[redacted]

Welcome to Auto-ISAC!

Monthly Virtual Community Call

April 7, 2021

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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:** ▪ **Dan Hoban,** *Exec. VP*, **Nuspire** ▪ **Josh Smith,** *Cyber Threat Analyst*, **Nuspire**
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

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

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

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

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

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

Engaging in the Auto-ISAC Community

❖ 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

39 *Supplier & Commercial Vehicle Members*

15 *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)*

TLP WHITE: Disclosure and distribution is not limited

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

Michael Feiri
Vice Chair of the Advisory Board
ZF

Chris Lupini
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

TLP WHITE: Disclosure and distribution is not limited

Member Roster
as of April 1, 2021

Member Roster

Highlighted = Change

Aisin	Hyundai	Oshkosh Corp
Allison Transmission	Infineon	PACCAR
Aptiv	Intel	Panasonic
Argo AI, LLC	John Deere	Polaris
AT&T	Kia	Qualcomm
Blackberry Limited	Knorr Bremse	Renesas Electronics
BMW Group	Lear	Subaru
Bosch	LGE	Sumitomo Electric
Continental	Magna	Tokai Rika
Cummins	MARELLI	Toyota
Denso	Mazda	TuSimple
Delphi Technologies	Mercedes-Benz	Valeo
FCA	Meritor	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Motional	Waymo
Google	Navistar	Yamaha Motors
Harman	Nexteer Automotive Corp	ZF
Hitachi	Nissan	
Honda	NXP	*61 Members*

Business Administration

- **Auto-ISAC Activities *Members Only***

  - **April 7, 2021** – **CISO Roundtable on Ransomware** – 2:00 p.m. – 3:00 p.m. EDT. Host: Josh Davis (Toyota) For invited CISOs, Deputy CISOs and Senior Security Leaders- **Members Only**

  - **April 14, 2021** – **Educational Webinar in partnership with Security Scorecard** – 10:00 – 11:00 a.m. EDT. Host: Faye Francy (Auto-ISAC ED) & Presenter: Alex Rich (Senior Strategic Alliances Director). **Members Only**

    Presentation Topics: Learn about the SecurityScorecard platform (**Members Only**):
    - Delivers cyber ratings through its continuous monitoring solution
    - Can be used to continuously monitor + manage your organization's cybersecurity posture
    - Can be used to continuously monitor + manage the cybersecurity posture of your third-party ecosystem, and drive improvements in your third-party risk management program

  - **April 21, 2021** – ***Members Teaching Members, Charlie Hart (Hitachi)*** –10:00 – 11:30 a.m. EDT. ***Presentation Topic***: SBoM Current Events **TLP:AMBER.** **Members Only**

- **Community Activities:**
  - **May 5th, 2021:** ***Community Call Speaker***: Norma Krayem, VP, Van Scoyoc Associates
  - ***Auto-ISAC Website Survey*** for Community, being sent on **Monday, April 6th**

- **October 13-14, 2021:** ***Auto-ISAC Annual Cybersecurity Summit,*** 8:00am – 5:00 pm

Auto-ISAC Intelligence

DRIVEN

- Read it daily
- Email us at analyst@automotiveisac.com with feedback and questions

Auto-ISAC 2020 Annual Report

- Read it
- Email us with feedback and questions

Intelligence Resources

- Auto-ISAC Intel Staff – Email us, we may be able to assist
- TLP:WHITE Cyber Intelligence Tradecraft – Carnegie Mellon, Recorded Future

Do you forward intelligence to others within your company who can act on it but are not on your team?

Notable Quote: Jason Schmitt, the General Manager of Synopsis Software Integrity Group, stated, “Like any other software, mobile apps are not immune to security weaknesses and vulnerabilities that can put customers and businesses at risk.”[1] (source link)

Question: How is your organization confronting this persistent issue to protect its products, information technology and operational technology?

CISA RESOURCE HIGHLIGHTS

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

- **Register no later than Monday 19 April 2021 at https://gateway[.]on24[.]com/wcc/eh/3049745/ICSJWG-2021-Spring-Virtual-Meeting/**
- **ICSJWG main page: https://us-cert[.]cisa[.]gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG**
- **ICSJWG Fact Sheet: https://us-cert[.]gov/sites/default/files/2019-10/CISA_ICS_FactSheet_ICSJWG_S508C_0.PDF**
- **ICSJWG upcoming and past meeting and webinar information: https://us-cert[.]cisa[.]gov/ics/icsjwg-meetings-and-webinars**

TLP: WHITE – CISA Current Activity - Supplemental Direction on Emergency Directive for Microsoft Exchange Server Vulnerabilities

- Directs federal departments and agencies to run newly developed tools to investigate whether their Microsoft Exchange Servers have been compromised.
- Tools highlighted in the Supplemental Direction are Microsoft's Test-ProxyLogon.ps1 script and Safety Scanner MSERT
- Includes references to CISA and vendor resources
- See https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/03/31/cisa-releases-supplemental-direction-emergency-directive-microsoft

TLP: WHITE – CISA Activity Alert - AA21-062A - Mitigate Microsoft Exchange Server Vulnerabilities

- **Originally released on March 3, 2021**
- **Includes revisions that highlight additional observed malicious activity and resources for malicious activity identification and response**
- **Highlights nine (9) CISA analysis reports that include IOCs for identified webshells**
- **Includes references to Federal (CISA, FBI, USSS) and vendor resources**
- **See https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-062a**

TLP: WHITE – CISA Current Activities – Resources for Detecting IOCs and TTPs associated with SolarWinds and Active Directory/M365 Compromise

- CISA Hunt and Incident Response Program (CHIRP) to find IOCs: See https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/03/18/using-chirp-detect-post-compromise-threat-activity-premises and https://github[.]com/cisagov

- Table of TTPs used by the APT. See https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/03/17/ttp-table-detecting-apt-activity-related-solarwinds-and-active and https://us-cert[.]cisa[.]gov/sites/default/files/publications/SolarWinds_and_AD-M365_Compromise-Detecting_APT_Activity_from_Known_TTPs.pdf

TLP: WHITE – CISA Current Activity - Guidance on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise

- **Two (2) new CISA resources on the follow-on activity on the SolarWinds and AD/M365 Compromise:**
  - **Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise – see https://us-cert[.]cisa[.]gov/remediating-apt-compromised-networks**
  - **CISA Insights: SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders – see https://www[.]cisa[.]gov/publication/solarwinds-and-ad-m365-compromise-risk-decisions-leaders**

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

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

Dan Hoban, Nuspire

Executive Vice President, Client Success

Dan Hoban has been with Nuspire for over 17 years. During that time Dan has worked with OEMs such as GM, Ford, Chrysler, VW, Subaru, and others on dealer technology & security initiatives. Dan has assisted OEMs with national and global dealer infrastructure assessments, technology rollouts, security guidance, and solution design.

Dan also leads the Dealer Infrastructure and Security Standards workgroup for STAR (Standards for Technology in Automotive Retail). This workgroup includes OEMs, vendors, dealers, and technology leaders. Annually, they produce dealer infrastructure and security guidelines for all North American auto dealers.

Dan's work has been sited by Automotive News, Retail Info Systems, Manufacturing Engineering, and Franchising Today.

Josh Smith, Nuspire

Cyber Threat Analyst, Security Intelligence & Analytics

Josh Smith is a Threat Analyst at Nuspire who has been working in the automotive retail security space for over four years. He has worked closely in the dealer threat landscape curating threat intelligence and authoring Nuspire's Quarterly Threat Landscape Report.

Josh holds a bachelor's degree in Cybersecurity and Computer Networking and is currently pursuing his master's degree in Cybersecurity Technology. Previously he served with the U.S. Navy as an Operations Specialist with 14-years of service.

Josh has been quoted in Forbes, CSO Online, Channel Futures, Betanews, information Security Buzz, and others.

The Dealer Threat Landscape

Agenda:

- Introductions (Nuspire and Speakers)
- The Dealer, The Vehicle, and The Automotive Industry
- Dealer Infrastructure
- The Dealer Threat Landscape
- Brining it all Together
- Summary and Recommendations

Key Take-Aways:

- A better Understanding of the Dealer Networks, Challenges, and Threats
- An understanding on how the Dealer, Vehicle, OEM, and Client are Intertwined
- Ideas to improve the Dealer Threat Posture, and Security of the auto-industry

Nuspire Introductions

[redacted]

20+ Years of Dealer Technology Solutions for OEMs

- **Automotive Experience:**
  - Dealer Technology Surveys (10,000+)
  - OEM technology Rollout and Support
  - Consulting
  - R&D
  - Onsite Services
  - Network Installation, Integration, & Management
  - Network Security
  - Call Center Services
- **Standards for Technology in Automotive Retail (STAR)**
  - Steering Committee Member
  - Dealer Infrastructure & Security Guidelines Workgroup Lead

The Dealer, Vehicle, and Auto Industry

Dealers are a critical part of the Supply Chain

- Vehicle Distribution
- Vehicle Maintenance
- Users of Critical Technology

Dealers are High Value Targets

- PII
- Financial Info
- Access to IP
- "The Weakest Link"

Dealer Security Risk to the Industry

- Financial
- Brand Loss
- Vehicle Safety Perception

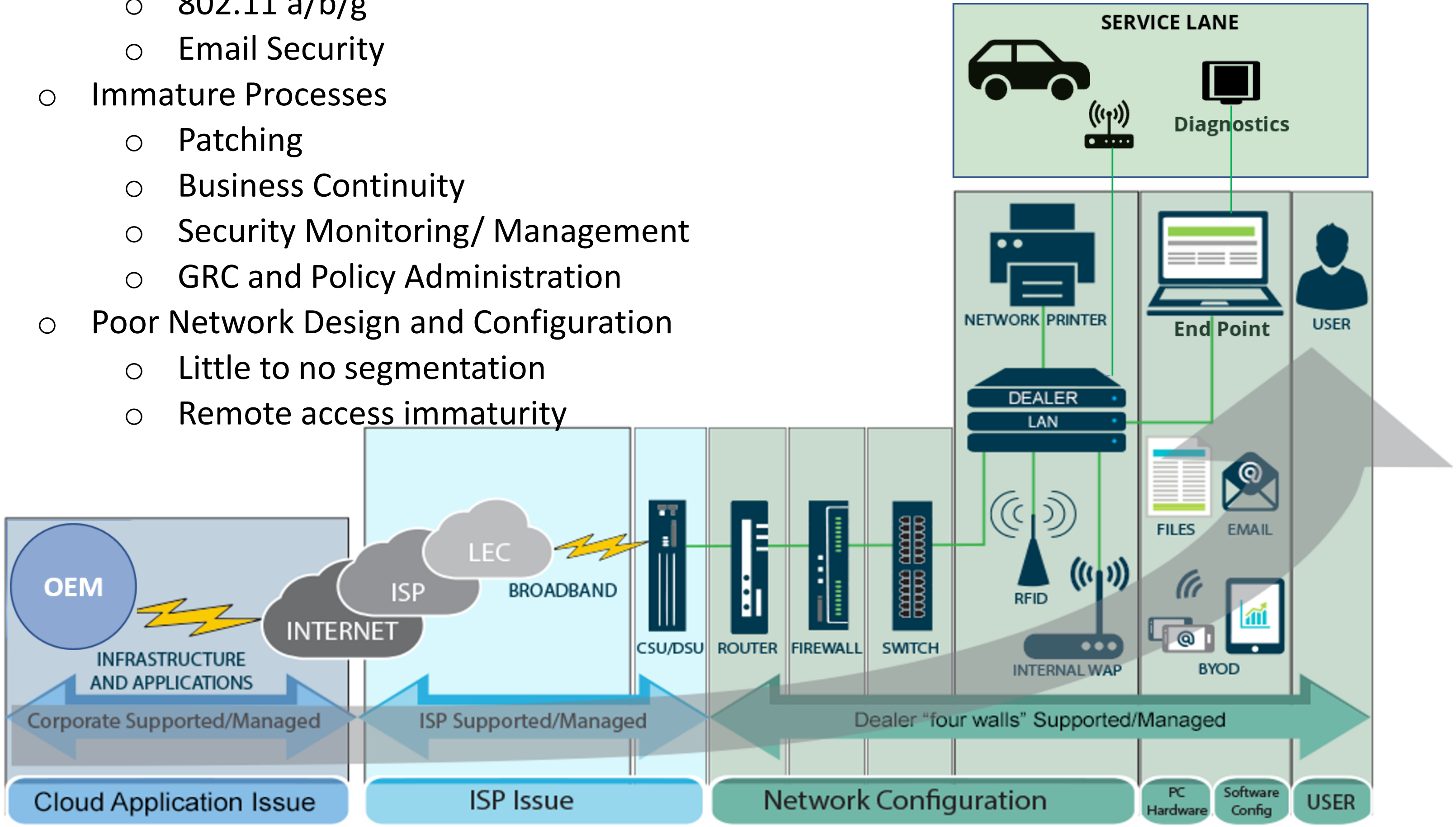
Dealer infrastructure

Technical Challenges

- Older Technologies
  - Windows 7, Windows XP
  - WEP
  - 802.11 a/b/g
  - Email Security
- Immature Processes
  - Patching
  - Business Continuity
  - Security Monitoring/ Management
  - GRC and Policy Administration
- Poor Network Design and Configuration
  - Little to no segmentation
  - Remote access immaturity

Business Challenges

- Both SMB and Enterprise
- Lack of Resources
- Business Model is Evolving



APT Groups Targeting Auto Industry

APT Group	Last Known Activity
Mofang (Superman)	Feb. 18th, 2021
APT32 (SeaLotus, OceanLotus, APT-C-00)	Mar. 5th, 2021
APT-C-36 (Blind Eagle)	Feb. 18th, 2021
TA505 (Graceful Spider, Hive0065, Dudear)	Mar. 5th, 2021
APT37 (ScarCruft, Reaper, Group 123, TEMP.Reaper)	Mar. 5th, 2021
APT40 (Leviathan)	Mar. 5th, 2021
APT18 (Dynamite Panda)	Feb. 27th, 2021
APT39 (Chafer)	Mar. 5th, 2021

High Priority Techniques and Procedures

Technique	Name	Tactic
T1204.002	Malicious File	Execution
T1059.003	Windows Command Shell	Execution
T1059.001	PowerShell	Execution
T1566.001	Spear-phishing Attachment	Initial-Access
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1105	Ingress Tool Transfer	Command and Control
T1027	Obfuscated Files or Information	Defense-Evasion

Top Dealer Botnet Activity

Torpig Mebroot

- **Dealer Risk: Email Security & Network Security Event Management**
- Botnet has been in existence for years and utilizes backdoor trojans.
- It has the capabilities of installing fraudulent certificates to lead their victims into believing they are visiting secured websites.
- The primary focus of this botnet is to capture banking credentials and can intercept API calls to steal usernames and passwords.
- It can be distributed via malicious software downloads or through malicious e-mail attachments.

Zeroaccess

- **Dealer Risk: Network Security Event Management**
- Monetarily focused botnet that is a kernel-mode rootkit.
- It adds its victims to the botnet and can install additional malware if desired by the operators.
- They can utilize the infected machine to perform cryptocurrency mining and spam the user with ads.
- Zeroaccess infections can happen from Cross-Site scripting attacks (XSS) or from untrusted software downloads, often from sites that host pirated software.

Remcos

- **Dealer Risk: Remote Access**
- botnet built on the Remcos Remote Administration Tool (RAT)
- commonly sold on hacking forums.
- This payload is often distributed through malicious Word/Excel documents embedded with macros.
- Remcos RAT can capture keyboard strokes, take screen captures, and execute commands on the infected machine.

Top Dealer Exploit Activity

GNU Bash Code Injection

- **Dealer Risk: Patch Management**
- (CVE-2014-6271) “Shellshock”
- Remote code injection vulnerability which allows threat actors to remotely issue commands on vulnerable servers.
- Older vulnerability that has been patched and stresses the importance of dealership administrators to keep their systems up to date as threat actors will still attempt to exploit older vulnerabilities in the search for “low hanging fruit.”
- Implementing a firewall with an intrusion prevention system (IPS) that has signatures to detect this type of attack can help prevent exploitation.

RDP Brute Force Login

- **Dealer Risk: Remote Access**
- Attempts by threat actors to break into remote desktop protocol through trying multiple username and password combinations.
- If successful, this would allow an attacker access into the network to gain a foothold and begin to load additional malware (such as ransomware) and exfiltrate data.
- APT39 and APT40 has previously been witnessed to target RDP instances to gain credentials for access and lateral movement throughout networks.
- Internet facing RDP should be disabled where possible and if not, restricted to trusted IP addresses.
- Strong and complex passwords should be required while also implementing multi-factor authentication.

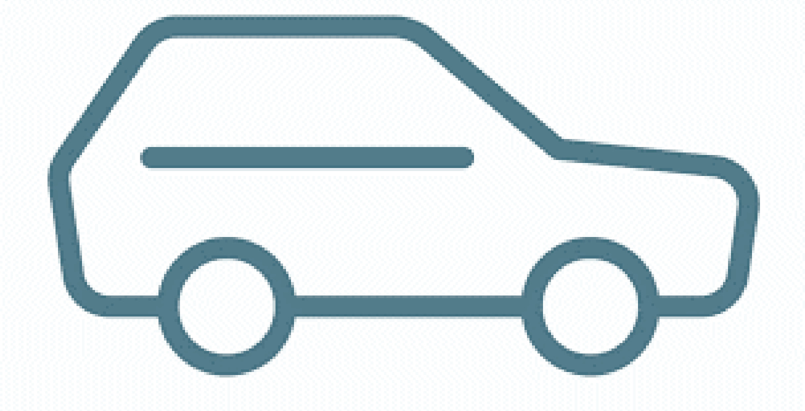
Cross-Site Scripting (XSS)

- **Dealer Risk: Compromise of Network**
- drive-by compromise attack and have been witnessed being utilized by APT32 and APT37.
- Attackers utilize malicious scripts in an attempt to inject commands into trusted websites.
- APT32 utilized spear-phishing e-mails to lure victims with a link to compromised websites while APT37 was witnessed compromising websites which then distributed malware to visitors.
- Web Application Firewalls can help detect and prevent XSS attacks and vulnerabilities.

Top Dealer Threat Activity

VBA Agent

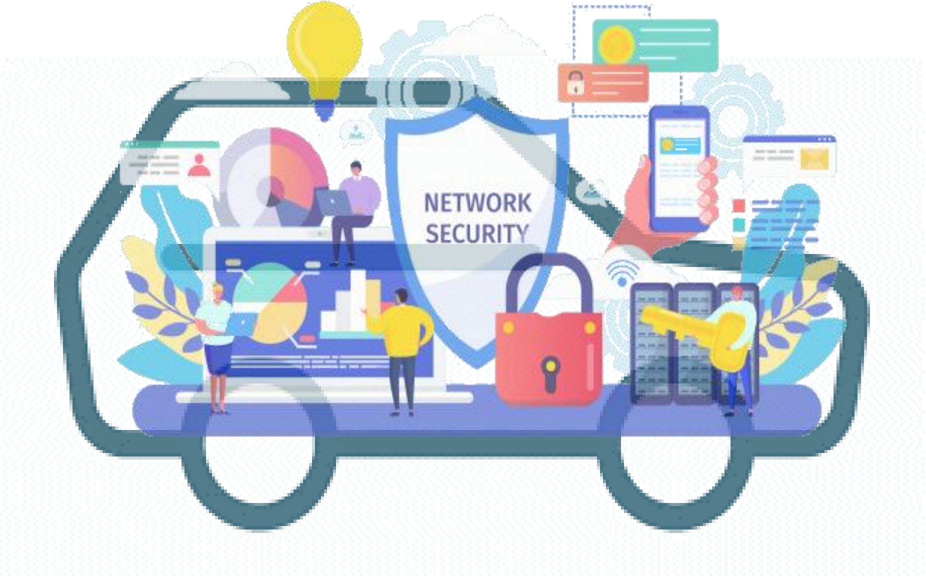
- **Dealer Risk: Email Security**
- Threat dominated Q4 not only dealer devices but with all devices monitored throughout Nuspire.
- These VBA Agents are typically Microsoft Office documents or excel files with malicious macros embedded.
- Every threat actor listed above (with the exception of APT18) is known for utilizing Spear-phishing Attachments and Malicious Files as one of their tactics/techniques for initial access into a network.
- Common lures include Invoices, HR documents, and common media themes such as the U.S. Election, Black Lives Matter protests, Tax Season documentation, and any other events trending in the world.



Bringing It all Together

Dealers are an Integral Part of the Auto Eco-system

- Physical Access to Vehicle
- Vehicle interface is dependent on dealer infrastructure
- Users of critical Technology
- Brand Identity
- Technology Enablement and Support



Dealers Have Challenges

- Hardware
- Resources
- Network Management and Monitoring
- Email Security
- Remote Access Challenges

There are active threats using tactics Dealers are ill prepared for

- Exploiting Patch Vulnerabilities
- Phishing
- C&C Networks
- Remote Access Exploits

Summery and Recommendations

Share Best Practices, Threats, and Threat Actor Behavior

- With Dealers, Suppliers, and Industry Stakeholders
- We are all one automotive community!

Endorse & Promote Standards for Dealer Security

- Individual Infrastructure and Security Guidelines
- STAR Dealer Security Recommendations

Unified messaging: Dealers Need to Upgrade Capabilities

- User Awareness Training
- Next Gen Security Technologies
- Patch Management
- Secure remote connections
- Security Management & Monitoring

Thank you

nuspire

Dan Hoban
www.Nuspire.com
248.212.5700
Dan.hoban@nuspire.com

Josh Smith
www.Nuspire.com
248.896.6160
Josh.Smith@nuspire.com

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

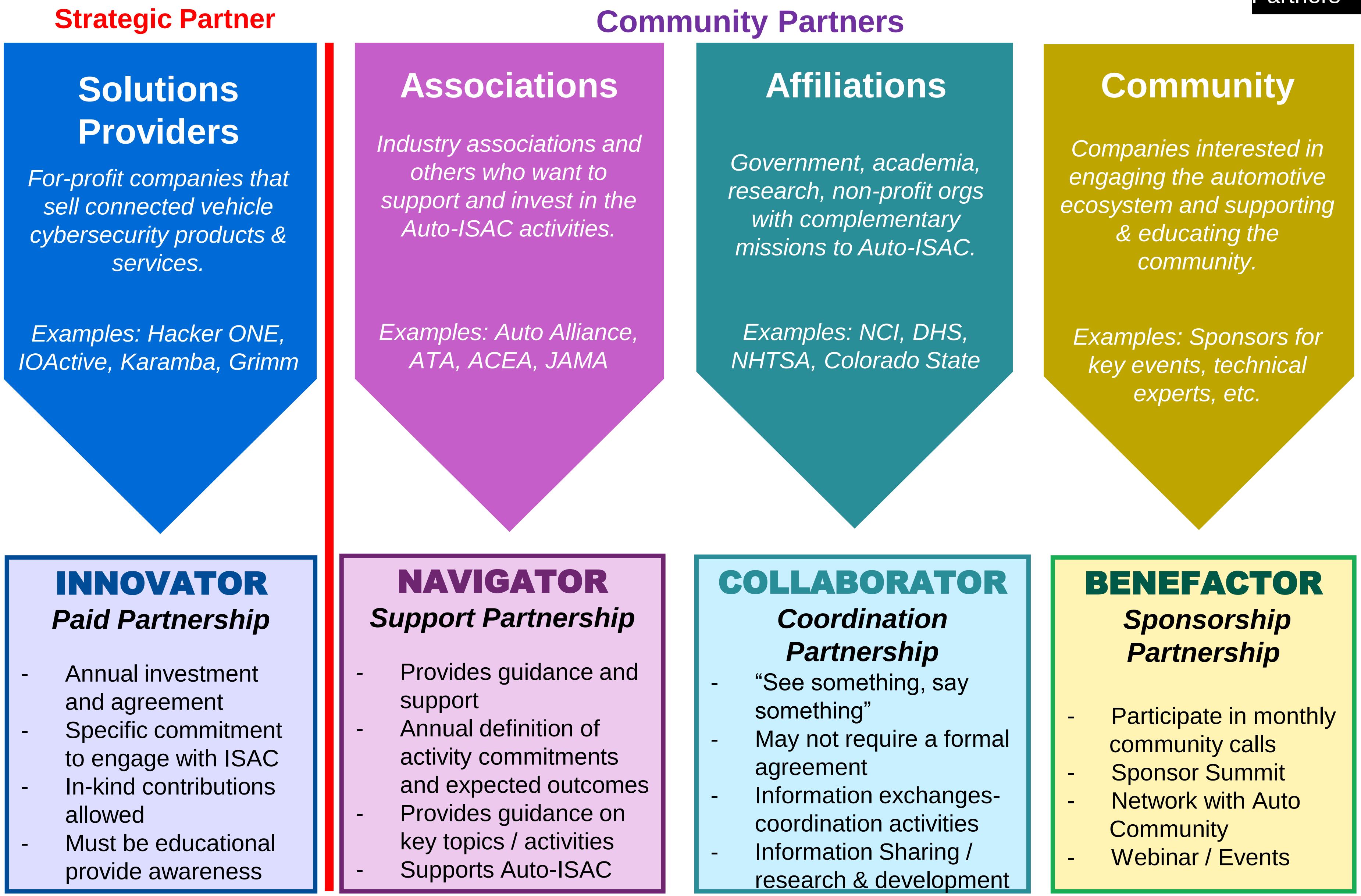
How to Get Involved: Membership

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

[redacted]

INNOVATOR

Strategic Partnership (15)

Security Scorecard
Cybellum
ArmorText
Celerium
Upstream
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

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!

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

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

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

www.automotiveisac.com
@auto-ISAC