



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

February 3, 2021



Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ Christopher Church, <i>Senior Mobile Forensic Specialist</i>, INTERPOL Global Complex for Innovation▪ Kamel Ghali, <i>Automotive Security Architect</i>, White Motion (Marelli)
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!



Welcome

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

Engaging

❖ 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!

21
OEM Members

19
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

37 *Supplier & Commercial Vehicle Members*

12
Innovator Partners

*Membership represents **99%** of cars on the road in North America*

*Coordination with **26** critical infrastructure ISACs through the National Council of ISACs (NCI)*

2021 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)



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



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



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



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



Todd Lawless
*Chair of the
Advisory Board*
Continental

2021 ADVISORY BOARD (AB) LEADERSHIP



Todd Lawless
*Chair of the
Advisory Board*
Continental



Brian Murray
*Vice Chair of the
Advisory Board*
ZF



Chris Lupini
Chair of the SAG
Aptiv



Larry Hilkene
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF FEBRUARY 1, 2021

Highlighted = Change

Aisin	Honda	PACCAR
Allison Transmission	Hyundai	Panasonic
Aptiv	Infineon	Polaris
Argo AI	Intel	Qualcomm
AT&T	Kia	Renesas Electronics
Blackberry Limited	Knorr Bremse	Subaru
BMW Group	Lear	Sumitomo Electric
Bosch	LGE	Tokai Rika
Continental	Magna	Toyota
Cummins	MARELLI	TuSimple
Delphi Technologies	Mazda	Valeo
Denso	Mercedes-Benz	Veoneer
FCA	Mitsubishi Motors	Volkswagen
Ford	Mitsubishi Electric	Volvo Cars
Garrett	Mobis	Volvo Group
General Motors	Navistar	Waymo
Geotab	Nexteer Automotive Corp	Yamaha Motors
Google	Nissan	ZF
Harman	NXP	
Hitachi	Oshkosh Corp	TOTAL: 58

Auto-ISAC Update:

➤ *Members Only:*

- 2021 Summit Task Force launched on January 20. **Summit planning begins!!**
- Information Technology / Operations Technology Working Group (IT/OT WG) launched!
- Auto-ISAC Europe 2021 Workshop & Collaboration with Members, held at **TLP:AMBER** on **Tuesday, February 23 from 13:00 – 17:00 CET (7:00 a.m. – 11:00 a.m. ET)**

➤ *ALL Community:*

- Auto-ISAC Annual Report **TLP:GREEN** to be released in February!
- October 13-14, 2021: *Auto-ISAC Annual Cybersecurity Summit* – 8:00a.m. – 5:00 p.m.



Automakers Must Continue to Utilize and Improve Defense-in-Depth Approaches in the Design and Implementation of Embedded Devices

- ***Implement common best practices such as those outlined in Auto-ISAC Security Development Lifecycle Best Practice Guide, SAE, NHTSA, OWASP, NIST, etc.***
- ***Remove unnecessary debugging or maintenance functionality (JTAG, USB, Uboot, Etc)***
- ***Leverage code signing to protect against firmware manipulation***
- ***Leverage encryption wherever possible to protect sensitive information and increase difficulty of reverse engineering***
- ***Perform static and dynamic code analysis to identify bugs and vulnerabilities in software***
- ***Perform security testing throughout development***

Rooting Bosch Icn2kai Headunit

My Nissan Xterra came with a (for the time) modern head unit that has a touch screen, built-in navigation, backup camera display, multimedia features and smartphone connectivity. Wouldn't it be neat if we were able to get code execution on the device and even develop extensions and apps of our own? I will share the code to reproduce this on your vehicle and a sample application that achieves the GPS data logging goal.

Hacking a Harley's Tuner (Part 1) (Part II)

The model studied here is a Power Vision for Harley Davidson, by Dynojet

TLDR

- Buffer overflow in proprietary file exchange protocol: control of Program Counter, hard to reach a code execution because of input validation
- Command execution function left in the code, likely for debug purposes
- Firmware encryption keys, log encryption keys, and root password uncovering

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – Current Activity – CISA Releases New Alert on Post-Compromise Threat Activity in Microsoft Cloud Environments and Tools to Help Detect This Activity

- APT actor seen by CISA using compromised applications in a victim's (M365)/Azure environment and using additional credentials and API access to cloud resources of private and public sector organizations
- Details captured in AA21-008A describe follow-on activity to what was previously detailed in AA20-352A
- Resource:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/01/08/cisa-releases-new-alert-post-compromise-threat-activity-microsoft](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/01/08/cisa-releases-new-alert-post-compromise-threat-activity-microsoft)



TLP: WHITE – Current Activity – Attackers Exploit Poor Cyber Hygiene to Compromise Cloud Security Environments

- **CISA is aware of several recent successful cyberattacks against various organizations' cloud services**
- **Tactics and techniques used include phishing and brute force logins, to attempt to exploit weaknesses in cloud security practices**
- **Technical details and indicators of compromise included in CISA Analysis Report AR21-013A**
- **Resource:**
 - **[https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/01/13/attackers-exploit-poor-cyber-hygiene-compromise-cloud-security](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/01/13/attackers-exploit-poor-cyber-hygiene-compromise-cloud-security)**



TLP: WHITE – CISA Activity Alert AA21-008A – Detecting Post Compromise Threat Activity in Microsoft Cloud Environments

- **AA21-008A is a companion alert to AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector**
- **Addresses activity that CISA attributes to an APT actor that's been observed to use compromise applications in a victim's Microsoft 365 (M365)/Azure environment**
- **The APT actor has also been seen to use additional credentials and API access to cloud resources of public and private sector organizations**
- **Resources:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-008a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-008a)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa20-352a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-352a)



TLP: WHITE – CISA Analysis Report AR21-013A – Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services

- Addresses threat actors' use of phishing and other vectors to exploit poor cyber hygiene practices within a victims' cloud services configuration
- Describes identified tactics, techniques, and procedures (TTPs) and provides indicators of compromise (IOCs)
- Provides recommended mitigations to strengthen cloud environment configurations to protect against, detect, and respond to potential attacks.
- Resources:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/analysis-reports/ar21-013a](https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar21-013a)
 - [https://us-cert\[.\]cisa\[.\]gov/sites/default/files/publications/AR21-013A.stix.xml](https://us-cert[.]cisa[.]gov/sites/default/files/publications/AR21-013A.stix.xml) (STIX-formatted IOCs)



TLP: WHITE – CISA Malware Analysis Report AR21-027A/MAR-10319053-1.v1 - Supernova

- AR21-027A provides detailed analysis of several malicious artifacts, affecting the SolarWinds Orion product, identified by FireEye as Supernova
- The report describes the analysis of a PowerShell script that decodes and installs SUPERNOVA, a malicious webshell backdoor
- Resources:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/01/27/cisa-malware-analysis-supernova](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/01/27/cisa-malware-analysis-supernova)
 - <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a>
 - [https://us-cert\[.\]cisa\[.\]gov/sites/default/files/publications/MAR-10319053-1.v1.WHITE_stix.xml](https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10319053-1.v1.WHITE_stix.xml) (IOCs)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA Newsroom - [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 Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - [https://www\[.\]us-cert\[.\]gov/resources/ncats/](https://www[.]us-cert[.]gov/resources/ncats/)
- CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)
- CISA COVID-19 Response – [https://www\[.\]cisa\[.\]gov/coronavirus](https://www[.]cisa[.]gov/coronavirus)





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

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



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*



Slides available on our website – www.automotiveisac.com



FEATURED SPEAKER



CHRISTOPHER CHURCH, INTERPOL

SENIOR DIGITAL FORENSIC SPECIALIST



Chris Church is a Senior Forensics Specialist for INTERPOL and its 194 member countries.

Chris is assisting 194 member countries with the challenges they face in new technologies and the implications for law enforcement.

As part of this role, he has been coordinating with member countries their interest in connected vehicles and the implications for law enforcement.

As part of this work, he has hosted alongside member countries several meetings exploring the issue and assisting in finding solutions and compromises for law enforcement and the motor industry.

Chris has also published the INTERPOL Framework for a Drone Incident for First Responders and Digital Forensics Specialists and hopes that similar work can be achieved in the law enforcement and motor industry to help both private industry and law enforcement understand the issues, challenges and potential solutions in this emerging area.

KAMEL GHALI, WHITE MOTION


AUTOMOTIVE SECURITY ARCHITECT, WHITE MOTION (MARELLI)



Kamel Ghali is a veteran of the automotive cybersecurity community, having spent over 3 years as an expert car hacker, technical trainer, and contributor to worldwide industry-focused communities such as the SAE, ASRG, and the Car Hacking Village. His particular areas of focus within vehicle security are IVN, Bluetooth, RF, and in-vehicle networks.

He currently works at White Motion – subsidiary of the global automotive supplier, Marelli – where he leads the vehicle security research team, assessing vehicle systems and training customers in state-of-the-art car-hacking techniques.

He has presented at numerous security conferences and communities including DefCON, ASRG, GRIMMCon, and more – sharing his automotive security expertise with audiences of every background.



Crossroads Of Motor Vehicle Data: Digital Forensics And Cyber Threats

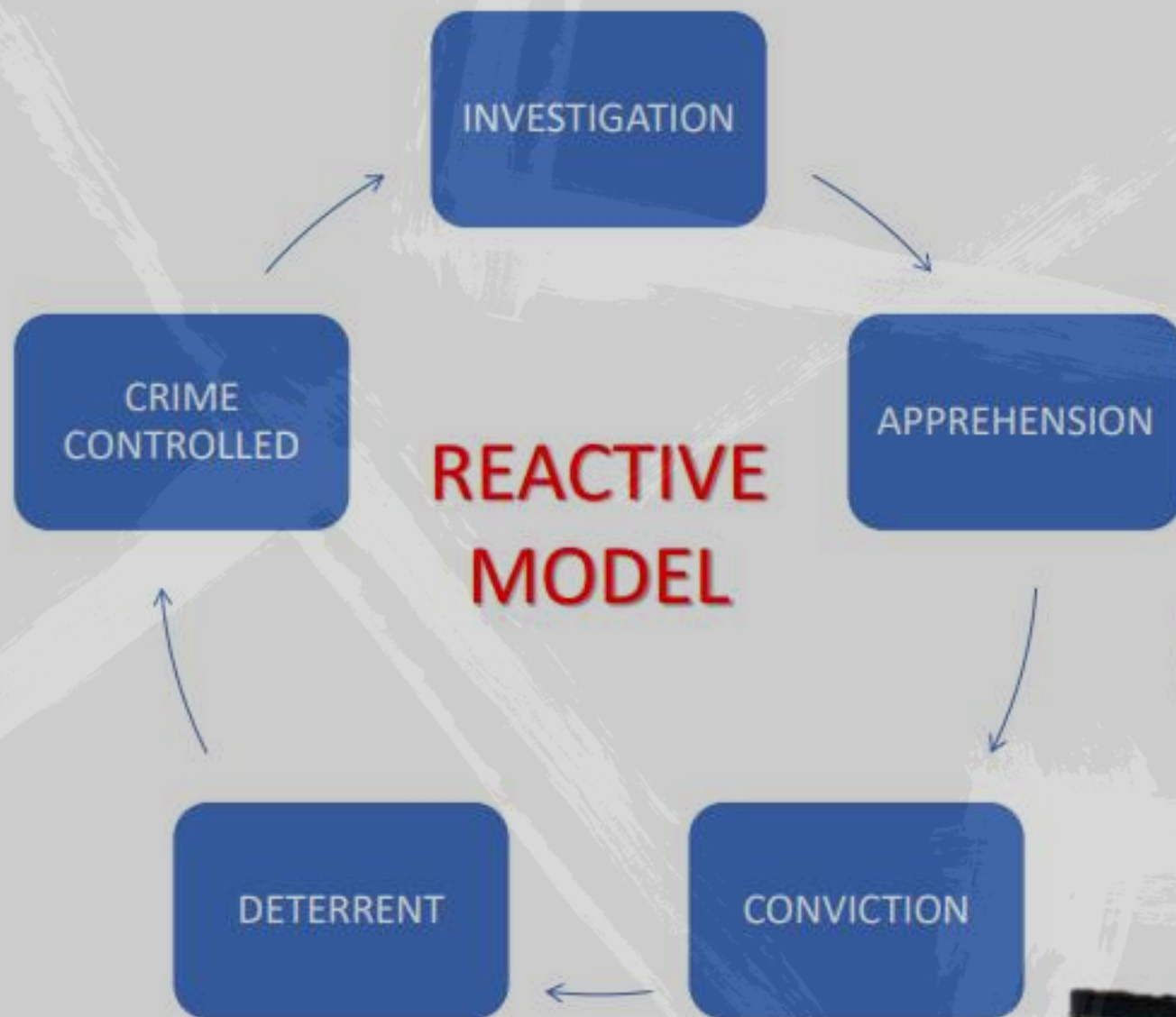
Chris Church

Senior Forensic Specialist
INTERPOL

Kamel Ghali

Automotive Cybersecurity Technology Architect
Whitemotion

REAL WORLD CRIME SHAPED THE LAW ENFORCEMENT OF TODAY



REAL WORLD CRIME

CRIME SCENE DO NOT CROSS

Proximity

Limited Scale

Physical constraints

Patterns

MODERN REAL WORLD CRIME

No Proximity

Unlimited Scale

No Physical Constraints

No Pattern

POLICE LINE DO NOT CROSS

CASE EXAMPLE

A furious motorist killed a teenage moped rider after his prized Mustang car was slightly damaged.

Bradley Clifford, 24, drunkenly chased a scooter at nearly double the speed limit on the wrong side of the road after a bottle was thrown at his high-powered sports car.

He ploughed into Jahshua Francis, 19, and his 18-year-old pillion passenger Sobhan Khan following the pursuit through Enfield, north London, in the early hours of August 5 last year.

Mr Khan was sent flying into the air, landing by a lamp-post in the street, fatally injured. Clifford got out and continued the attack, shouting at the teenager, saying he "deserved" it and punching him hard nine times, the Old Bailey heard.

It was "pure chance" that the victim's friend, Mr Francis, was not badly hurt in the crash, jurors were told. Before the killing, Clifford threatened to put a knife down the throats and "rain hell" on anyone who interfered with his beloved Mustang in a WhatsApp message to his girlfriend

The car telematics as well as the moped electronics was examined and they were able to recreate the drivers action leading up to the accident.

News

Mustang owner drove at and killed teenager after bottle thrown at his prized car



Save



Before the killing, Bradley Clifford threatened to 'rain hell' on anyone who interfered with his beloved Mustang. CREDIT: METROPOLITAN POLICE/PA

Follow

By Telegraph Reporters

4 MAY 2018 • 3:38PM

A

furious motorist killed a teenage moped rider after his prized Mustang car was slightly damaged.

Life of a Modern Motor Vehicle



Motor Vehicles have a life span of 5-15 years

Generates up to 25 GB data/hour

Connectivity – Bluetooth, Wi-Fi and Mobile Data plus Cloud

With all the elements connected a motor vehicle becomes a prime target for hackers and criminal enterprise:

- Key fob Hacking
- Hacking odometers
- Hacking interfaces
- Hacking road infrastructure and vehicle behaviour
- Hacking components
- Stealing data for ransom or intelligence



Remote Key Fob Relay Attack has created a new wave of Car Criminals

- easy and quick to initiate
- No expertise required – YouTube University
- Difficult to overcome
- 15 year timeline for security
- Negative Publicity
- Owners may come to harm during car theft



100M CAR

100+ ECUs

Different hardware architecture

Different computation and storage capability

Ever increasing software complexity

100M+ lines of code

No central repository

Missing vehicle knowledge management

Missing dependency resolvers



100M ECU

Multiple Firmware versions

Per Firmware dependencies

Inter-module dependencies

100+ Vendors

Different Software development cycle

Increasing system complexity

More independent software suppliers

Organization structure not suitable to run SW development

THREE DATA SETS AVAILABLE ON A VEHICLE



VEHICLE DATA



TELEMATICS



INFOTAINMENT

KEY EVIDENCE DATA SETS



Connected Devices



Location Data



Vehicle Events





Connected Devices

Identify devices that have been connected to a vehicle via Wi-Fi, Bluetooth and/or USB and all associated with those devices



Location Data

Recover location data and navigation information such as tracklogs, saved locations, active routes and previous destinations



Vehicle Events

See events associated with a vehicle such as doors opening/closing. Lights turning on/off.



ACQUISITION PROCESS



1. Identify



2. Acquire



3. Analyse



IMPORTANT CONSIDERATIONS

Strategy

Triage

What Vehicle do I have?

What systems does it contain?

What data types am I after?

What value could it add to other digital strategies?

What data is Law Enforcement Really Interested in?



View information about devices that have been connected to a vehicles USB Port, WiFi and Bluetooth.



Identify devices that have been connected to a vehicle via Wi-Fi, Bluetooth and/or the USB and all of the data associated with those devices



Recover location data and navigation information such as track logs, saved locations, active routes and previous destinations



Parse data from applications installed on the infotainment system like traffic, weather, Facebook, Twitter, Pandora, Yelp and Bing.

See events associated with a vehicle such as doors opening/ closing and lights turning on/ off locations and timestamps.



VEHICLE DATA

- What data can be pulled from a vehicle?

IT DEPENDS

Why? Make/Model of Car

Why? Year of Manufacture

Why? Trim level within model range

How do I find the answers?

Solution 1: VIN Number

Solution 2: Manufacturer Data Sheet

Solution 3: Internet Research

Solution 4: Digital Forensic Expert

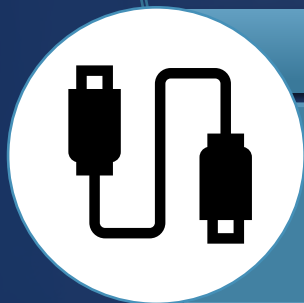
Network





IDENTIFY

Investigators identify the need for motor vehicle forensics based on identification of vehicle, systems installed and types of data required to assist case



ACQUIRE

Specialist identify the method to acquire the system data by locating the modules that contain the data and their location within the vehicle and how to connect and acquire the data



ANALYSE

Examiners review and analyse the data from the acquisition and identify key data of interest and verify the data





DIRECT CONNECT

Remove the target system, disassemble it down to the PCB level and connect directly to it



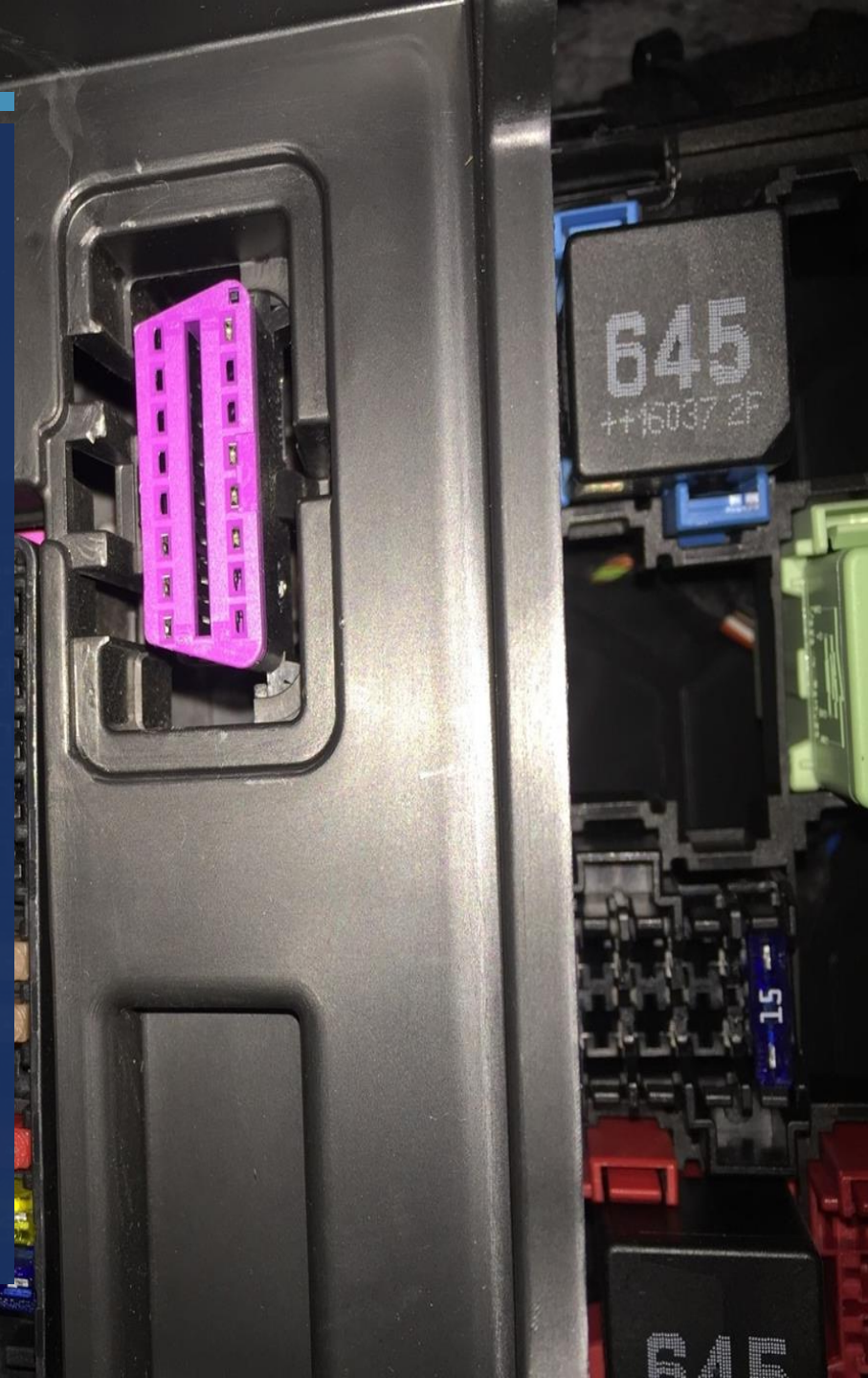
MEDIA

Custom cable that connects directly into the USB port of the centre console.



DIAGNOSTIC

Diagnostic port located within 1 meter of the steering column – known as the ODB2 port



WHAT

- Provide insight on the sequence of events that took place leading up to an incident
- Identify patterns of life and unusual events that happened around an incident
- Determine timeline of activity and establish a chain of events

WHERE

- Provide historical data to show where a vehicle was at specific times
- Identify areas frequently visited, new locations travelled or planned
- Determine how long particular locations were visited

WHO

- Provide unique identifiers that tie an individual to a specific vehicle
- Identify known associates and establish communication patterns between them
- Determine who may have been present or aware of key information during an incident





IS THERE
DIGITAL
FORENSIC
DATA
PRESENT
IN THIS
CAR?



Car Interior



Infotainment System





Infotainment Hard Drive



Infotainment Unit

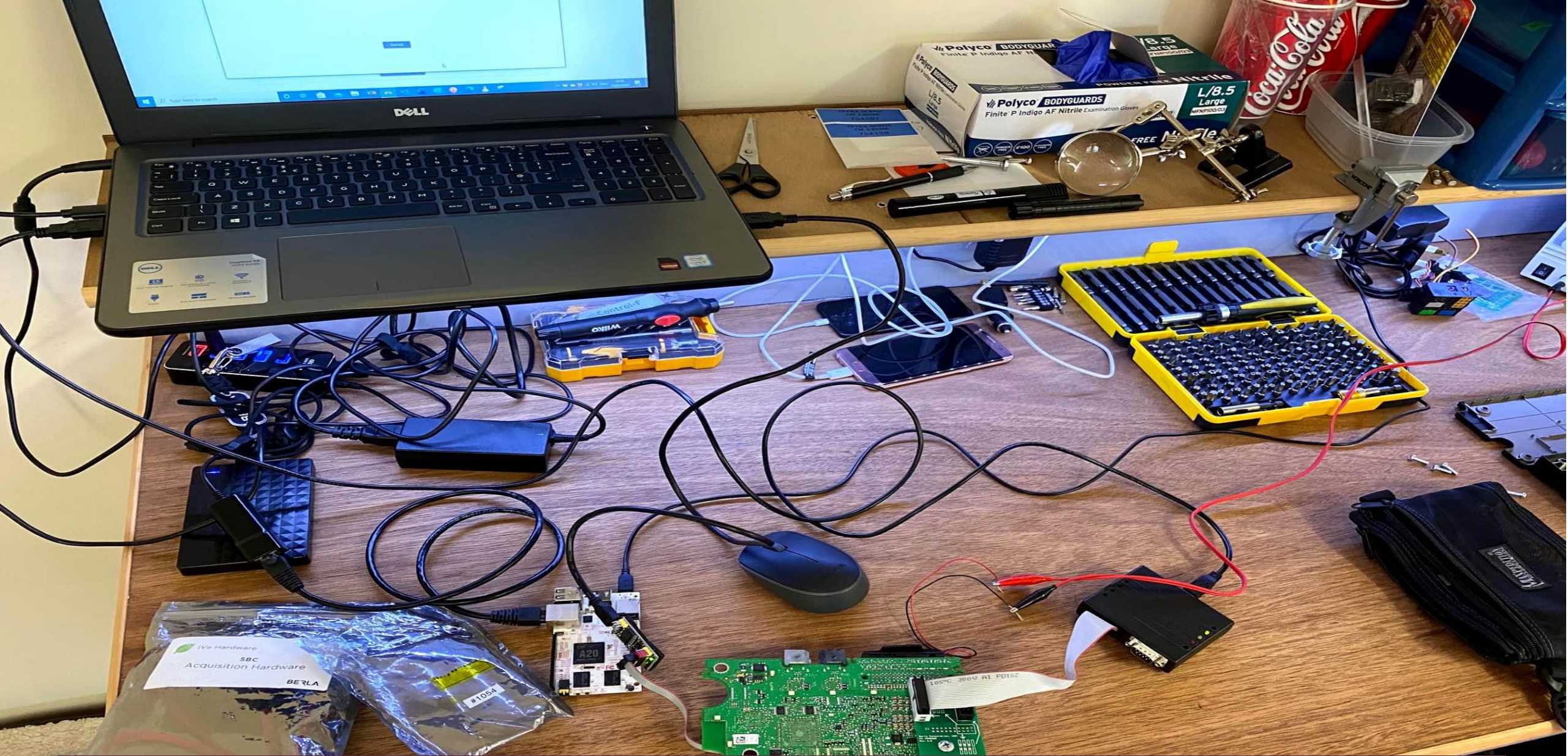


Infotainment Internally



A Car Interior Taken Apart for Access to ECU

Source: Harper Shaw Investigations



A Car ECU being examined in a DF lab



Digital Forensics



Cyber Threats/Forensics



As Stated,

- Uninformed

 - No training or knowledge surrounding novel automotive cybercrime

- Unequipped

 - Lack of tools and software to streamline investigations

- Unprepared

 - No systems or procedures in place to respond to automotive cybercrime

CYBERCRIME → REAL WORLD

■ Vehicle Theft

- More novel ways to steal vehicles through hacking/exploitation of weak technology implementations are constantly being discovered
 - Tesla Model X Key Fob Hack
 - Bluetooth, Lack of Signatures
- This is an example of a vehicle cybercrime that directly relates to something law enforcement is used to dealing with – stolen vehicles

Ready to unlock the target car...

fbf566f
60312

CYBERCRIME → NO REAL WORLD?

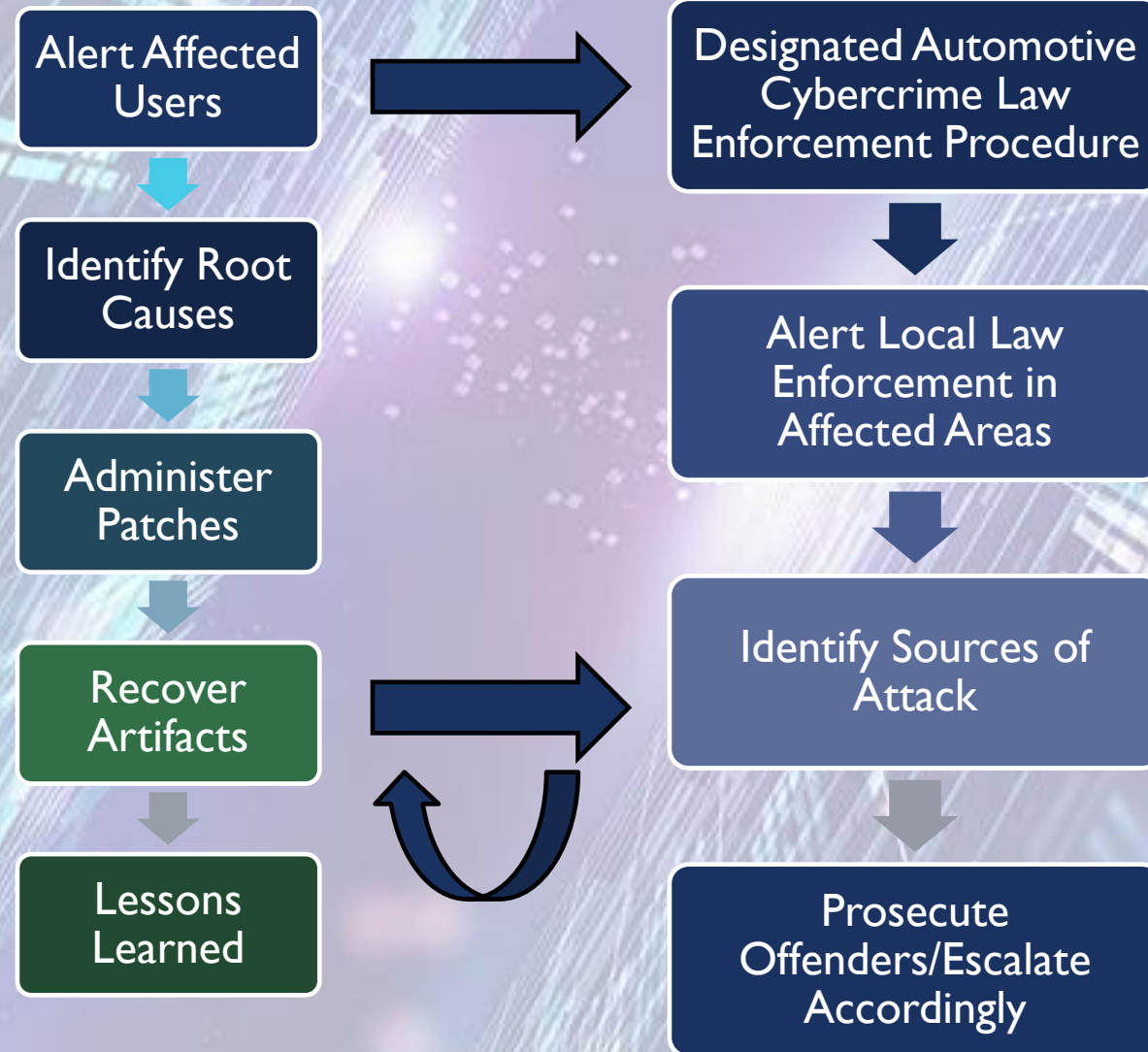
- ▶ While not as easily identified, cybercrime can manifest in ways that have no direct physical results – yet are devastating nonetheless
 - ▶ Spying/Covert surveillance
 - ▶ Ransomware
 - ▶ Identity theft
- ▶ Vehicles need timely detection mechanisms
 - ▶ Initiate law enforcement action
 - ▶ Initiate internal incident response

JOINT INCIDENT RESPONSE

- Industry incident response plans need to incorporate law enforcement
 - Prevention of Further Attacks
 - Protecting Victims from Legal Liability
 - Prosecution



JOINT INCIDENT RESPONSE



NECESSARY PRECURSORS

- ▶ Training for Law Enforcement
 - ▶ Awareness
 - ▶ Understanding
 - ▶ Technical Expertise
- ▶ Cooperation
 - ▶ Streamlined Exchange of Data
 - ▶ Appropriately Limited Scope
- ▶ Procedures
 - ▶ Proactive, not Reactively Implemented
 - ▶ CSMS, Local Regulations and Legislations
 - ▶ Practiced
 - ▶ Drills, Wargames

IN CONCLUSION

- ▶ Automotive Cybercrime is an Unprecedented Challenge for Law Enforcement
- ▶ Preemptive Industry Cooperation is Paramount
- ▶ Joint Incident Response
- ▶ Effective, Responsible Sharing of Data



THANK YOU

C.CHURCH@INTERPOL.INT

KAMEL.GHALI@WHITE-MOTION.COM

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 or Partnership,
please contact Auto-ISAC! fayefrancy@automotiveisac.com*

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partner

Solutions Providers

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

Examples: Hacker ONE, IOActive, Karamba, Grimm

INNOVATOR
Paid Partnership

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

Community Partners

Associations

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

Examples: Auto Alliance, ATA, ACEA, JAMA

NAVIGATOR
Support Partnership

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

Affiliations

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

Examples: NCI, DHS, NHTSA, Colorado State

COLLABORATOR
Coordination Partnership

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

Community

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

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

BENEFACTOR
Sponsorship Partnership

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

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

INNOVATOR

*Strategic Partnership
(12)*

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

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

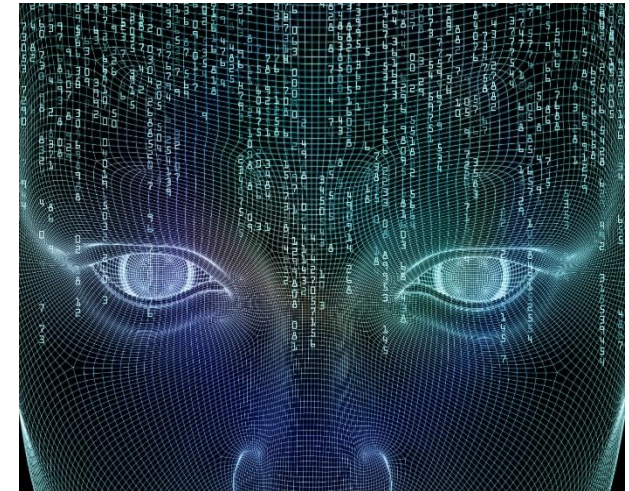
BENEFACTOR

*Sponsorship
Partnership*

2019 Summit Sponsors-
Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
Valimail

AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

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
Cordinator



20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com



www.automotiveisac.com
[@auto-ISAC](#)