Welcome to Auto-ISAC!

Monthly Virtual Community Call

January 6, 2021

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 ➢ What’s Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ▪ David Turetsky, **Professor** of Practice at the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany (SUNY). ▪ Brian Nussbaum, **Assistant Professor** in the Department of Emergency Preparedness, Homeland Security and Cybersecurity ▪ Unal Tatar, **Assistant Professor** in the College of Emergency Preparedness, Homeland Security and Cybersecurity
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: The level of this meeting is **TLP:GREEN** - it may be shared within the Auto-ISAC Community and is “off the record”

How to Connect: For further info, questions or to add other POCs to the invite, please contact us! (lisascheffenacker@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!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ 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*

❖ 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*

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

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

2020 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

2020 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

[redacted]

Highlighted = Change

Member Roster

as of January 1, 2021

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

TOTAL: 58

TLP WHITE: Disclosure and distribution is not limited

AUTO-ISAC ACTIVITIES

Upcoming Key Events for January 2021:

- **January 13, 2021:** ***Auto-ISAC 2020 PIR Update Workshop*** – 9:00a.m. – 11:00a.m.

- **January 20, 2021:** ***Auto-ISAC ETSC Sponsored Event*** – Discussion on Risk Assessment Methodology for 21434 Compliance – 10:00 a.m. – 11:30 a.m.

  Featured Speakers Include:
  - Scott Sheahan, Aptiv
  - Tito Spinelli, ZF
  - Markus Tschersich, Continental
  - Bill Mazzara, FCA

- **October 13-14, 2021:** ***Auto-ISAC Annual Cybersecurity Summit*** – 8:00a.m. – 5:00 p.m.

Supply Chain Compromise is Increasingly Popular Among Cyber Threat Actors

Vietnam Targeted in Complex Supply Chain Attack

A group of mysterious hackers has carried out a clever supply chain attack against Vietnamese private companies and government agencies by inserting malware inside an official government software toolkit. The attack, discovered by security firm ESET and detailed in a report named "Operation SignSight," targeted the Vietnam Government Certification Authority (VGCA), the government organization that issues digital certificates that can be used to electronically sign official documents. The VGCA incident marks the fifth major supply chain attack this year after the likes of:

- SolarWinds - Russian hackers compromised the update mechanism of the SolarWinds Orion app and infected the internal networks of thousands of companies across the glove with the Sunburst malware.
- Able Desktop - Chinese hackers have compromised the update mechanism of a chat app used by hundreds of Mongolian government agencies.
- GoldenSpy - A Chinese bank had been forcing foreign companies activating in China to install a backdoored tax software toolkit.
- Wizvera VeraPort - North Korean hackers compromised the Wizvera VeraPort system to deliver malware to South Korean users.

As discussions regarding the Solarwinds/Solarigate compromise continue to unfold, the Auto-ISAC recommends the community take notice of additional supply chain compromises in the past year. Recent events suggest supply chain attacks are highly effective and may be challenging to detect and/or prevent. Given the automotive industry has a large and complicated supply chain, securing vehicles against similar attacks will be a challenge. Collaboration in industry groups such as the ISAC, SBOM, SAE/ISO and others addressing supply chain security will be critical to protect connected vehicles. Further, vehicles such as electric or otherwise powered vehicles are increasingly interacting with other critical infrastructure with complicated supply chains.

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

CISA RESOURCE HIGHLIGHTS

TLP:WHITE – Industrial Control System Joint Working Group (ICSJWG) – Upcoming Events

- ICSJWG Webinar – Bow Tie Model of Destructive Malware—ICS Historian Case Study
  - Wednesday January 27, 2021 – 2:15PM ET
  - Register with your work-related email at https://cvent[.]me/kMLmKZ
- ICSJWG Spring 2021 Meeting – Save-the-Date - April 2021
  - Updates for this event will be provided at https://us-cert[.]cisa[.]gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG
- Contact ICSJWG.Communications@cisa.dhs.gov for additional information

TLP:WHITE – CISA Emergency Directive ED21-01

- **Addresses malicious actor exploitation of SolarWinds Orion products**
- **Directs required actions applicable to Federal civilian agencies, made publicly available for use by the private sector**
- **Resources:**
  - **ED21-01: https://cyber[.]dhs[.]gov/ed/21-01/**
  - **Activity Alert AA20-352A: https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-352a**
  - **Supply Chain Compromise resources: https://www[.]cisa[.]gov/supply-chain-compromise**
  - **CISA Insights: https://www[.]cisa[.]gov/sites/default/files/publications/CISA Insights - What Every Leader Needs to Know About the Ongoing APT Cyber Activity - FINAL_508.pdf**

TLP: WHITE – Current Activity – CISA Releases Free Detection Tool for Azure/M365 Environment

- Available at CISA’s GitHub page
- The tool is narrowly focused on activity that is endemic to the recent identity- and authentication-based attacks seen in multiple sectors
- Resources:
  - https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/12/24/cisa-releases-free-detection-tool-azurem365-environment
  - https://github[.]com/cisagov/Sparrow
  - https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/12/17/nsa-releases-cybersecurity-advisory-detecting-abuse-authentication

TLP: WHITE – Additional Resources From CISA

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

For more information:

cisa.gov

Questions?

CISAServiceDesk@cisa.dhs.gov

1-888-282-0870

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY

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***

Slides available on our website – www.automotiveisac.com

Featured Speaker

AUTO-ISAC
Automotive Information Sharing and Analysis Center

David Turetsky, University at Albany

Professor of Practice the College of Emergency Preparedness, Homeland Security and Cybersecurity

David Turetsky is currently Professor of Practice at the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany (SUNY), and affiliated faculty at Albany Law School. He held senior positions as co-leader of the cybersecurity and privacy practice of a global law firm; Chief of the Public Safety and Homeland Security Bureau of the Federal Communications Commission, leading that agency’s work on White House-led cyber initiatives; Deputy Assistant Attorney General for Antitrust in the Justice Department.

Supported by a William and Flora Hewlett Foundation grant, Mr. Turetsky leads a research project on information sharing success stories and co-hosted a related conference with MS-ISAC. This led to an article in Lawfare in July 2020, and release of a longer study of success stories. He is an American Bar Association cybersecurity Legal Task Force member and co-led the privacy and security working group of the Information Sharing and Analysis Organization (ISAO) Standards Organization. In 2020, he became a member of the ISAO Standards Organization Hall of Fame.

He graduated from the University of Chicago Law School, Amherst College *magna cum laude*, and studied at the London School of Economics and Political Science.

Unal Tatar, University at Albany

Assistant professor in the College of Emergency Preparedness, Homeland Security and Cybersecurity

Unal Tatar is an assistant professor in the College of Emergency Preparedness, Homeland Security and Cybersecurity. His main topics of interest are privacy, economics of cybersecurity, cyber insurance, cybersecurity risk management, cybersecurity education, and blockchain.

Dr. Tatar worked as a principal cybersecurity researcher in government, industry, and academia over 15 years. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar is the director of the NATO Advanced Research Workshop on A Framework for a Military Cyber Defense Strategy.

Dr. Tatar holds a BS in Computer Engineering, an MS in Applied Mathematics/Cryptography, and a Ph.D. in Engineering Management and Systems Engineering. His research is funded by the National Science Foundation, National Security Agency, Department of Defense, and NATO.

Brian Nussabaum, University at Albany

Assistant professor in the College of Emergency Preparedness, Homeland Security and Cybersecurity

Brian Nussbaum is an assistant professor in the Department of Emergency Preparedness, Homeland Security and Cybersecurity. His focus is on cybersecurity, terrorism, homeland security, and intelligence studies.

Nussbaum previously served as senior intelligence analyst with the New York State Office of Counter Terrorism (OCT), a part of the New York State Division of Homeland Security and Emergency Services (DHSES).

Nussbaum received his Ph.D. and master's degree in political science from the University at Albany and bachelor's degree in political science from Binghamton University. His work has appeared in numerous books and journals including Studies in Conflict and Terrorism, Global Crime, the International Journal of Intelligence and Counterintelligence, and the Journal of Cyber Policy.

Information Sharing Success Stories

Auto-ISAC

January 6, 2021

David Turetsky, Brian Nussbaum, Unal Tatar

College of Emergency Preparedness, Homeland Security and Cybersecurity

University at Albany (SUNY)

What inspired this project and what did we do?

- Non-experts, sometimes lawyers, others. Easier to understand the costs and risks to companies than possible future benefits. Understood that as a policymaker and cybersecurity practice co-leader
- If the theory of information sharing is clear, the benefits should be as well
- Success stories– instances where certain or high likelihood that information sharing led to avoidance or reduction of harm
- Methodology– interviews (protecting trust), conference

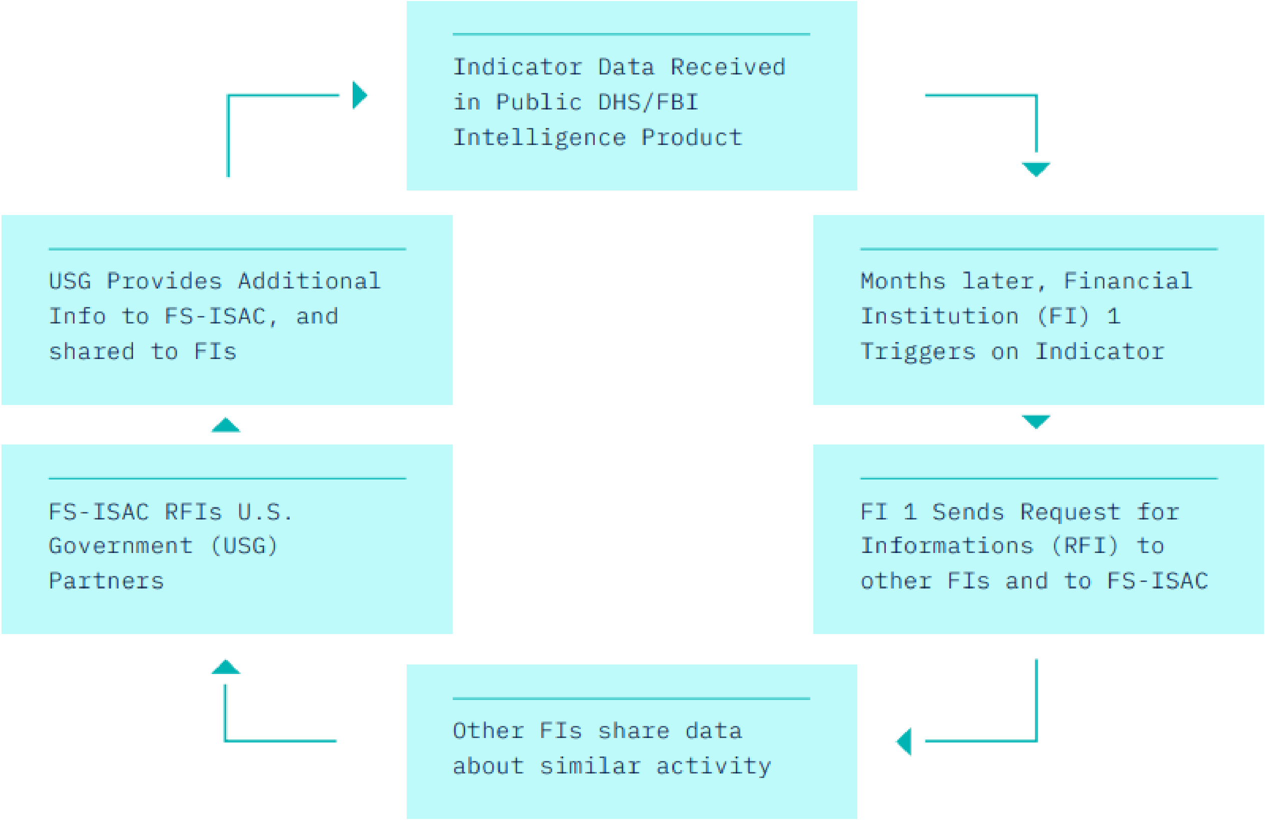
Aimed at Three Audiences for Success Stories

1. Companies and other entities deciding whether to engage in information sharing

2. ISACs and ISAOs interested in expanding membership, sharpening their understanding of what is working, and underscoring the importance and value of identifying success stories

3. Policymakers. Have supported voluntary information sharing and created incentives

Financial services company uses government and FS-ISAC information to identify a threat



Indicator Data Received in Public DHS/FBI Intelligence Product

Months later, Financial Institution (FI) 1 Triggers on Indicator

FI 1 Sends Request for Informations (RFI) to other FIs and to FS-ISAC

Other FIs share data about similar activity

FS-ISAC RFIs U.S. Government (USG) Partners

USG Provides Additional Info to FS-ISAC, and shared to FIs

Major Retailer: Formal and Informal Sharing

- Saw threat
- Shared information with a few major retailers, then with ISAC
- Spotted same threats

Supply Chain

- Streaming video devices beaconing abroad

- Manufacturer with compromised components got involved

Pulling the string: Sharing one malicious IP address leads to…

- Successful investigation leads to discovery of a real problem

- Involvement of both government and the private sector to address a cross-sectoral problem

Effective Information Sharing in Academia

- Information sharing leads to early discovery of a spreading threat

Aviation DDoS Attack

- Shared information led to effective collaboration and assistance

[redacted]

Information Sharing Success Stories

- Conclusion

- Questions?

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 Partners

Strategic Partner

Community Partners

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

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

[redacted]

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

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

Thank you!

рахмат
danke
謝謝
ngiyabonga
شكراً جزيلاً
Баярлалаа
spas
teşekkür ederim
mersi
kia ora
barka
welalin
tack
mahalo
спасибо
faafetai lava
vinaka
спасібі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
tapadh leat
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
thank you
gracias
хвала
asante
manana
aciu
dankon
akun
bedankt
bayarlalaa
gràçie
hvala
obrigada
murakoze
tenki
enkosi
djiere dieuf
tau
mochchakkeram
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
taiku
go raibh maith agat
chokrane
sobodi
dēkuji
sağolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercê
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

Our contact info

Faye Francy
Executive Director

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

Sharmila Khadka
Executive Organizational Secretary

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

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC