Welcome to Auto-ISAC!

Monthly Virtual Community Call

October 4, 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:** ➢ **Brandon Barry, CEO, Block Harbor** ➢ **Niraj Kaushik, MD North America, VicOne** ➢ **Brian Gorenc, VP Threat Research Trend Micro** ➢ **Title: *"Pwn2Own for Automotive @ Automotive World Tokyo"***
11:55	**Q&A & Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ ***Stay informed of Auto-ISAC activities***
- ✓ ***Share information on key vehicle cybersecurity topics***
- ✓ ***Learn about exciting initiatives within the automotive community from our featured speakers***

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: TLP:GREEN - May be shared within the Auto-ISAC Community and "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!

(sharmilakhadka@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

AUTO-ISAC
Automotive Information Sharing and Analysis Center

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

30
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

46 *Supplier & Commercial Vehicle Members*

20
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 October 1, 2023

77 Members + 4 Pending

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

Pending: Amazon.com**,** Dana Inc, Phinia Inc, Stoneridge

**All times are in ET

Auto-ISAC Business Updates and Events

- **Community Call:** **Wednesday, November 1st Time:** ***11:00am – 12:00 p.m.*** **TLP:GREEN Speaker:** ***Adam Robbie, Senior Staff Researcher, Palo Alto Networks*** **Title:** ***"The Game of IT/OT Security: Unveiling New Critical Developments in Our Critical Infrastructure Threat Landscape"***

- **Auto-ISAC Summit will be October 17th-18th, 2023 in Torrance, California. We hope to see you there!**

- **Automotive Cybersecurity Training (ACT) Program: In person ACT Advanced courses have been rescheduled to Q1/Q2 2024, but ACT Fundamental courses are available on demand. Register: http://www.automotiveisac.com/act! Please email ACT@automotiveisac.com with any questions.**
  - **ACT Fundamental Course Block: Online, On-Demand, Anytime, Anywhere, and by Anyone $500/course**
  - **Cybersecurity Basics (32 hrs.) | Security Engineering (28 hrs.) | Security Operations/Management (22.5 hrs.)**

❑ **Advanced courses [New Dates]:**

- **Advanced Engineering: January 22 - 26, 2024**
- **Wireless: February 5 - 9, 2024**
- **EV and EV Infrastructure: March 4 - 8, 2024**
- **Guided Attacks: April 29 - May 4, 2024**

ACCELERATING CASE SECURITY

7th Annual Auto-ISAC Cybersecurity Summit

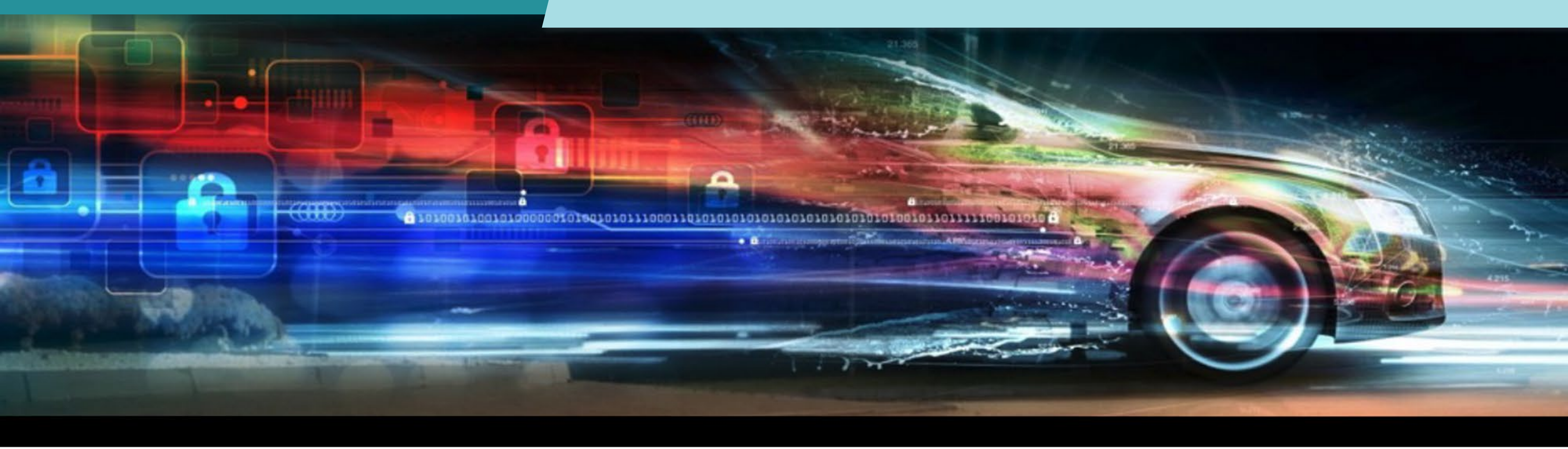
October 17-18, 2023

Torrance, CA

HONDA

The Power of Dreams

AUTO-ISAC



Auto-ISAC Intelligence Highlight

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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 (Russia-Ukraine [1], China [2], North Korea, Iran [3]); however, more signs of diplomacy observed.**
    - **Ransomware [4] Groups Targeting Automotive: ALPHV, Play, 8Base, Knight, Akira, Ransomhouse, LockBit 3.0, RA World**
    - **Security researchers targeted by North Korean cyber threat actors (Google)**
    - **Notable Resources: InfoCon[dot]org; ASRG Secure Our Streets Presentations.**
    - **Notable TTPs and Tools: Exploitation of Libwebp (The Hacker News); Credential Stuffing to Obtain Automotive Customer Data (Kasada); Exploitation of iOS Zero-Days (Securityweek, Securityweek); Exploitation of Apex One Zero-Day (Securityaffairs); Committing Fake Malicious Proof of Concept on GitHub (Unit 42); Uploading Malicious Packages to Software Repositories (SecurityWeek, Fortinet) Employing Stolen Microsoft Accounts in Ransomware Attacks (BleepingComputer); Malicious Modification of Router Firmware (CISA); Smishing and Voice Cloning (Retool); HijackLoader (Zscaler); ZenRAT (Proofpoint); BADBAZAAR, BADSIGNAL, BADSOLAR, IRONSQUIRREL (Volexity).**

CISA Resource Highlights

- Joint Cyber Defense Collaborative

Jeff Terra
10/4/2023

NSA, FBI, CISA, and Japanese Partners Release Advisory on PRC-Linked Cyber Actors

- The CSA details activity by cyber actors, known as BlackTech, linked to the People's Republic of China (PRC).

- The advisory provides BlackTech tactics, techniques, and procedures (TTPs) and urges multinational corporations to review all subsidiary connections, verify access, and consider implementing zero trust models to limit the extent of a potential BlackTech compromise.

- BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships to pivot from international subsidiaries to headquarters in Japan and the United States, which are the primary targets.

#StopRansomware: Snatch Ransomware

- The FBI and CISA are releasing this joint CSA to disseminate known ransomware IOCs and TTPs associated with the Snatch ransomware variant identified through FBI investigations as recently as June 1, 2023.
- Since mid-2021, Snatch threat actors have consistently evolved their tactics to take advantage of current trends in the cybercriminal space and leveraged successes of other ransomware variants' operations.
- Mitigations include:
  - Secure and closely monitor Remote Desktop Protocol (RDP)
  - Maintain offline backups of data
  - Enable and enforce phishing-resistant multifactor authentication

CISA Releases its Open-Source Software Security Roadmap

- CISA released an Open-Source Software Security Roadmap to lay out—in alignment with the National Cybersecurity Strategy and the CISA Cybersecurity Strategic Plan—how we will partner with federal agencies, open-source software (OSS) consumers, and the OSS community, to secure OSS infrastructure.

- The roadmap details four key goals:

  - Establish CISA's role in supporting the security of OSS
  - Understand the prevalence of key open-source dependencies
  - Reduce risks to the federal government
  - Harden the broader OSS ecosystem

Security/Software Updates

For September 2023:

- Apple Releases Multiple Security Updates
- Atlassian Releases Security Updates
- Fortinet Releases Security Updates
- Adobe Releases Security Updates
- Microsoft Releases Security Updates
- Mozilla Releases Security Updates
- CISCO Releases Security Updates
- VMWare Releases Security Updates
- Drupal Releases Security Guidance

- **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.
- For the period of 9/1/23- 9/30/23 approximately 35 advisories have been issued.
- Affected systems include Fujitsu Limited, Drover Fueling Solutions, Phoenix Contact TC Router, Rockwell Automation (multiple products), Siemens (multiple products), Omron Engineering, Real Time Automation, DEXMA DexGate and many others.
- For current ICS advisories please check CISA.gov regularly

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 23 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of September. 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*

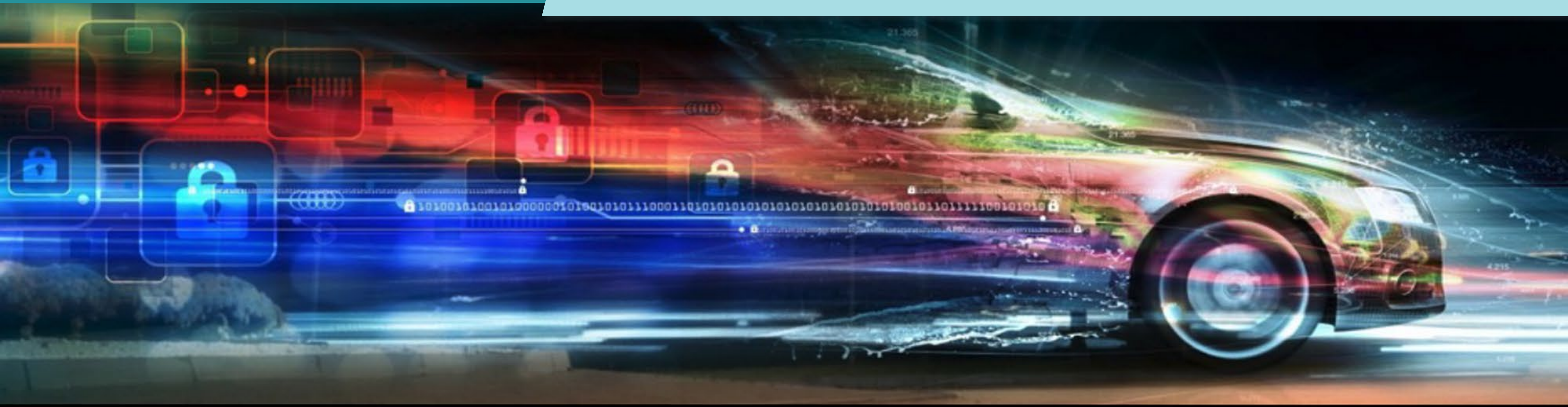
30+ *Featured Speakers to date*

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

Meet the Speaker

Brandon Barry

Brandon Barry is the CEO and founder of Block Harbor, a leading vehicle cybersecurity company that built the Vehicle Security Engineering Cloud, a platform to centralize, automate, and manage core activities in vehicle cybersecurity engineering. Spun out from Fiat-Chrysler and founded in 2014, Block Harbor's expertise is built on a decade of performing services with automakers, suppliers, and auditors in vehicle cybersecurity with our Vehicle Security Operations and Vehicle Cybersecurity Labs teams.

Brandon also leads the Americas for the Automotive Security Research Group (ASRG), a global non-profit focused on building a community for vehicle cybersecurity practitioners. With over 13,000 members and almost 50 chapters globally, the ASRG is the biggest community in vehicle cybersecurity.

On weekends, Brandon's passion for cars and their future bleeds into competitive drift racing, where he pilots a Ford Performance-powered Mustang all around the US.

Brandon has a bachelor's degree Computer Engineering with a research focus on Vehicle Cybersecurity from Brown University.

Meet the Speaker

Niraj Kaushik

Niraj Kaushik is the MD of North America operations and part of the leadership team at VicOne. He has decades of leadership experience in Engineering, Cybersecurity and IT leadership positions.

Niraj is passionate about cybersecurity, collaborating on community initiatives and building great relationships. In his spare time, he is a budding piano player, food and beverage enthusiast and loves fantasy fiction.

VicOne is the Automotive & EV charging cybersecurity subsidiary of global leader Trend Micro. VicOne’s mission is to make the Automotive world more secure through contextual intelligence and a collaborative platform approach.

Meet the Speaker

Brian Gorenc

Brian Gorenc is the Vice President of Threat Research at Trend Micro. In this role, he leads a globally dispersed research organization responsible for the delivery of comprehensive protection technology and threat intelligence to defend against sophisticated attacks.

Gorenc is also responsible for the Zero Day Initiative (ZDI) program, which represents the world's largest vendor-agnostic bug bounty program. The ZDI works to expose and remediate weaknesses in the world's most popular software. Brian is also responsible for organizing and adjudicating the ever-popular Pwn2Own hacking competitions.

His work led to the remediation of thousands of critical vulnerabilities in Microsoft, Adobe, Oracle, OSS, ICS/SCADA, IoT, embedded devices and automotive systems. He has presented at numerous security conferences such as Black Hat, DEF CON, Recon, OffensiveCon, and RSA.

Prior to joining Trend Micro, Gorenc worked for Lockheed Martin on the F-35 Joint Strike Fighter (JSF) program. In this role, he led the development effort on the Information Assurance (IA) products in the JSF's mission planning environment. In addition to degrees from Southern Methodist University and Texas A&M, Brian holds multiple certifications including (ISC)2's CISSP and CSSLP.

