



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

July 5, 2023

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



AUTO-ISAC ANTITRUST STATEMENT

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.

Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.






This meeting is being held at

TLP:CLEAR

Disclosure is not limited.

TRAFFIC LIGHT PROTOCOL (TLP)

VERSION 2.0 DEFINITIONS

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</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>TLP:AMBER+STRICT</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>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.</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>TLP:GREEN</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>TLP:CLEAR</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>

Source: <https://www.us-cert.gov/tlp>

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ Intelligence Highlights
11:15	DHS CISA Community Update <ul style="list-style-type: none">➤ Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Roy Zur, President, CEO, ThriveDX Enterprise➤ Title: "Driving a Cyber-Secure Culture in Auto Manufacturing: The Essential Role of the Human Factor"
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

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

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

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

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

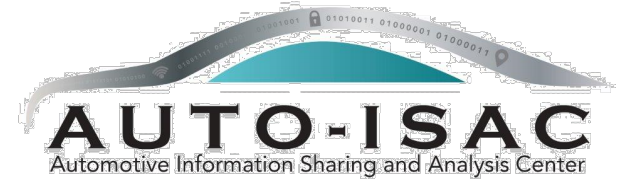
How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*



❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

29
OEM Members

21
Navigator
Partners

46 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)



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



Ravi Puvvala
Chair of the SAG
Fleet Defender



Monica Mitchell
Polaris



Bob Kaster
Bosch



Brian Witten
Aptiv

AUTO-ISAC MEMBER ROSTER

AS OF JULY 1, 2023

75 MEMBERS + 5 PENDING

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

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

AUTO-ISAC BUSINESS UPDATES AND EVENTS

**All times are in ET

Upcoming Meetings:

- **Members Teaching Members:** Wednesday, July 19th **Time:** 10:00am – 11:30 a.m. **TLP:AMBER**;
Speaker: Mortiz Minzlaff, ETAS **Title:** “An Industry on the Move: Raising cyber maturity in Automotive”
- **Auto-ISAC Summit** will be Tuesday, October 17th-18th, 2023 in Torrance, California. Sponsorship opportunities are still available. <https://automotiveisac.com/2023-annual-summit>
Register now! Early bird pricing for US summit ends September 8th.
- **ACT Fundamentals Courses:** Registration opens this summer for the 3 Automotive Cybersecurity Training (ACT) Fundamentals Courses that form the basic building blocks towards Certified Automotive cyberSecurity Engineer (CASE) certification. Registration information will be posted here: <https://automotiveisac.com/automotive-cybersecurity-training>

ACCELERATING
CASE
SECURITY



**7th Annual Auto-ISAC
Cybersecurity Summit**

October 17-18, 2023

Torrance, CA

HONDA
The Power of Dreams


AUTO-ISAC



AUTO-ISAC INTELLIGENCE HIGHLIGHT

This document is Auto-ISAC Sensitive and Confidential.

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 (1st Iteration) included.
 - **Send feedback**, contributions, or questions to analyst@automotiveisac.com
- Intelligence Notes
 - Although small signs of de-escalation are starting to appear, geopolitical tensions involving Russia, China, North Korea, and Iran remain **high** with Russia- Ukraine in crisis. Threat of cyberattack spillover increases **if**: (1) the Russia-Ukraine war leads to kinetic clashes with the West (possible but unlikely), and (2) any other hotspots escalate into crises (possible) ([Russia-Ukraine](#) ¹, [China](#) ^{2 3 4}, [North Korea](#), [Iran](#)).
 - Ransomware ⁵ Groups Targeting Automotive: [8Base](#), [CI0p](#), [BlackBasta](#), [LockBit 3.0](#), [Akira](#), [BianLian](#).
 - Threat actors continue to advertise access to automotive organizations' databases or files containing stolen data on sites such as Leakbase, XSS, and MalwareBazaar.
 - Logs of +100K raccoon stealer-infected devices with ChatGPT account credentials for sale on unspecified dark web marketplaces in the past year ([Group-IB](#)).
 - Notable TTPs and Tools: Hijacking S3 buckets ([Checkmarx](#)); Employing voice cloning & ChatGPT ([Trend Micro](#)); Stealing credentials from MQTT server—non-automotive case ([Kaspersky](#)); Layer 7 DDoS Attacks ([Microsoft](#)); Process injection ([Security Joes](#)); Exploitation of VMware vRealize ([BleepingComputer](#)); Fileless Attacks ([CSO](#)); Credential stealing ([The Hacker News](#)); Exploitation of network-attached storage ([SecurityWeek](#)); Flipper Zero ([TechCrunch](#)); Metasploit ([Rapid7](#)); Triangulation ([BleepingComputer](#)); ObserverStealer ([Medium](#)).

CISA Resource Highlights

- Joint Cyber Defense Collaborative



JOINT CYBER DEFENSE
COLLABORATIVE

Jeff Terra
7/5/2023



- CISA is aware of open-source reporting of targeted denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks against multiple organizations in multiple sectors.
- Contact your network administrator to confirm whether the service outage is due to maintenance or an in-house network issue. Network administrators can also monitor network traffic to confirm the presence of an attack, identify the source, and mitigate the situation by applying firewall rules and possibly rerouting traffic through a DoS protection service.
- Contact your internet service provider to ask if there is an outage on their end or if their network is the target of an attack and you are an indirect victim. They may be able to advise you on an appropriate course of action.

- Please note all information provided is TLP Amber

- The Homeland Security Systems Engineering and Development Institute, sponsored by the Department of Homeland Security and operated by MITRE, has released the 2023 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses.
- The CWE Top 25 is calculated by analyzing public vulnerability data in the National Vulnerability Data (NVD) for root cause mappings to CWE weaknesses for the previous two calendar years.
- These weaknesses lead to serious vulnerabilities in software. An attacker can often exploit these vulnerabilities to take control of an affected system, steal data, or prevent applications from working.

CISA and Partners Release Joint Guide to Securing Remote Access Software

16

- CISA, FBI, NSA, MS-ISAC, and the Israel National Cyber Directorate (INCD) released the Guide to Securing Remote Access Software.
- This joint guide is the result of a collaborative effort to provide an overview of legitimate uses of remote access software, as well as common exploitations and associated tactics, techniques, and procedures (TTPs), and how to detect and defend against malicious actors abusing this software.
- Remote access software provides organizations with a broad array of capabilities to maintain and improve information technology (IT), operational technology (OT), and industrial control system (ICS) services; however, malicious actors often exploit this software for easy and broad access to victim systems.
- CISA encourages organizations to review this joint guide for recommendations and best practices to implement in alignment with their specific cybersecurity requirements to better detect and defend against exploitation.

- Please note all information provided is TLP Amber

Security/Software Updates

For the period of 6/1/23 - 6/30/23:

- VMWare Releases Security Update: vCenter Server and Aria
- Juniper Releases Security Advisor: Junos OS and other products
- Progress Software Releases Security Advisor: MoveIT Transfer
- Baracuda Networks Releases Update: ESG Vulnerability
- Fortinet Releases Vulnerability Advisories and Security Updates
- Adobe Releases Security Updates: Multiple products
- Microsoft Releases Security Updates:
- Mozilla Releases Security Updates: Multiple products

- **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 6/1/23- 6/30/23 approximately 43 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 24 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of June. 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
7/5/2023



AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- ❖ Goal is to showcase a rich & balanced variety of topics and viewpoints
- ❖ *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

30+
*Featured
Speakers to
date*

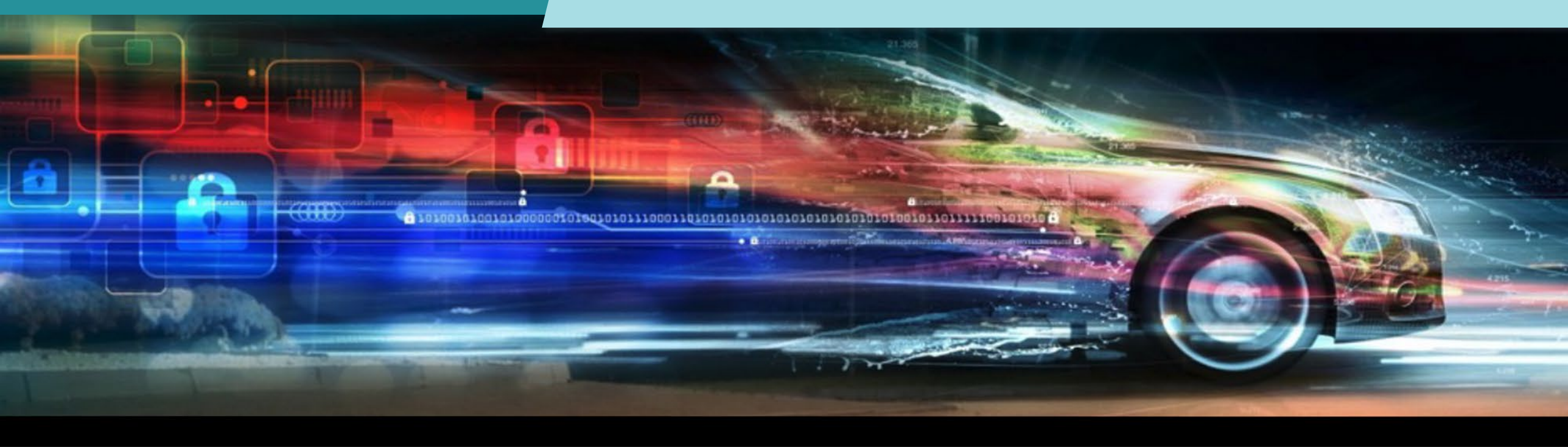
How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



ROY ZUR

FOUNDER & CEO OF THRIVEDX'S



Roy Zur, a serial entrepreneur, is Founder & CEO of ThriveDX's Enterprise Division the global education company committed to transforming lives through digital skills training and solutions. In August of 2021, ThriveDX acquired Cybint Solutions where he also served as CEO since founding the company in 2014.

Roy is a 15-year veteran of the vaunted Unit 8200 of the Israeli Defense Force, where he served as a Major, which instilled in him early a passion for addressing the “human factor” of cybersecurity training – currently the #1 vulnerability across the threat landscape.

In addition to steering the vision of ThriveDX's Enterprise Division, Roy serves as adjunct professor of risk management in cybersecurity at IDC Herzliya in Israel. He is also Founder and Chairman of the non-profit Israeli Institute for Policy and Legislation, and a member of the Forbes Business Council.

ThriveDX



Driving a Cyber-Secure Culture In Auto-Manufacturing

The Essential Role of the Human Factor

Human Factor Challenge - Talent Shortage & Skills Gap

3.5M

Unfilled jobs globally in
cybersecurity as
of 2022

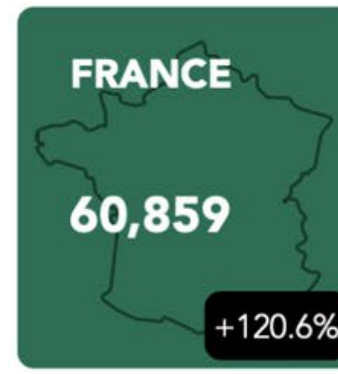
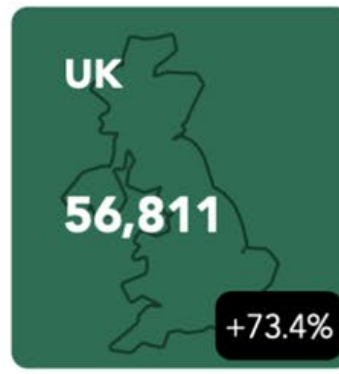
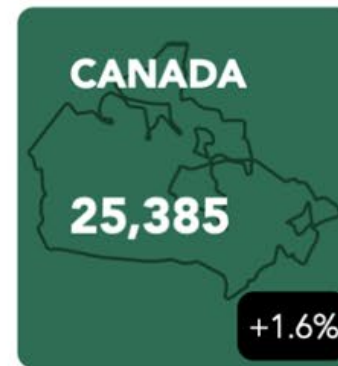
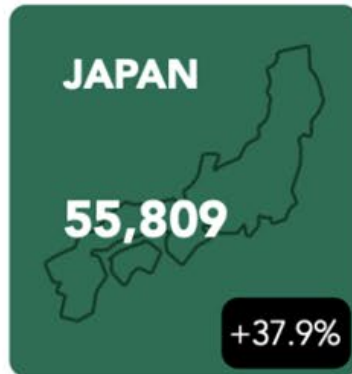


95%

of cyber breaches involve
the HUMAN FACTOR

Challenge #1 - Cybersecurity Talent Shortage

FIGURE 2-B



CYBERSECURITY SUPPLY/DEMAND HEAT MAP

- All
- Public Sector Data...
- Private Sector...
- Total job openings

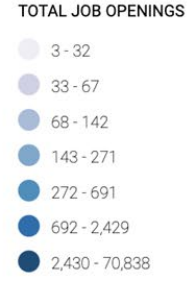
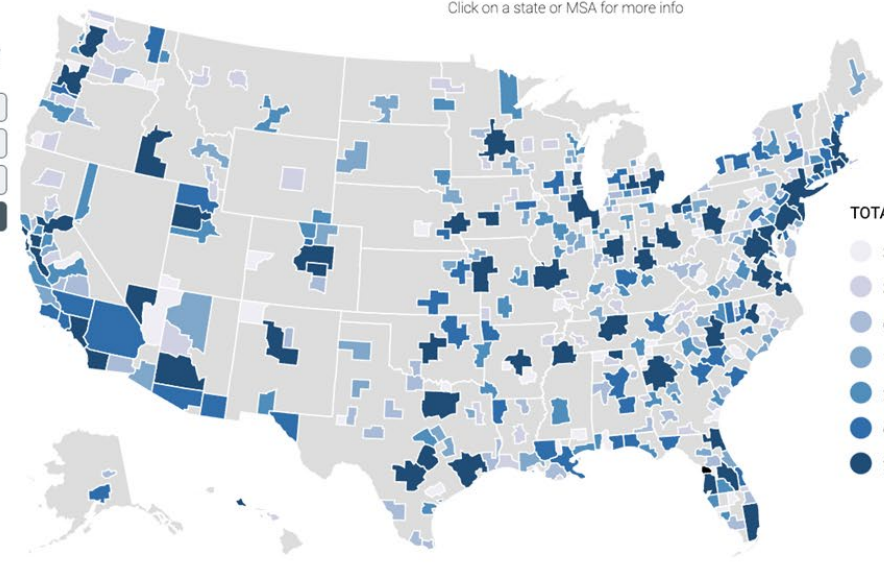
Reset

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

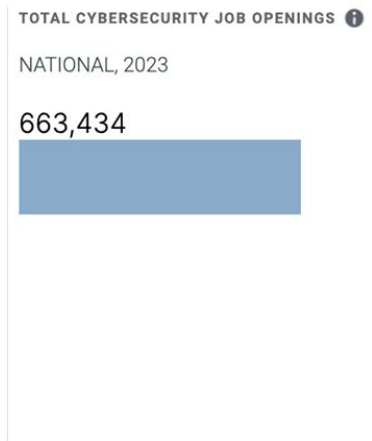
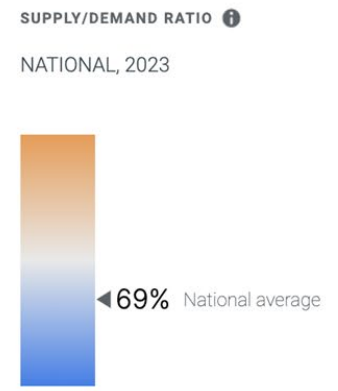
- Share
- Embed

Current Date (2023) States Metro Areas Search Metro Area

- Filter Metro Area by population
- Small
 - Medium
 - Large
 - All

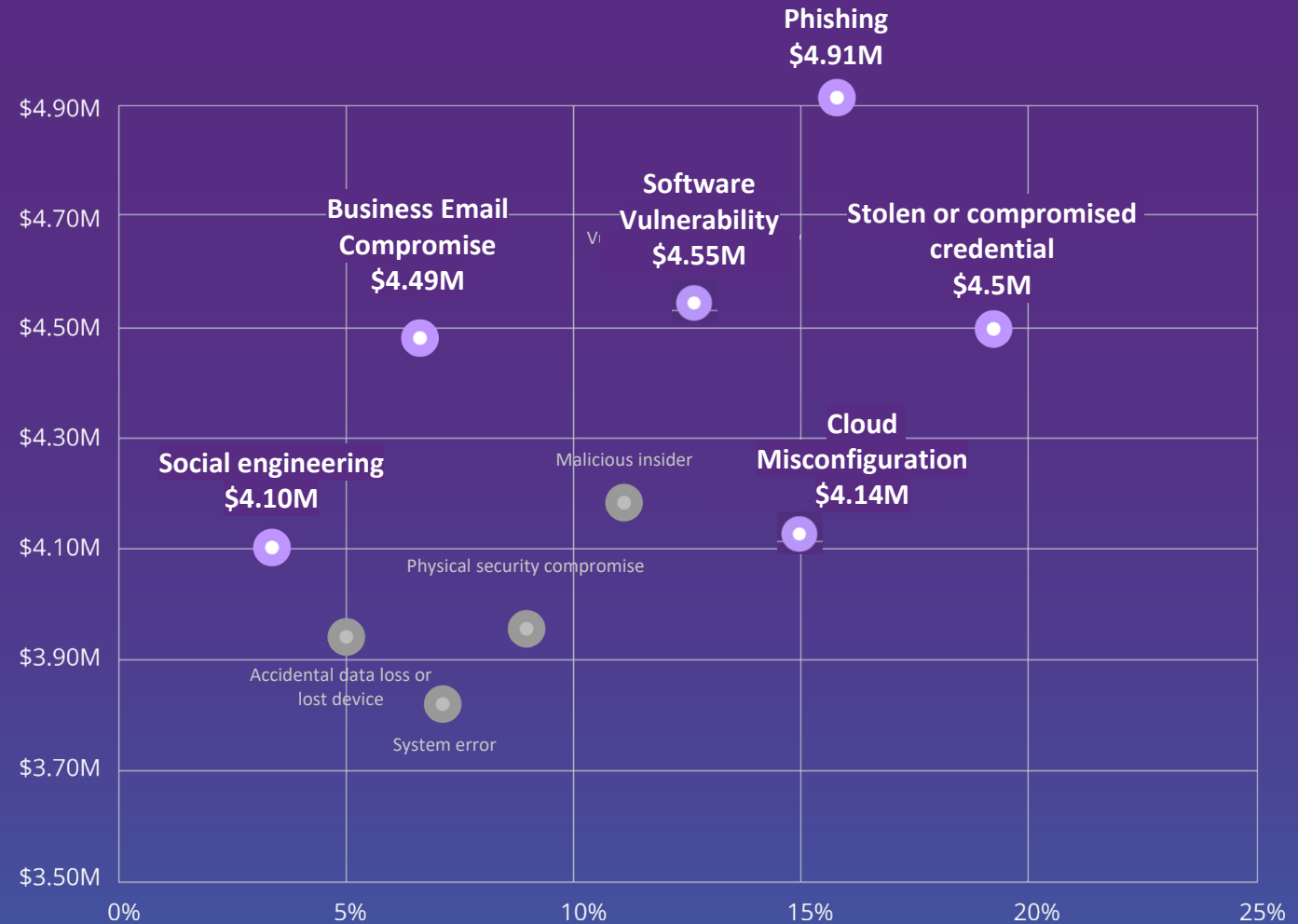


National Level



Challenge #2 Cybersecurity Skills Gap

Most Frequent &
Costly Attack Vectors
are **Human Factor**
Related



Average cost and frequency
of data breaches by initial attack vector



Worldwide, 80% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills and/or awareness.

Here are a few examples:

The survey shows that 64% of organizations experienced breaches that resulted in lost revenue and/or cost them fines during the past year. A staggering 38% of organizations reported breaches that cost them more than a million dollars (USD).

A key factor is that organizations struggle to find and retain certified cybersecurity people. Global leaders indicate that:

- 60% struggle to recruit cybersecurity talent
- 52% struggle to retain qualified people
- 67% agree that the shortage of qualified cybersecurity candidates creates additional risks for their organizations

They're not wrong.



Organizations need qualified cybersecurity professionals now more than ever, which is why 76% of organizations indicate that their board of directors now recommends increases in IT and cybersecurity headcount.

In this report, we analyze the results from our survey to explore five central themes about why the current cybersecurity skills gap matters, and how organizations are attempting to fill it.

Automotive Industry - Talent & Skills Gap

[Insights](#)[Industries](#)[Services](#)[Events](#)[Careers](#)[About us](#)

Cyber security in the automotive...



Skills shortage worries the entire industry

Respondents also state that the skills shortage, which was already considered very relevant in the 2021 survey, continues to concern them. A lack of cybersecurity skills is of most concern to the industry - regardless of the maturity of the company.

Also complex for companies is cybersecurity budgeting. Almost 50 per cent of respondents see this as a "major challenge". Representatives of established companies report constant and increasing budgets, while younger, smaller companies often lack fixed budgets - and in some cases the budgets are even unknown.



Toyota Breach - May 2023

<https://www.drive.com.au/news/toyota-data-breach-japan-australia-not-affected/>

'Human error' exposed vehicle data of 2.15 million Toyota customers for over a decade

Tokyo, Japan • Edited By: Moohita Kaur Garg • Updated: May 13, 2023, 02:24 PM IST



Toyota Motor Corp on Friday admitted that the vehicle data of 2.15 million customers in Japan, including those of its luxury brand Lexus, had been publicly available for almost a decade due to a 'human error'. The incident, which affected nearly the entire customer base who signed up for Toyota's main cloud service platforms since 2012, was caused by a cloud system being set to public instead of private.

Responding to a question regarding why it took Toyota so long to realise the mistake, a spokesperson for the company said, "There was a lack of active detection mechanisms, and activities to detect the presence or absence of things that became public."



End
Users

Hyundai Breach - April 2023

<https://www.infosecurity-magazine.com/news/hyundai-experiences-cybersecurity/>

NEWS 14 APR 2023

Hyundai Experiences Cybersecurity Issues: Breach and App Bugs



Alessandro Mascellino

Freelance Journalist

Email Alessandro Follow @a_mascellino



Automotive manufacturer [Hyundai](#) has recently disclosed a breach that has affected an unspecified number of Italian and French car owners as well as individuals who booked a test drive.



The company notified affected individuals via email. Several of them posted a screenshot of the message on [Twitter](#) earlier this week.



"I am sorry to inform you that our company has recently learned that an **unauthorized third party has had access to some information contained in our customer database,**" reads the mail (translated from Italian by *Infosecurity* journalists). "As soon as we were informed of the incident, we immediately launched an investigation and put in place all measures to contain it."

The company added that it also blocked the affected server and removed it from its network.

Data impacted by the breach included contact information (such as email, addresses and phone numbers) and vehicle data (such as chassis numbers).



Developer



Tester



Systems Administrator

101100
010110

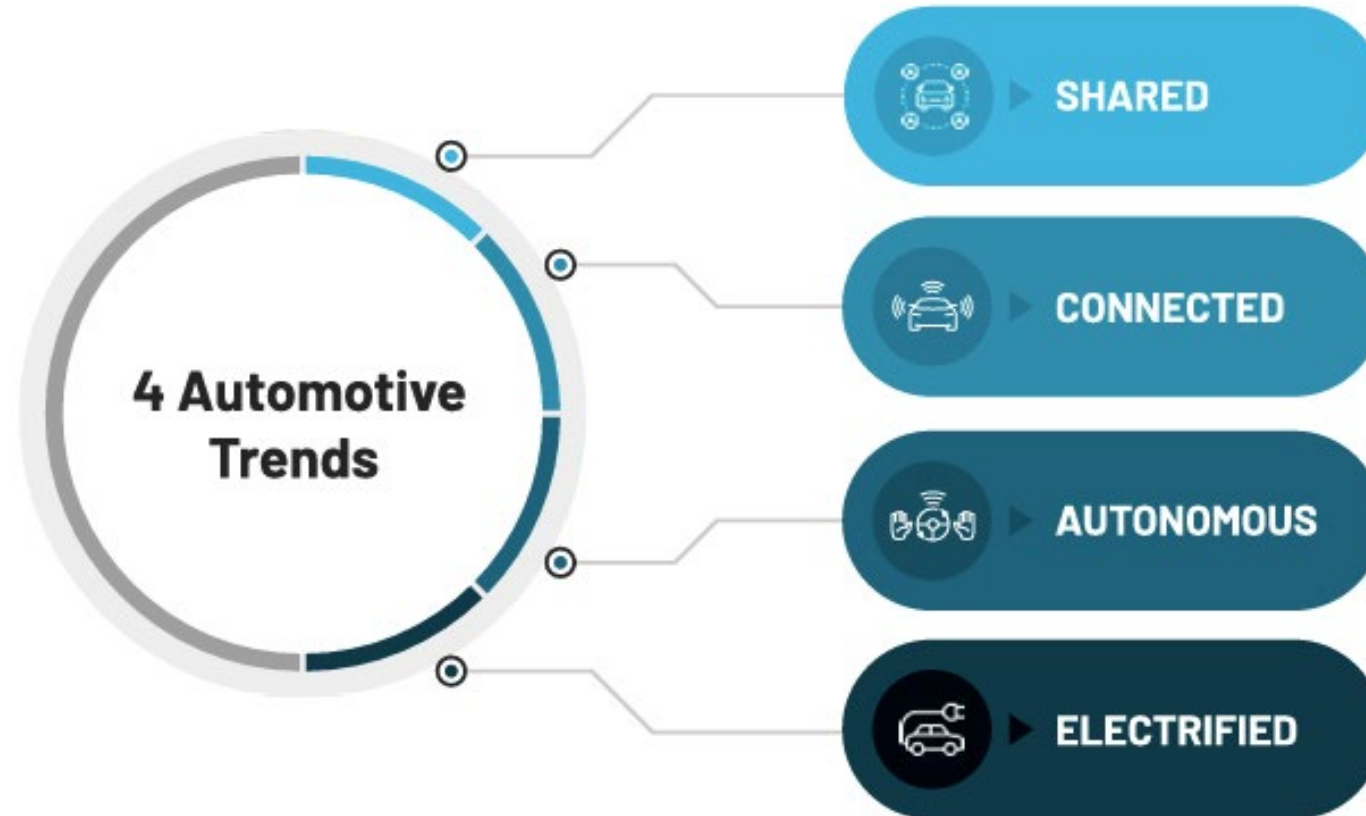


"The sheer number of websites and services managed by a complex international business like Hyundai is staggering, and it's possible that one of these sites may not have had the company's standard security controls applied," Freeman added.

Days after the data breach was disclosed, various security researchers [revealed on Twitter](#) **new flaws in Hyundai mobile apps that exposed different car models** after 2012 to remote attacks allowing vehicles to be unlocked and started.

"As modern vehicles become increasingly electronic-based products, they are both more connected and more software-driven," explained [Approov](#) CEO, Ted Miracco. "These trends make all automotive companies much more vulnerable to cyberattacks, particularly those emanating from mobile apps or devices."

Automotive Trends - CASE Security



The human factor can cause a significant impediment to Industry 4.0 elements. (MDPI)



Engineering

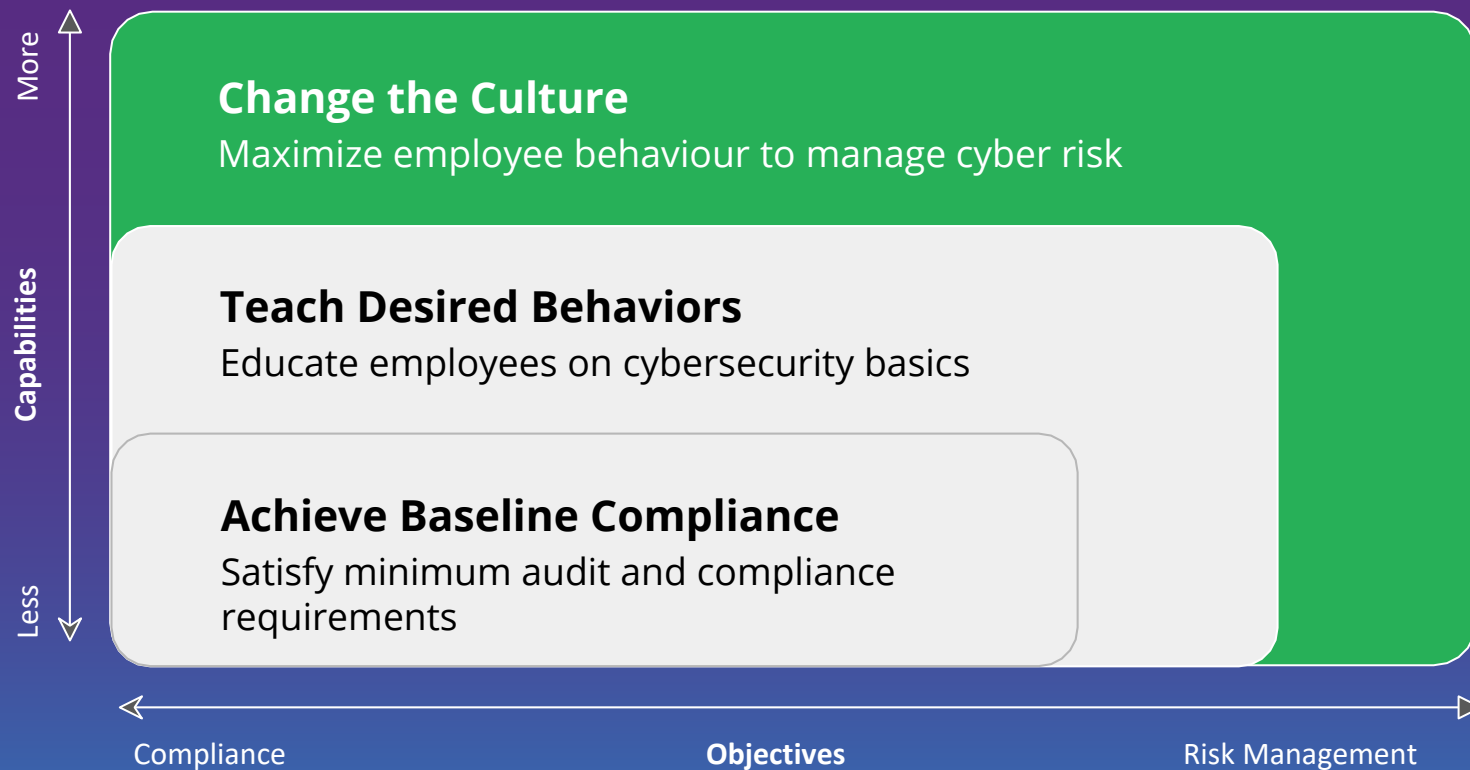


Management



Production

Traditional Security Awareness Training **Doesn't Work!**



Gartner®



Traditional "Security Awareness"



Security Behavior and Culture Program (SBCP)

People are the Entire Security Chain (Gartner 2023)




People Are Everywhere

Traditional Awareness Programs Focus Efforts **Here**



Decisions **Here** Mitigate or Exacerbate Security Challenges **Here**

Who's the Weakest Link?

	 Engineering	 Management	 Production
Knowledge on I4.0 Technology	36-70%	33-56%	12-30%
Human Factor Involvement	Unsecure coding & apps SOC cyber risks Vulnerabilities in 3rd parties	Lack of cybersecurity mindset Lack of coordination between departments	Lack of cybersecurity awareness & knowledge Complex supply chain with multiple blind spots

Human Factor in Industry 4.0



Employee Training: Conduct awareness training for all employees involved in the development, manufacturing, and maintenance of connected vehicles



Secure Code Training: Implement secure software development practices, such as secure coding guidelines to prevent vulnerabilities in connected systems



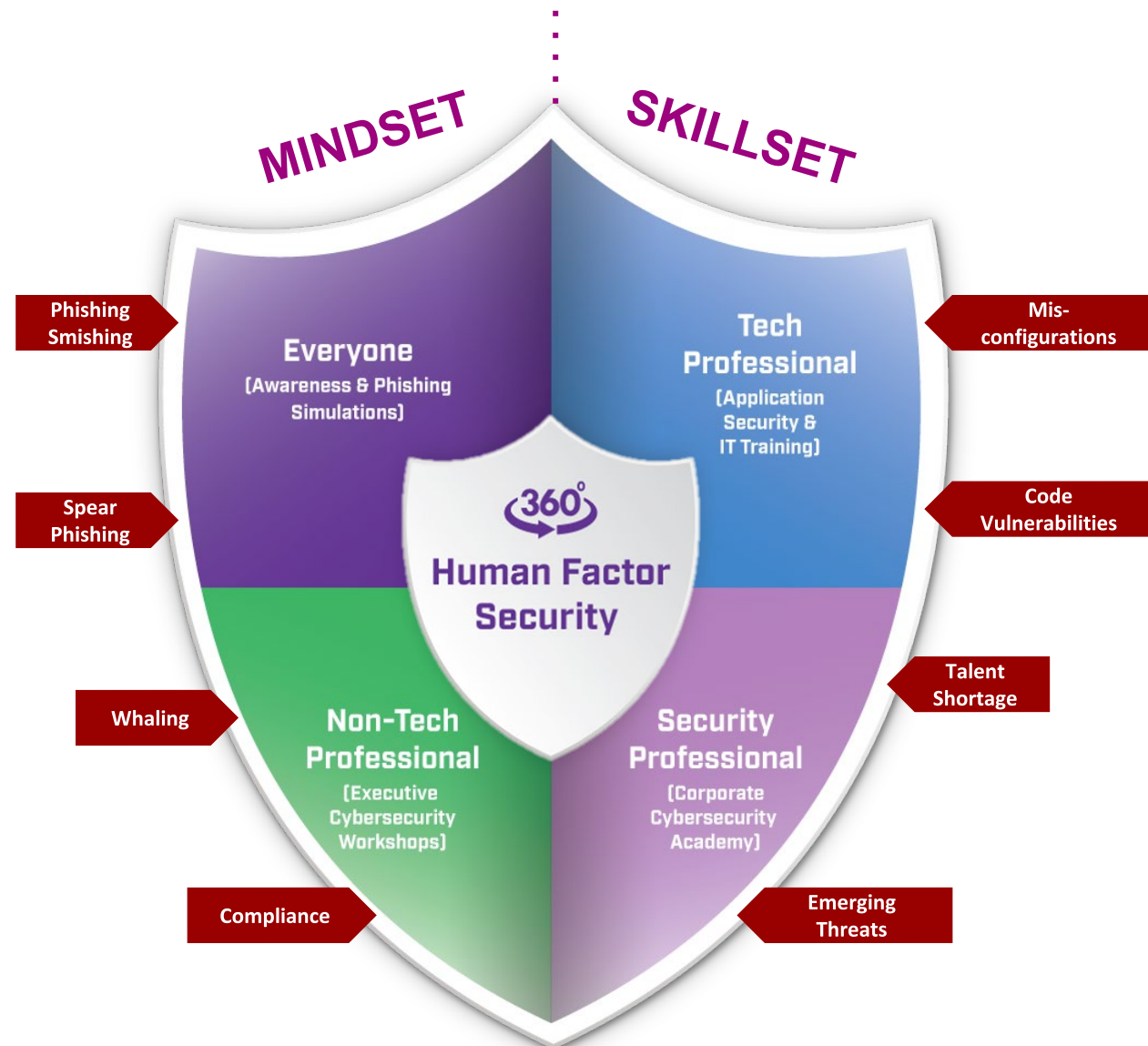
Supply Chain Weak Spots Mapping: Hundreds of hands touch the car until it hits the road, map the teams and roles that create the biggest awareness pain points



Post-Production Security Mindset: Strong awareness approach makes it possible to create mechanisms that challenge the customer to maintain security in their vehicles

HUMAN FACTOR SECURITY - HOLISTIC APPROACH

360° VIEW - BEYOND AWARENESS



BOSCH USE CASE - 300,000+ Employees



BOSCH

Enterprise
Cyber Academy

Your Own Cyber Academy Suite

Promoting **Diversity** and **Inclusion** through **Internal & External Reskilling** in Cybersecurity



Pre-Training
Screening

40+

Global University
Partners

1000+

Hours Of
Quality Content

100+

Real-World
Simulations



Post-Training
Matching

ThriveDX

The Cyber Academy Solution

Cyber Academy Training

Equip your talent with the necessary skills to excel in the industry

Pre-Training Screening

Evaluating candidates to find the best fit

Post-Training Matching

Matching acquired skills to suitable roles within the organization

The image displays a collage of screenshots from the ThriveDX Learner Dashboard. The central screenshot shows the 'My Activity' section with a 'GO TO MY ACTIVITY' button, followed by 'My Progress' with filters for 'Not Started', 'In Progress', and 'Completed'. Below these are 16 items, including 'Mid-Bootcamp Exam', 'Secure Design Principles', 'Overview and Preparations', 'Flexible Bootcamp Demo', 'Bootcamp Introduction', 'Network Administration', 'Cybersecurity Fundamentals', 'Week 1 - Bootcamp Introduction', and 'Company-Wide Training'. To the left, a 'Personality Test (Big 5 Model)' screenshot shows '0 Avg. Score', '13 Avg. Minutes', and '1 Candidates'. To the right, a 'Feedback' screenshot shows a radar chart and a list of traits: 'Innovative', 'Networker', and 'Adaptable'.



Join us

In solving the Talent Shortage & Skills Gap in Cybersecurity



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.
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).
 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

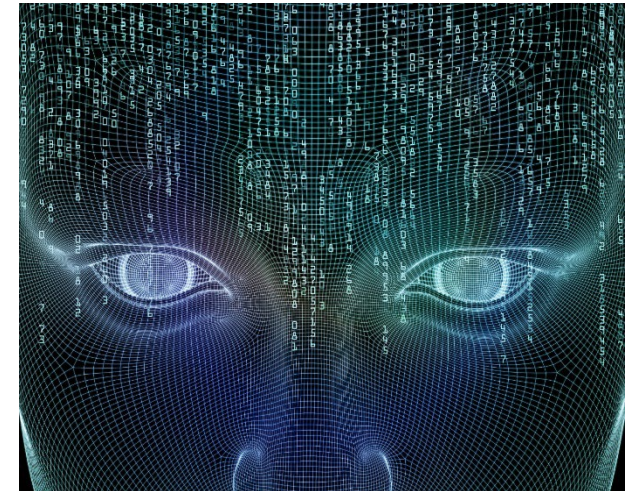
**Sponsorship
Partnership**

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 Northwest
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



AUTOMOTIVEISAC.COM