



WELCOME TO AUTO-ISAC!





MONTHLY VIRTUAL COMMUNITY CALL

September 1, 2021

TLP:WHITE



DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

From: <https://www.us-cert.gov/tlp>

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ Ms. Kayle Giroud, <i>Partnership Associate Director, GCA</i>▪ Ms. Gill Thomas, <i>Director of Engagement, Capacity & Resilience Program, GCA</i>
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

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

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

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

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

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

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



❖ Participate

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

22
OEM Members

21
Navigator Partners

❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

41 *Supplier & Commercial Vehicle Members*

15
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)*



2020 - 2021 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)

**2022-2023
Elections coming!**



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

2020 - 2021 ADVISORY BOARD (AB) LEADERSHIP



Todd Lawless
*Chair of the
Advisory Board*
Continental



Michael Feiri
*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 SEPTEMBER 1, 2021

63 Members

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

BUSINESS ADMINISTRATION

➤ Members ONLY Activities: TLP:AMBER

- **Auto-ISAC Members Teaching Members:** Wednesday, September 15, 2021, 10-11:30 am ET
 - Todd Lawless, *Sr. Automotive Cybersecurity Specialist, Continental*
 - Presentation Title: *“A Tier 1 Perspective on Automotive Cybersecurity Operations”*

➤ Community Activities: TLP: GREEN

- **Community Call Speaker:** Wednesday, October 6th, 2021, 11-12 pm ET
 - Darrell Russell, *Director of Operations-Vehicles, National Insurance Crime Bureau (NCIB);*
 - Presentation Title: *“The National Insurance Crime Bureau: An overview and discussion about the state of vehicle theft”*

➤ Auto-ISAC Annual Cybersecurity Summit: TLP:WHITE

- Hybrid, October 13-14, 2021, 8:00 am – 5:00 pm
- GM Titanium Sponsor at RenCen, Detroit, MI
- Please REGISTER!!!



AUTO-ISAC CYBERSECURITY SUMMIT | OCT 13-14TH | HYBRID



**Event Host
Titanium Sponsor**

TAKE → CHARGE

SUMMIT
Oct. 13-14,
2021
Detroit | Virtual

Registration Open || Agenda & Themes on Website || Sponsor Prospectus on Website



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
- Know our strategic perception of and outlook for the cyber threat environment by reading the 2020 Threat Assessment in the Auto-ISAC 2020 Annual Report. The 2021 Annual Report and Threat Assessment are in production
 - Email us to request the report, provide feedback, or ask questions
- Intelligence Notes
 - Once vulnerabilities become public knowledge, the race is on for automotive organizations to assess and appropriately address risks before threat actors attack ([Cyware](#)).
 - Assess risk and, if necessary, appropriately address BadAlloc vulnerabilities ([CISA](#), [Microsoft](#), [MITRE](#), [Blackhat](#), [Blackberry](#)).
 - Other recent memory-related vulnerabilities ([IoTInspector](#), [Cisco Talos](#)).
 - Reminder: The Auto-ISAC exists to facilitate **timely** and **secure** sharing/exchange of cyber threat and vulnerability information among automotive organizations.
 - Monitor alliances (“Cartels”) among ransomware groups as they increasingly leverage each other’s infrastructure and notoriety to pressure victims to pay ransoms ([Darkreading](#), [BleepingComputer](#), [FireEye](#)).

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – CISA Industrial Control Systems Joint Working Group (ICSJWG) Fall Virtual Meeting – 20-21 September 2021

- **Registration to attend is required. Register by September 17, 2021 at [https://gateway\[.\]on24\[.\]com/wcc/eh/3049745/icsjwg-2021-fall-virtual-meeting](https://gateway[.]on24[.]com/wcc/eh/3049745/icsjwg-2021-fall-virtual-meeting)**
- **Current Activity entry for the ICSJWG meeting is at [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/08/27/icsjwg-2021-fall-virtual-meeting](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/08/27/icsjwg-2021-fall-virtual-meeting)**
- **ICSJWG resources are available at [https://us-cert\[.\]cisa\[.\]gov/ics/icsjwg-meetings-and-webinars](https://us-cert[.]cisa[.]gov/ics/icsjwg-meetings-and-webinars)**
- **Contact the ICSJWG team at [ICSJWG.Communications@cisa\[.\]dhs\[.\]gov](mailto:ICSJWG.Communications@cisa[.]dhs[.]gov) for more information**



TLP: WHITE – CISA National Cyber Awareness System (NCAS) Vulnerability Summaries

- **Bulletins are posted on a weekly basis that provide summaries of new vulnerabilities that are posted in the National Vulnerability Database (NVD)**
- **Details can include Common Vulnerability Scoring System (CVSS) scores (if assigned), identifying information, values, definitions, and related links**
- **Patch information is included when available**
- **Can sign up to have these bulletins sent to you via email, or sign up for the RSS feed**
- **See [https://us-cert\[.\]cisa\[.\]gov/ncas/bulletins](https://us-cert[.]cisa[.]gov/ncas/bulletins) for details and the weekly summaries**



TLP: WHITE – CISA Current Activity (CA) – Hurricane-Related Scams

- **CISA’s reminder to remain alert for malicious cyber activity targeting potential disaster victims and charitable donors following a hurricane**
- **Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks**
- **Be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events.**
- **See [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/08/21/hurricane-related-scams](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/08/21/hurricane-related-scams)**



TLP: WHITE – FBI-CISA Advisory on Ransomware Awareness for Holidays and Weekends

- **Joint cybersecurity advisory (CSA) released to urge organizations to ensure they protect themselves against ransomware attacks during holidays and weekends—when offices are normally closed**
- **The Joint CSA identifies both immediate and longer term actions organizations can take to protect against the rise in ransomware.**
- **Details at:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/08/31/fbi-cisa-advisory-ransomware-awareness-holidays-and-weekends](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/08/31/fbi-cisa-advisory-ransomware-awareness-holidays-and-weekends)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-243a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-243a)



TLP: WHITE – CISA Current Activity (CA) – CISA Provides Recommendations for Protecting Information from Ransomware-Caused Data Breaches

- Fact sheet introduced to address the increase in malicious cyber actors using ransomware against potential victims
- CISA encourages organizations to adopt a heightened state of awareness and implement the recommendations listed in the fact sheet to reduce their risk to ransomware and protect sensitive and personal information
- Resources at:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/08/18/cisa-provides-recommendations-protecting-information-ransomware](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/08/18/cisa-provides-recommendations-protecting-information-ransomware)
 - [https://www\[.\]cisa\[.\]gov/stopransomware](https://www[.]cisa[.]gov/stopransomware)



TLP: WHITE – CISA Current Activity (CA) – BadAlloc Vulnerability Affecting Devices Incorporating Older BlackBerry QNX Products

- CISA released Alert AA21-229A on August 17, issued update on August 23. Blackberry had also publicly disclosed the QNX Real Time Operating System was vulnerable to CVE-2021-22156
- Exploitation of this vulnerability could lead to a denial of service or arbitrary code execution in affected devices
- AA21-229A includes technical details and affected products
- See:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-229a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-229a)
 - [https://support\[.\]blackberry\[.\]com/kb/articleDetail?articleNumber=000082334](https://support[.]blackberry[.]com/kb/articleDetail?articleNumber=000082334)



TLP: WHITE – CISA Current Activity (CA) – Microsoft Azure Cosmos DB Guidance

- **Misconfiguration vulnerability identified in Azure Cosmos DB, which has been fixed within the Azure cloud**
- **CISA encourages Azure Cosmos DB customers to roll and regenerate their certificate keys and to review Microsoft’s guidance on securing access to data in Azure Cosmos DB**
- **See:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/08/27/microsoft-azure-cosmos-db-guidance](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/08/27/microsoft-azure-cosmos-db-guidance)
 - [https://docs\[.\]Microsoft\[.\]com/en-us/azure/cosmos-db/secure-access-to-data?tabs=using-primary-key](https://docs[.]Microsoft[.]com/en-us/azure/cosmos-db/secure-access-to-data?tabs=using-primary-key)
 - [https://msrc-blog\[.\]Microsoft\[.\]com/2021/08/27/update-on-vulnerability-in-the-azure-cosmos-db-jupyter-notebook-feature/](https://msrc-blog[.]Microsoft[.]com/2021/08/27/update-on-vulnerability-in-the-azure-cosmos-db-jupyter-notebook-feature/)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA NCAS – <https://us-cert.cisa.gov/>
- 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 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



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



KAYLE GIROUD, GLOBAL CYBER ALLIANCE

PARTNERSHIP ASSOCIATE DIRECTOR



Kayle Giroud is an experienced project management professional. She was trained in both public and private sectors, having worked on collaborative projects in multiple countries for the United Nations, the Swiss Federal Government, and various non-for-profit organizations. She is now Partnership Associate Director at the Global Cyber Alliance. With her background in international development, she has a culturally sensitive approach to problems with a response which is user-centric, solution-oriented and collaborative to generate growth and opportunities.

Kayle holds a MSc from Durham University in Defense, Development and Diplomacy and a PMP® certification.

In addition to her primary job functions, Kayle is dedicated to increasing access to culture by managing a networking platform for artists. She has also exhibited her own paintings in multiple art galleries in Europe.

GILL THOMAS, GLOBAL CYBER ALLIANCE

DIRECTOR OF ENGAGEMENT, CAPACITY & RESILIENCE PROGRAM



Gill joined GCA in June 2018 after spending her early career enjoying various roles within the telecommunications industry – through technical, sales and business development. After spending time out with her young family, she returned to a very different landscape whereupon she became increasingly fascinated by cybersecurity and the devastating impact cyber incidents have across global communities.

Gill is now Director of Engagement for the Capacity & Resilience Program. As such, she engages partners around a similar mission: protecting vulnerable communities against those intent on using the Internet for malicious gain, drive change, address systemic cyber risk and enable a secure and trustworthy Internet for all.

INTRODUCING GCA

Presentation to the Sep 1, 2021 Auto-ISAC Community Call

Alejandro Fernández-Cernuda, Gill Thomas, and Shehzad Mirza





GCA'S MISSION

FOUNDING MEMBERS



CITY OF LONDON
POLICE



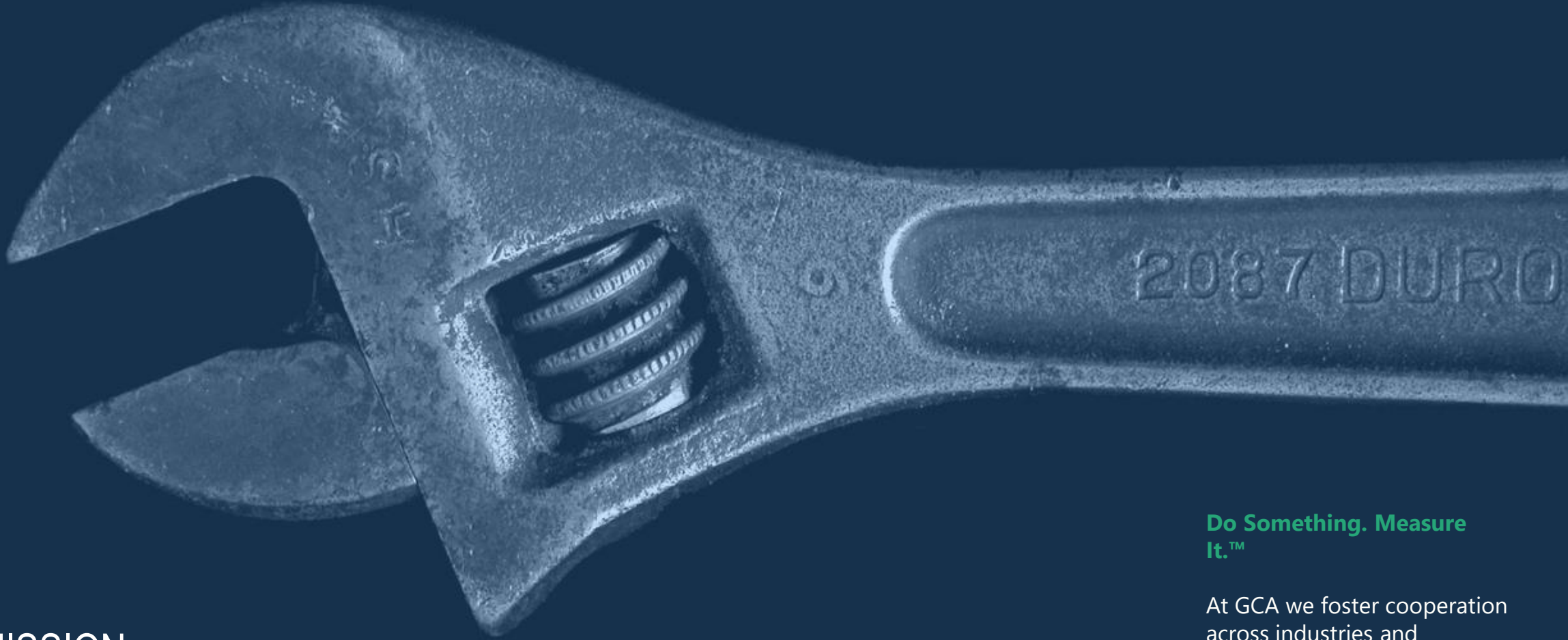
Center for
Internet Security®



GCA'S MISSION
A TRUSTWORTHY INTERNET

Enabling a Secure
and Trustworthy Internet

At GCA we build programs, partnerships, and tools to make the connected world safer and more secure for all.



GCA'S MISSION

MEASURABLE ACTION TO REDUCE CYBER RISK

**Do Something. Measure
It.™**

At GCA we foster cooperation across industries and governments. We build tools and develop programs that make a difference, and we make them available for free.



GLOBAL
CYBER
ALLIANCE™

GCA'S MISSION

ONE MISSION. TWO PATHS.



INTERNET INTEGRITY

AIDE - IoT, Domain Trust, Routing Security, Quad9.

Solutions at the systemic or infrastructure level, with the potential to scale worldwide.

CAPACITY & RESILIENCE

Cybersecurity Toolkits, DMARC.

Empowering communities, with a long-term view to creating demand for cybersecurity solutions.

GCA'S MISSION

ONE MISSION. TWO PATHS.

INTERNET INTEGRITY

AIDE - IoT, Domain Trust, Routing Security, Quad9.

Solutions at the systemic or infrastructure level, with the potential to scale worldwide.



CAPACITY & RESILIENCE

Cybersecurity Toolkits, DMARC.

Empowering communities, with a long-term view to creating demand for cybersecurity solutions.



GCA'S MISSION

ONE MISSION. TWO PATHS.



GLOBALLY APPLICABLE

Mapped to CIS, NCSC, NIST, ACSC

Addresses most common cyber threats – reducing risk by up to 85%

Tailored for different communities (Small Business, Journalists, Elections)

5 languages (English, French, German, Spanish, Indonesian)



GUIDED SELF-SERVICE TOOLKIT

Tools are straightforward to implement

Support via an online forum



ONE-STOP SHOP

Tools to implement. Policy templates to adopt. Checklists to use.

Videos and guides to explain. Courses to learn.

Community Forum to support.



IMPACT

In-country projects (ie Indonesia, Africa)

Specific sectors (non profit, financial, small business, journalist.)

500,000+ visits from 200+ countries

Cybersecurity Toolkits

Effective and vetted tools at no cost, to improve capacity to defend against cyber threats and build resilience

A Collaborative Effort

AIDE is a platform that enables automated collection, analysis, distribution, and display of attacks on IoT devices, as a means to ultimately implement mechanisms of distributed defense within the large IoT community (from manufacturers and researchers to smart cities and regulators).



COLLECTION

AIDE is fed by a mechanism that automatically collects IoT attack data from **honeyfarms** located in IP space around the world (including, GCA's, with hundreds of devices and data feeds from partners); **virtual IoT devices** on simulated networks; and **ProxyPots** distributed around the world, backed by real IoT devices and software.



ANALYSIS

The attack data is aggregated into a common analysis platform that can be used by researchers to study IoT attack signatures, patterns, and changes.



DISTRIBUTION

The data feeds will be made available to the ecosystem partners to enable mitigation of IoT attacks. Partners will be able to use the data as they wish.



DISPLAY

AIDE offers a real-time visualization of high-level results by means of a project-specific website.



ProxyPot

- AIDE also includes ProxyPot, a proprietary **honeypot** technology that can combine physical or virtualized IoT devices to build honeyfarms in a **scalable** and **flexible** way
- This effort was to fill the void in the industry for a platform that could enable defenders to emulate thousands of different IoT devices in a virtual environment distributed around the globe
- The technology is also compatible with other deception technologies and can be deployed in any environment, from smart cities to Industrial Internet of Things (IIoT) platforms

AIDE: Automated IoT Defense Ecosystem

THE PROXYPOT TECHNOLOGY

I SMART CITIES: endless opportunities; first full deployment to be announced soon

II POLICIES & STANDARDS: data-driven evidence to improve the rules of the game

III CONTINUOUS INNOVATION: NGI Explorers, new integration capacities...



IV AD-HOC DEPLOYMENTS: the Which? experiment, IIoT...

V RESEARCH: academia, research and industry groups...

VI FUNDRAISING: Horizon Europe and other large funding programs



AIDE & AUTOMOBILE

A BRILLIANT FUTURE AHEAD

THANK YOU

kgiroud@globalcyberalliance.org

<https://www.globalcyberalliance.org>



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.
For Partnership, please contact sharmilakhadka@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 that 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 or individuals 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
(15)*

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

2020 Summit Sponsors-

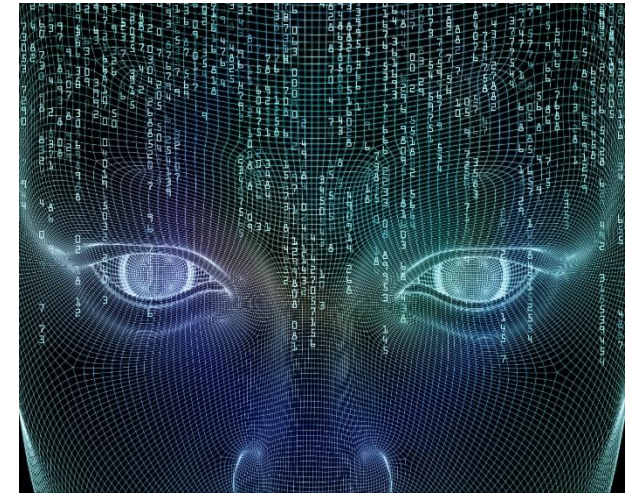
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

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

THANK YOU!



OUR CONTACT INFO

Faye Francy
Executive Director



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

Sharmila Khadka
Information Technology Executive
Coordinator



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



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