Pwn2Own Automotive

Exploit Intelligence for the Automotive Industry

Brandon Barry, *Block Harbor*

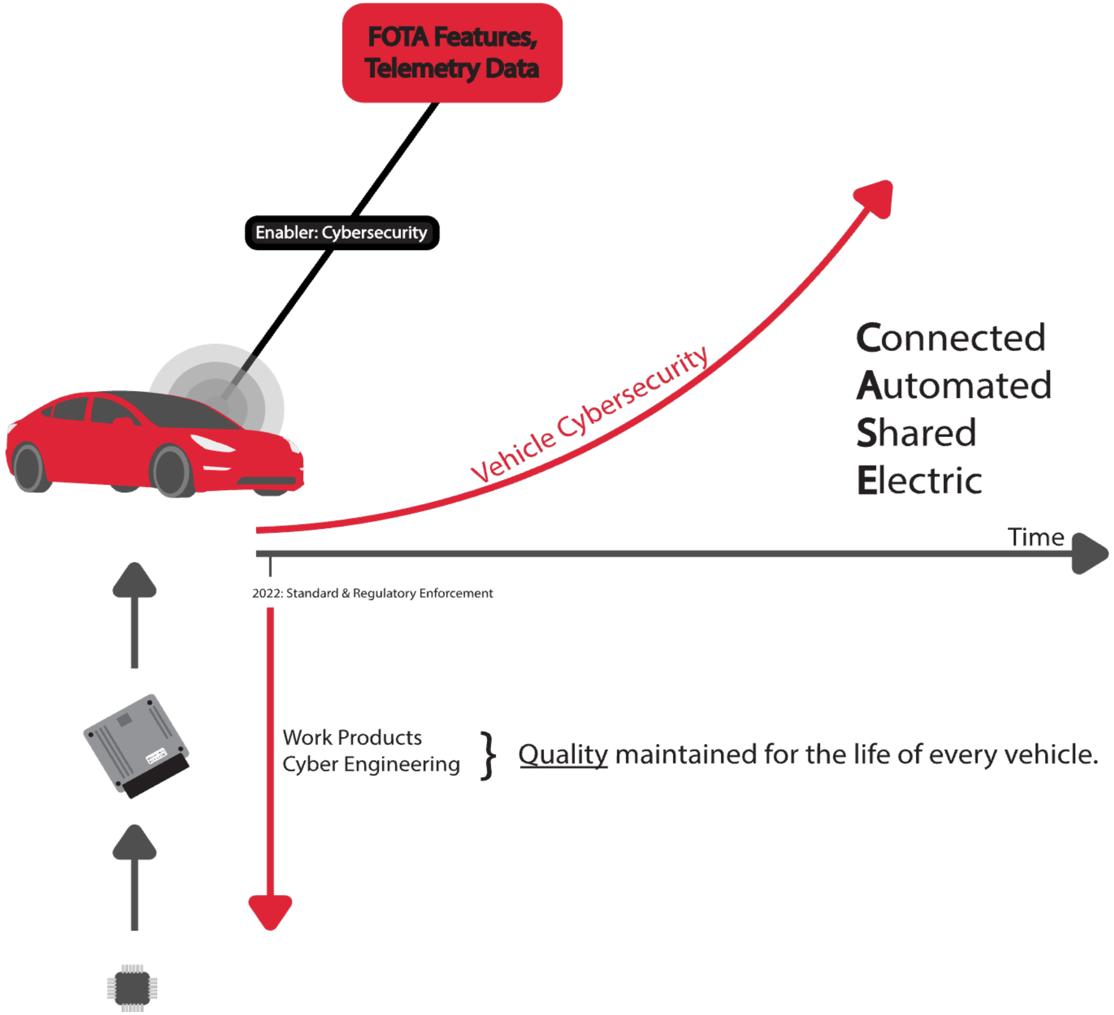
Niraj Kaushik, *VicOne Inc.*

Brian Gorenc, *Trend Micro Zero Day Initiative*

Why hackers hack.

Money & Clout

..let’s set nation-state aside.


FOTA Features, Telemetry Data
Enabler: Cybersecurity
Vehicle Cybersecurity
Connected
Automated
Shared
Electric
Time
2022: Standard & Regulatory Enforcement
Work Products
Cyber Engineering
} Quality maintained for the life of every vehicle.

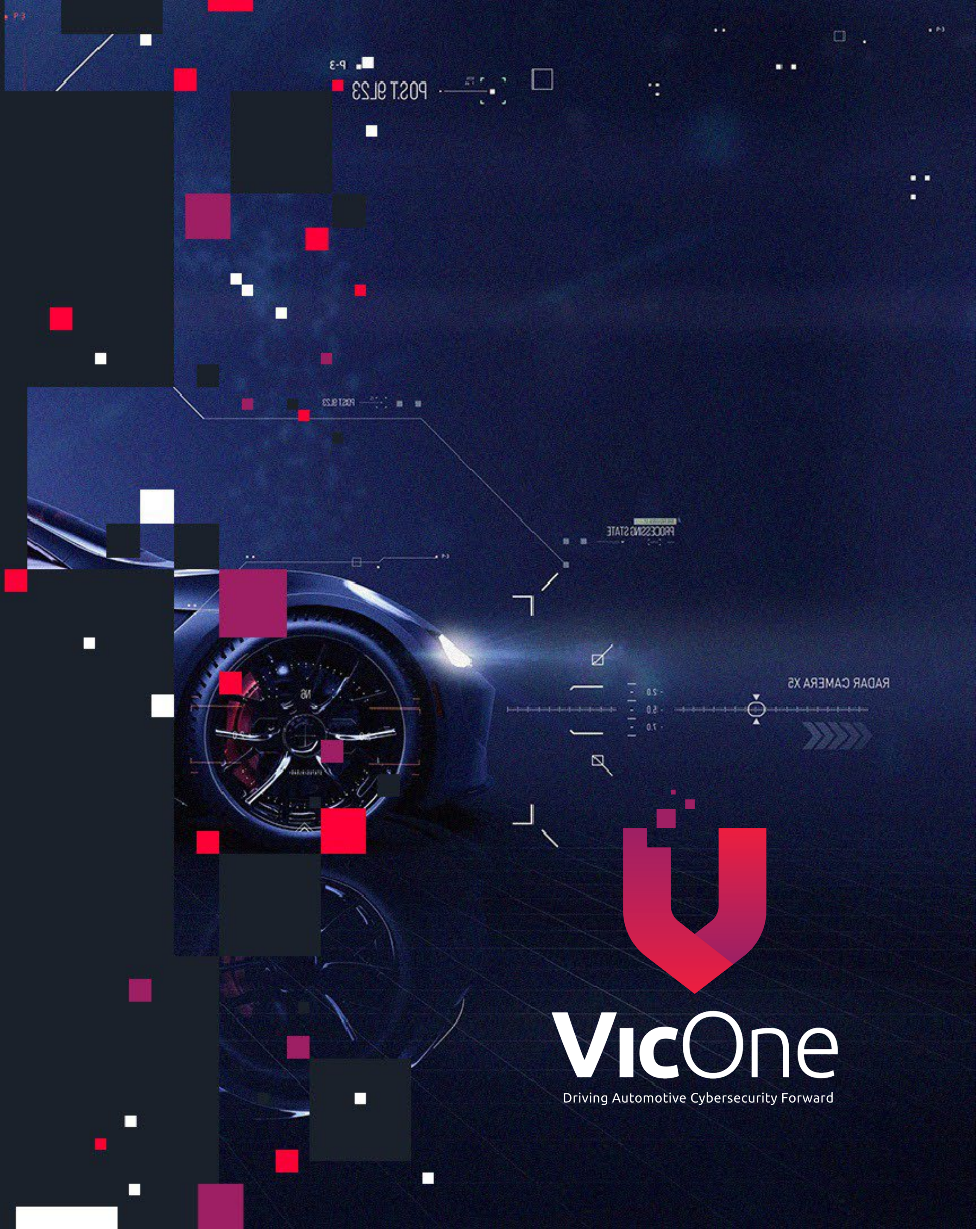
More

Money & Clout

To be had.

Vulnerability Disclosure Programs, Bug Bounties, and other existing white-hat research avenues still have challenges.

Why is VicOne spending all this money?



VicOne

Driving Automotive Cybersecurity Forward

The **Zero Day Initiative**

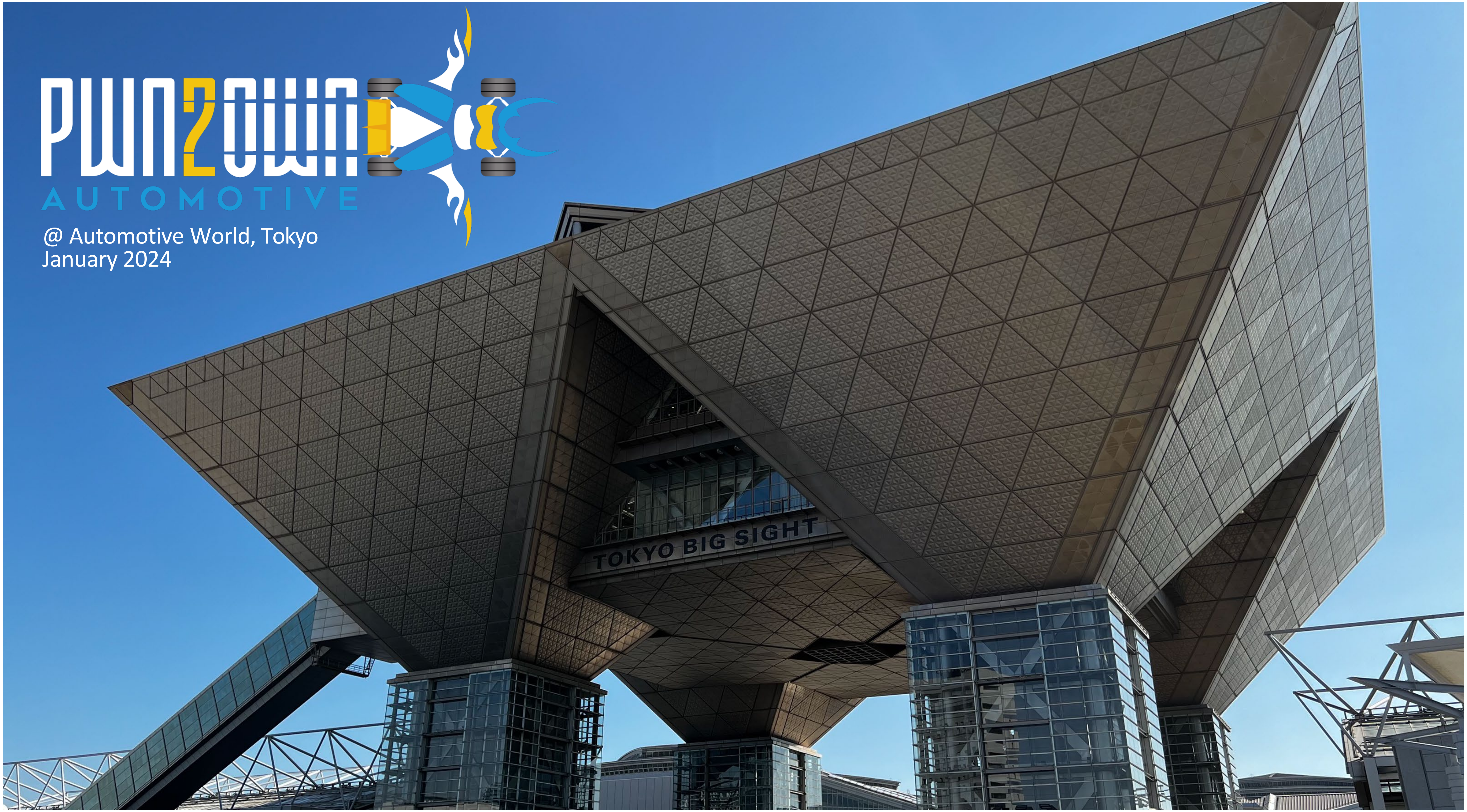
World’s largest vendor-agnostic bug bounty program

Purchase 0-day bugs from independent researchers around the globe

Threat intelligence provided across Trend Micro and VicOne

What is Pwn2Own?

Automotive Since 2019



PWN2OWN AUTOMOTIVE

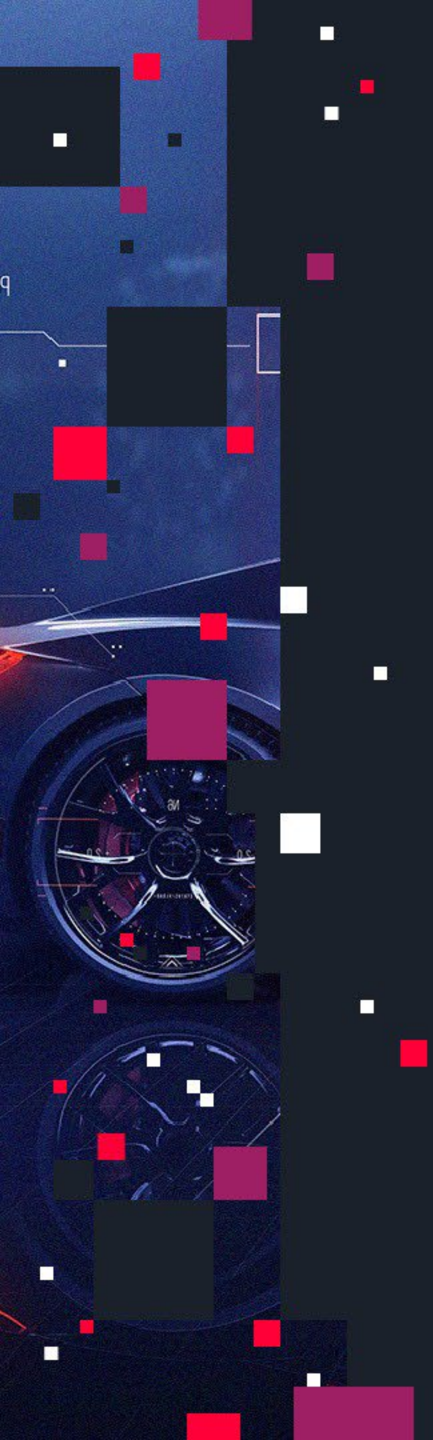
@ Automotive World, Tokyo
January 2024

Primary Goals

1. **Provide an avenue to encourage automotive research.**
   We want to offer a place where researchers can submit and be financially rewarded for reports targeting various products and platforms.

2. **Incentivize vendors to participate in the security research community.**
   We want to connect our global community of security researchers with automotive manufacturers to help improve their security and resiliency.

3. **Bring a focus to the sub-components of a vehicle.**
   Rather than looking at the vehicle as a monolithic unit, we want to bring attention to the multiple complex systems that comprise a modern automobile.



Tesla

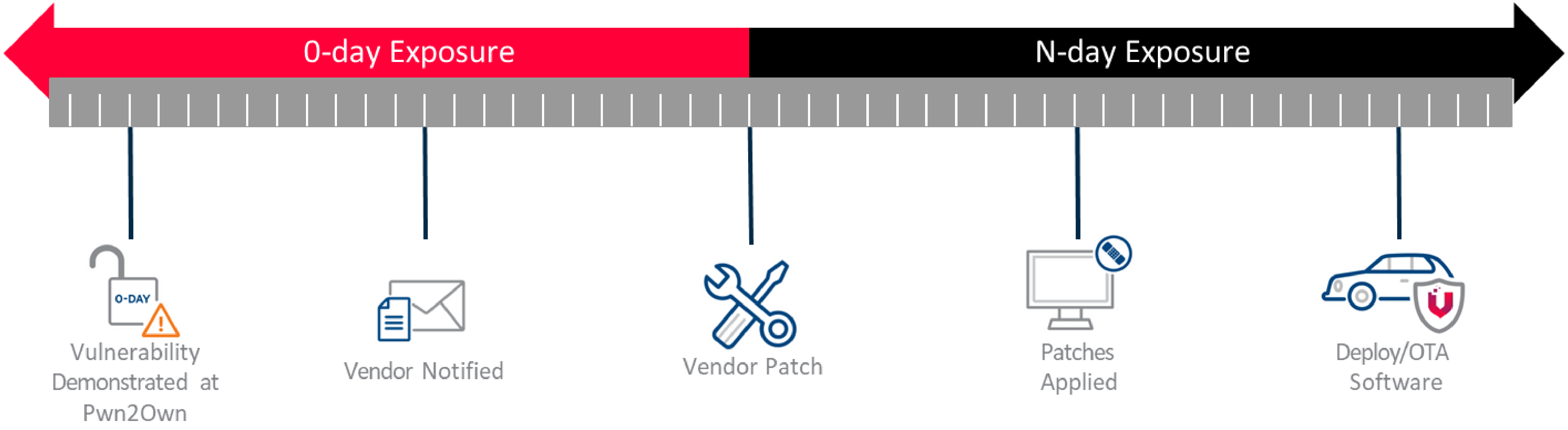
In-Vehicle Infotainments

EV Chargers

Operating Systems

https://www.zerodayinitiative.com/blog/2023/8/28/revealing-the-targets-and-rules-for-the-first-pwn2own-automotive

Vulnerability Handling



Share Lessons Learned with Auto ISAC

Get Involved!

Looking for vendors to join us

Help us identify which attack surfaces are used in the contest

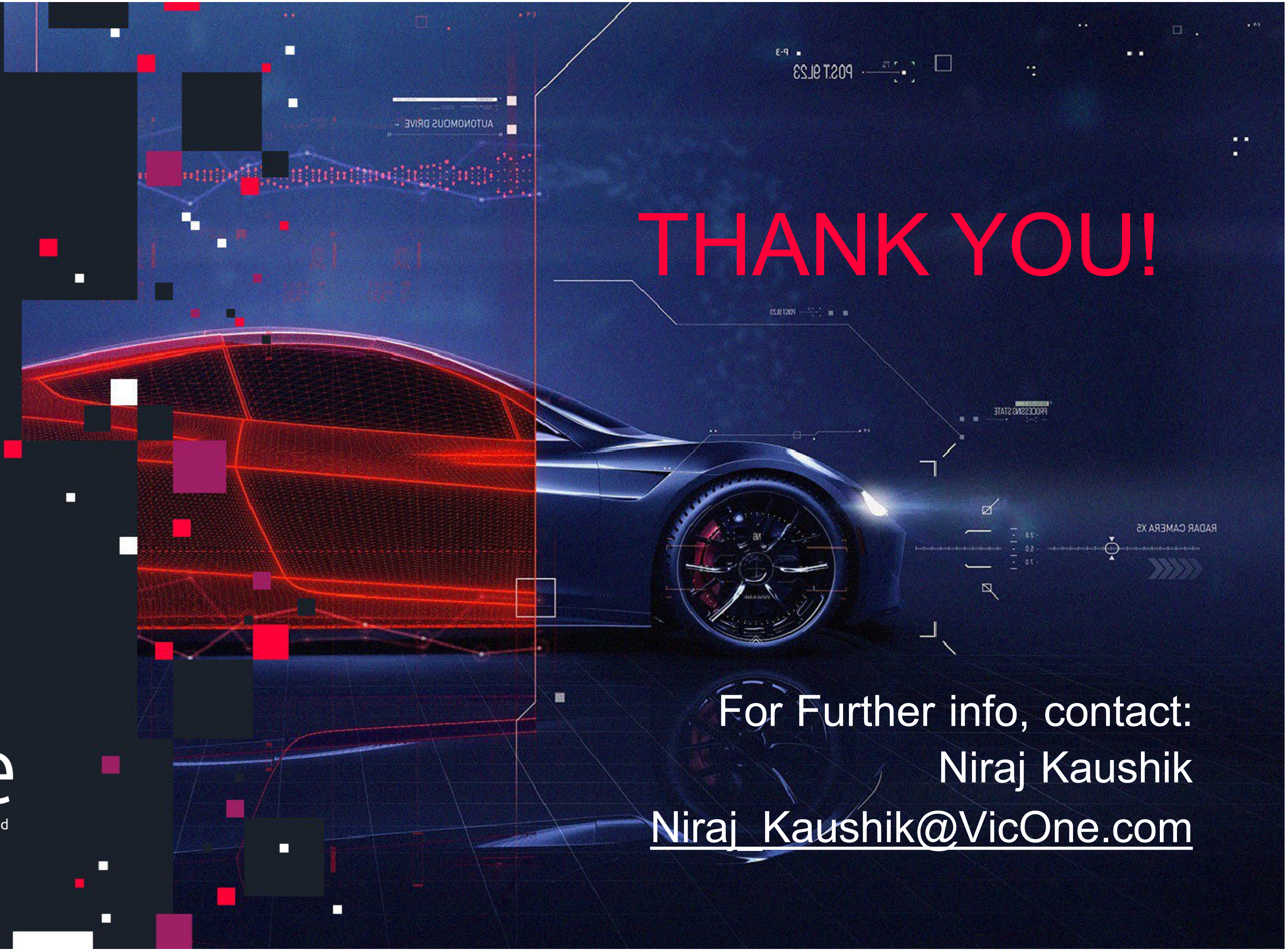
Guide and influence research in products

Encourage research into your technologies

Establish relationships with the research community

Waiving sponsorship fee for one Auto ISAC member

VicOne will cover the bounty costs!



THANK YOU!

For Further info, contact:
Niraj Kaushik
Niraj_Kaushik@VicOne.com

VicOne
Driving Automotive Cybersecurity Forward

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 and Partnership, please contact melissacromack@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 (20)

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
VicOne
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

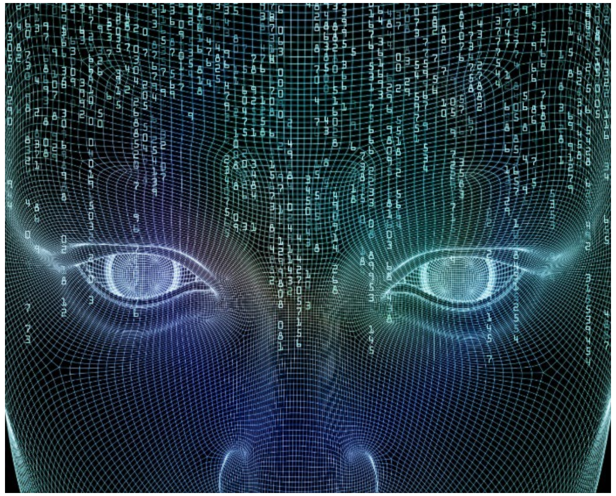
Sponsorship Partnership

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

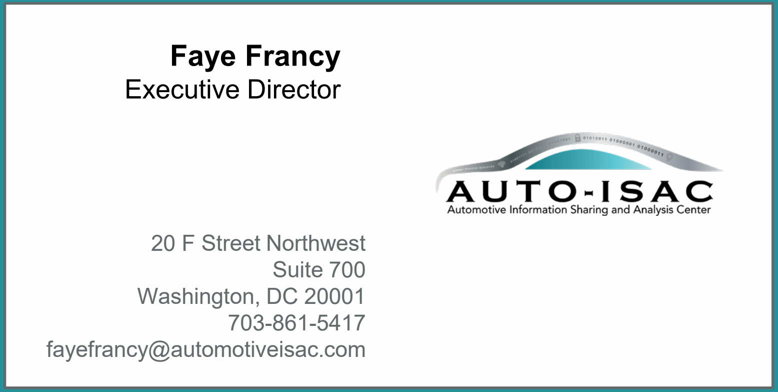


Building Resiliency Across the Auto Industry

Thank You

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

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM