[redacted]

Welcome to Auto-ISAC!

Monthly Virtual Community Call

March 3, 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:** ▪ **John Sheehy,** *SVP, Research and Strategy*, **IOActive, Inc.**
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

TLP WHITE: Disclosure and distribution is not limited

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!

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)*

2021 Board of Directors

Executive Committee (ExCom)

2021 BoD/AB Leadership

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

Member Roster

as of March 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

- **Successful *Auto-ISAC Europe 2021 Workshop -* TLP:AMBER Event, Feb 23rd**

- **Upcoming Key Events**:
  - **March 17, 2021 – *All Members Meeting*** – **TLP:AMBER** – 1:00 – 3:00 p.m. EDT.
    SCAG Quarterly Report / ISAC Operations Report
  - **March 18, 2021 – *1Q21 Advisory Board Meeting*** – **TLP:AMBER** – 9:00 – 11:00 a.m. EDT.
  - **March 18, 2021 – *1Q21 Board of Director's Meeting***– **TLP:AMBER** – 2:00 – 4:00 p.m. EDT.
  - **March 24, 2021** – ***Members Teaching Members Senior Leadership Presentation*** – **TLP:AMBER** – 10:00 – 11:30 a.m. EDT. ***Presentation Title*:** "Agile Software Ate My Vehicle" – A drive to a more modern and integrated vehicle system.

- **Membership Call-2-Action:**
  - **IT/OTWG:** Seeking Members interested in contributing to the newly-formed IT/OTWG.

- **Community Call:**
  - **April 7th, 2021: *Community Call Speaker***: Daniel Hoban, Nuspire

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

Threat Actors Are Increasingly Targeting Operational Technology

Ransomware Gangs Now Have Industrial Targets in Their Sights

Ransomware attacks are a potential danger for any organization, with ransomware variants including Conti, Egregor, Maze and many others still successfully compromising victims across all industries – but there are some industries that criminal gangs are targeting more than others. The ransomware attacks are successful because many organizations can't afford for their network to be out of service for a sustained period of time, so many businesses are still taking what they perceive to be the quickest and easier route to restoring the network by giving into the ransom demands of criminals. A recent report by cybersecurity company Digital Shadows examined which industries were most targeted by ransomware during 2020. While almost every industry found itself dealing with ransomware gangs over the course of the past 12 months, industrial goods and services was the most targeted, accounting for 29% – or almost one in three – ransomware attacks.

Hackers Tied to Russia's GRU Targeted the US Grid for Years

For all the nation-state hacker groups that have targeted the United States power grid—and even successfully breached American electric utilities—only the Russian military intelligence group known as Sandworm has been brazen enough to trigger actual blackouts, shutting the lights off in Ukraine in 2015 and 2016. Now one grid-focused security firm is warning that a group with ties to Sandworm's uniquely dangerous hackers has also been actively targeting the US energy system for years.

China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions

Since early 2020, Recorded Future's Insikt Group observed a large increase in suspected targeted intrusion activity against Indian organizations from Chinese state-sponsored groups. From mid-2020 onwards, Recorded Future's midpoint collection revealed a steep rise in the use of infrastructure tracked as AXIOMATICASYMPTOTE, which encompasses ShadowPad command and control (C2) servers, to target a large swathe of India's power sector. 10 distinct Indian power sector organizations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for operation of the power grid through balancing electricity supply and demand, have been identified as targets in a concerted campaign against India's critical infrastructure. Other targets identified included 2 Indian seaports.

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

CISA RESOURCE HIGHLIGHTS

Presenter's Name
March 3, 2021

TLP: WHITE – CISA Ransomware Guidance and Resources

- CISA Ransomware Guide (September 2020)
- CISA Insights Ransomware outbreak preparation and response guidance
- CISA Ransomware Campaign Toolkit
- CISA Ransomware Reference Material for K-12
- Resource locations:
  - https://www[.]cisa[.]gov/publication/ransomware-guide
  - https://www[.]cisa[.]gov/publication/ransomware-campaign-toolkit
  - https://us-cert[.]cisa[.]gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf
  - https://www[.]cisa[.]gov/ransomware-reference-materials-k-12

TLP: WHITE – CISA Activity Alert AA21-042A – Compromises of U.S. Water Treatment Facility

- Unidentified cyber actors obtained unauthorized access to the facility's SCADA system and initiated change to a water treatment process
- Alert personnel immediately detected the change and took corrective action, maintaining normal water treatment operation
- AA21-042A includes technical details and mitigation strategies
- Resource:
  - https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-042a

TLP: WHITE – Activity Alert AA21-048A – AppleJeus: Analysis of North Korea’s Cryptocurrency Malware

- Joint Advisory of the analytical efforts among the FBI, CISA and Treasury and U.S government partners, highlighting cyber threat to cryptocurrency posed by North Korean state-sponsored advanced persistent threat (APT) actors
- APT actors targeting individuals and companies, including cryptocurrency exchanges and financial service companies globally
- Activity also highlighted in CISA Activity Alerts AA20-239A "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks" and AA20-106A "Guidance on the North Korean Cyber Threat"

TLP: WHITE – Activity Alert AA21-048A – AppleJeus: Analysis of North Korea’s Cryptocurrency Malware (continued)

- **Reports available at:**
  - **https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-048a**
- **Full technical details of AppleJeus malware and associated IOCs are provided in the following seven (7) Malware Analysis Reports (MARs)**
  - **Celas Trade Pro - https://us-cert[.]gov/ncas/analysis-reports/ar21-048a**
  - **JMT Trading - https://us-cert[.]gov/ncas/analysis-reports/ar21-048b**
  - **Union Crypto - https://us-cert[.]gov/ncas/analysis-reports/ar21-048c**
  - **Kupay Wallet - https://us-cert[.]gov/ncas/analysis-reports/ar21-048d**
  - **CoinGoTrade - https://us-cert[.]gov/ncas/analysis-reports/ar21-048e**
  - **Dorusio - https://us-cert[.]gov/ncas/analysis-reports/ar21-048f**
  - **Ants2Whale - https://us-cert[.]gov/ncas/analysis-reports/ar21-048g**
- **HIDDEN COBRA - https://www.us-cert[.]cisa[.]gov/northkorea**

TLP: WHITE – Joint Advisory AA21-055A : Exploitation of Accellion File Transfer Appliance

- **Collaborative effort by the cybersecurity authorities of Australia, New Zealand, Singapore, the United Kingdom, and the United States**

- **Zero-day vulnerability identified in December 2020, followed by a patch release**

- **CISA reports (advisory, IOCs, and MAR):**
  - https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-055a
  - https://us-cert[.]cisa[.]gov/sites/default/files/publications/AA21-155A.stix.xml
  - https://us-cert.cisa.gov/sites/default/files/publications/MAR-10325064.r1.v1.WHITE_stix.xml

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 SECURITY AGENCY

CISA

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

John Sheehy, IOActive, Inc.

SVP, Research and Strategy

Bio: John has overseen multiple projects delivering identity management, threat modeling, industrial control systems security, risk assessment, security policy, secure device design, and incident & breach simulation and response services. His experience includes over 20 years of system architecture, systems integration, and information security experience working in Enterprise Architecture, Identity & Access Management, Vulnerability & Threat Management, Operations Technology, Security Strategy, Systems Architecture, and Hardware/Application Security domains.

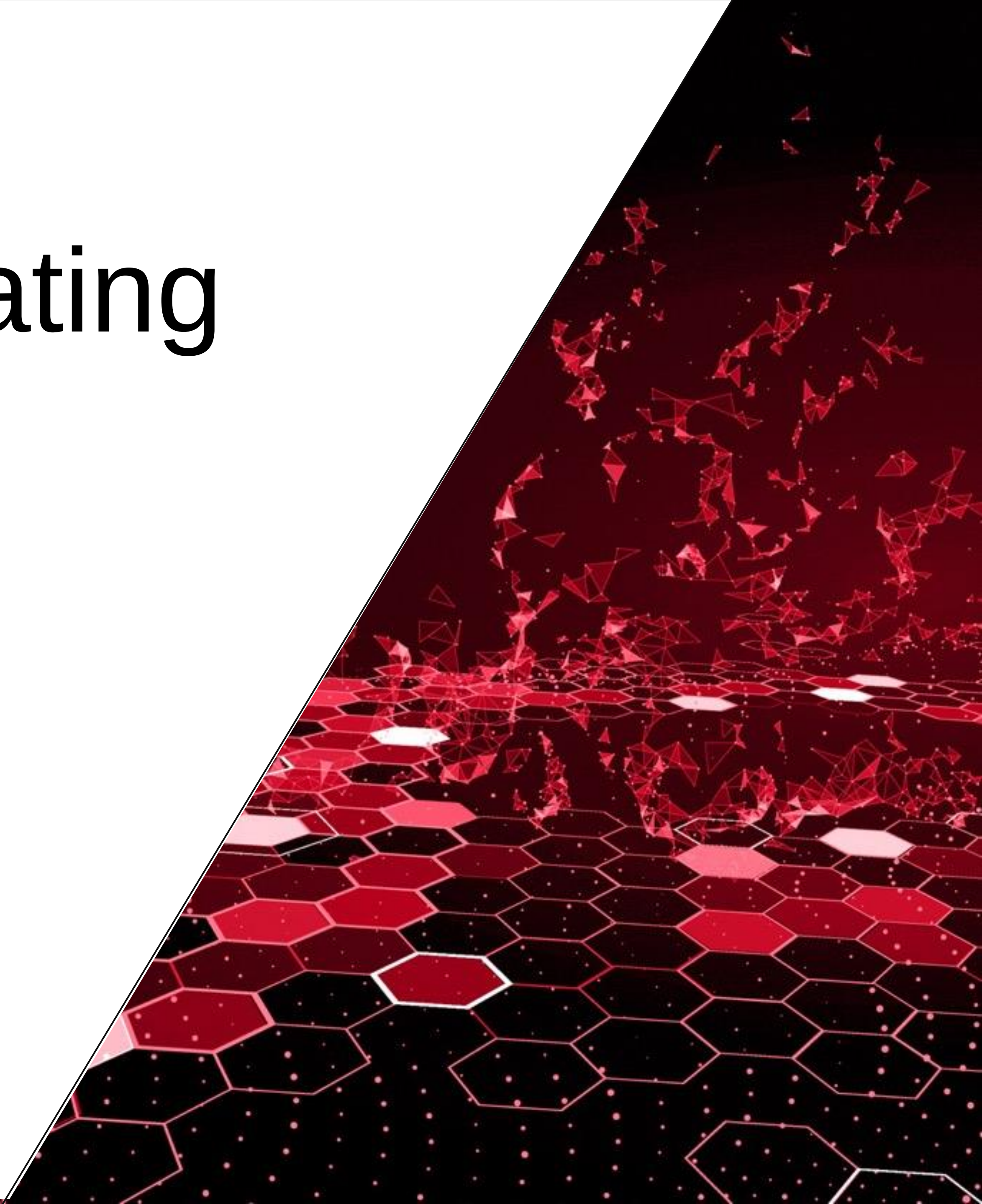
He currently leads IOActive's research program, corporate strategy, and service offering development.

Addressing Accelerating Supply Chain Risks

John Sheehy

SVP, Research and Strategy

IOActive®



IOActive Presentation Content

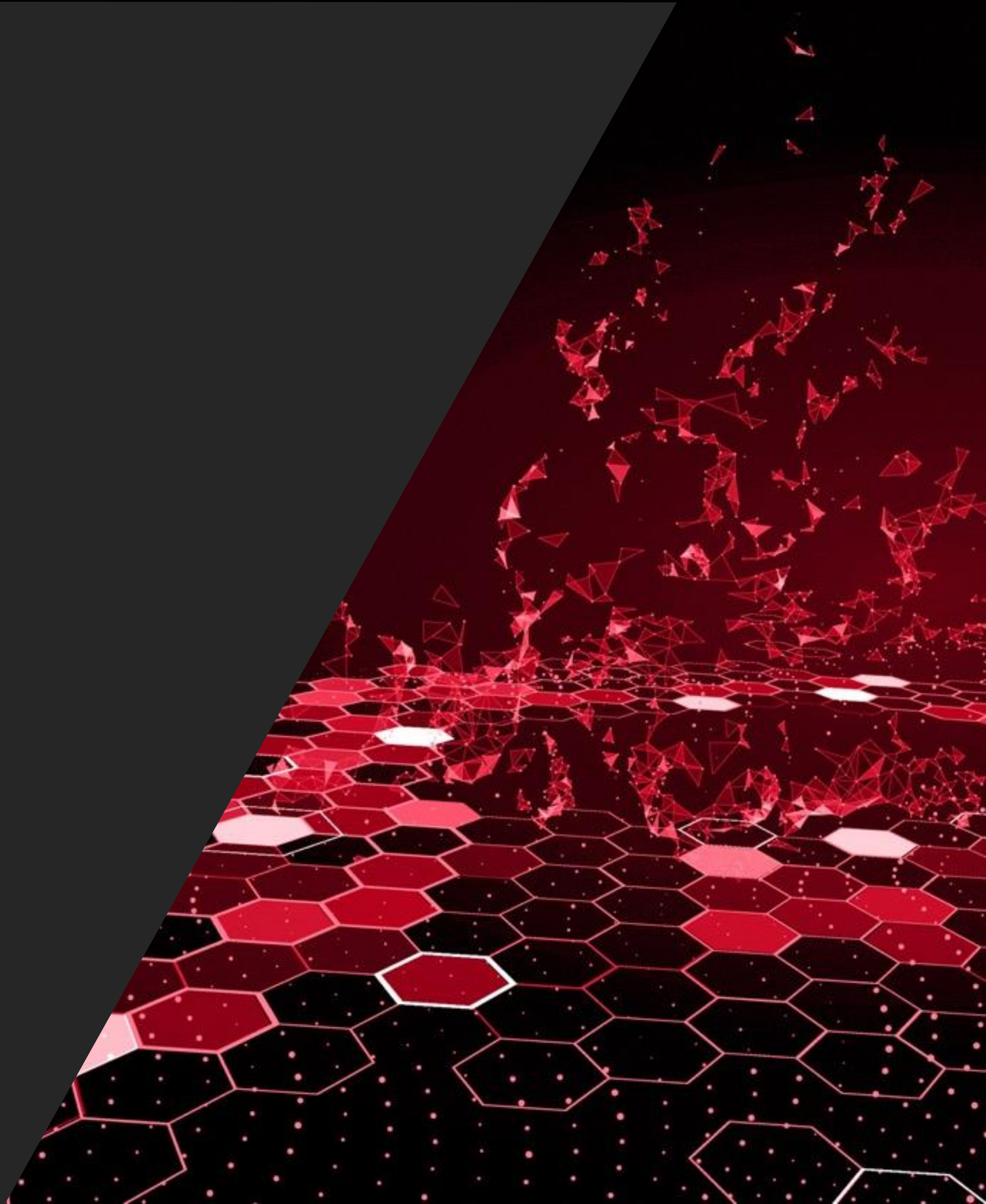
Legal Notices

- **Disclaimer Notification**
  The views, opinions, findings, conclusions, positions, and/or recommendations expressed herein are those of the authors individually and do not necessarily reflect the views, opinions, or positions of IOActive, Inc.
- **No Warranties or Representations**
  The information presented herein is provided "AS IS" and IOActive disclaims all warranties whatsoever, whether express or implied. Further, IOActive does not endorse, guarantee, or approve, and assumes no responsibility for nor makes any representations regarding the content, accuracy, reliability, timeliness, or completeness of the information presented. Users of the information contained herein assume all liability from such use.
- **Publicly Available Material**
  All source material referenced in this presentation was obtained from the Internet without restriction on use.
- **Fair Use**
  This primary purpose of this presentation is to educate and inform. It may contain copyrighted material, the use of which has not always been specifically authorized by the copyright owner. We are making such material available in our efforts to advance understanding of cyber safety and security. This material is distributed without profit for the purposes of criticism, comment, news reporting, teaching, scholarship, education, and research, and constitutes fair use as provided for in section 107 of the Copyright Act of 1976.
- **Trademarks**
  IOActive, the IOActive logo and the hackBOT logo are trademarks and/or registered trademarks of IOActive, Inc. in the United States and other countries. All other trademarks, product names, logos, and brands are the property of their respective owners and are used for identification purposes only.
- **No Endorsement or Commercial Relationship**
  The use or mention of a company, product or brand herein does not imply any endorsement by IOActive of that company, product, or brand, nor does it imply any endorsement by such company, product manufacturer, or brand owner of IOActive. Further, the use or mention of a company, product, or brand herein does not imply that any commercial relationship has existed, currently exists, or will exist between IOActive and such company, product manufacturer, or brand owner.
- **Copyright**
  ©2021 IOActive, Inc. All rights reserved. This work is protected by US and international copyright laws. Reproduction, distribution, or transmission of any part of this work in any form or by any means is strictly prohibited without the prior written permission of the publisher.

Agenda

- Supply Chain Basics
  - What is a Supply Chain?
  - Definitions
  - Potential Supply Chain Disruptions
  - Supply Chain Integrity
- Real Examples of Supply-chain Events
- Trust, Verify or Both?
- What Can Be Done?
- Final Thoughts

Supply Chain Basics



IOActive®

What is a Supply Chain?

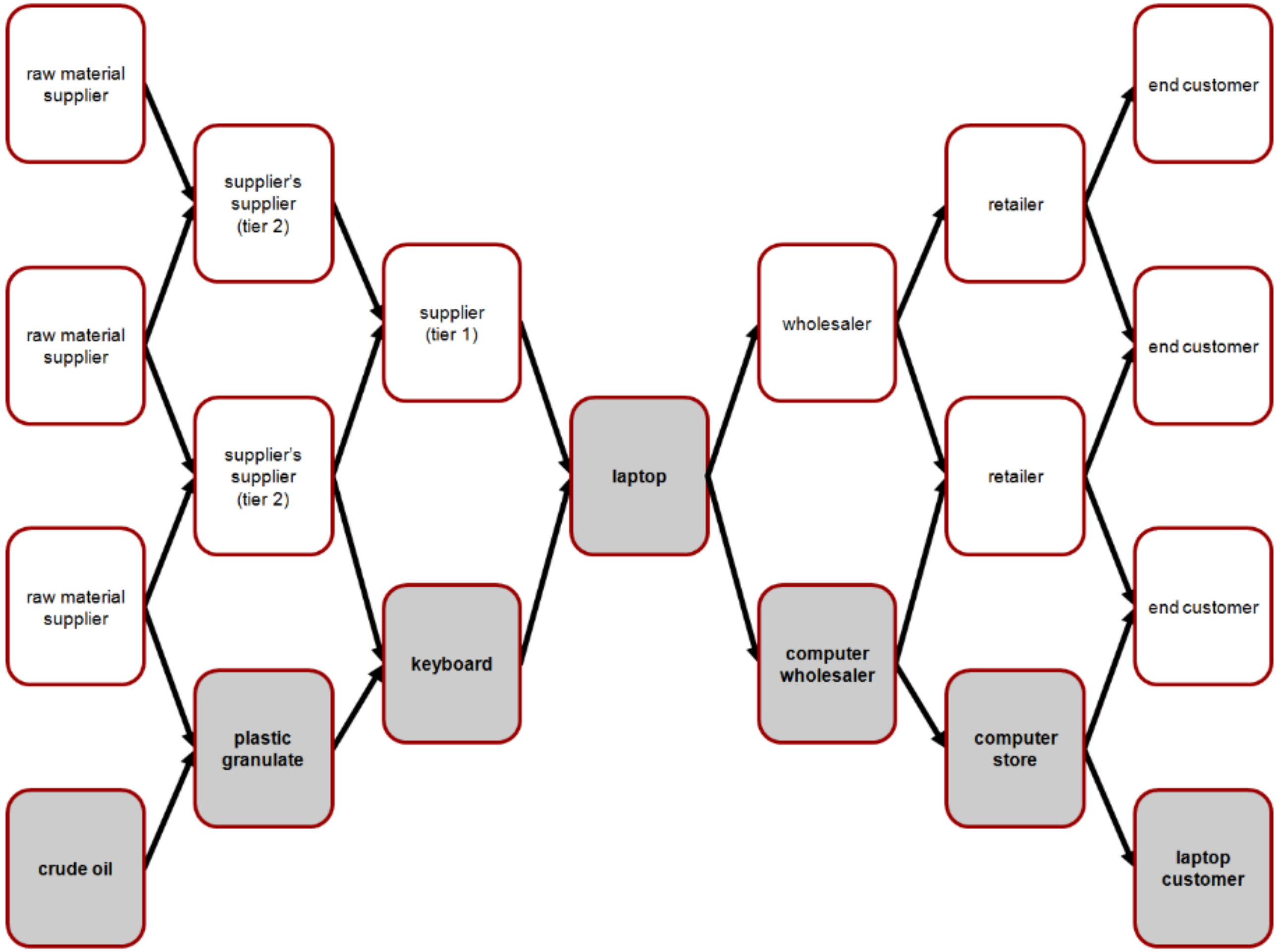


Image: Creative Commons 3.0, https://creativecommons.org/licenses/by/3.0/us/

- A network of entities used to produce a product or service
- A directed graph of entities through which goods or services pass to the final consumer

Definitions

- Tier 1 – Entity directly supplying the
- Tier 2 – Entity supplying the Tier 1
- Tier N – Entity supplying the Tier N-1 supplier
- Supply Chain Interdiction – Surreptitious intercept (typically physical) of component(s) in the supply chain in order to compromise them.
- Supply Chain Management (SCM) – The management of the flow of good of services through entire sourcing, production and delivery process with an emphasis on business outcomes.
- Resilience – The ability to cope with a crisis and quickly return to pre-crisis state.

Potential Supply Chain Disruptions

- Accident
- Contract Dispute
- Cybersecurity Event
- Fire
- Labor Dispute
- Natural Disaster
- Pandemic
- Regulatory Change
- Sabotage
- Tax Change
- Tariff Change
- War

With so many potential disruptions, what's the right strategy?

Resilience

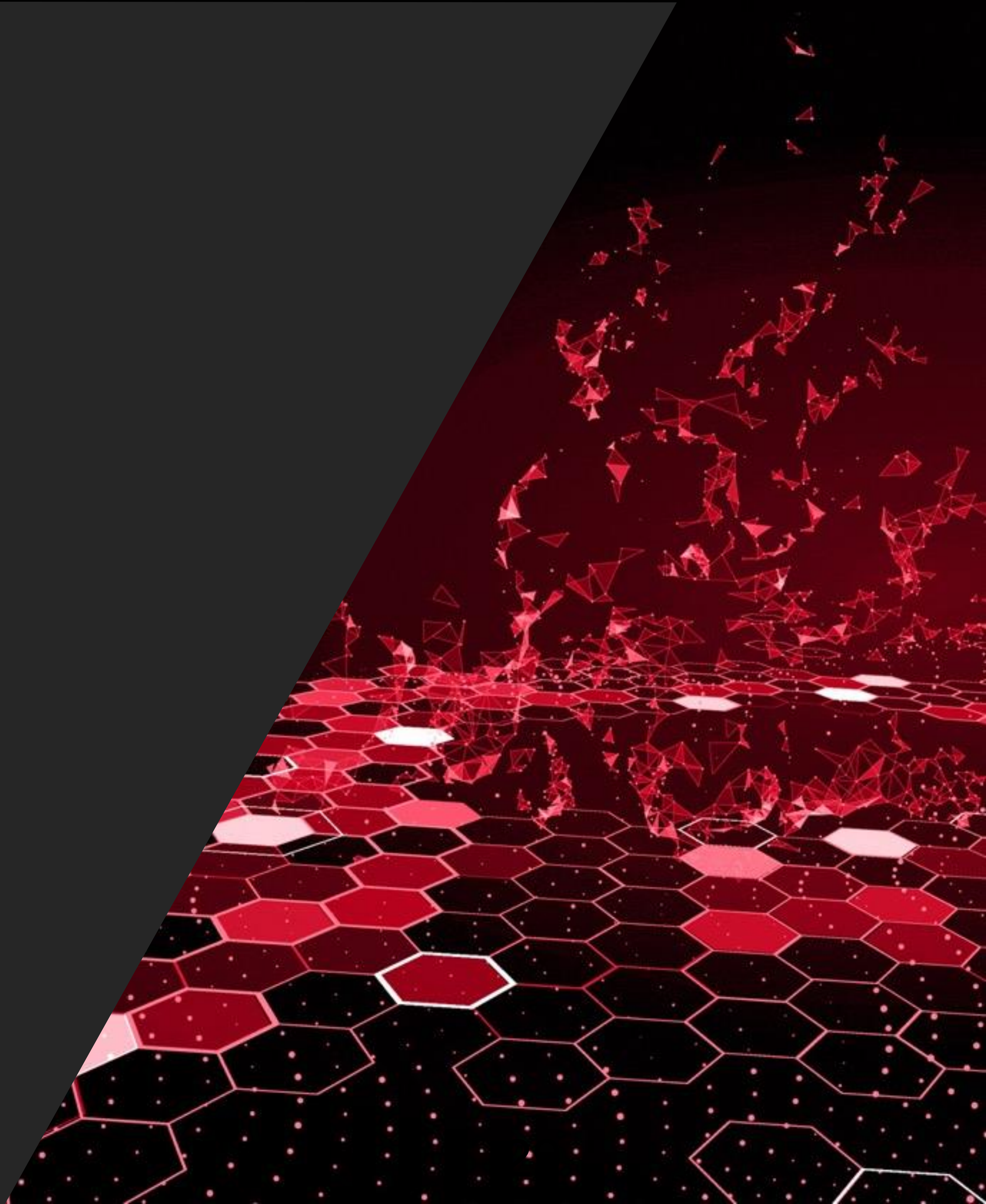
One can manage each of these risks, but none is entirely in one's control.

Focus on continuity of operations during and after any event.

What is Supply Chain Integrity?

- Not too different than data integrity
- No improperly modified goods or services as they flow
- Output matches expectations
- Closely related to quality
  - Don’t bother looking for malicious nation state implants, if you don’t look for quality issues with a security impact (i.e. counterfeits)
  - No need for a threat actor to use a slow, high-risk, costly supply chain compromise, if you don’t patch your servers
  - Don’t worry about low likelihood event, if you don’t do the basics

Real-world Examples of Supply Chain Events



IOActive®

Compromised Managed Service - Target

- Significant breach in 2014
- Stores POS systems compromised via Refrigeration and HVAC contractor with remote access
- Motivation was profit generated theft of PCI data
- Detectable and preventable with cost-effective effort

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

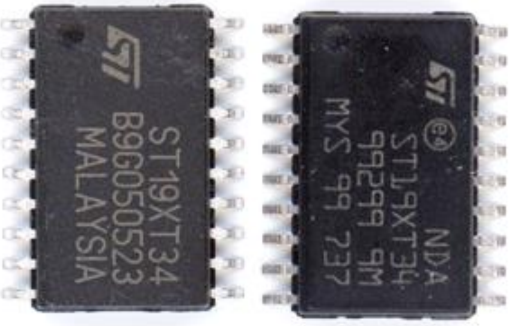
Counterfeit Chips – VisionTech

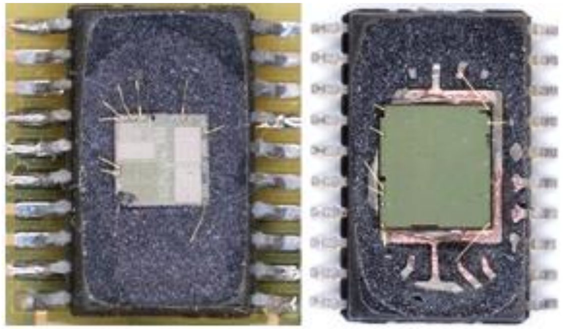
- Charged in 2010
- Sold at least 59,000 counterfeit microchips to US Navy
- Motivation was enhanced profit generated by selling sub-specification parts for use in critical systems
- Detectable with cost-effective effort

http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406468.html

Counterfeit Chips – Hong Kong Inventory

- IOActive purchased ST19XT34 chips from www.hkinventory.com in 2013
- Fraudulent markings apparent only after decapsulation
- Motivation appeared to be enhanced profit generated by selling substandard parts
- Detectable with cost-effective effort
- https://ioactive.com/spotting-fake-chips-in-the-supply-chain/





Counterfeit Chips – PRB Logics Corporation

- Charged in 2018
- Resold used and outdated chips that Chinese companies had repainted and remarked with counterfeit logos
- Major brands of FPGAs were targeted
- Also falsified test results that would have identified the chips as fakes
- Motivation was enhanced profit generated by selling sub-specification parts for use in critical systems
- Detectable with cost-effective effort

https://www.sourcetoday.com/distributor-news/owner-independent-distributor-charged-counterfeit-chips-scheme

Counterfeit Routers & Switches

- Several Cisco partners sold counterfeit switches, routers and router components to US military and US government entities
- Partners failed to perform adequate due diligence on unreasonably low-cost equipment from non-standard sources
- Indictments issued in 2007
- Motivation appears to be profit generated by selling lower-cost parts into the gray market
- No indication this was an effort to introduce implants
- Sub-standard equipment did cause instability in authentic Cisco gear
- Detectable with cost-effective effort

https://www.zdnet.com/article/cisco-partners-sell-fake-routers-to-us-military/

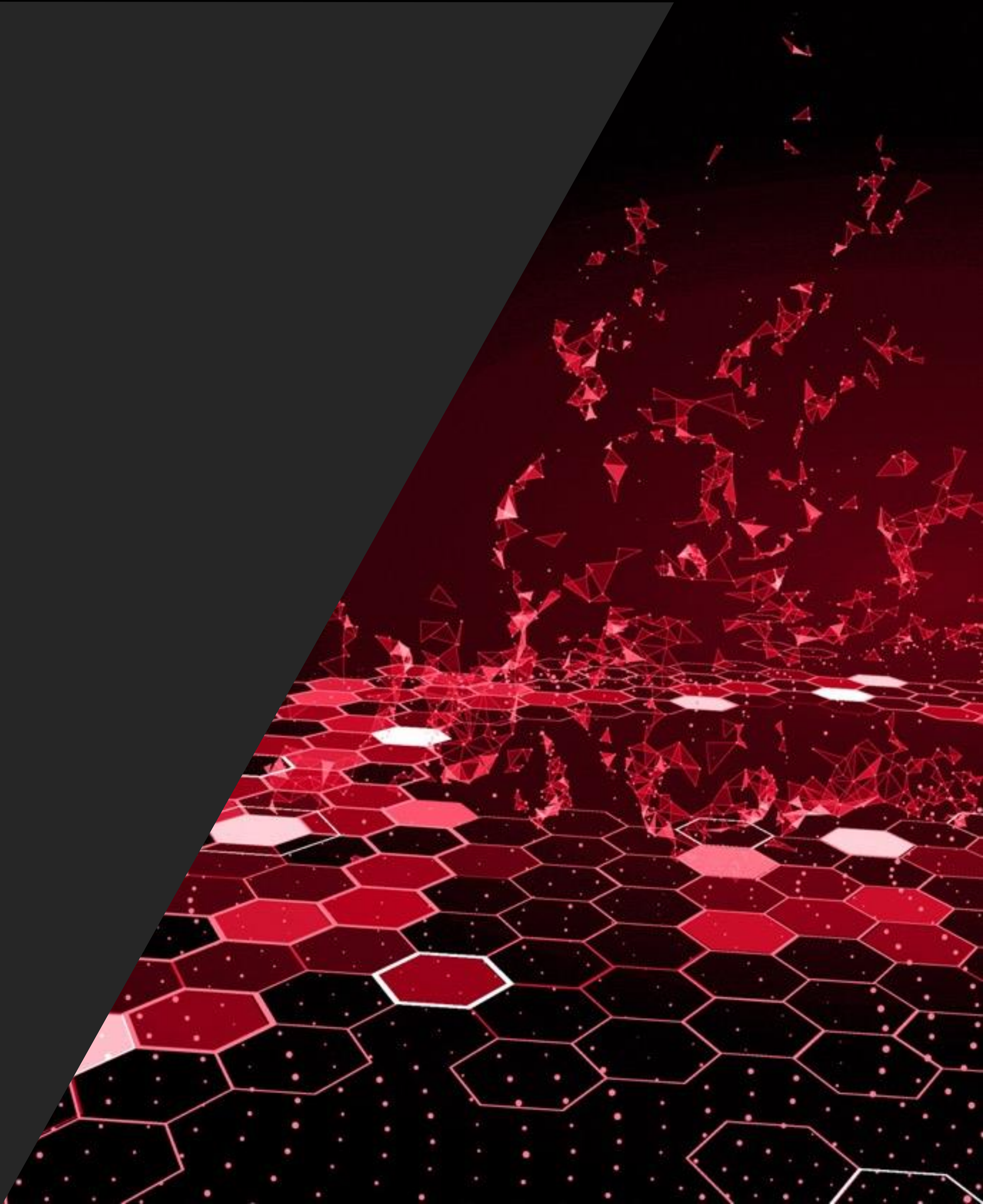
Supply Disruption – Global Semiconductor Shortage (Automotive)

- Pandemic-related demand forecasting accuracy issue for microchips
  - OEMs not usually the direct buyer of microchips
- Compounded by increase in demand for consumer electronics by consumers in lockdown
- Estimated $14-billion Q1-2021 reduction in revenue for global automotive industry; Estimated $61-billion reduction for 2021[1]
- US Government looking to address shortages and risks of supplier concentration
- "Detroit-area attorney Dan Sharkey, who represents suppliers, said one client in early January scoured the internet for chips to fulfill orders."[2]

1 - https://www.bloomberg.com/news/articles/2021-01-27/covid-pandemic-slows-down-chipmakers-causes-car-shortage

2 - https://www.wsj.com/articles/car-chip-shortage-ford-vw-gm-11613152294

Trust, Verify or Both?



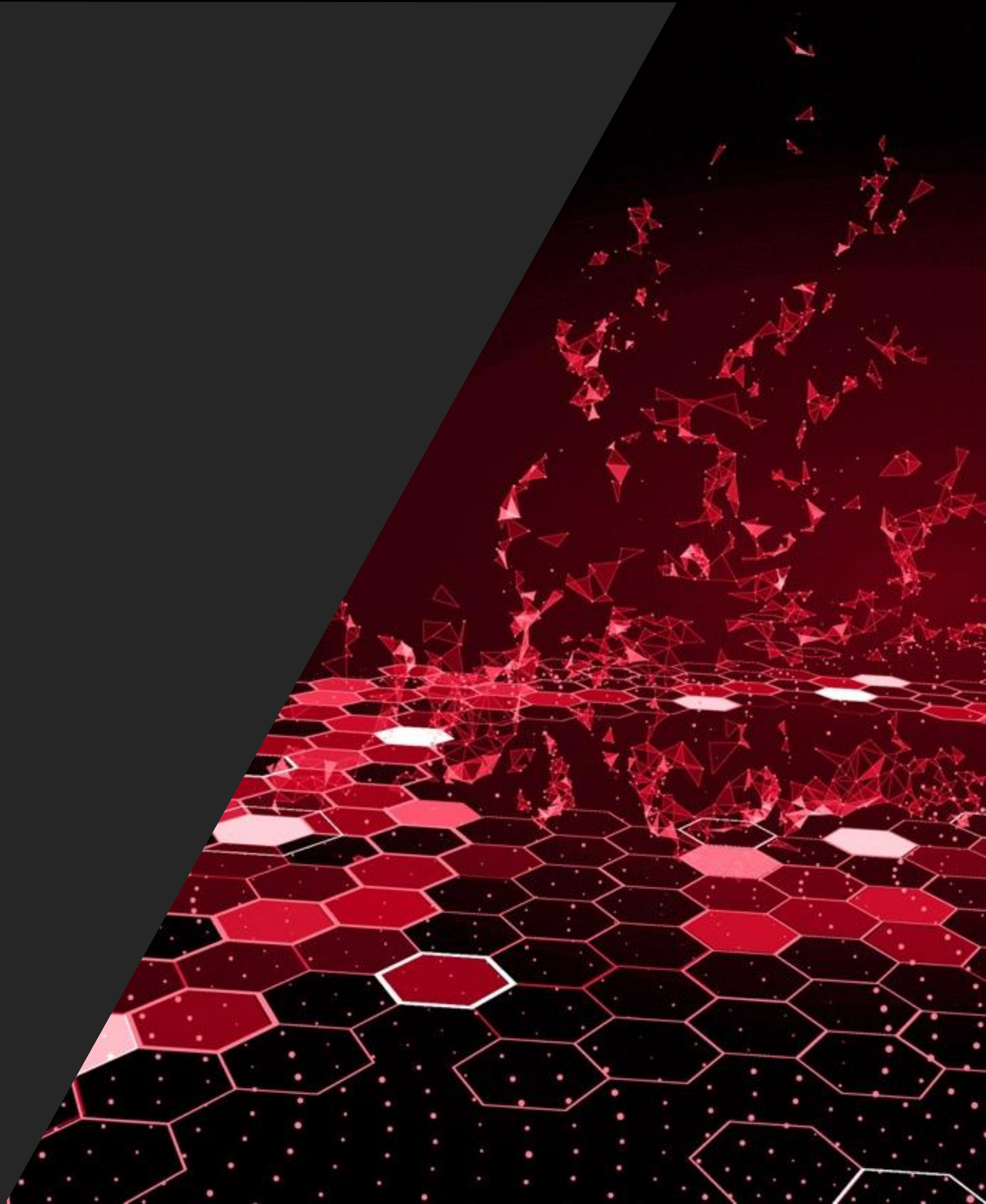
Trust or Verification?

- Trust – Confidence in integrity of something due to an assessment of the provider
- Verification – Confidence in something due to an assessment of the thing by you or someone you trust

Which is the Correct Approach?

- It should be one or the other
- Verify what you cannot trust
- Trust what you cannot verify
- Ideally, do both
  - Verification of something form a trusted party can increase the trust placed in the counterparty
  - Ensure things are performed in a way in which you have confidence that they were properly done, and this will reduce the level of verification effort required
  - Best approach for the highest impact things
- Always a business decision, but don’t forget your obligation and the potential impacts to your customers

What Can Be Done?



Strategy

- Don’t worry too much about supply chain attacks, if you don’t patch
- Don’t worry about supply chain attacks, if you don’t require secure components and products from suppliers
- If you can’t trust or verify something, don’t introduce it to your supply chain
- Have a supply chain integrity program that blends trust and verification inclusive of programmatic and technical elements
- Work to raise the cost to the threat actors you face
    - Both in raising the level of effort to launch a supply chain attack and the consequences after one is discovered
- Ensure your suppliers are focused on supply chain integrity too
- Don’t forget the risk you pose to your customers

Supply Chain Program Basics

- Identify the members of your supply chain (includes OSS)
- Threat model the supply chain against attacks
  - Include analysis of likely adversaries
- Prioritize on the high-risk, high-impact items (e.g. roots of trust)
- Handle the low-hanging fruit (e.g. counterfeits)
- Work with business leaders to contextualize the risk
- Get assessment of current state
- Develop roadmap for program to get to desired maturity level
- Reassess controls on a regular basis
- Seek longevity of relationships
- Design your supply chain with integrity in mind

Relevant Standards

- ISO 9001
- ISO 27001
- NIST CSF
- ISO 26262
- SAE J3061
- ISO 21434
- ISO 28001
- NIST 800-161
- NISTIR 8179

Standard Gaps

- OT-focused cybersecurity requirements
  - Can apply ISO 27001 framework with proper domain knowledge
- EVSE Cybersecurity Standard
  - Work in progress[1,2]
  - Major concern from perspective of electric-vehicle user and those relying on services provided by operators of a fleet of electric vehicles.
- End-to-end Supply Chain Risk Management Standard
  - Inclusive of IT, OT, product development, direct and indirect suppliers, and transportation/delivery
- Software Bill of Materials (SBOM)
  - What libraries, packages, components are in a product? Which versions?

1 - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8294.pdf
2 - https://github.com/nmfta-repo/nmfta-hvcs-xfc

ISO28001:2007

- Not perfect, but suitable existing framework for Supply Chain security
  - Primarily developed by Technical Committee ISO/TC 8, *Ships and marine technology,* in early 2000’s*.*
  - Originally driven by customs chain-of-custody requirements
  - https://www.iso.org/obp/ui/#iso:std:iso:28001:ed-1:v1:en

ISO 28001:2007 – Annex B

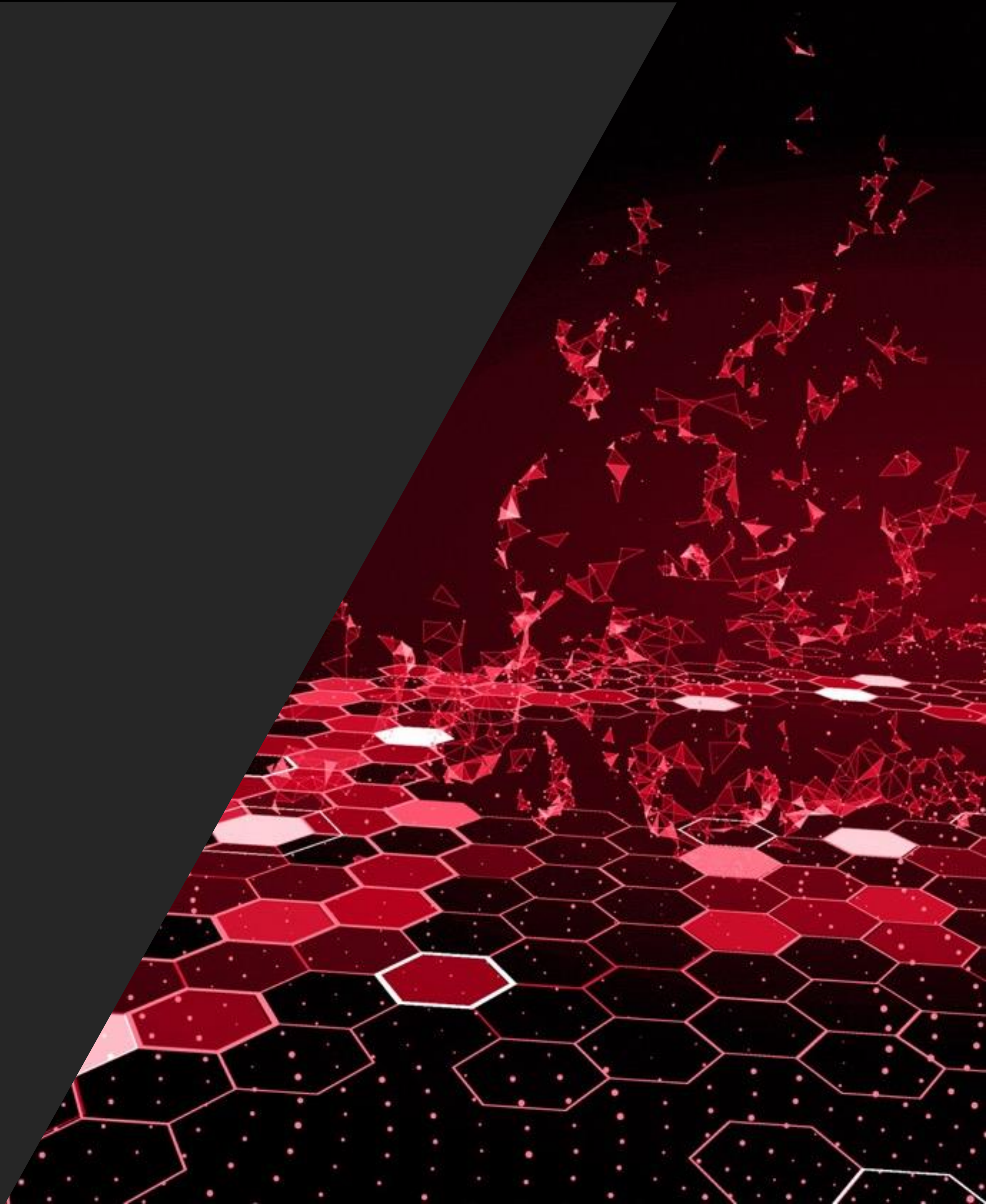
- Methodology for security risk assessment and development of countermeasures
  - B.1 General
  - B.2 Step one – Consideration of the security threat scenarios
  - B.3 Step two – Classification of consequences
  - B.4 Step three – Classification of likelihood of security incidents
  - B.5 Step four – Security incident scoring
  - B.6 Step five – Development of countermeasures
  - B.7 Step six – Implementation of countermeasures
  - B.8 Step seven – Evaluation of countermeasures
  - B.9 Step eight – Repetition of the process
  - B.10 Continuation of the process

Source: https://www.iso.org/obp/ui/#iso:std:iso:28001:ed-1:v1:en

NIST 800-161

- Not perfect, but also suitable starting framework
- Focused on US government IT and Communications systems
  - Neglects most OT
  - Doesn’t address product development
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Final Thoughts

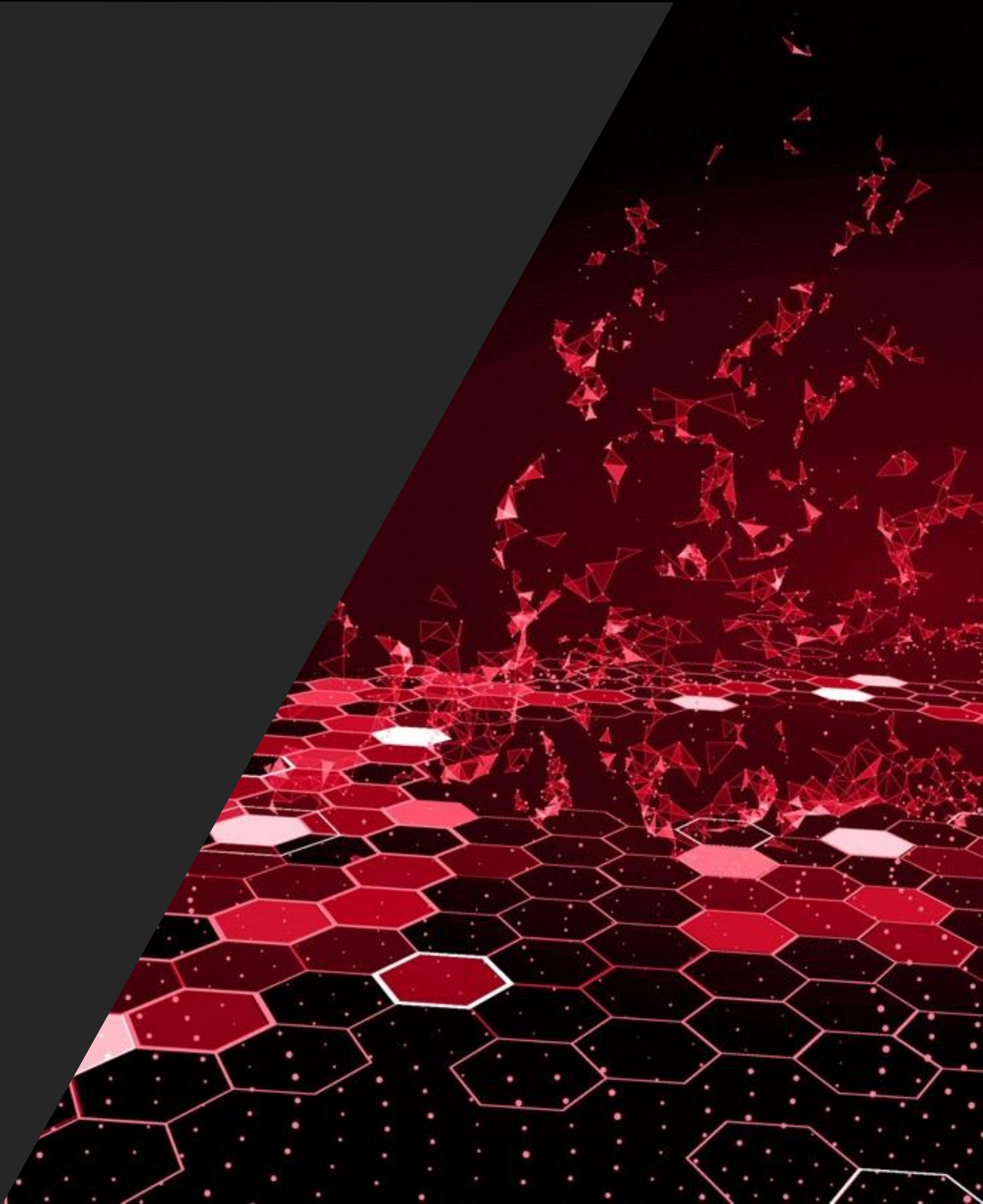


IOActive®

Final Thoughts

- The world is changing.
- Bretton Woods era is ending.
- Global free trade will be significantly changed.
- Most supply chains are global today.
- Supply chains will need to adjust to new reality.
- Geopolitical risk matters for all companies.
- Active management of the risks is superior approach.
- Suppliers and customers are interdependent upon each other.

Questions?



IOActive®

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!

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

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
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC