



# **WELCOME TO AUTO-ISAC!**

## *MONTHLY VIRTUAL COMMUNITY CALL*






May 3rd, 2023

**This Session will be recorded.**

**TLP: CLEAR**



# DHS TRAFFIC LIGHT PROTOCOL (TLP) 2.0 CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p><b>TLP:RED</b></p>  <p>Not for disclosure, restricted to participants only.</p>	<p>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.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p><b>TLP:AMBER+STRICT</b></p>  <p>Limited disclosure, restricted to participants' and its organization.</p>	<p>Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.</p>	<p>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.</p>
<p><b>TLP:AMBER</b></p>  <p>Limited disclosure, restricted to participants' organization and its clients.</p>	<p>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 organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.</p>	<p>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.</p>
<p><b>TLP:GREEN</b></p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</p>	<p>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.</p>
<p><b>TLP:CLEAR</b></p>  <p>Disclosure is not limited.</p>	<p>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.</p>	<p>Recipients may share this information without restriction. Information is subject to standard copyright rules.</p>

# AGENDA

Time (ET)	Topic
11:00	<b>Welcome</b> <ul style="list-style-type: none"><li>➤ Why We're Here</li><li>➤ Expectations for This Community</li></ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"><li>➤ Auto-ISAC Activities</li><li>➤ Heard Around the Community</li><li>➤ Intelligence Highlights</li></ul>
11:15	<b>DHS CISA Community Update</b> <ul style="list-style-type: none"><li>➤ <b>Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)</b></li></ul>
11:20	<b>Featured Speaker:</b> <ul style="list-style-type: none"><li>➤ <b>Nalindrani Malimage, Cybersecurity Consultant at Burns and McDonnell</b></li><li>➤ <b>Title: : Cybersecurity Challenges in the Electric Vehicle Market</b></li></ul>
11:45	<b>Around the Room</b> <ul style="list-style-type: none"><li>➤ Sharing Around the Virtual Room</li></ul>
11:55	<b>Closing Remarks</b>

# 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](mailto:sharmilakhadka@automotiveisac.com))

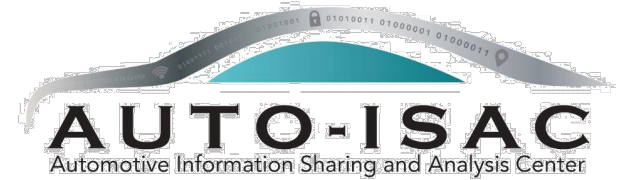




# ENGAGING IN THE AUTO-ISAC COMMUNITY

## ❖ 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 (1<sup>st</sup> Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

**27**  
*OEM Members*

**21**  
*Navigator Partners*

**48** *Supplier & Commercial Vehicle Members*

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

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

**19**  
*Innovator Partners*

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

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



**TLP: CLEAR**

# 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**



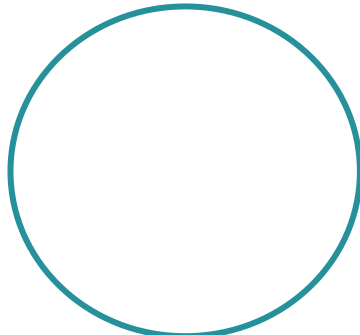
**Tim Geiger**  
*Treasurer of the  
Board of the Directors*  
**Ford**



**Andreas 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

75 MEMBERS + 5 PENDING

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

Pending: CNH Industrial, Daimler Truck, Micron, Rivian, Stoneridge

# AUTO-ISAC BUSINESS UPDATES AND EVENTS

**\*\*All times are in ET**

## Upcoming Meetings:

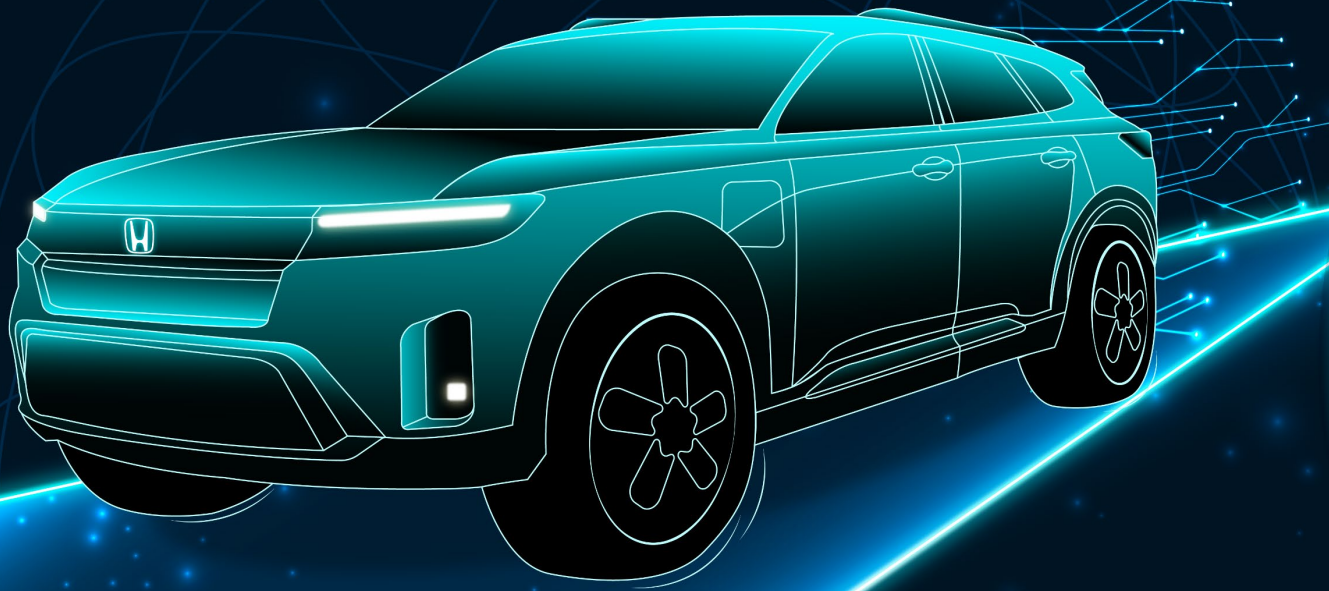
- **Members Teaching Members:** Wednesday, May 17<sup>th</sup> **Time:** 10:00am – 11:30 a.m. **TLP:AMBER**;  
**Speaker:** Jonathan Mohring, Dirk Leopold, & Gerhard Steininger; itemis **Title:** “Key Technologies for performing TARAs Efficiently”
- **Auto-ISAC Partner’s Week Event** May 22<sup>nd</sup> – May 26<sup>th</sup> 11-1 pm ET, *Virtual*. [Registration is open.](#)
- **Auto-ISAC’s first European Summit** will be June 13<sup>th</sup>-14<sup>th</sup>, 2023 with June 12<sup>th</sup> having Members-only activities. <https://automotiveisac.com/2023-europe-summit>  
**Register now! Early bird pricing for Eu summit ends May 5<sup>th</sup>.**
- **Auto-ISAC Summit** will be Tuesday, October 17<sup>th</sup>-18<sup>th</sup>, 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 8<sup>th</sup>.**

**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](mailto: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 17<sup>th</sup> 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](mailto:AlisonHwang@automotiveisac.com) with any questions.



ACCELERATING  
C A S E  
S E C U R I T Y

**HONDA**

The Power of Dreams



2023 Auto-ISAC Cybersecurity Summit | October 17-18 | Torrance, CA / [Virtual Information here](#)



**AUTO-ISAC EUROPE**

Automotive Information Sharing and Analysis Center

## 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 HIGHLIGHT

**TLP: CLEAR**





# 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 (1<sup>st</sup> Iteration) included.
  - **Send feedback**, contributions, or questions to [analyst@automotiveisac.com](mailto: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](#)).

# 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



JOINT CYBER DEFENSE  
COLLABORATIVE

Jeff Terra  
5/3/2023



- 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

- 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>
- ❑ Free Cybersecurity Services and Tools - <https://www.cisa.gov/free-cybersecurity-services-and-tools>
- ❑ 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 Cybersecurity Directives - <https://cyber.dhs.gov/directives/>



**JOINT CYBER DEFENSE  
COLLABORATIVE**

For more information:

**cisa.gov**

Questions?

**Central@cisa.dhs.gov**

**1-888-282-0870**

**Jeff Terra**  
5/3/2023





## FEATURED SPEAKER

**TLP: CLEAR**



# **NALINDRANI MALIMAGE,** *CYBERSECURITY CONSULTANT, BURNS AND McDONNELL*



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*



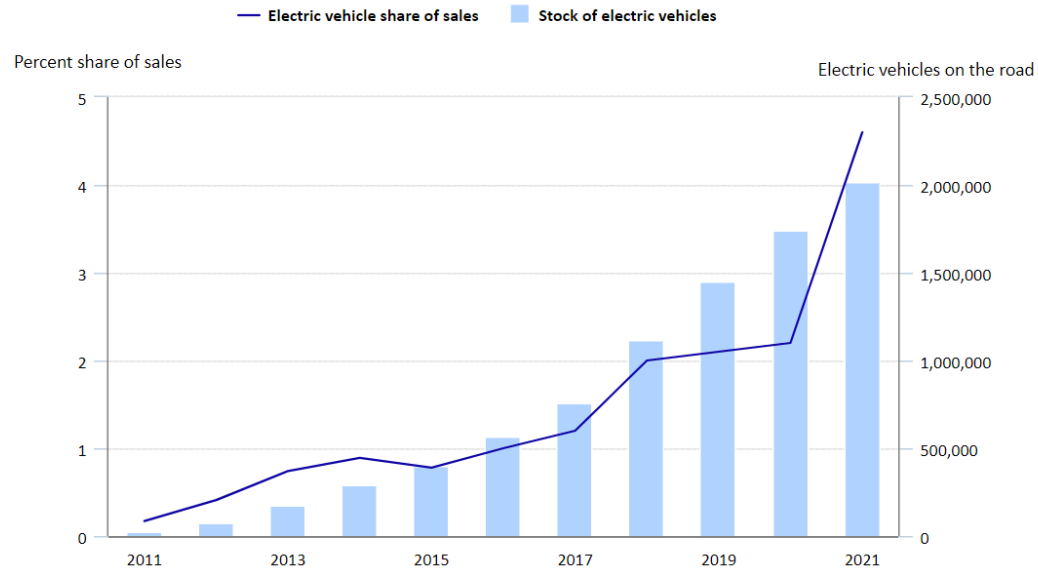
# Content

- 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...**

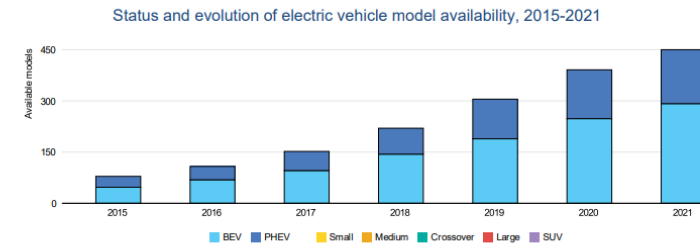
# Electric Vehicle Market Industry Overview

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

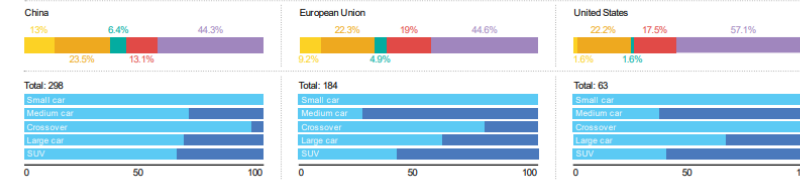


Source: U.S Bureau of Labor Statistics, February 2023

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



Available EV models by vehicle segments and powertrain

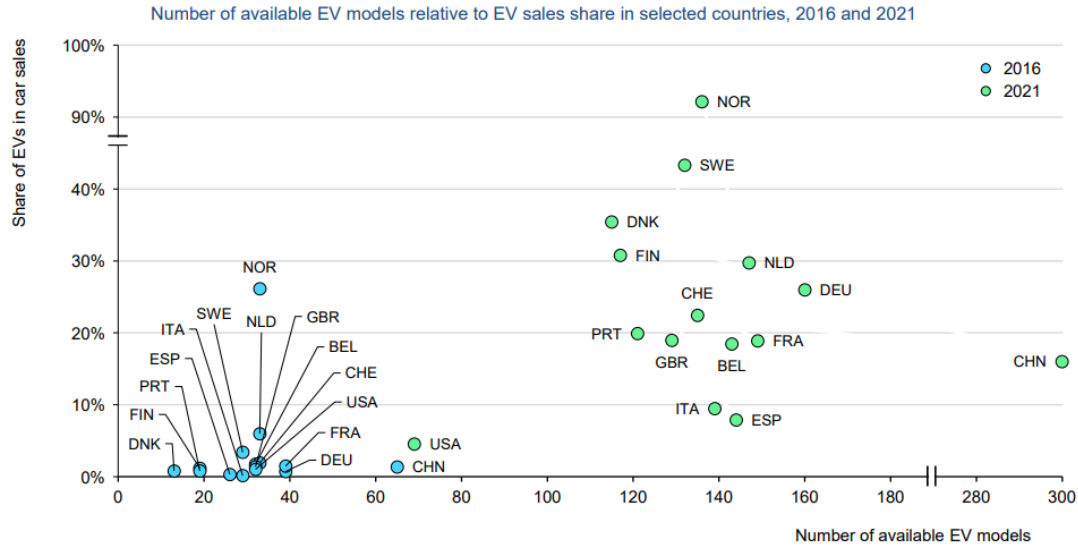


Notes: BEV = battery electric vehicle; PHEV = plug-in hybrid vehicle. Small cars include A and B segments. Medium cars include C and D segments. Crossovers are a type of sports utility vehicle (SUV) built on a passenger car platform. Large cars include E and F segments and multi-purpose vehicles. Vehicle models do not include the various trim levels. Sources: IEA analysis based on [EV Volumes and Marklines](#). IEA. All rights reserved.

Source: Global Electric Vehicle Outlook

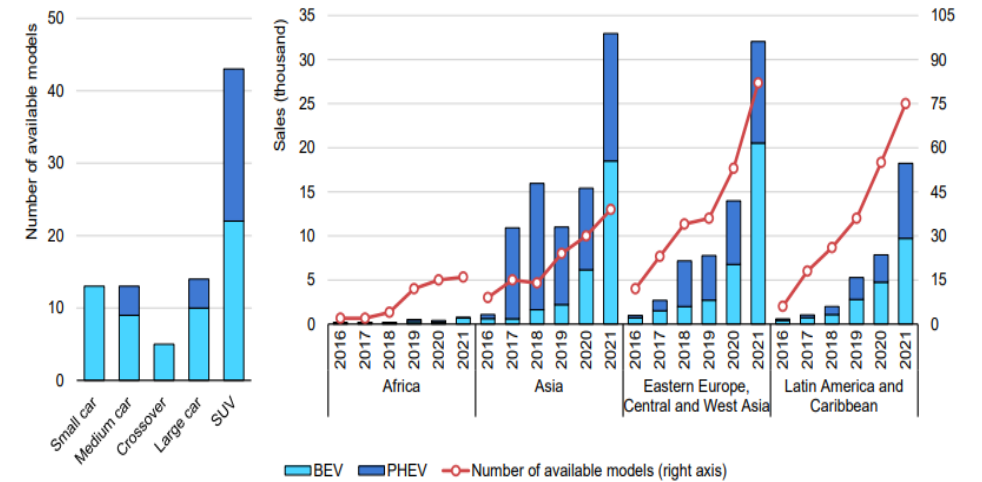
# Electric Vehicle Market Industry Overview

## EV model availability and sales share have increased significantly



## Electric car sales spiked in emerging markets in 2021

Electric car models available in selected emerging markets by segment (left), sales and models available by region 2016-2021 (right)

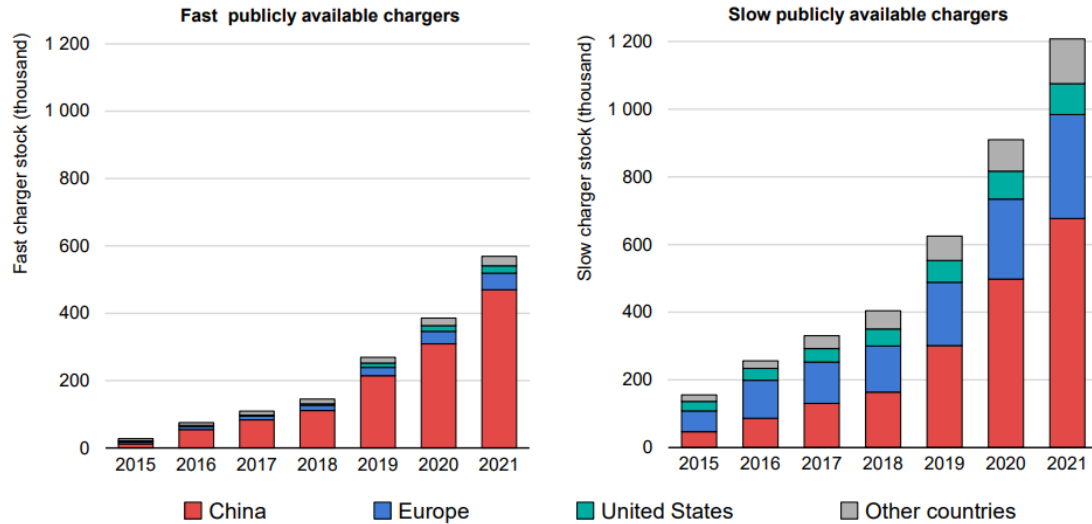


Source: Global Electric Vehicle Outlook

# 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)

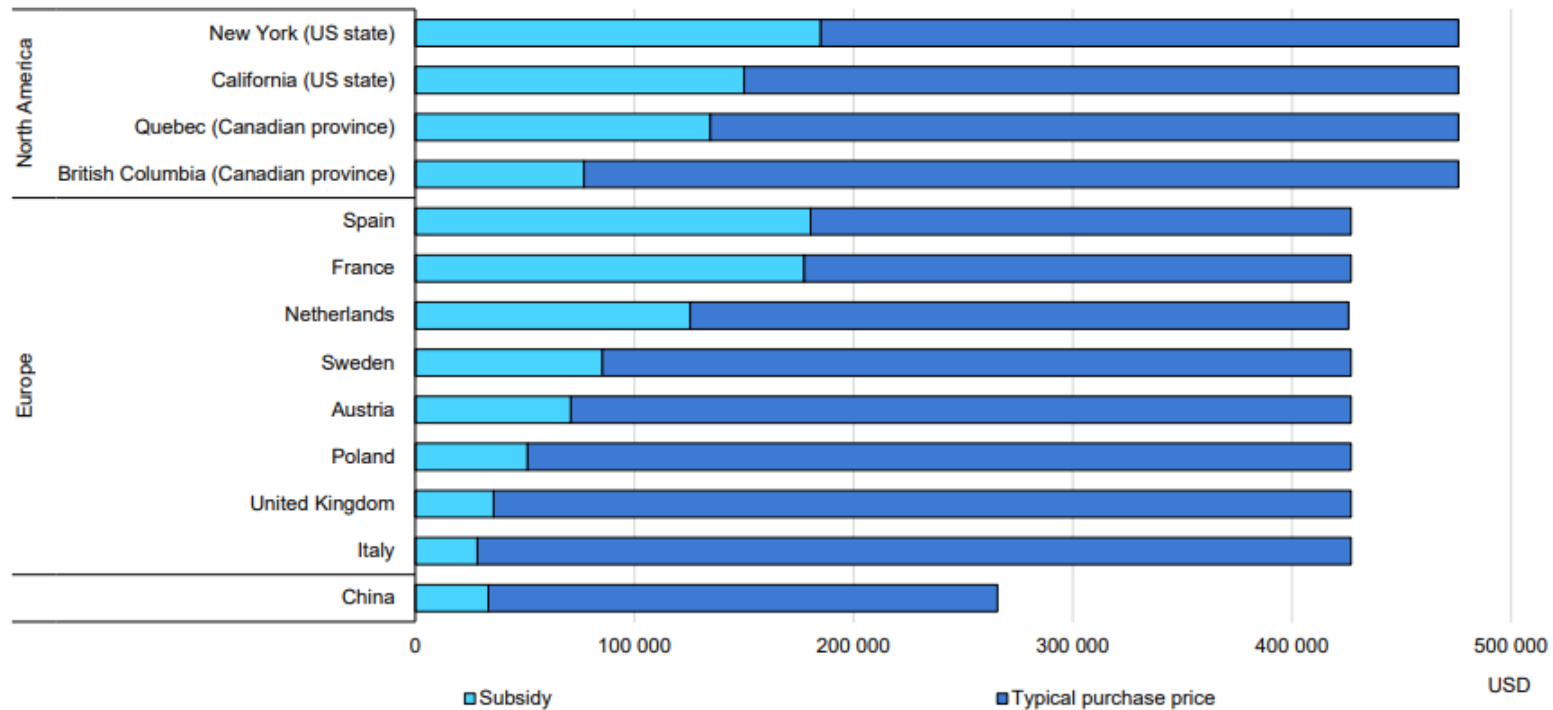
	Stations	Points	Level 1	Level 2	DC fast
<b>Total</b>	<b>50.7</b>	<b>130.7</b>	<b>3.3</b>	<b>104.8</b>	<b>22.6</b>
<b>Public</b>	<b>47.2</b> <i>93%</i>	<b>116.6</b> <i>89%</i>	<b>1.2</b> <i>35%</i>	<b>93.2</b> <i>89%</i>	<b>22.3</b> <i>99%</i>
<b>Highway</b>	<b>8.8</b> <i>17%</i>	<b>22.7</b> <i>17%</i>	<b>0.3</b> <i>9%</i>	<b>16.8</b> <i>16%</i>	<b>5.7</b> <i>25%</i>
<b>Interstate</b>	<b>3.2</b> <i>6%</i>	<b>9.3</b> <i>7%</i>	<b>0.1</b> <i>3%</i>	<b>5.7</b> <i>5%</i>	<b>3.6</b> <i>16%</i>

Source: Global Electric Vehicle Outlook

# Subsidies by state for electric trucks purchase

## Subsidies for electric trucks purchases vary

Purchase subsidies and typical prices for ZEV heavy-duty freight vehicles in selected jurisdictions, 2021



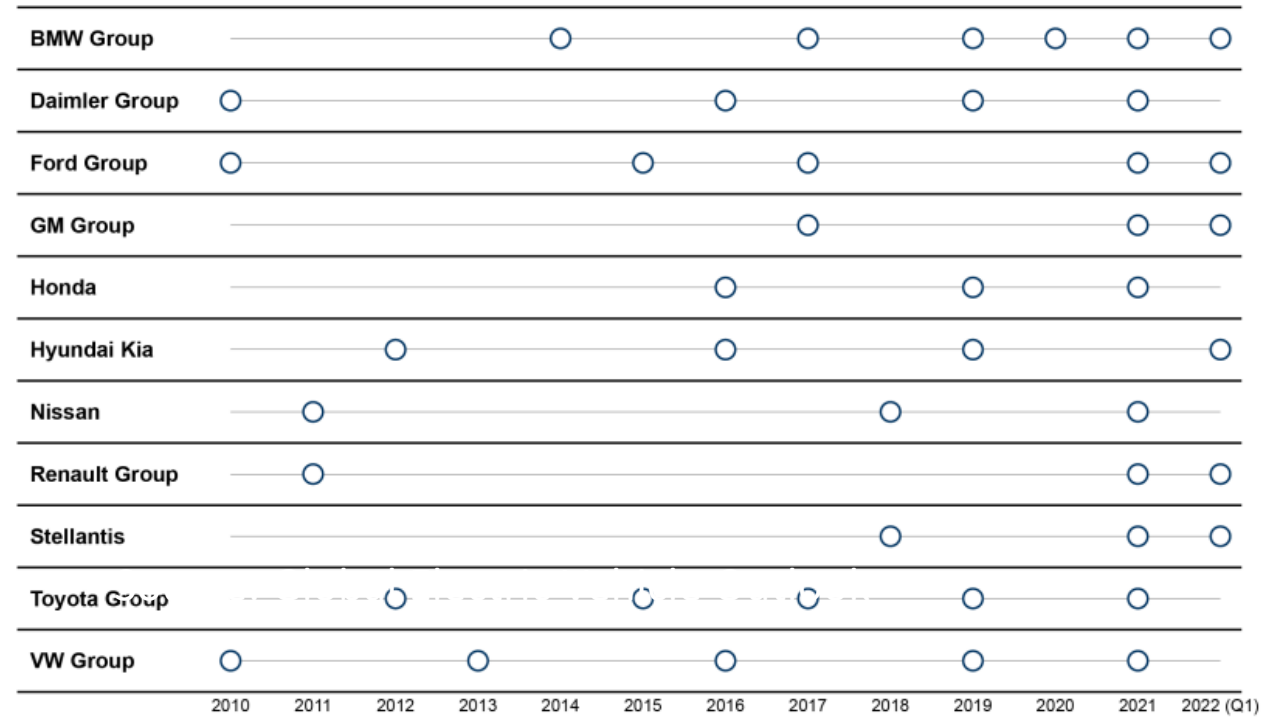
Source: Global Electric Vehicle Outlook



# Electric Vehicle Market Industry Overview

## Major automakers accelerate electrification plans

EV sales target announcements, 2010-2022 (Q1)

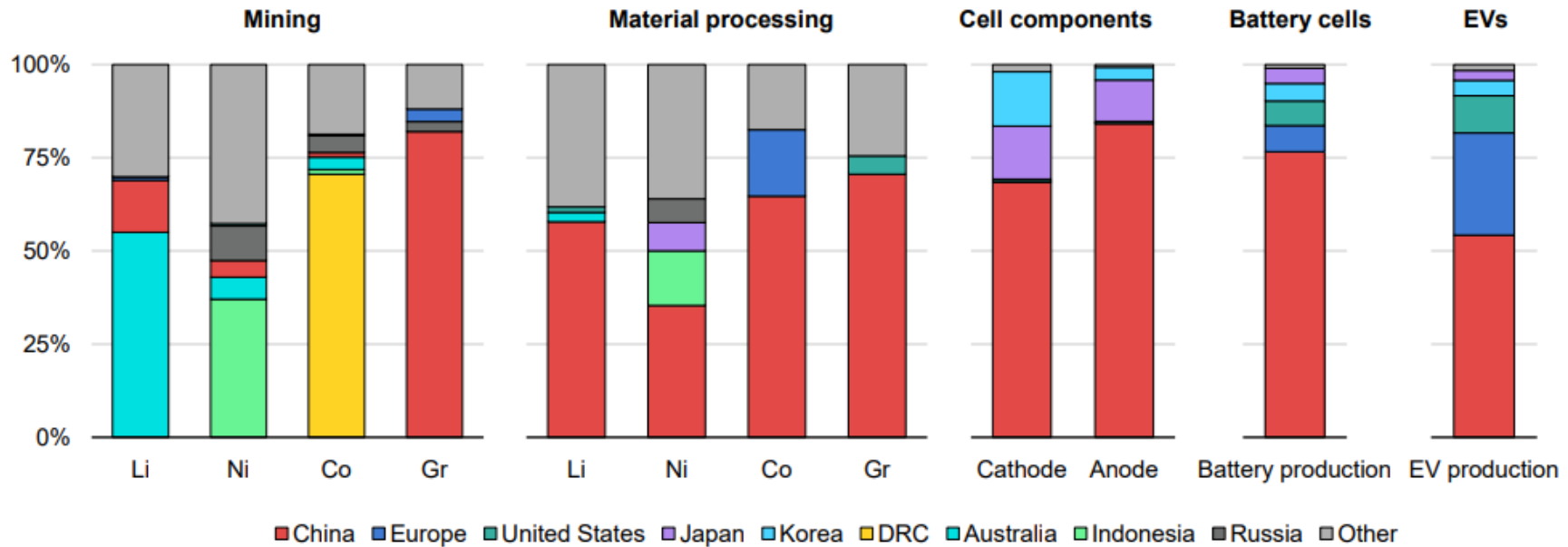


Source: Global Electric Vehicle Outlook

# Electric Vehicle Market Industry Overview

## China dominates the entire downstream EV battery supply chain

Geographical distribution of the global EV battery supply chain



IEA. All rights reserved.

Source: Global Electric Vehicle Outlook

# Electric Vehicle Market Industry Overview

**Table 1. Employment projections, 2021–31, and worker characteristics, 2021, for select electric vehicle-related occupations (employment numbers in thousands)**

Occupation title	Employment, 2021	Employment, 2031	Employment change, 2021–31	Percent employment change, 2021–31	Occupational openings, 2021–31 annual average	Median annual wage, 2021 <sup>1</sup>	Typical education needed for entry
<b>Total, all occupations</b>	158,134.7	166,452.1	8,317.4	5.3	19,532.5	\$45,760	<sup>2</sup>
<b>Software developers</b>	1,425.9	1,796.5	370.6	26.0	143.4	120,730	Bachelor's degree
<b>Electrical engineers</b>	192.4	195.5	3.1	1.6	12.3	100,420	Bachelor's degree
<b>Electronics engineers, except computer</b>	111.4	118.0	6.7	6.0	7.8	104,820	Bachelor's degree
<b>Chemical engineers</b>	26.9	30.7	3.7	13.9	2.0	105,550	Bachelor's degree

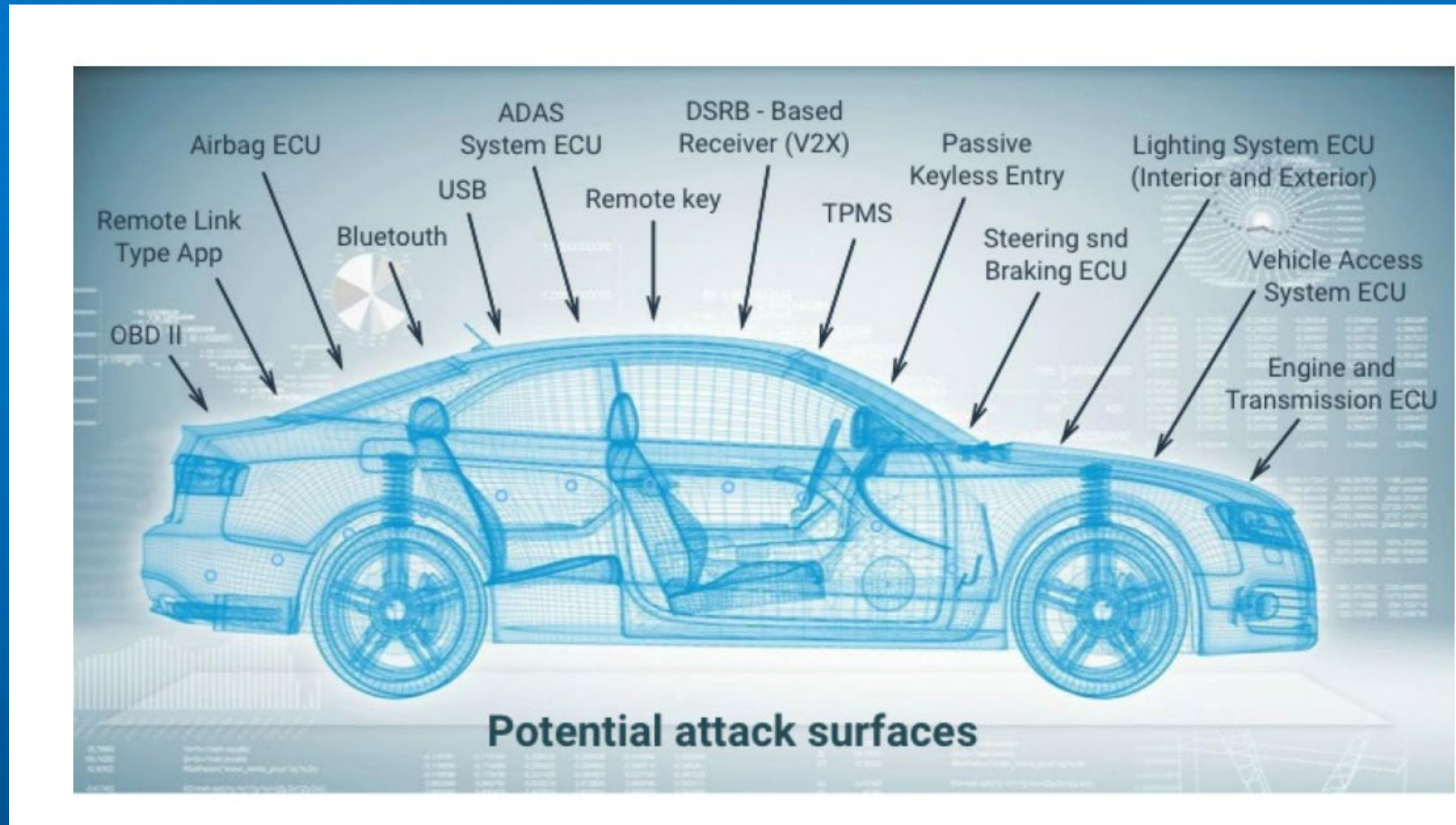
<sup>1</sup> Data are from the Occupational Employment and Wage Statistics (OEWS) program, U.S. Bureau of Labor Statistics. Wage data cover non-farm wage and salary workers and do not cover the self-employed, owners and partners in unincorporated firms, or household workers.

<sup>2</sup> Not applicable.

Source: U.S. Bureau of Labor Statistics.

# **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

```
void JSArray::sort(ExecState* exec, JSValue compareFunction,
CallType callType, const CallData& callData)
{
    checkConsistency();
    ArrayStorage* storage = m_storage;
    // .....
    // Copy the values back into m_storage.
    AVLTree<AVLTreeAbstractorForArrayCompare, 44>::Iterator
iter;
    iter.start_iter_least(tree);
    JSGlobalData& globalData = exec->globalData();
    for (unsigned i = 0; i < numDefined; ++i) {
        storage->m_vector[i].set(globalData, this,
tree.abstractor().m_nodes[*iter].value);
        ++iter;
    }
    .....
}
```

Table 2 Code Snippet of the Vulnerable Function

# 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



# Are DLP Practices in Place?

*“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..”*



## Tesla Experiences Internal Breach, Leaking Valuable Company Data



by Will Houcheime on February 3, 2021

During his two-week employment, a former Tesla Inc. software engineer stole more than 6,000 scripts, or files of code, that automate a broad range of company functions. The software automation engineer, Alex Khatilov, was hired as one of a few employees to have access to the files, which the company says were unrelated to his job.




# Aftermath of giving every employee Local Admin Rights – Access Control Policies

“The hacking software used by Tripp was operating off of 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..”

INFOSEC NEWS

## Tesla Becomes Victim of Insider Threat, Former Employee Steals Gigabytes of Data


by  Isaac Kohlen

posted on June 22, 2018

[f](#) [t](#) [+](#)

Tesla has been struck by an insider attack; the very category of attack that cyber security experts have been stressing industries to establish formidable mitigations against.

#Tesla deals with #insiderthreat attack as gigabytes of data is stolen.

[CLICK TO TWEET](#) 

# 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..”

The screenshot shows a CNBC news article. The top navigation bar includes 'MARKETS', 'BUSINESS', 'INVESTING', 'TECH', 'POLITICS', 'CNBC TV', 'INVESTING CLUB', and 'PRO'. The article is categorized under 'TECH' and has the headline 'Tesla sues former employee for allegedly stealing software code'. It was published on Friday, January 22, 2021, at 9:08 PM EST and updated at 9:50 PM EST. The author is Lora Kolodny (@LORAKOLODNY). A 'KEY POINTS' section is visible, containing three bullet points: 1) Tesla is suing a former employee and software engineer named Alex Khatilov for trade secret theft and breach of contract. 2) This is one of a string of suits Tesla has filed against former employees alleging trade theft, some still ongoing. 3) 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.

TECH

## Tesla sues former employee for allegedly stealing software code

PUBLISHED FRI, JAN 22 2021-9:08 PM EST | UPDATED FRI, JAN 22 2021-9:50 PM EST

Lora Kolodny  
@LORAKOLODNY

SHARE [f](#) [t](#) [in](#) [✉](#)

**KEY POINTS**

- According to a legal filing on Friday, Tesla is suing a former employee and software engineer named Alex Khatilov alleging trade secret theft and breach of contract.
- This is one of a string of suits Tesla has filed against former employees alleging trade theft, some still ongoing.
- 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.

# Supply Chain Breaches! Continued Vendor Risk Assessments & Due Diligence

*“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..”*

LILY HAY NEWMAN

SECURITY MAR 13, 2021 9:00 AM

## Security News This Week: Hackers Accessed Security Cameras Inside Tesla and Beyond

Plus: A Molson-Coors hack, Github controversy, and more of the week's top security news.

# 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..”

## Tesla investigates claims of crypto-currency hack

© 21 February 2018 · Comments



Tesla has confirmed that its cloud computing platform has been compromised by hackers.

RedLock, the company that alerted it to the breach, believes the attackers may have done this to mine crypto-currency - an attack known as crypto-jacking.

Tesla said it had addressed the vulnerability "within hours" and that no customer data had been stolen.



# 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. ”

Business / China Business

## Chinese EV maker Nio is being blackmailed by hacker for US\$2.25 million in bitcoin after data breach

- Shanghai-based carmaker 'is doing everything possible to support its users', CEO says
- Internal investigation finds that part of Nio's user and vehicle sales information before August 2021 has been compromised


 **Pearl Liu** [+ FOLLOW](#)  
Published: 4:30pm, 21 Dec, 2022 [Why you can trust SCMP](#)

12

- 
- 
- 
- 
- 
- 
- 
- 

Post

- 
- 



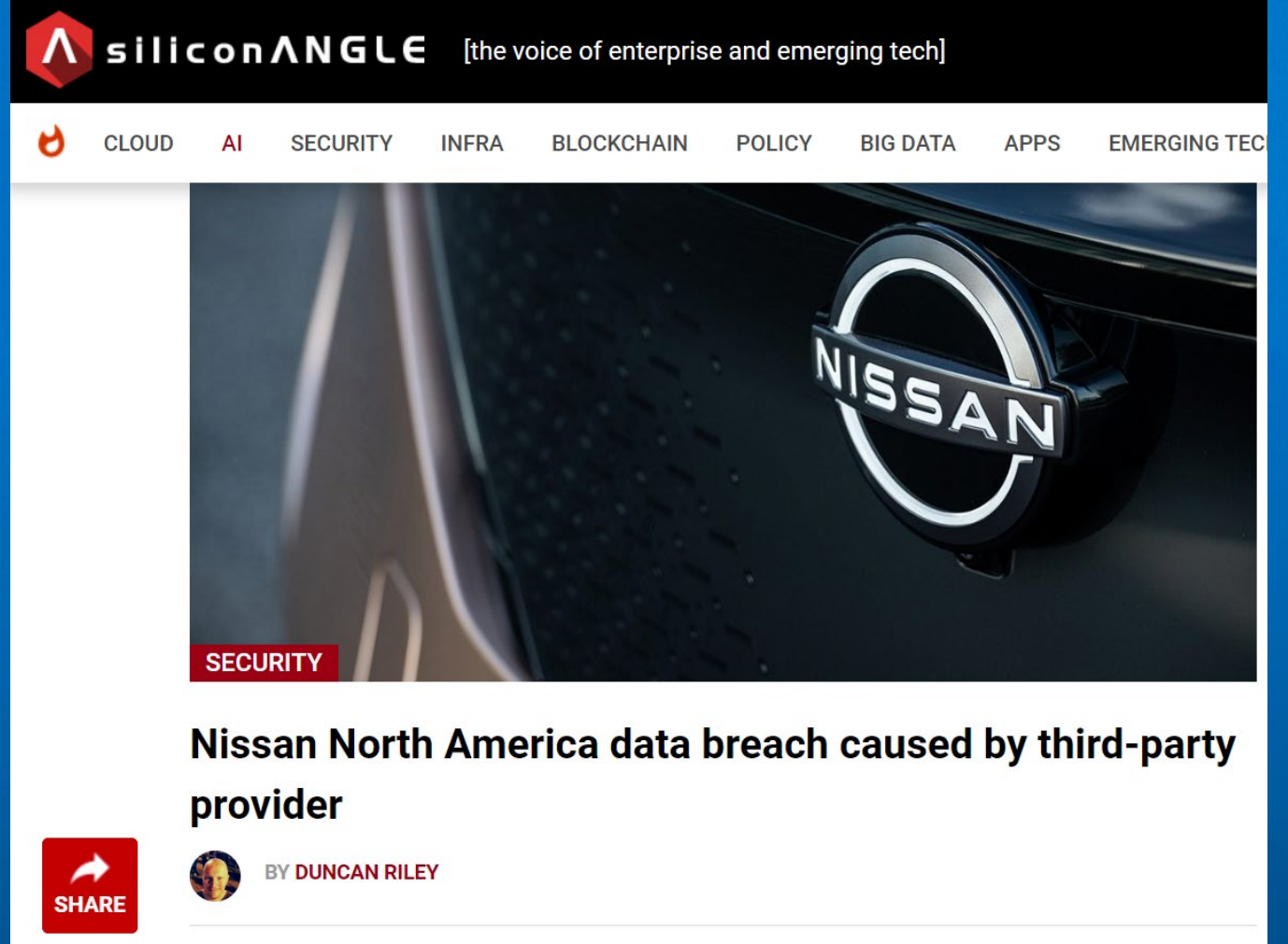
# Data Breach at NISSAN

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 the these leaks occurred due to employee internal threats and external security weaknesses across the automotive supply chain.



The screenshot shows the SiliconANGLE website header with the tagline "[the voice of enterprise and emerging tech]". The navigation menu includes categories like CLOUD, AI, SECURITY, INFRA, BLOCKCHAIN, POLICY, BIG DATA, APPS, and EMERGING TEC. The main content area features a large image of a Nissan logo on a car's grille. Below the image is a red "SECURITY" tag. The article title is "Nissan North America data breach caused by third-party provider" by Duncan Riley. A red "SHARE" button is visible in the bottom left corner of the article preview.

**siliconANGLE** [the voice of enterprise and emerging tech]

CLOUD AI SECURITY INFRA BLOCKCHAIN POLICY BIG DATA APPS EMERGING TEC

**SECURITY**

## Nissan North America data breach caused by third-party provider

BY DUNCAN RILEY

SHARE

# 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.”



The screenshot shows a webpage from SecurityWeek. The header includes the SecurityWeek logo and navigation menus for Malware & Threats, Security Operations, Security Architecture, Risk Management, CISO Strategy, ICS/OT, and Funding/M&A. The article is categorized under CYBERCRIME. The main headline is "Hacker Selling Data Allegedly Stolen From Volvo Cars Following Ransomware Attack". Below the headline is a sub-headline: "A hacker is offering to sell data allegedly stolen from Swedish vehicle manufacturer Volvo Cars following a ransomware attack carried out in late December." The author is identified as Eduard Kovacs, with a date of January 4, 2023. A social media sharing bar is visible. A trending section on the right lists "Google Patches Second Chrome Zero-Day Vulnerability of 2023" as the top item. A partial article snippet at the bottom reads: "put up for sale on a public hacker forum on December 31. The seller".



# **Compliance and Regulations surrounding EV Industry**



# ISO/SAE 21434:2021

## Road vehicles — Cybersecurity Engineering



# **Gaps in the Industry and How to Prepare**

# Supply Chain Attacks

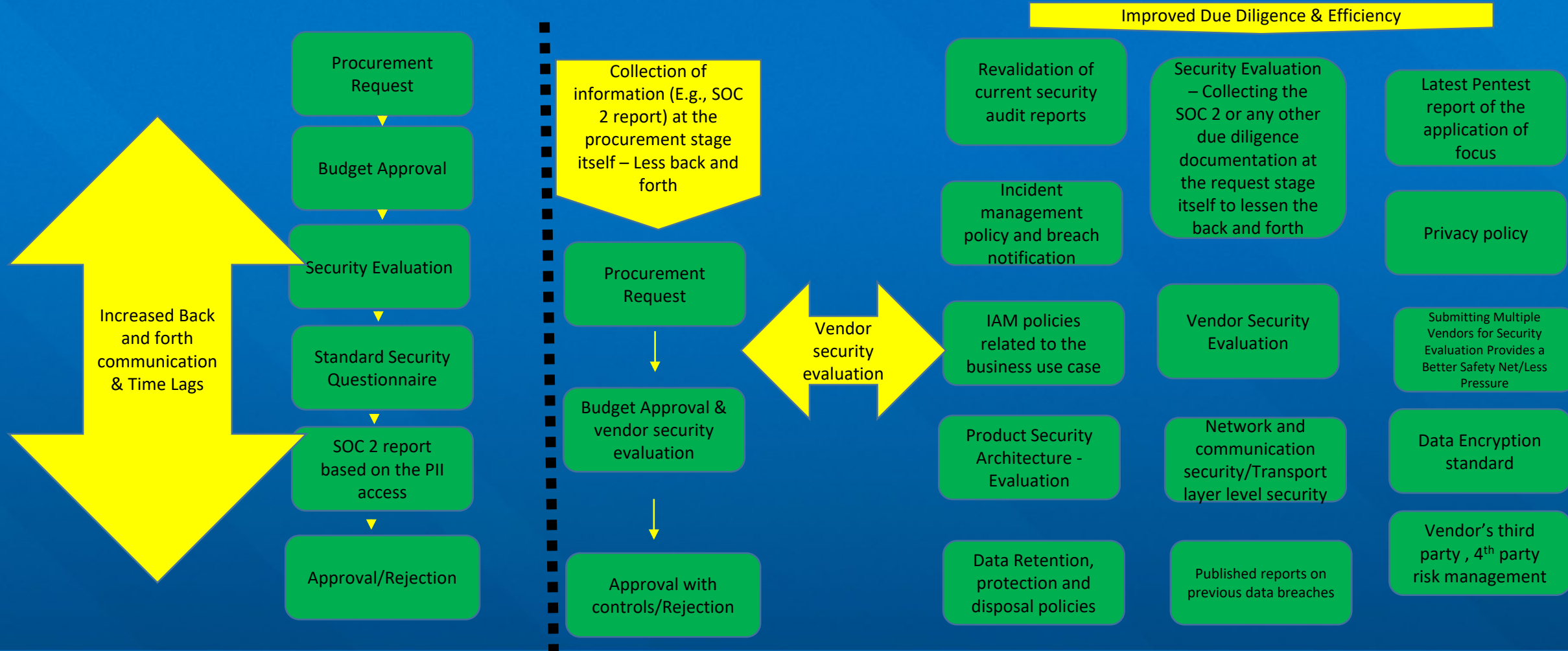


## Cost of Supply Chain Attacks:

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

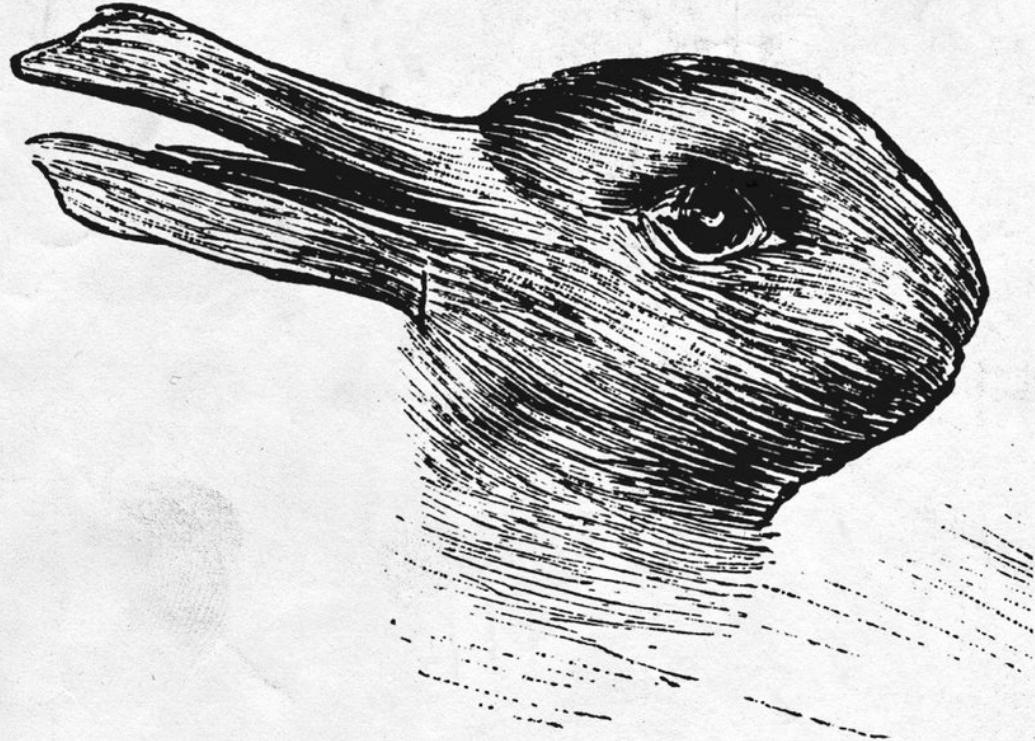
## From Process Driven to Business Case Specific Evaluation:





# Security Incident Response - Limitations

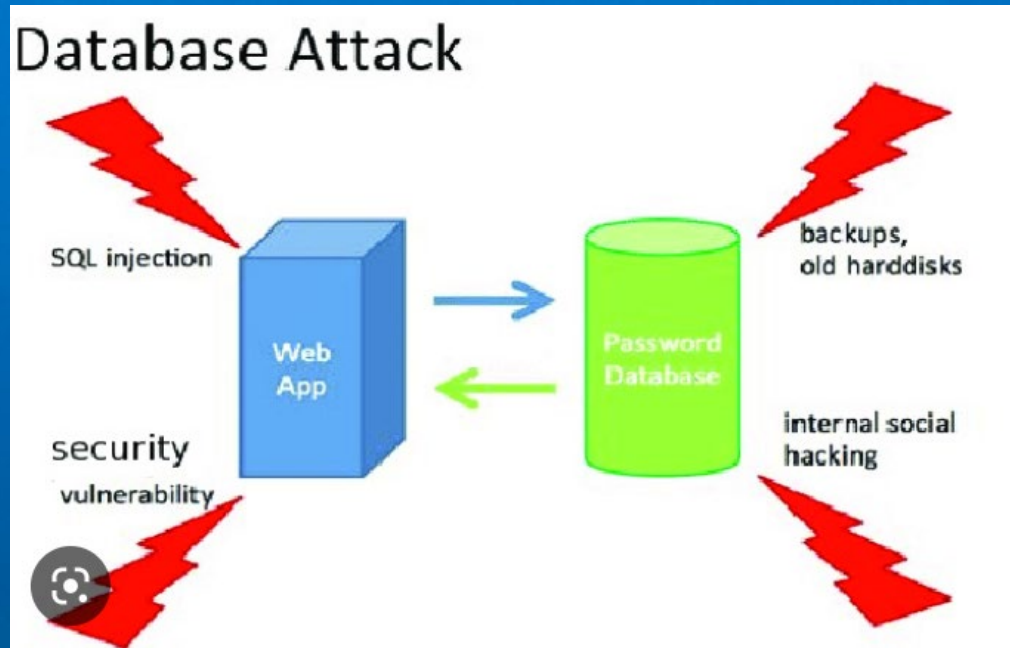
**Who Sees a Duck? Who sees a Rabbit?**





# 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

**BURNS  MCDONNELL®**

## OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE  
TOPICS FOR DISCUSSION?*



# HOW TO GET INVOLVED: MEMBERSHIP

**IF YOU ARE AN OEM, SUPPLIER OR COMMERCIAL VEHICLE,  
CARRIER OR FLEET, PLEASE JOIN THE AUTO-ISAC!**

- *REAL-TIME INTELLIGENCE SHARING*
- *INTELLIGENCE SUMMARIES*
- *REGULAR INTELLIGENCE MEETINGS*
- *CRISIS NOTIFICATIONS*
- *MEMBER CONTACT DIRECTORY*
- *DEVELOPMENT OF BEST PRACTICE GUIDES*
- *EXCHANGES AND WORKSHOPS*
- *TABLETOP EXERCISES*
- *WEBINARS AND PRESENTATIONS*
- *ANNUAL AUTO-ISAC SUMMIT EVENT*

**To learn more about Auto-ISAC Membership, please contact [melissacromack@automotiveisac.com](mailto:melissacromack@automotiveisac.com).  
For Partnership, please contact [sharmilakhadka@automotiveisac.com](mailto: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).
  2. Formal agreements: **NDA, SPA, SoW, CoC** required.
  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.
  4. Participate in **Auto-ISAC Monthly Community Calls**.
  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

*Thanks for your Support to our Many Partners*

### COMMUNITY PARTNERS

#### INNOVATOR

**Strategic Partnership  
(19)**

ArmorText  
BlockHarbor  
Cybellum  
Deloitte  
FEV  
GRIMM  
HackerOne  
Irdeto  
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  
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  
OASIS  
ODNI  
Ohio Turnpike & Infrastructure Commission  
SANS  
The University of Warwick  
TSA  
University of Tulsa  
USSC  
VOLPE  
W3C/MIT  
Walsh College

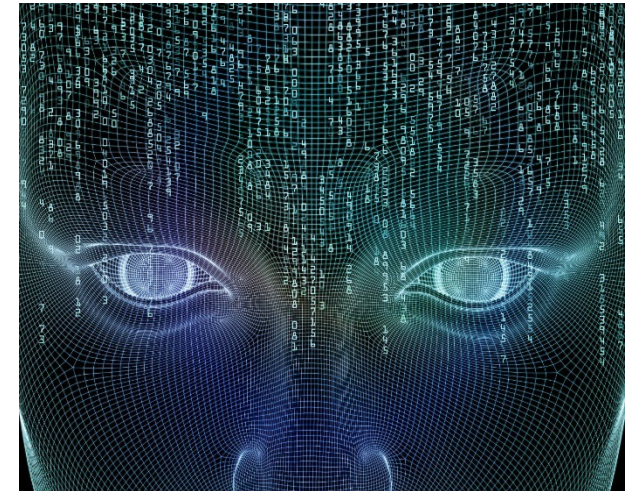
#### BENEFACTOR

**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](http://www.automotiveisac.com)  
@auto-ISAC