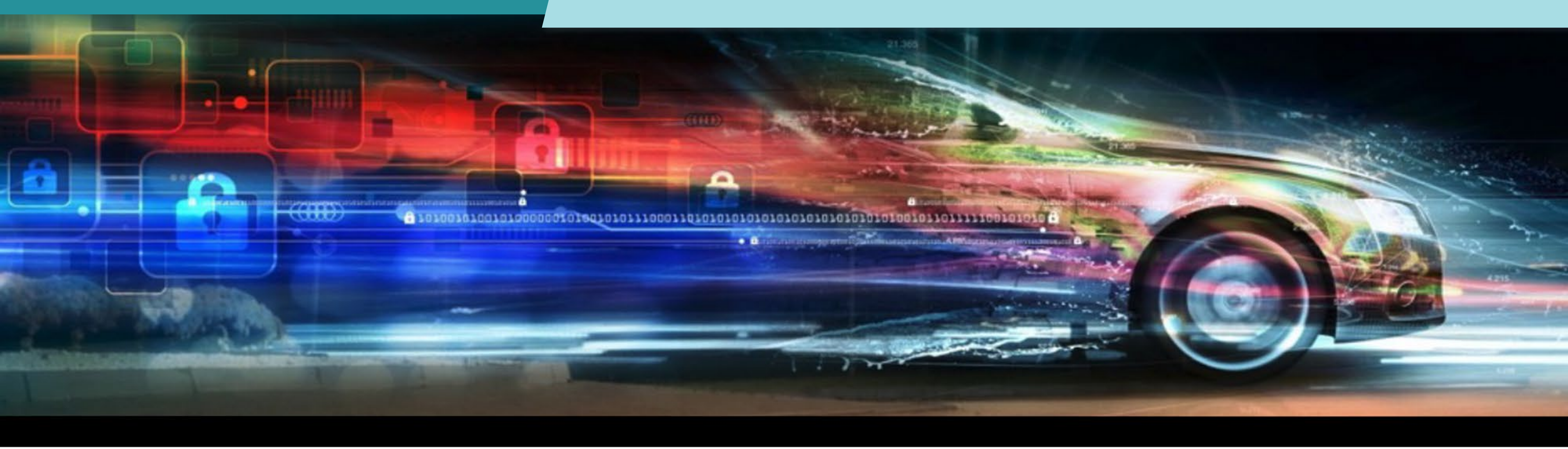


Welcome to Auto-ISAC!

Monthly Virtual Community Call

June 7, 2023

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Antitrust Statement

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.

Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.

This meeting is being held at

TLP:CLEAR

Disclosure is not limited.

Traffic Light Protocol (TLP)

Version 2.0 Definitions

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 without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	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+STRICT ○ 🟡 ○	**Limited disclosure, restricted to participants' and its organization.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ○ 🟡 ○	**Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ○ ○ 🟢	**Limited disclosure, restricted to the community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ⚪ ⚪ ⚪	**Disclosure is not limited.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: 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*** ➢ **Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)**
11:20	**Featured Speaker:** ➢ **Justin Montalbano, *President*, Car Hacking Village** ➢ **Title: "What is the Car Hacking Village (CHV)?"**
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

AUTO-ISAC
Automotive Information Sharing and Analysis Center

❖ 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!

❖ 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

29 *OEM Members*

21 *Navigator Partners*

46 *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)*

2023 Board of Directors

Thank you for your Leadership!

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

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

Stephen Roberts
Secretary *of the*
Board of the Directors
Honda

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

Andreas Ebert
Chair *of the EuSC*
Volkswagen

Andrew Hillery
Chair *of the CAG*
Cummins

Ravi Puvvala
Chair *of the SAG*
Fleet Defender

Monica Mitchell
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

Auto-ISAC Member Roster

As of June 1, 2023

75 Members + 4 Pending

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

Pending: CNH Industrial, Daimler Truck, Micron, Stoneridge

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Business Updates and Events

**All times are in ET

Upcoming Meetings:

- **Members Teaching Members: Wednesday, June 21st Time: *10:00am – 11:30 a.m.* TLP:AMBER; Speaker: Amit Geynis, Security Researcher, Argus Title: *"Tales From a Penetration Testing Team"***

- **Auto-ISAC's first European Summit will be June 13th-14th, 2023 with June 12th having Members-only activities. https://automotiveisac.com/2023-europe-summit Register now!**

- **Auto-ISAC Summit will be Tuesday, October 17th-18th, 2023 in Torrance, California. You can find more information and registration here: https://automotiveisac.com/2023-annual-summit**
  Register now! Early bird pricing for US summit ends September 8th.

NOTE: If you wish to submit a proposal to be a featured speaker on our monthly Community call, please reach out to Sharmilakhadka@automotiveisac.com. The presentation must be educational and relevant to Automotive cybersecurity.

AUTO-ISAC EUROPE

1ST ANNUAL EUROPEAN

CYBERSECURITY SUMMIT

June 13 - 14 / Sochaux, France

THE FUTURE OF

CONNECTED SECURITY

TITANIUM SPONSOR

STELLANTIS

June 12 Members Only: TLP:AMBER
Monday, June 12: 11:00 – 20:00 CET

Open to Auto-ISAC Members only
Register here

June 13-14 Open to Public: TLP:CLEAR
Tuesday, June 13: 8:00 – 20:00 CET
Wednesday, June 14: 8:00 – 16:00 CET

Open to Auto-ISAC Members and External Partners
Register here

ACCELERATING CASE SECURITY

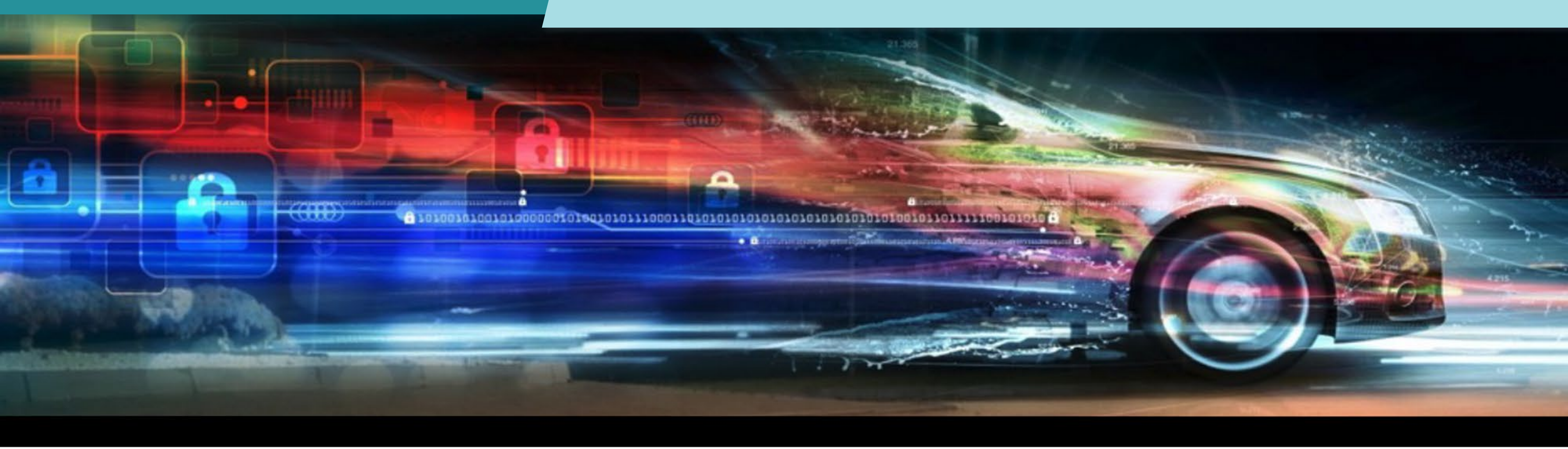
7th Annual Auto-ISAC Cybersecurity Summit

October 17-18, 2023

Torrance, CA

HONDA
The Power of Dreams

AUTO-ISAC



Auto-ISAC Intelligence Highlight

Auto-ISAC Intelligence

- **Know what we track daily: subscribe to the DRIVEN; TLP:GREEN Auto-ISAC 2022 Threat Assessment released with Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) included.**
  - **Send feedback, contributions, or questions to analyst@automotiveisac.com**
- **Intelligence Notes**
  - **Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia- Ukraine in crisis. Threat of cyberattack spillover increases if: (1) the Russia-Ukraine war leads to kinetic clashes with the West (possible but unlikely), and (2) any other hotspots escalate into crises (possible) (Russia-Ukraine [1], China [2] [3] [4], North Korea, Iran [5]).**
  - **Ransomware [6] Groups Targeting Automotive: BlackSuit, Darkrace, Trigona, Abyss*, Rancoz*, Monti, Cl0p [7], AlphV/BlackCat, BianLian, Snatch, Black Basta, LockBit 3.0 Royal, Nokoyawa, Play, Dunghill***
  - **Anonymous Sudan appears to be a potent distributed denial-of-service threat and claims to have targeted a tactical vehicle manufacturer (Trustwave, Cybernews).**
  - **Threat actors continue to use Telegram to advertise access to automotive organizations' databases or files containing stolen data.**
  - **Notable TTPs and Tools: Fooling ChatGPT into recommending malicious packages planted by threat actors (Vulcan); Mass exploitation of MOVEit MFT zero-day (BleepingComputer); iOS zero-click, SMS-delivered malware with code execution capabilities (Securelist).**

CISA Resource Highlights

- Joint Cyber Defense Collaborative

Jeff Terra
6/7/2023

CISA and FBI Release Joint Advisory in Response to Active Exploitation of Papercut Vulnerability

- CISA and FBI have released a joint Cybersecurity Advisory (CSA), Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG.
- In early May 2023, FBI observed a group self-identifying as the Bl00dy Ransomware Gang attempting to exploit vulnerable PaperCut servers against the Education Facilities Subsector.
- The advisory further provides detection methods for exploitation and details known indicators of compromise (IOCs) related to the group’s activity.
- This vulnerability occurs in certain versions of PaperCut NG and PaperCut MF and enables an unauthenticated actor to execute malicious code remotely without credentials. PaperCut released a patch in March 2023.

- Please note all information provided is TLP Amber

CISA and Partners Update the #StopRansomware Guide, Developed through the Joint Ransomware Task Force (JRTF)

- CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) published an updated version of the #StopRansomware Guide
- Ransomware actors have accelerated their tactics and techniques since its initial release in 2020.
- The update incorporates lessons learned from the past two years and includes additional recommended actions, resources, and tools to maximize its relevancy and effectiveness and to further help reduce the prevalence and impacts of ransomware.

CISA and Partners Release Cybersecurity Advisory Guidance detailing PRC state-sponsored actors evading detection by "Living off the Land"

- CISA joined the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and international partners in releasing a joint cybersecurity advisory highlighting recently discovered activities conducted by a People's Republic of China (PRC).
- This advisory highlights how PRC cyber actors use techniques called "living off the land" to evade detection by using built-in networking administration tools to compromise networks and conduct malicious activity.
- The authoring agencies have identified potential indicators associated with these techniques. To hunt for this activity, CISA and partners encourage network defenders to use the actor's commands and detection signatures provided in this advisory.

- Please note all information provided is TLP Amber

Security/Software Updates

For the period of 5/1/23 - 5/31/23:

- CISCO Releases Security Advisories: Multiple products
- Microsoft Releases Security Updates: Multiple products
- Mozilla Releases Security Updates: Multiple products

- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

CISA Releases Industrial Control Advisories

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations
- For the period of 5/1/23- 5/31/23 approximately 33 advisories have been issued
- The advisories span the following sectors: Information Technology, Critical Manufacturing, Energy and Multiple Sectors
- Cybersecurity Alerts & Advisories | CISA

Please note all information provided is TLP Amber

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 added 19 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of May. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

Additional Resources from CISA

- ❑CISA Homepage - https://www.cisa.gov/
- ❑CISA NCAS – https://cisa.gov/resources-tools/all-resources-tools
- ❑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

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*

30+ ***Featured Speakers to date***

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!

7 ***Best Practice Guides available on website***

2000+ ***Community Participants***

Featured Speaker

Justin Montalbano

President, Car Hacking Village

Justin is the problem and the solution. He's been apart of the Car Hacking Village (CHV) since year one in 2015 and has been crucial in bringing together the automotive security community. Aside from hacking things, he's typically out in the woods enjoying the complex chaos of nature!

Justin is no stranger to the security industry, with over 10 years of experience, his array of expertise include; leadership, penetration testing, incident response, forensics, research & development, public speaking, running Capture the Flag (CTF) events, and training in the art of exploitation.

Justin's varied expertise and background helps provide the perfect foundation of knowledge and understanding to assist in the corporate integration of hackers.

DELPHI • APTIV • UNIVERSITY OF MICHIGAN

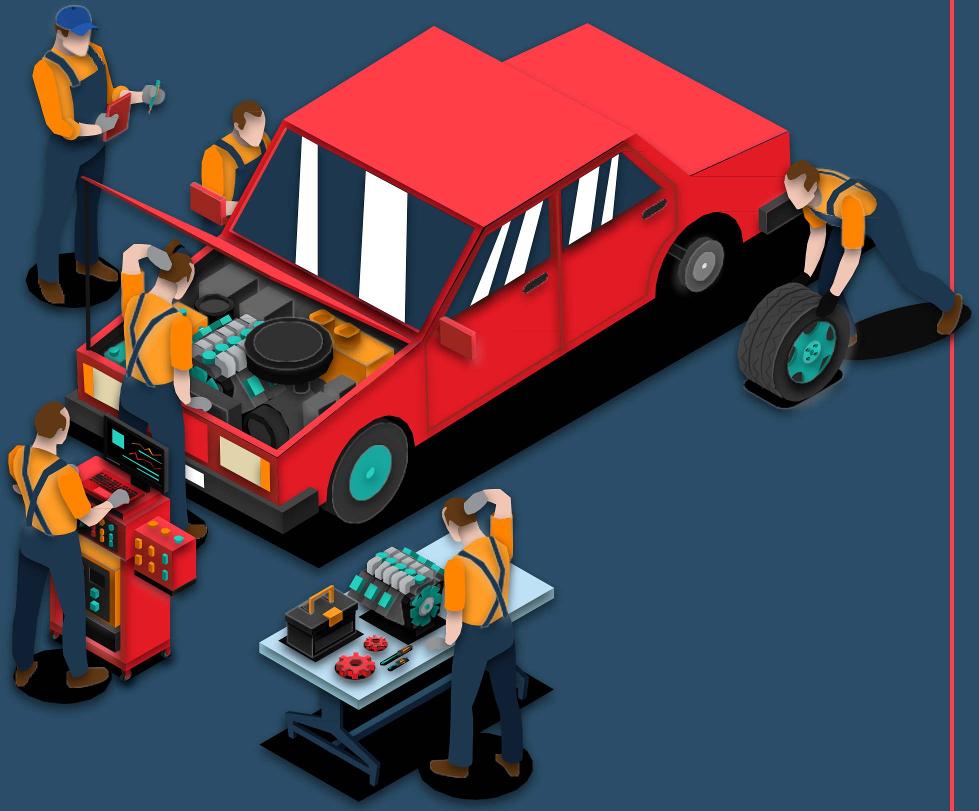
Blue Cross Blue Shield of Michigan ARGO AI BOOM

What is the Car Hacking Village (CHV)?

carhackingvillage.com

Justin Montalbano
President

DISCOVER DEFEND
CAR HACKING VILLAGE
SECURING CRITICAL AUTOMOTIVE SYSTEMS



About Me

Justin Montalbano - Sr. Cybersecurity Engineer, Boom Supersonic | President, Car Hacking Village

CAR HACKING VILLAGE

ARGO AI

APTIV

DELPHI

M

Overview

→ What is DefCON?

→ What is the Car Hacking Village (CHV)?

→ Capture the Flag (CTF) / Challenges

→ Badges

→ Past Sponsors

→ How to get involved?

→ Contact Details

DANGERS OF DEFCON BEING IN TOWN

YOU ARE AT RISK OF GETTING HACKED

What is DefCON?

defcon.org

→ One of the world's largest and most renowned hacker conventions

→ Talks on a wide range security related topics across all industries (automotive, aerospace, information security, industrial controls, maritime, IoT)

→ Villages, SkyTalks and the "Wall of Sheep"

→ Prestigious Capture the Flag competition

→ One-of-a-Kind Badge Community

What is the Car Hacking Village?

carhackingvillage.com

- → Founded in 2015 by Robert Leale of CanBusHack
- → 501c3 Non-profit organization
- → CHV can be found in the US, Japan, UK, Hong Kong, and Philippines

CANBUSHACK

CAR HACKING VILLAGE
SECURING CRITICAL AUTOMOTIVE SYSTEMS
DISCOVER DEFEND

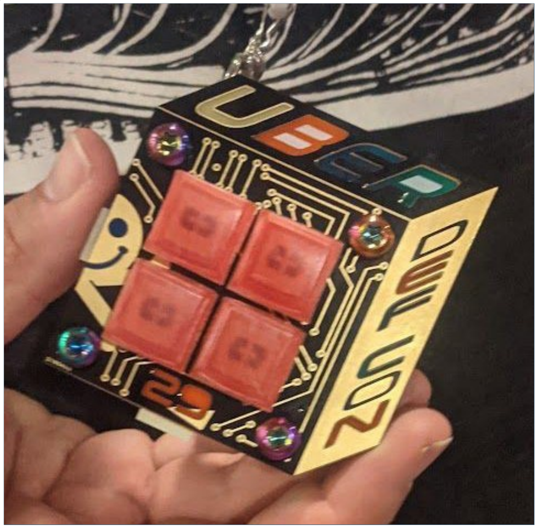
What is the Car Hacking Village?

carhackingvillage.com

→ Automotive Capture the Flag event

→ Badge Life

→ CHV Contributors teach AutoISAC CASE classes



Where is the Car Hacking Village?

carhackingvillage.com

DEFCON

BSIDES

GrrCON
GrrCON.org

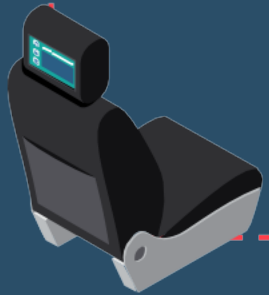
black hat

DEFCON 神州 CHINA 1.0

ROOTCON

HITB

TEXAS CYBER SUMMIT
CONFERENCE
BRIEFINGS
MMXXI

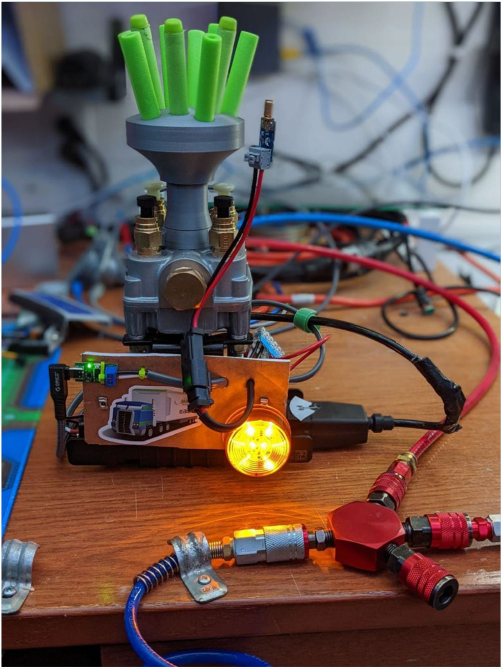


Capture the Flag (CTF) / Challenges

Semi-truck hacking

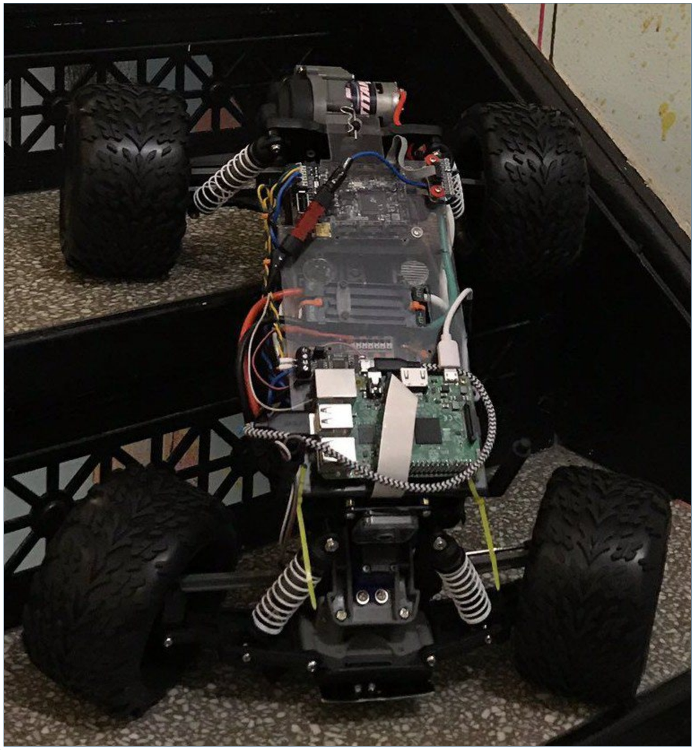
Capture the Flag (CTF) / Challenges

Air Brake Air Darts



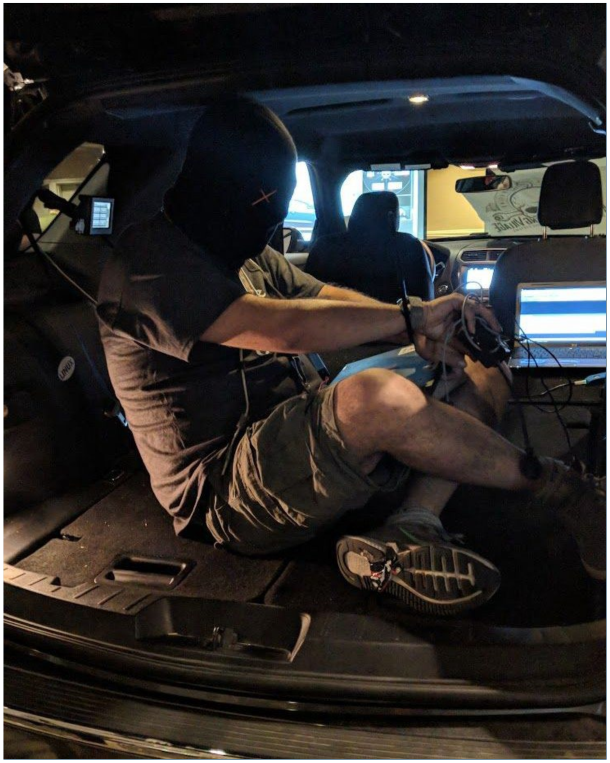
Capture the Flag (CTF) / Challenges

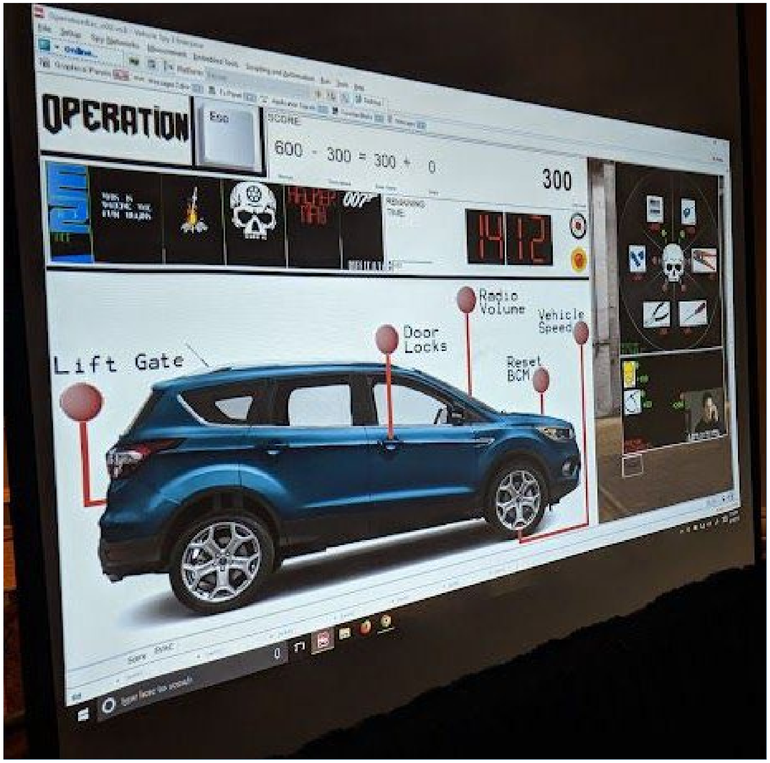
RoboCars



Capture the Flag (CTF) / Challenges

Escape Challenge



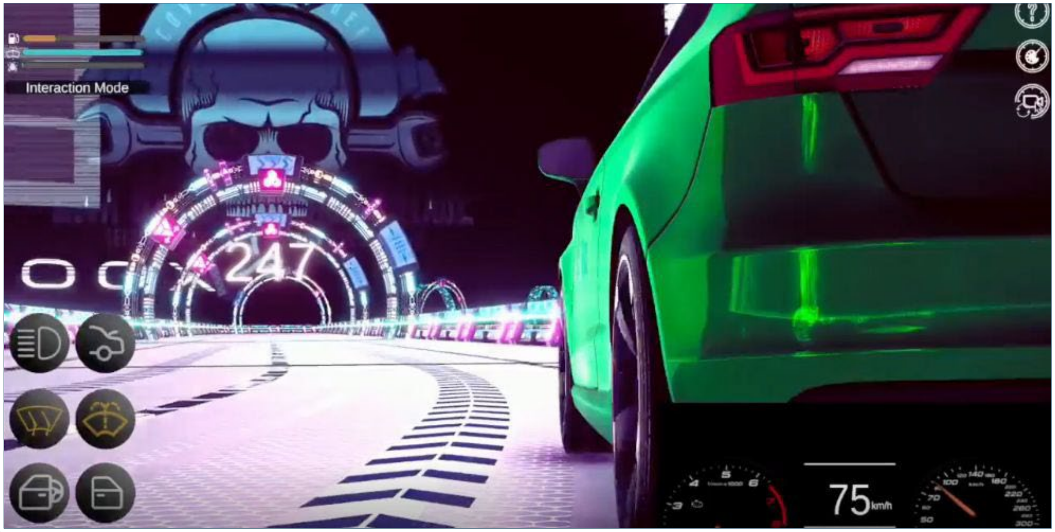


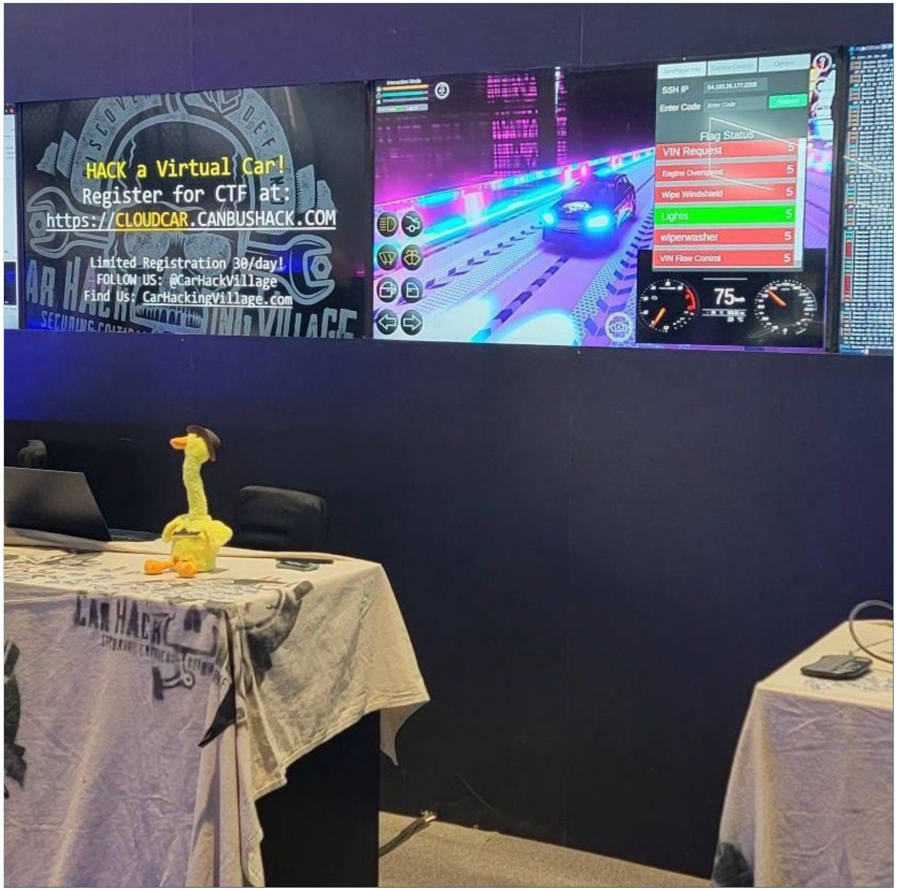
Capture the Flag (CTF) / Challenges

Car Simulator

Capture the Flag (CTF) / Challenges

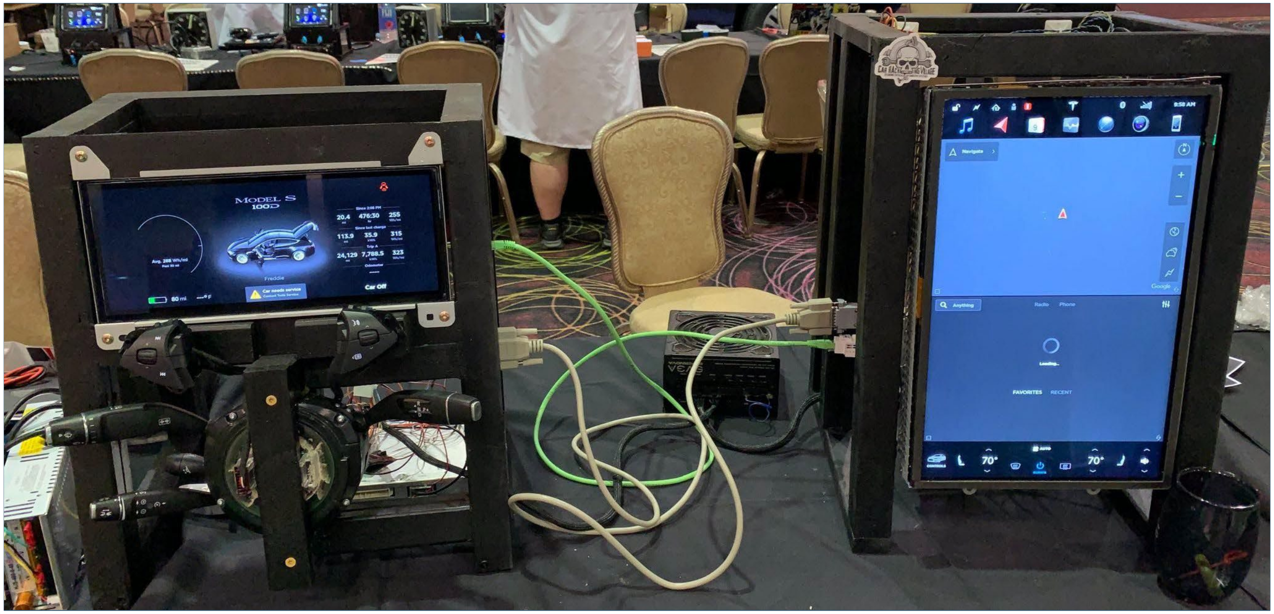
Cloud Car





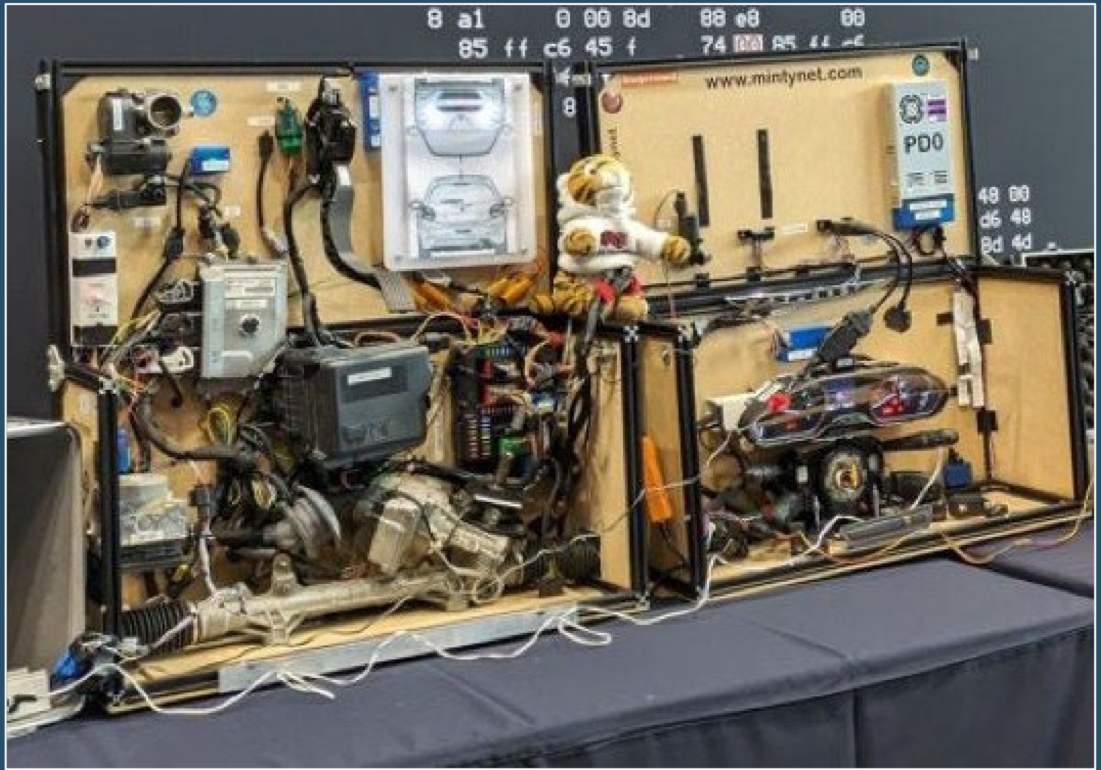
Capture the Flag (CTF) / Challenges

Tesla in the Loop



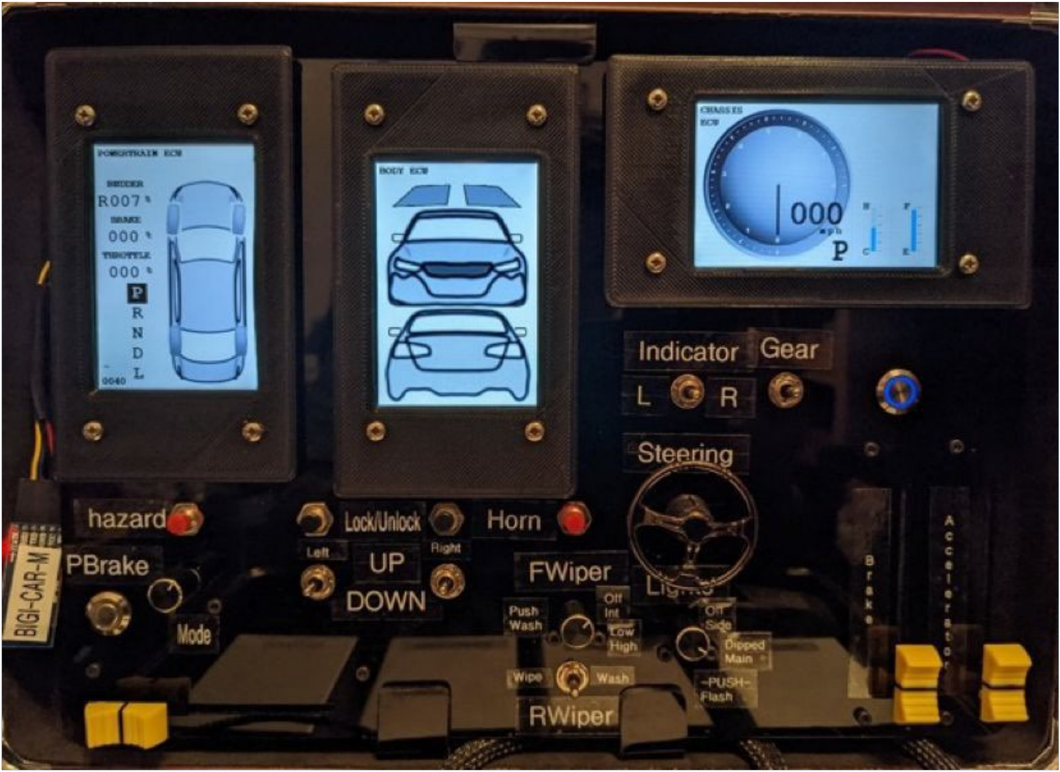
Capture the Flag (CTF) / Challenges

PDO



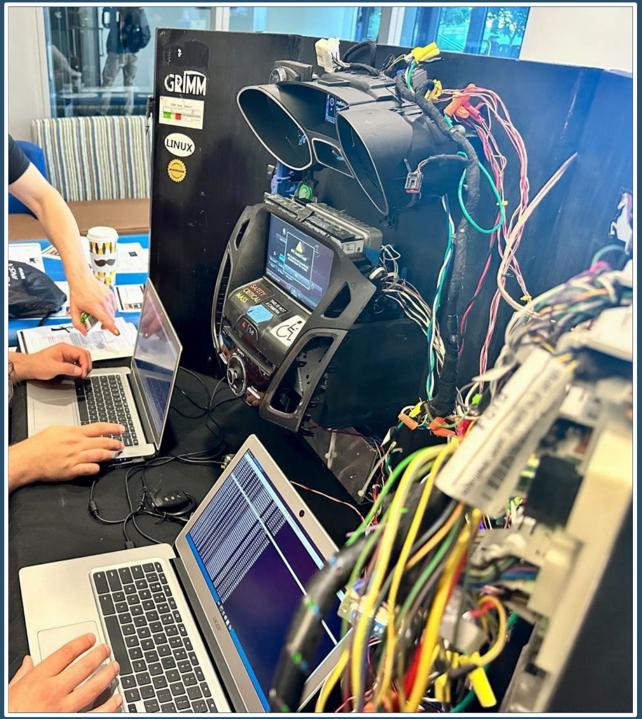
Capture the Flag (CTF) / Challenges

Car in a Case



Capture the Flag (CTF) / Challenges

C3PO

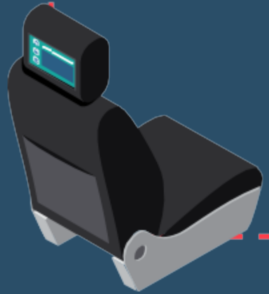


Capture the Flag (CTF) / Challenges

Head Unit Hackathon

Capture the Flag (CTF) / Challenges

Bluetooth Challenges



Capture the Flag (CTF) / Challenges

Honda Key Fob 2022 CVE

CTF Prizes

AutoNation DERIVE Systems
DEFCON
ANZO

DEFCON
Rodshop

Car Hacking Village

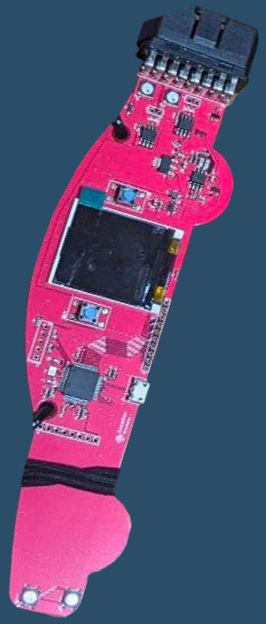
Logic Bomb
P1

My Other Computer is your ECU

Badges

Previous Years

2015



2016

2017

2018

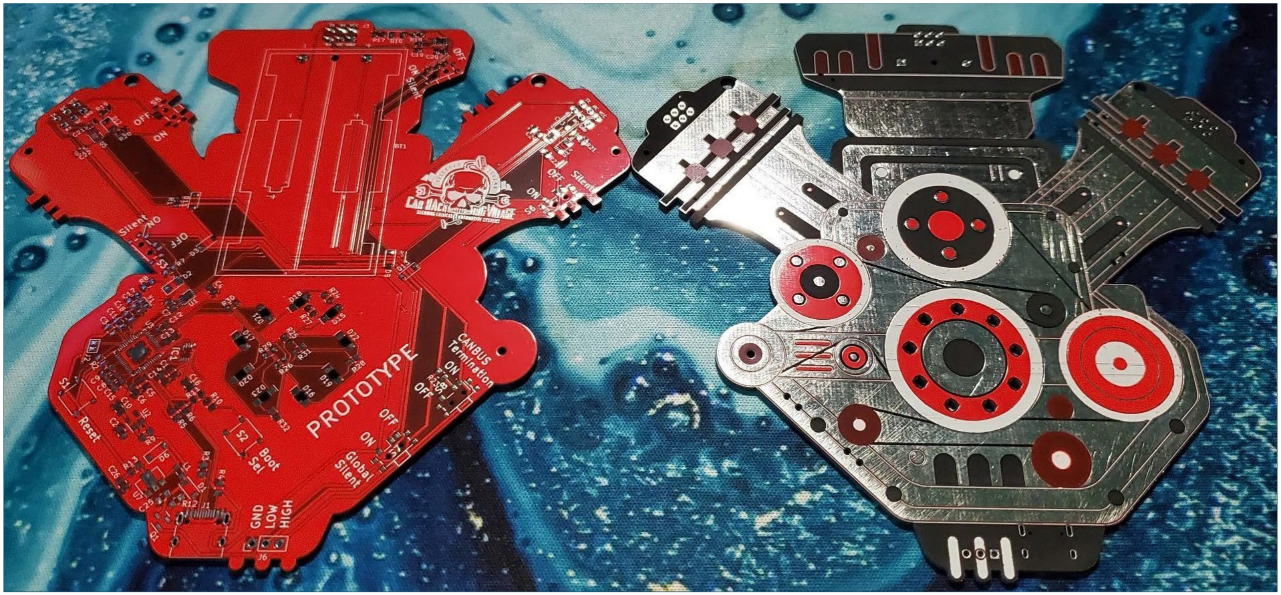
2019

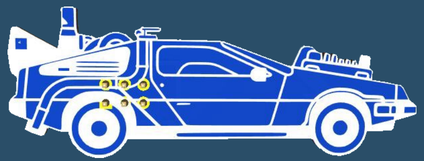
2020

2022

Badges

This Year (2023)





github.com/linted/CHV_SAO_Specification

Past Sponsors

CANBusHack

accenture

NXP

APTIV

ARGO AI

FCA

NMFTA
National Motor Freight Traffic Association, Inc.

GRIMM

DS

IntrepidCS

DELPHI

mazda

bugcrowd

NOVETTA

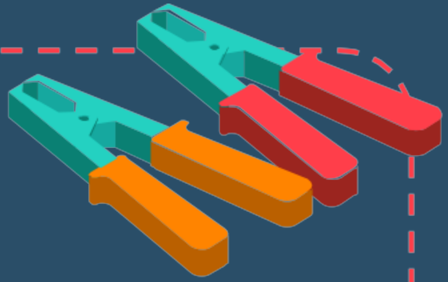
Motional

RAPID7

ETAS

ZOOX

Red Balloon Security



How to get involved?

- → Develop CTF flags / challenges or Volunteer
- → Attend DefCON 31 to access CHV
- → Attend other conferences to access CHV
- → Join our Discord
  - ◆ discord.gg/JWCcTAM
- → Sponsorship
  - ◆ Contact: jennifer@carhackingvillage.com

Contact Details

Email: justin@carhackingvillage.com

Website: carhackingvillage.com

Discord: discord.gg/JWCcTAM

Twitter: twitter.com/CarHackVillage

YouTube: youtube.com/@carhackingvillage

THANK YOU!

DISCOVER DEFEND

CAR HACKING VILLAGE

SECURING CRITICAL AUTOMOTIVE SYSTEMS

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 (19)

ArmorText
BlockHarbor
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

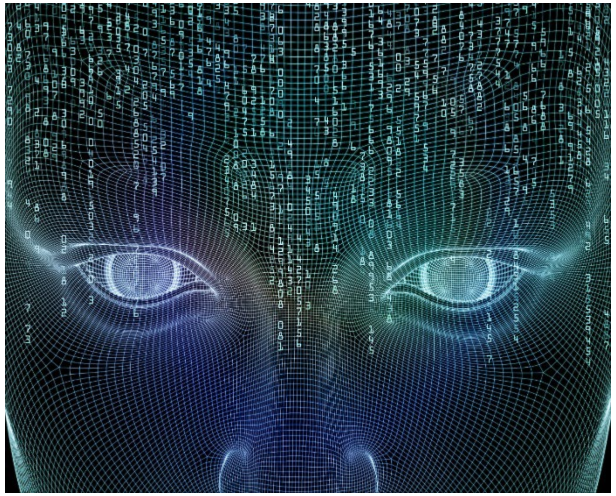
BENEFACTOR

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 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

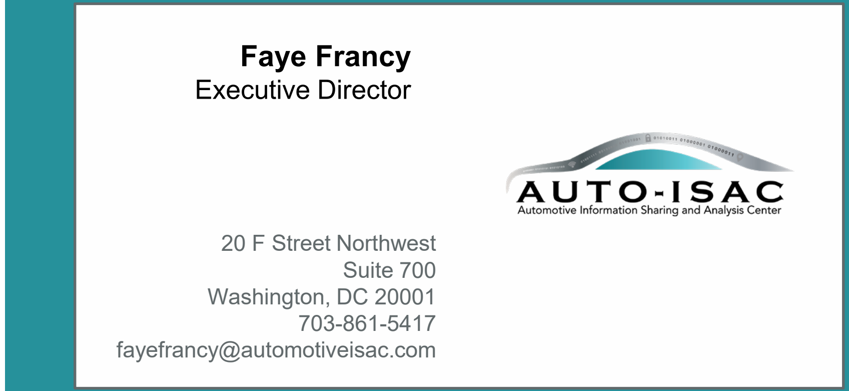


Building Resiliency Across the Auto Industry

Thank You

JUSPAXAR
OBRIGADO
MATONDO
KIA ORA
SALAMAT
MAAKE
KIITOS
MULTUMESC
MOCHCHAKKERAM
TERMA KASIH
RAIBH MAITH AGAT
CHOKRANE
SALAMAT
GRAZIE
MULTUMESC
MERCI
CAM ON BAN
RAIBH MAITH AGAT
MERCI
MERCI
MOCHCHAKKERAM
THANK
OBRIGADO
MOCHCHAKKERAM
GRAZIE
ASANTE
CHOKRANE
MATUR NUWUN
UA TSAUG RAU KOJ
MOCHCHAKKERAM
MATONDO
WELALIN
YOU
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
OBRIGADO
DANK JE
RAIBH MAITH AGAT
VINAKA
NIRRINGRAZZJAK
MAMANA
SPASIBO
SPASIBO
ARIGATO
KIITOS
MAAKE
DANKON
MULTUMESC
OBRIGADO
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO

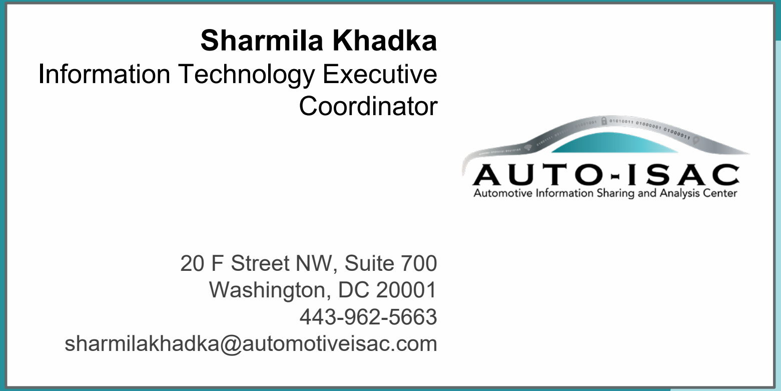
Our Contact Info



Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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



Sharmila Khadka
Information Technology Executive
Coordinator

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM