Welcome to Auto-ISAC!

Monthly Virtual Community Call

May 3rd, 2023
This Session will be recorded.
## DHS Traffic Light Protocol (TLP) 2.0 Chart

<table>
<thead>
<tr>
<th>COLOR</th>
<th>WHEN SHOULD IT BE USED?</th>
<th>HOW MAY IT BE SHARED?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLP:RED</strong></td>
<td>Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>TLP:AMBER+STRICT</strong></td>
<td>Limited disclosure, restricted to participants' and its organization.</td>
<td>Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.</td>
</tr>
<tr>
<td><strong>TLP:AMBER</strong></td>
<td>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.</td>
<td>Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.</td>
</tr>
<tr>
<td><strong>TLP:GREEN</strong></td>
<td>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</td>
<td>Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.</td>
</tr>
<tr>
<td><strong>TLP:CLEAR</strong></td>
<td>Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>Recipients may share this information without restriction. Information is subject to standard copyright rules.</td>
</tr>
</tbody>
</table>
## Agenda

<table>
<thead>
<tr>
<th>Time (ET)</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>Welcome</td>
</tr>
<tr>
<td></td>
<td>- Why We’re Here</td>
</tr>
<tr>
<td></td>
<td>- Expectations for This Community</td>
</tr>
<tr>
<td>11:05</td>
<td>Auto-ISAC Update</td>
</tr>
<tr>
<td></td>
<td>- Auto-ISAC Activities</td>
</tr>
<tr>
<td></td>
<td>- Heard Around the Community</td>
</tr>
<tr>
<td></td>
<td>- Intelligence Highlights</td>
</tr>
<tr>
<td>11:15</td>
<td>DHS CISA Community Update</td>
</tr>
<tr>
<td></td>
<td>- Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)</td>
</tr>
<tr>
<td>11:20</td>
<td>Featured Speaker:</td>
</tr>
<tr>
<td></td>
<td>- Nalindrani Malimage, Cybersecurity Consultant at Burns and McDonnell</td>
</tr>
<tr>
<td></td>
<td>- Title: Cybersecurity Challenges in the Electric Vehicle Market</td>
</tr>
<tr>
<td>11:45</td>
<td>Around the Room</td>
</tr>
<tr>
<td></td>
<td>- Sharing Around the Virtual Room</td>
</tr>
<tr>
<td>11:55</td>
<td>Closing Remarks</td>
</tr>
</tbody>
</table>
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!

- **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

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)

27 OEM Members

21 Navigator Partners

48 Supplier & Commercial Vehicle Members

19 Innovator Partners

3 May 2023
2023 Board of Directors

Thank you for your Leadership!

Josh Davis
Chair of the Board of the Directors
Toyota

Kevin Tierney
Vice Chair of the Board of the Directors
GM

Stephen Roberts
Secretary of the Board of the Directors
Honda

Tim Geiger
Treasurer of the Board of the Directors
Ford

Andrew Ebert
Chair of the EuSC
Volkswagen

Andrew Hillery
Chair of the CAG
Cummins

TBD
Chair of the SAG

Monica Mitchell
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv
# Auto-ISAC Member Roster

**As of May 1, 2023**

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

**Pending:** CNH Industrial, Daimler Truck, Micron, Rivian, Stoneridge
Auto-ISAC Business Updates and Events

Upcoming Meetings:

- **Members Teaching Members**: Wednesday, May 17th Time: 10:00am – 11:30 a.m. Speaker: Jonathan Mohring, Dirk Leopold, & Gerhard Steininger; itemis Title: “Key Technologies for performing TARAs Efficiently”

- **Auto-ISAC Partner’s Week Event** May 22nd – May 26th 11-1 pm ET, Virtual. Registration is open.

- **Auto-ISAC’s first European Summit** will be June 13th-14th, 2023 with June 12th having Members-only activities. https://automotiveisac.com/2023-europe-summit

  Register now! Early bird pricing for Eu summit ends May 5th.

- **Auto-ISAC Summit** will be Tuesday, October 17th-18th, 2023 in Torrance, California. You can find more information and registration here: https://automotiveisac.com/2023-annual-summit

  Register now! Early bird pricing for US summit ends September 8th.

### NOTE:
If you wish to submit a proposal to be a featured speaker on our monthly Community call, please reach out to Sharmilakhadka@automotiveisac.com. The presentation must be educational and relevant to Automotive cybersecurity.
Call For Participation: SBOM Tools Demo

- The SBOM Working Group (WG) invites all vendors with an SBOM Tool to present their tools on May 17th between 1:00 - 4:30 ET to Auto-ISAC Members (virtual/in person: Farmington Hills, MI).
  - The meeting will be held at TLP:CLEAR.
  - Participants include members of the Auto-ISAC SBOM WG and other representatives from Auto-ISAC Membership.
  - Vendor participants in the Tools Demo may also be Members. Members may also be competitors.
  - Presentations should focus on information that is publicly available/market facing including objective criteria, such as features, functionality and interoperability of the tools.
  - There will be no discussion of pricing or costs.
  - The objective of the Tools Demo is to facilitate access to and understanding of available SBOM Tools.
- If interested, please complete a quick survey https://www.surveymonkey.com/r/SBOMToolsDemo.
  - Vendor responses may enable Auto-ISAC Members to understand where tools are available to automate SBOM operations, facilitate SBOM sharing and/or vulnerability management.
  - Please contact AlisonHwang@automotiveisac.com with any questions.
2023 Auto-ISAC Cybersecurity Summit | October 17-18 | Torrance, CA / Virtual

Information here
Auto-ISAC Europe Cybersecurity Summit
12–14 June 2023 | The Peugeot Adventure Museum, Sochaux, France

REGISTRATION IS LIMITED!

June 12 Members Only: TLP:AMBER
Monday, June 12: 11:00 – 20:00 CET
Open to Auto-ISAC Members only

June 13-14 Open to Public: TLP:CLEAR
Tuesday, June 13: 8:00 – 20:00 CET
Wednesday, June 14: 8:00 – 16:00 CET
Open to Auto-ISAC Members and External Partners
Auto-ISAC Intelligence

Know what we track daily: subscribe to the DRIVEN; TLP:GREEN Auto-ISAC 2022 Threat Assessment released with Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) included.

- Send feedback, contributions, or questions to analyst@automotiveisac.com.

Intelligence Notes

- Q2 Threat Outlook
  - Ransomware groups will target some automotive companies.
  - Other cybercriminals will attempt to steal sensitive data from some automotive companies for resell or to extort targeted companies.
  - Cyber-enabled vehicle theft will continue.
  - Generative AI such as ChatGPT is an urgent concern and serious potential threat automotive organizations should be proactively studying and tracking today (Bard, SistemmaGPT (hxxps://sistemma[dot]ru), ERNIE Bot, Tongyi Qianwen, Bedrock).
  - Cyber threat actors sponsored by Russia, China, North Korea, and Iran will remain a threat to the confidentiality of sensitive information and the availability of IT and OT infrastructure as long as heightened geopolitical tensions and geostrategic economic competition persist (Russia-Ukraine, China, North Korea, Iran).

TLP:CLEAR
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**
CISA Resource Highlights

• Joint Cyber Defense Collaborative
CISA Releases Malware Analysis Report on ICONICSTEALER

• CISA has released a new Malware Analysis Report (MAR) on an infostealer known as ICONICSTEALER.

• This trojan has been identified as a variant of malware used in the supply chain attack against 3CX’s Desktop App.

• CISA recommends users and administrators to review the following resources for more information, and hunt for the listed indicators of compromise (IOCs) for potential malicious activity:

• Please note all information provided is TLP Amber
APT28 Exploits Known Vulnerability To Carry Out Reconnaissance and Deploy Malware on Cisco Routers

- NCSC, NSA, CISA, and FBI have released a joint advisory to provide details of tactics, techniques, and procedures (TTPs) associated with APT28's exploitation of Cisco routers in 2021.

- By exploiting the vulnerability CVE-2017-6742, APT28 used infrastructure to masquerade Simple Network Management protocol (SNMP) access into Cisco routers worldwide, including routers in Europe, U.S. government institutions, and approximately 250 Ukrainian victims.

- Jaguar Tooth is a non-persistent malware that targets Cisco IOS routers.

  - Collects device information
  - Exfiltrates over TFTP
  - Enables unauthenticated backdoor access
  - It is deployed and executed via exploitation of patched SNMP

- CISA encourages personnel to review NCSC’s Jaguar Tooth malware analysis report for detailed TTPs and indicators of compromise which may help detect APT28 activity.
Shifting the Balance of Cybersecurity Risk: Security-by-Design and Default Principles

• Security-by-Design and Default Principles serves as a cybersecurity roadmap for manufacturers of technology and associated products.

• Authoring agencies are CISA, FBI, NSA, Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand’s Computer Emergency Response Team, United Kingdom’s National Cyber Security Centre, Germany’s Federal Office for Information Security (BSI), and the Netherlands’ National Cyber Security Centre.

“Secure-by-Default” means products are resilient against prevalent exploitation techniques out of the box without additional charge.

“Secure-by-Design” means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure.

• Please note all information provided is TLP Amber
Security/Software Updates

For the period of 4/1/23 - 4/30/23:

- Drupal Releases Security Update: Drupal Core
- CISCO Releases Security Advisories: Multiple products
- Oracle Releases Security Updates
- Apple Releases Security Updates: Multiple products
- Microsoft Releases Security Updates: Multiple products
- Mozilla Releases Security Updates: Multiple products
- Adobe Releases Security Updates: Multiple products
- Fortinet Releases Security Updates: Multiple products
- Juniper Networks Releases Security Updates
- VMware Releases Security Updates: Aria Operations for Logs

- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber
CISA Releases Industrial Control Advisories

• These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

• CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

• For the period of 4/1/23-4/30/23 approximately 34 advisories have been issued.

• The advisories span the following sectors: Information Technology, Critical Manufacturing, Energy and Multiple Sectors.

• Cybersecurity Alerts & Advisories | CISA

Please note all information provided is TLP Amber.
CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.

CISA added 17 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of April. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber.
Additional Resources from CISA

- CISA Homepage - https://www.cisa.gov/
- CISA NCAS – https://cisa.gov/resources-tools/all-resources-tools
- CISA Shields Up - https://www.cisa.gov/shields-up
- CISA News Room - https://www.cisa.gov/cisa/newsroom
- CISA Blog - https://www.cisa.gov/blog-list
- CISA Cybersecurity Directives - https://cyber.dhs.gov/directives/
Featured Speaker
Nalindrani Malimage works as a cybersecurity consultant at Burns and McDonnell. She has worked in the information security space for almost 11 years and started her career in 2008 in Sri Lanka. She has worked in different industries including tobacco, FMCG and software before entering into the transmission and distribution sector.

She has various experience from Fortune 500 companies to startups. She has led some of the most challenging projects in the information security space and has a passion for threat investigations and compliance. She is also a chartered management accountant and an economist who has previously published research in the space of development economics.

In 2010, Nalindrani also became an award winner and a gold medalist at Chartered Management Accountants in the United Kingdom, where she became the world number 6 for Enterprise Strategy out of over 5000 professional accountants worldwide. She is a generalist in cybersecurity and has worked in almost all areas within information security. She is currently studying for CISSP.
Cybersecurity Challenges in the in Electric Vehicle Market

Nalindrani Malimage
Cybersecurity Consultant – Operational Technology
Content

• Industry Overview
• EV architecture and attack surface
• Data Breaches in the EV industry
• Compliance standards
• How to be better prepared
• Conclusion
Let’s look at some industry stats...
Electric Vehicle Market Industry Overview

Chart 1. Electric vehicles share of car sales and stock, 2011–21

- Electric vehicle share of sales
- Stock of electric vehicles

Available electric car models may reached 450 in 2021, with particular expansion of SUVs


Source: Global Electric Vehicle Outlook
Electric Vehicle Market Industry Overview

Source: Global Electric Vehicle Outlook
Electric Vehicle Market Industry Overview

Charging infrastructure is expanding significantly

Publicly accessible LDV charging points by power rating and region, 2015-2021

Charging by type and location in the United States (thousand)

<table>
<thead>
<tr>
<th></th>
<th>Stations</th>
<th>Points</th>
<th>Level 1</th>
<th>Level 2</th>
<th>DC fast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>50.7</td>
<td>130.7</td>
<td>3.3</td>
<td>104.8</td>
<td>22.6</td>
</tr>
<tr>
<td>Public</td>
<td>47.2</td>
<td>116.6</td>
<td>1.2</td>
<td>93.2</td>
<td>22.3</td>
</tr>
<tr>
<td>Highway</td>
<td>8.8</td>
<td>22.7</td>
<td>0.3</td>
<td>16.8</td>
<td>5.7</td>
</tr>
<tr>
<td>Interstate</td>
<td>3.2</td>
<td>9.3</td>
<td>0.1</td>
<td>5.7</td>
<td>3.6</td>
</tr>
</tbody>
</table>

Source: Global Electric Vehicle Outlook
Subsidies by state for electric trucks purchase

Source: Global Electric Vehicle Outlook
## Electric Vehicle Market Industry Overview

### Major automakers accelerate electrification plans

<table>
<thead>
<tr>
<th>Source: Global Electric Vehicle Outlook</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BMW Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daimler Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ford Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GM Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Honda</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyundai Kia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nissan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Renault Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stellantis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toyota Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VW Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Electric Vehicle Market Industry Overview

China dominates the entire downstream EV battery supply chain

Geographical distribution of the global EV battery supply chain

Source: Global Electric Vehicle Outlook
## Electric Vehicle Market Industry Overview

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total, all occupations</td>
<td>158,134.7</td>
<td>166,452.1</td>
<td>8,317.4</td>
<td>5.3</td>
<td>19,532.5</td>
<td>$45,760</td>
<td>2</td>
</tr>
<tr>
<td>Software developers</td>
<td>1,425.9</td>
<td>1,796.5</td>
<td>370.6</td>
<td>26.0</td>
<td>143.4</td>
<td>120,730</td>
<td>Bachelor's degree</td>
</tr>
<tr>
<td>Electrical engineers</td>
<td>192.4</td>
<td>195.5</td>
<td>3.1</td>
<td>1.6</td>
<td>12.3</td>
<td>100,420</td>
<td>Bachelor's degree</td>
</tr>
<tr>
<td>Electronics engineers, except computer</td>
<td>111.4</td>
<td>118.0</td>
<td>6.7</td>
<td>6.0</td>
<td>7.8</td>
<td>104,820</td>
<td>Bachelor's degree</td>
</tr>
<tr>
<td>Chemical engineers</td>
<td>26.9</td>
<td>30.7</td>
<td>3.7</td>
<td>13.9</td>
<td>2.0</td>
<td>105,550</td>
<td>Bachelor's degree</td>
</tr>
</tbody>
</table>

1 Data are from the Occupational Employment and Wage Statistics (OEWS) program, U.S. Bureau of Labor Statistics. Wage data cover non-farm wage and salary workers and do not cover the self-employed, owners and partners in unincorporated firms, or household workers.

EV Security Architecture & Attack Surface
Potential Attack Surface

Source: Auto-ISAC
Charging Infrastructure - What are the Risks?

• Interoperability
• Malware installation
• Eavesdropping / Tracking
• Remote code execution and control
So many white hat hackers had published many ways to hack EVs but no actual security incidents had been reported so far

- Let’s take a quick look at how to hack a Tesla
How to Hack a TESLA S model

- Anything that’s connected to the network can be hacked
- Here we are able to identify a browser vulnerability, spoof a network and gain access to the user’s password system that’s stored in plaintext
Published Data Breaches in the EV Industry
Let’s Explore a Few Data Breaches in the EV Industry & Causes

• Insider threats
• Competitiveness – Selling data to competitors
• Lack of implementation of best practices related to data handling, data classification and access control
• Overlooking security over convenience
“Khatilov stated that after being hired in December, Tesla sent files to his personal dropbox, which contained sensitive information that could be accessed from his personal computer.”
Aftermath of giving every employee Local Admin Rights – Access Control Policies

“The hacking software used by Tripp was operating off 3 separate computers. It was formatted to continue to export sensitive data off to unknown third parties even after Tripp left Tesla. “ Exfiltrating data by a disgruntled employee.”
What Happened to Implementing Least Privilege Principle?

“The complaint filed by Tesla says the ex-employee uploaded code used in the company’s backend software system, WARP drive, to manage a wide range of business processes..”
“Hackers breached the video surveillance services company Verkada on Monday, Bloomberg reported, gaining access to a “super admin” account that let them see more than 150,000 live feeds as well as video archives from Verkada’s customers. Exposed organizations included jails, schools, and hospitals—like the Madison County Jail in Huntsville, Alabama, and Sandy Hook Elementary School—as well as tech companies like Tesla and Cloudflare.”
Cloud Security & Password Protection

“Tesla has confirmed that its cloud computing platform has been compromised by hackers. According to RedLock, the hackers discovered log-in details to Tesla's Amazon Web Services environment on a Kubernetes console - a system originally designed by Google to manage applications. The console was reportedly not password-protected.”
Need for DLP Policies and Least Access Privilege

“Another Rivian employee named in the suit had previously worked in the environmental health and safety department at Tesla. Tesla alleges the former employee sent documents to a personal account related to setting up a factory, such as robotics and other manufacturing automation processes.”
Ransomware Attacks

“The hackers claimed to hold personal data regarding Nio's employees and car owners, including their addresses. They also have information about orders and vehicle owners' loans.”
Data Breach at NISSAN

It appears that the theft was targeting company R&D data, not customer information. Volvo said it “does not see, with currently available information, that this has an impact on the safety or security of its customers’ cars or their personal data.”

The media outlet Inside-it, which was the first to report the breach, found a screenshot on the dark web that showed Volvo’s data was released on the website of a ransomware gang called Snatch.

A report released in fall 2021 by digital risk protection company CybelAngel found that the automotive industry is at severe risk of ransomware attacks due to the availability of hundreds of thousands of exposed credentials online.

The company’s six-month investigation of automotive companies found that highly sensitive information was leaked, including trade secrets, personally identifiable information, blueprints of engines and production facilities, confidential agreements, human resources documents and more. The company concluded that these leaks occurred due to employee internal threats and external security weaknesses across the automotive supply chain.
Ransomware Attack at Volvo

“The cause of the breach is described as the result of data embedded within the code during software testing unintentionally and temporarily stored in a cloud-based public repository — in other words, another case of data exposure on an unsecured cloud instance.

Data exposed in the breach may have included names, dates of birth and account numbers. Credit card information and Social Security numbers were not exposed. While noting that it has no evidence that the data has been misused, Nissan is offering credit monitoring through Experian plc, a company that has its own problems with data breaches.”

Hacker Selling Data Allegedly Stolen From Volvo Cars Following Ransomware Attack

A hacker is offering to sell data allegedly stolen from Swedish vehicle manufacturer Volvo Cars following a ransomware attack carried out in late December.

By Eduard Kucou
January 4, 2023

A hacker is offering to sell data allegedly stolen from Swedish vehicle manufacturer Volvo Cars following a ransomware attack carried out in late December.

Google Patches Second Chrome Zero-Day Vulnerability of 2023

Can We Ever Stop Cyber Hijacking?
Compliance and Regulations surrounding EV Industry
ISO/SAE 21434:2021
Road vehicles — Cybersecurity Engineering

- Software security and SDLC
- Security Awareness and Culture
- Incident Management
- Define Clear Software Security Requirements
- Keep Inventory of Your Software Projects
- Risk Assessment and Risk Management
- Risk Assessment and Risk Management
- Vendor Security Compliance
- Risk Assessment and Risk Management
Gaps in the Industry and How to Prepare
Supply Chain Attacks

Cost of Supply Chain Attacks:

1. Negative publicity
2. Drop in business value
3. Administrative burden
4. Reactive threat response and sudden allocation of extra resources
5. Reporting obligations
Vendor Security Evaluation

From Process Driven to Business Case Specific Evaluation:

- Collection of information (e.g., SOC 2 report) at the procurement stage itself – Less back and forth
- Approval with controls/Rejection
- Security Evaluation
- Revalidation of current security audit reports
- Incident management policy and breach notification
- IAM policies related to the business use case
- Product Security Architecture - Evaluation
- Data Retention, protection and disposal policies
- Published reports on previous data breaches
- Network and communication security/Transport layer level security
- Vendor’s third party, 4th party risk management
- Latest Pen-test report of the application of focus
- Privacy policy
- Submitting Multiple Vendors for Security Evaluation Provides a Better Safety Net/Less Pressure

Increased Back and forth communication & Time Lags

- Procurement Request
- Budget Approval
- Security Evaluation
- Standard Security Questionnaire
- SOC 2 report based on the PII access
- Approval/Rejection
- Procurement Request
- Budget Approval & vendor security evaluation
- Approval with controls/Rejection
- Vendor security evaluation

Improved Due Diligence & Efficiency
Security Incident Response - Limitations

Who Sees a Duck? Who sees a Rabbit?
Security Incident Response - Limitations

- SQL Injection Attack & Phishing Attack
Security Incident Response – How to Address the Limitations

- Subjective Vs. Research Based
- Reactive Vs. Proactive
- Skills to look for in an incident responder?
- Reporting obligations
Q&A
Any questions about the Auto-ISAC or future topics for discussion?
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 melissacromack@automotiveisac.com. For Partnership, please contact sharmilakhadka@automotiveisac.com.
Auto-ISAC Partnership Programs

Strategic Partnership

- **For-profit** companies such as “Solutions Providers” that sell connected vehicle cybersecurity products & services.
- **Examples:** Hacker ONE, Upstream, IOActive, Karamba, Grimm

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
3. **In-kind contributions** allowed. Currently no fee.
4. **Does not overtly sell or promote** product or service.
5. Commits to support the Auto-ISAC’s mission.
6. Engages with the automotive ecosystem, supporting & educating Auto-ISAC Members and its Community.
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth priority.
9. **Engagement must provide Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates in information sharing** Auto-ISAC activities.
11. **Supports our mission through educational webinars and sharing of information.**

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- **Includes** Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non-Profit, Technical Experts, Auto-ISAC Sponsors.
- **Examples:** Autos Innovate, ATA, ACEA, JAMA, MEMA, CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.

1. **No formal agreement** required.
2. **No approval** required.
3. Added to Auto-ISAC Community Distro List to stay engaged in Community events and activities.
5. Learn what is trending in the ISACs and hear from key leaders during the special topic of interest presentation.
6. Added to Auto-ISAC DRIVEN list to receive our daily cyber automotive newsletter.
7. Part of the Network with Automotive Community and the extended automotive ecosystem.
8. **Invitation to attend and support** our yearly Summit.
Current Partnerships
Many organizations engaging

Community Partners

Thanks for your Support to our Many Partners

INNOVATOR
Strategic Partnership
(Available)
- ArmorText
- BlockHarbor
- Cybellum
- Deloitte
- FEV
- GRIMM
- HackerOne
- Irdeo
- Itemis
- Karamba Security
- KELA
- Pen Testing Partners
- Red Balloon Security
- Regulus Cyber
- Saferide
- Security Scorecard
- Trustonic
- Upstream
- Vultara

NAVIGATOR
Support Partnership
- AAA
- ACEA
- ACM
- American Trucking Associations (ATA)
- ASC
- ATIS
- Auto Alliance
- EMA
- Global Automakers
  - IARA
  - IIC
  - JAMA
  - MEMA
  - NADA
  - NAFA
  - NMFTA
  - RVIA
  - SAE
  - TIA
  - Transport Canada

COLLABORATOR
Coordination Partnership
- AUTOSAR
- Billington Cybersecurity
- Cal-CSIC
- Comptest
- Cyber Truck Challenge
- DHS CSV
- DHS HQ
- DOT-PIF
- FASTR
- FBI
- GAO
- ISAO
- Macomb Business/MADCAT
- Merit (training, np)
- MITRE
- National White Collar Crime Center
  - NCTA
  - NDIA
  - NHTSA
  - NIST
- Northern California Regional Intelligence Center (NCRIC)
  - NTIA
  - OASIS
- ODNI
- Ohio Turnpike & Infrastructure Commission
- SANS
- The University of Warwick
- TSA
- University of Tulsa
- USSC
- VOLPE
- W3C/MIT
- Walsh College

BENEFCTOR
Sponsorship Partnership
2022 Summit Sponsors-
- Argus
- BGNetworks
- Bosch
- Blackberry
- Block Harbor
- BlueVoyant
- Booz Allen Hamilton
- C2A
- Cybellum
- CyberGRX
- Cyware
- Deloitte
- Denso
- Finite State
- Fortress
- Itemis
- Keysight Technologies
- Micron
- NXP
- Okta
- Sandia
- Securonix
- Tanium
- UL
- Upstream
- VicOne
Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency

Building Resiliency Across the Auto Industry
Thank You!
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