



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

NOTE: A **New Community Call invite** for Feb 2024- Jan 2025 has been sent. Please advise if you haven't received it.

February 07, 2024

This Session will be recorded.






This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



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, Joint Cyber Defense Collaborative (JCDC)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Shira Sarid-Hausirer , Upstream Security➤ Title: "2024 Global Automotive Cybersecurity Report: Key Findings & Insights"
11:55	Q&A & 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: Slides are at **TLP:CLEAR** and on our [website](#). Discussions are **TLP:GREEN** & may be shared across Auto-ISAC Community, “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! *“Cybersecurity is a Team Sport!”*

28
OEM Members

21
Navigator
Partners

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

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

48 Supplier &
Commercial
Vehicle Members

20
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)

2024 BOARD OF DIRECTORS

Thank you for your Leadership!



Kevin Tierney
*Chair of the
Board of the Directors*
GM



Josh Davis
*Vice Chair of the
Board of the Directors*
Toyota



Stephen Roberts
*Secretary of the
Board of the Directors*
Honda



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



Oliver Creighton
Chair of the EuSC
BMW



Andrew Hillery
Chair of the CAG
Cummins



Amine Taleb
Chair of the SAG
Harman



Maryann Combs
Polaris



Bob Kaster
Bosch



Brian Witten
Aptiv

AUTO-ISAC MEMBER ROSTER

AS OF FEBRUARY 1, 2024

76 MEMBERS + 3 PENDING

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

Pending: Dana Inc, Jaguar Land Rover, Renault SAS

AUTO-ISAC BUSINESS UPDATES AND EVENTS

- **Community Call:** Wednesday, March 6th **Time:** 11:00am – 12:00 p.m. **Speaker:** Jay Schwartz, SAE G-32: S.A.E. Cyber-Physical Systems Committee. **Title:** “The SAE Electric Vehicle Charging Station Illustrative Example: How to apply JA7496 standard to Electric Charging Scenarios”
- **Auto-ISAC 2nd European Summit - BMW Welt in Munich, Germany:** June 12th – June 13th. The Titanium sponsor of the 2024 event will be BMW. Stay tuned for more details on our website.
- **Auto-ISAC is Hiring!**
- **ACT Fundamental Course Block:** Online, On-Demand, Anytime, Anywhere, and by Anyone \$500/block
 - 3 Blocks: **Cybersecurity Basics** (32 hrs.) | **Security Engineering** (28 hrs.) | **Security Operations/Management** (22.5 hrs.)
 - 10% Discount for organizations signing up 30 or more students!
 - More information on [website](#)
- **ACT Advanced Courses: *ACT Now!***
 - ❑ **Cost per ADV Course:** ***\$2000 (Member Pricing), (\$2250 Non-Member Pricing) with discount code.
 - **Advanced Engineering:** January 22 - 26, 2024 **FULL**
 - **Wireless:** February 5 - 9, 2024 **FULL**
 - **EV and EV Infrastructure:** March 4 - 8, 2024 **OPEN**
 - **Guided Attacks:** April 29 - May 4, 2024 **OPEN**
 - **CAPEX to follow | Become CASE Certified!!**



AUTO-ISAC INTELLIGENCE HIGHLIGHT

RICKY BROOKS, INTELLIGENCE OFFICER

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



AUTO-ISAC INTELLIGENCE

➤ Know what we track daily: [subscribe](#) to the **DRIVEN**; Auto-ISAC 2024 Threat Assessment for Members is complete; **TLP:GREEN** version pending.

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

➤ Intelligence Notes

- Geopolitical tensions involving Russia, China, North Korea, and Iran remain **high** with Russia-Ukraine and Israel-Hamas in crises ([Russia-Ukraine](#) ^{1,2}, [Israel-Hamas](#) ³, [Iran](#) ⁴, [China](#) ^{5,6}, [North Korea](#) ⁷).
- Ransomware ^{8,9} Groups Targeting Automotive: [8Base](#), [Akira](#), [Black Basta](#), [Cactus](#), [LockBit 3.0](#).
- **Notable TTPs:** Abusing GitHub for malicious infrastructure ([Recorded Future](#)); Leveraging Microsoft SQL servers for initial access ([Securonix](#)); Infiltrating Réseaux IP Européens Network Coordination Centre (RIPE NCC) accounts ([BleepingComputer](#)); Exploiting vulnerabilities in: Ivanti Connect Secure and Privacy Secure ([Volexity](#))*, SonicWall Next Generation Firewalls ([BishopFox](#)), Unified Extensible Firmware Interfaces ([arsTechnica](#)), VMware ([BleepingComputer](#)), Google Chrome and the open-source Perl library ([Bleeping Computer](#)), Unitronics VisiLogic ([CISA](#)); ColdFusion ([CISA](#)); Microsoft Outlook and Azure HDInsight ([Microsoft](#), [Darkreading](#)), Barracuda Email Security Gateway appliances; ([BleepingComputer](#)), and JetBrains TeamCity ([CISA](#)); Botnet exploitation of Network Video Recorder vulnerability ([BleepingComputer](#)); various detection evasion techniques ([Microsoft](#)); leveraging affordable devices for digital odometer fraud ([KSLTV](#))*. **Notable Tools:** EV Open Vehicle Monitoring System ([Hackaday](#))*, Rhadamanthys Stealer ([Check Point](#)), Medusa Stealer ([Resecurity](#)), SpectralBlur ([Securityweek](#)), Androxgh0st ([CISA](#)), SnappyTCP ([Hunt&Hackett](#)), Android/Xamalicious ([McAfee](#)), PikaBot ([Flashpoint](#)), and various other malware ([Unit 42](#)).

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.
- ❖ 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*





FEATURED SPEAKER

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



MEET THE SPEAKER



**Shira Sarid-Hausirer, VP Marketing
Upstream Security**

Shira Sarid-Hausirer leads Upstream's marketing team, bringing more than 15 years of experience in strategic marketing for deep tech companies.

Prior to joining Upstream, Shira jumpstarted and led all marketing activities for Varada, a cloud data lake analytics platform (acquired by Starburst Data). Shira also led product marketing activities for private cloud infrastructure startup Stratoscale and managed marketing teams in various startups in the fields of cyber and ecommerce. Shira started her career as an investment banker for Tech & Media corporations for Bank of America.

Shira holds an MBA with honors from Georgetown University, and an BSc in Computer Science and LLb in Law from Haifa University in Israel.

Upstream



The 2024 Automotive Cyber Inflection Point: From Experimental Hacking to Massive-Scale Attacks

Shira Sarid-Hausirer | VP Marketing

Get insights from
2024 report!



WEBINAR AGENDA



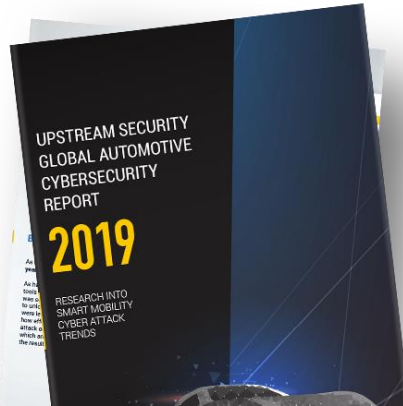
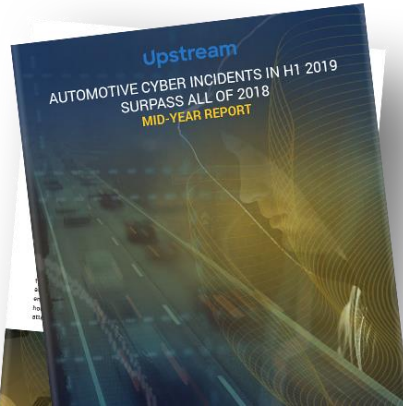
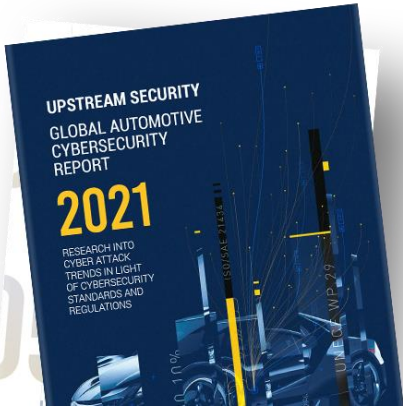
- 2023 report recap
- 2024 report: the fundamental trends
- The automotive cyber inflection point: scale & impact
- The threat actors landscape
- The financial impact
- The power of GenAI
- Our predictions for 2024

Supporting the Automotive Cybersecurity Community

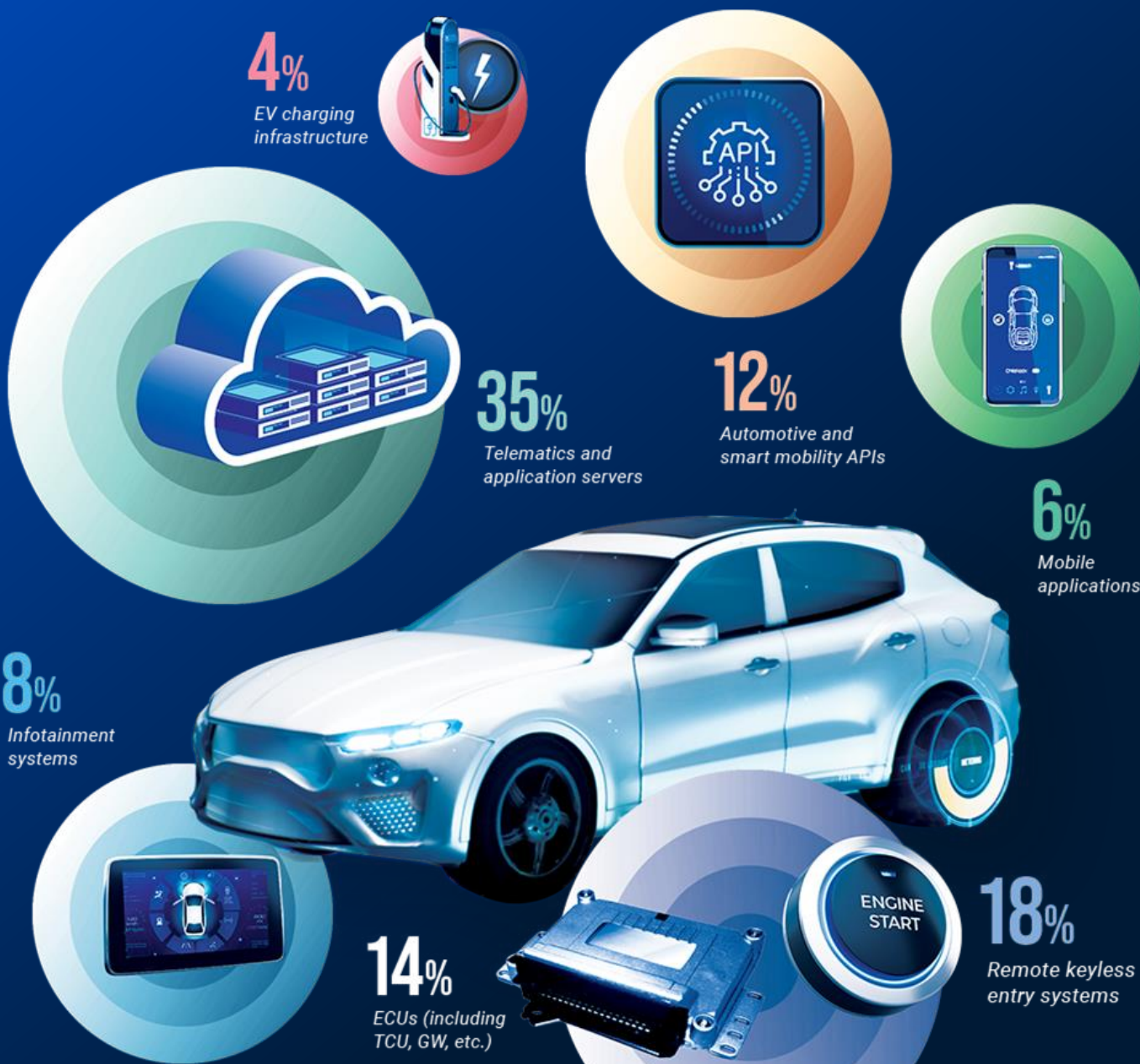
Delivering automotive & smart mobility cybersecurity insights since 2019



NEW!



Upstream's 2023 Report: The Automotive Industry Expands into the Smart Mobility Ecosystem



THE AUTOMOTIVE INFLECTION POINT

Cyber risks at scale

/ Automotive cyber inflection point

Threat actor landscape

Financial impact

Power of GenAI

2024 Predictions

The state of Automotive cybersecurity of Automotive Cybersecurity

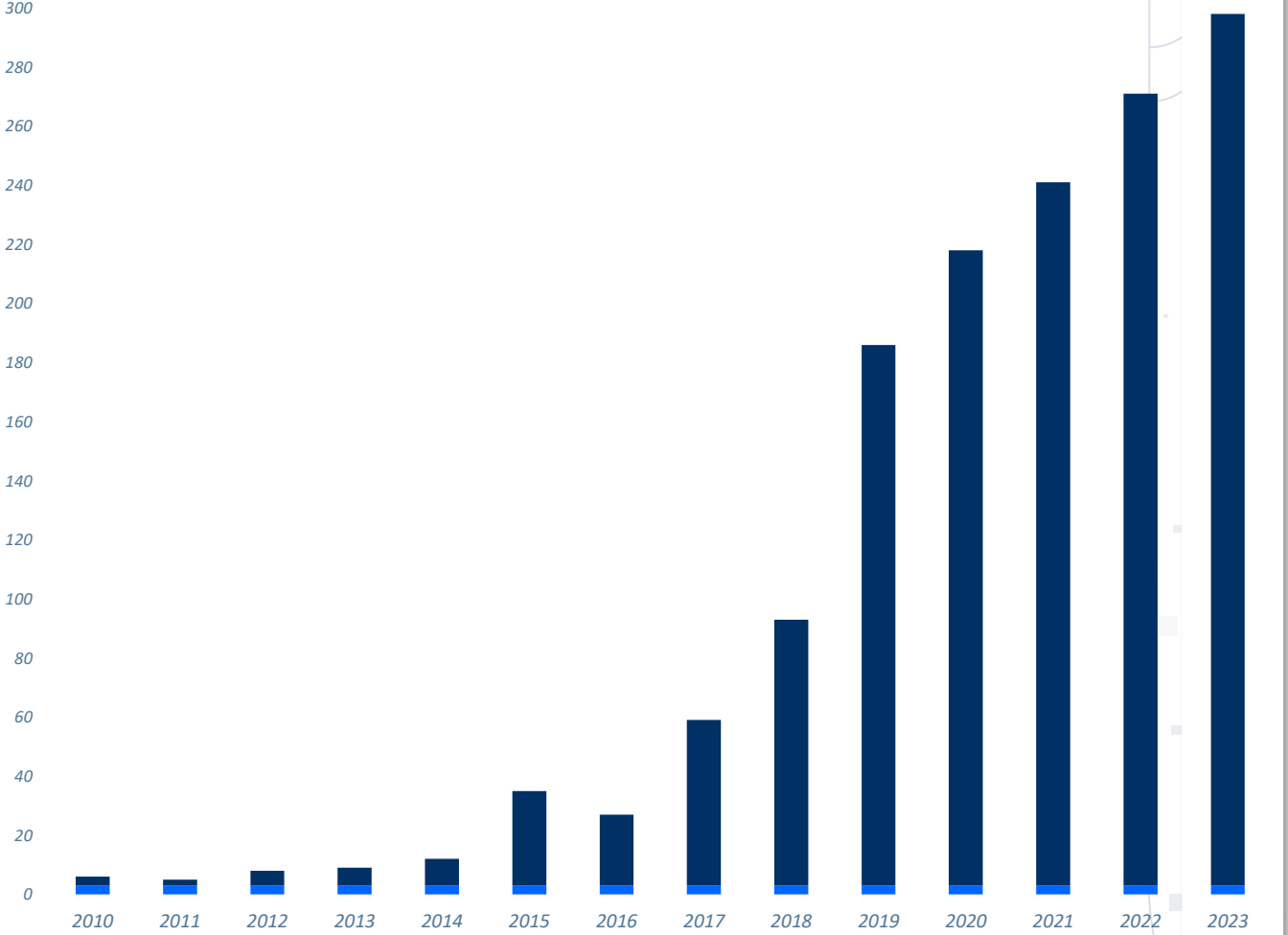
Automotive & Smart Mobility incidents continue to grow

2010-2023 incidents

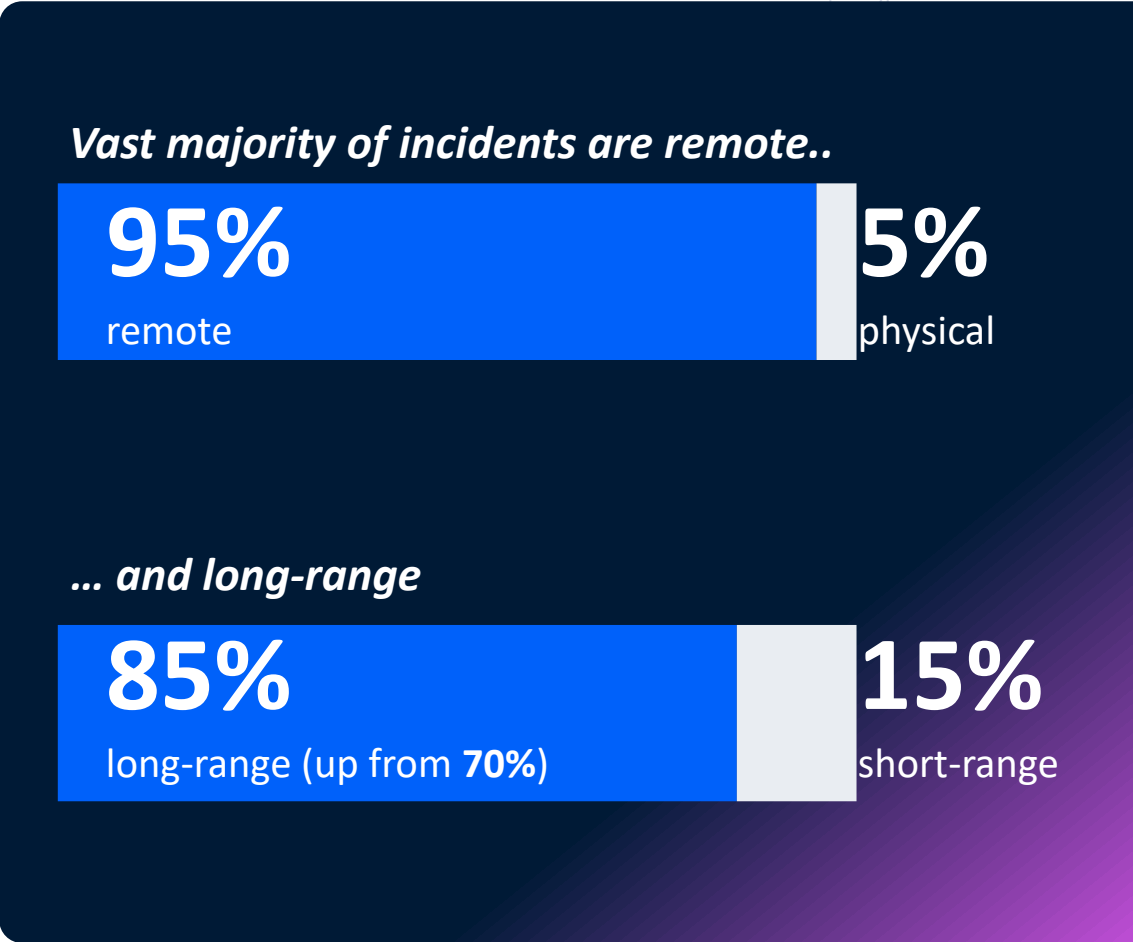
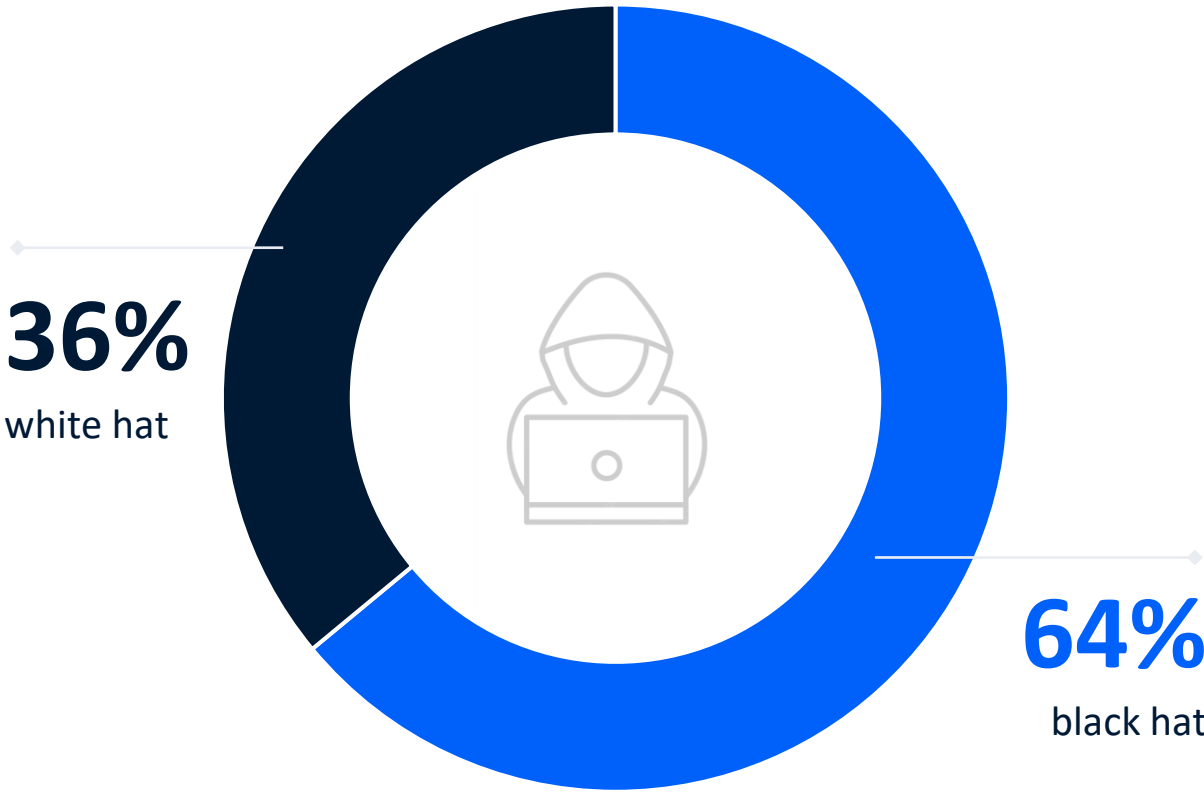
1,468

2023 incidents

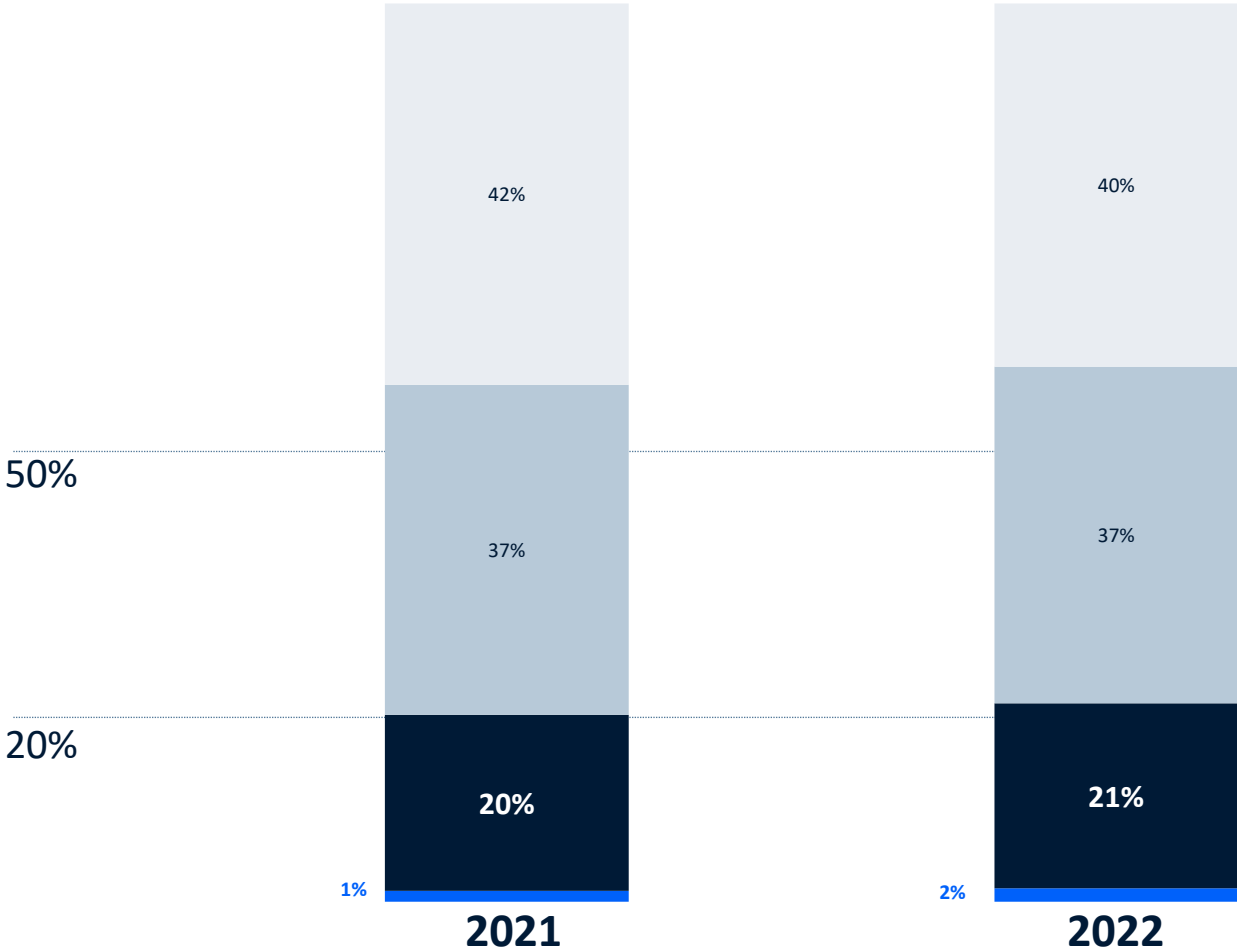
295



The state of Automotive cybersecurity



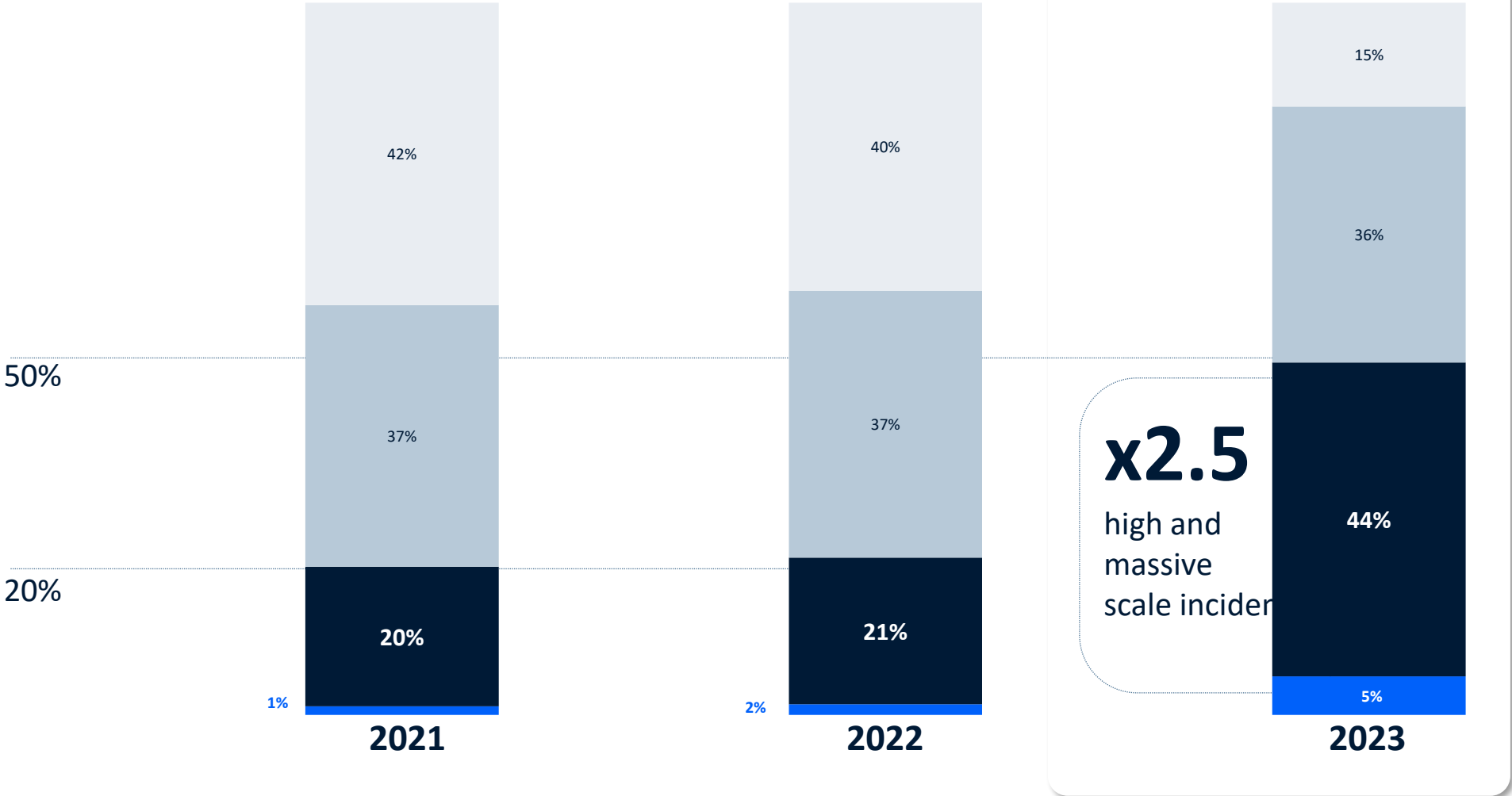
The Inflection Point: shifting to large-scale attacks



Breakdown of publicly disclosed cybersecurity incidents by potential scale


- Low**
Up to 10 mobility assets
- Medium**
Up to 1,000 mobility assets
- High**
Thousands of mobility assets
- Massive**
Millions of mobility assets

The Inflection Point: shifting to large-scale attacks




- Low**
Up to 10 mobility assets
- Medium**
Up to 1,000 mobility assets
- High**
Thousands of mobility assets
- Massive**
Millions of mobility assets

The scale is evident in many recent attacks

 **r/Truckers** • 24 days ago
by KappaFishxD Join





Anyone else effected by the [redacted] outage?

I've been running with paper logs due to the outage, which they say the end is nowhere in sight. Problem is my safety manager is a complete tool and he wants me to send him a picture so he can "compare it to the gps movements." Really nothing better to do? Oh well. Hope you all enjoy your paper logs

 **HowlingWolven** • 23 days ago

Yeah, been on motive in paper mode since Wednesday. Apparently their data provider got ransomware?

The fluffing dumb bit is that if my tablet had a USB port I could stuff a flash drive into, it'd be a compliant standalone elog and I wouldn't need to manually transcribe my log into my phone, because the box in the dash works just fine, but it can't send the logs to the notership.

 1   Reply  Share ...


BLEEPINGCOMPUTER

Home > News > Security > ORBCOMM ransomware attack causes trucking fleet management outage

[redacted] ransomware attack causes trucking fleet management outage

By Lawrence Abrams

September 15, 2023 09:33 AM 0



The Record.
Recorded Future News




IMAGE: CALEB RUITER VIA UNSPLASH


Jonathan Greig
September 15th, 2023

Industry Briefs
Cybercrime

Major trucking software provider confirms ransomware incident

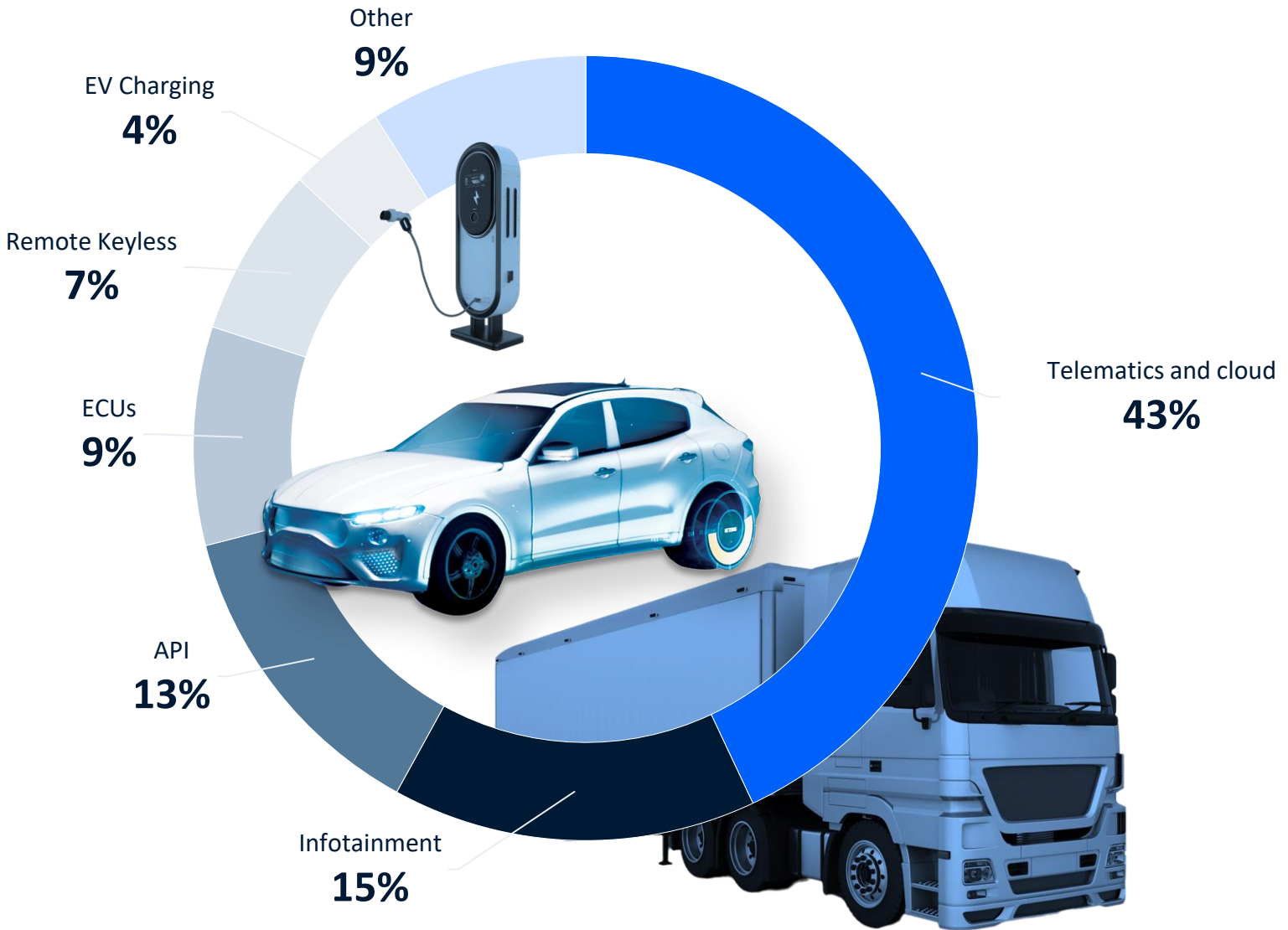
One of the biggest providers of software for the trucking industry acknowledged a ransomware attack on Friday after reports emerged of issues that customers had with its products.

An executive of the company, New Jersey-based [redacted], confirmed the attack to Recorded Future News but would not say which ransomware group was behind the incident or whether a ransom would be paid.



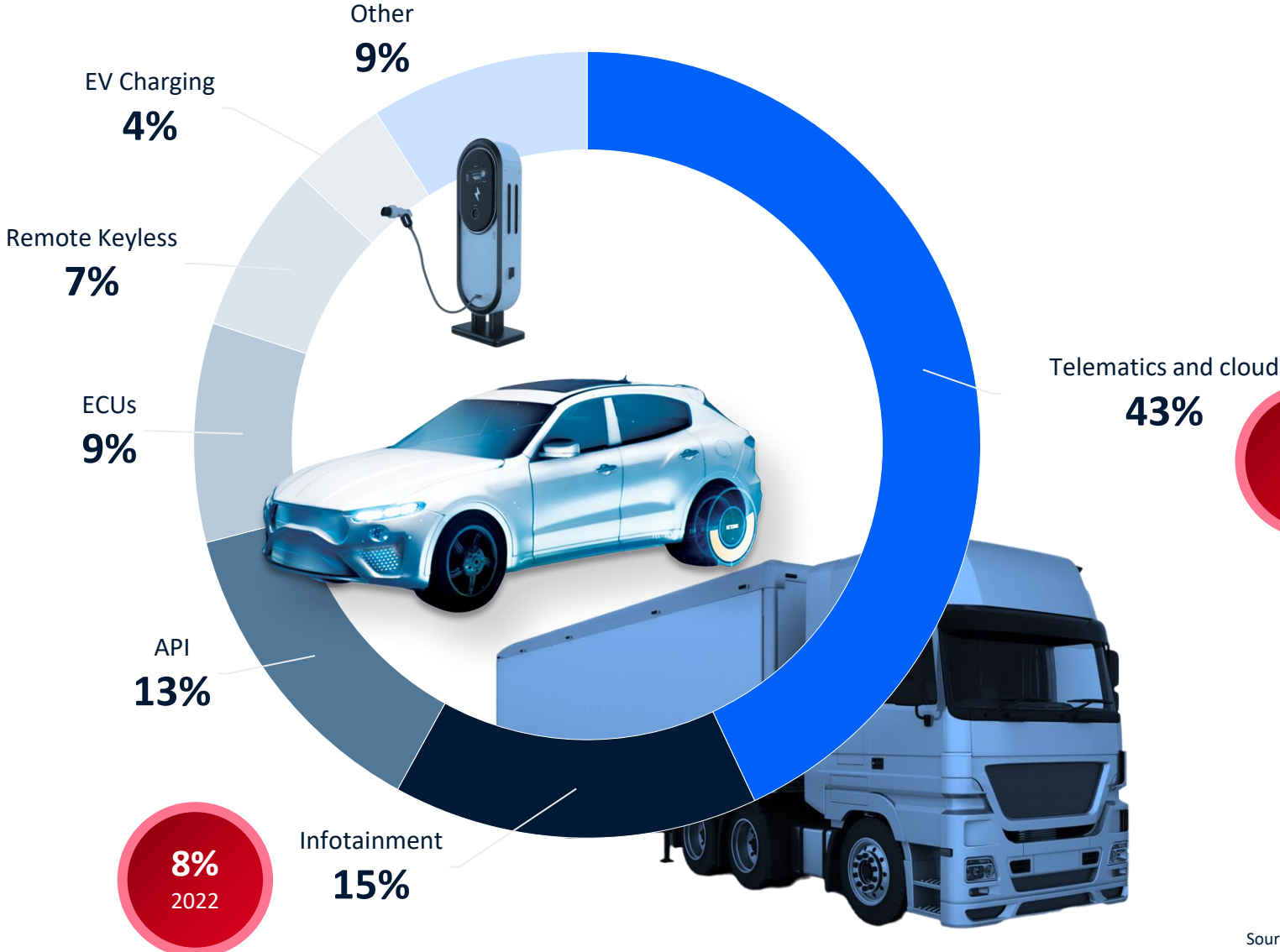
Scale is also reflected in the evolving attack vectors

2023 attack vectors



Scale is also reflected in the evolving attack vectors

2023 attack vectors



Recap: publicly reported incidents prove a shift to scale & impact

95% of 2023 incidents were remote...

64% of 2023 incidents were performed by black hats

and **85%** were long-range

50% of 2023 incidents had the potential to impact thousands – millions of mobility assets

DIVING INTO THE DEEP AND DARK WEB

The threat actor landscape

Automotive cyber inflection point

/ Threat actor landscape

Financial impact

Power of GenAI

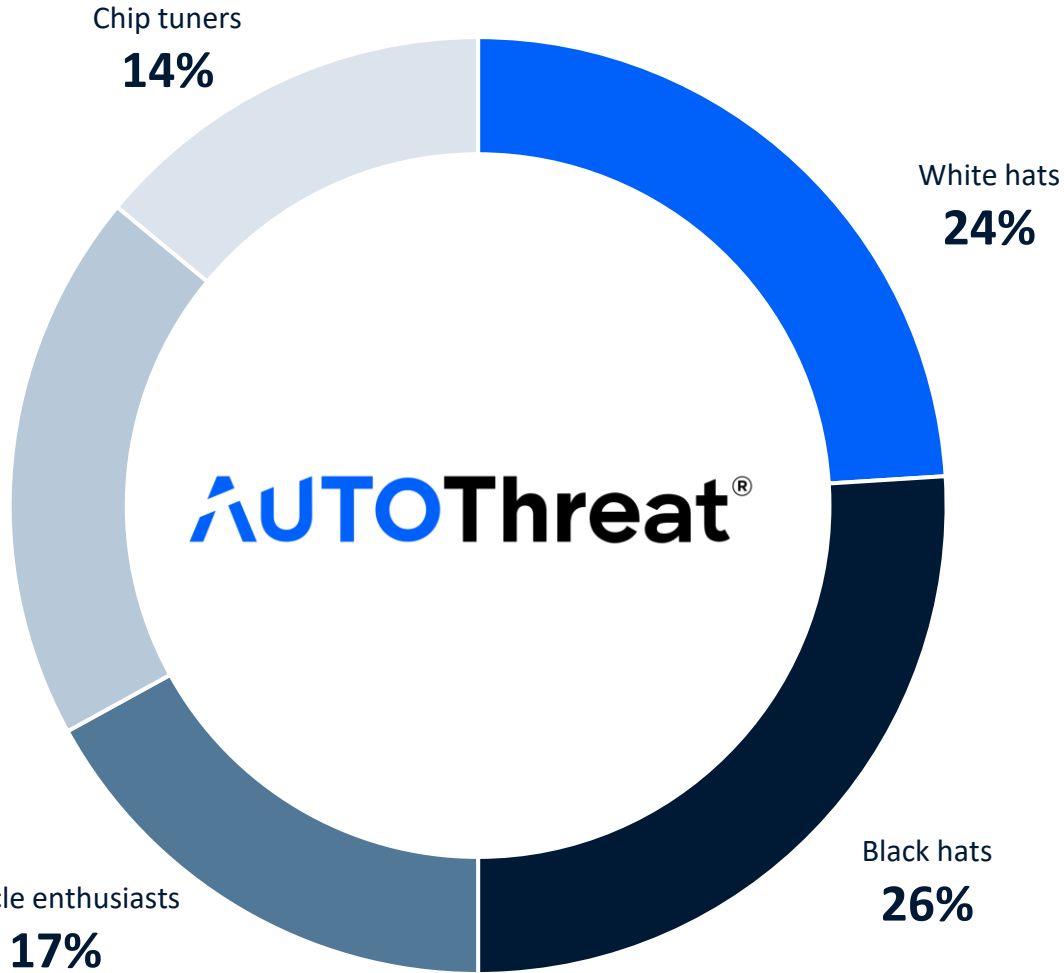
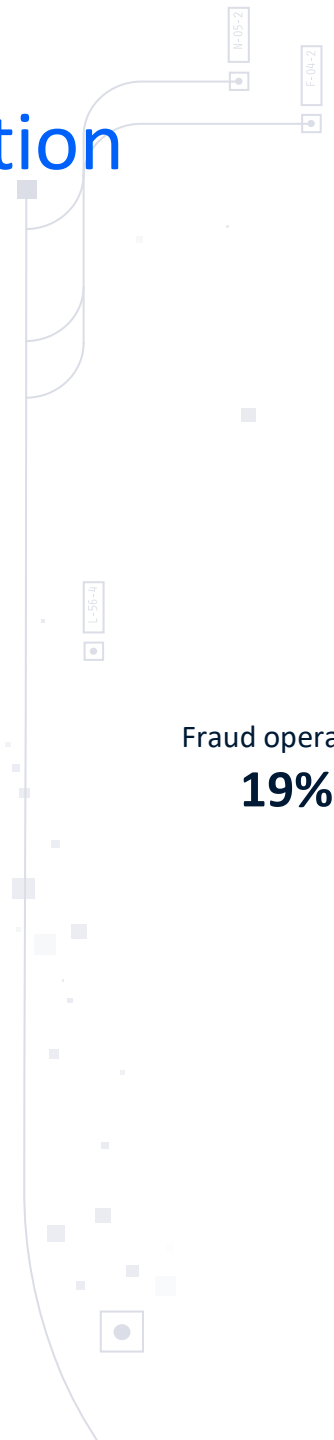
2024 Predictions

Threat actors motivation

DEEP & DARK WEB ACTIVITIES

300

threat actors, 2023



Threat actors' motivation has also shifted towards scale...

DEEP & DARK WEB ACTIVITIES

300
threat actors, 2023



AUTOThreat®
Threat actors' activities by potential scale, 2023

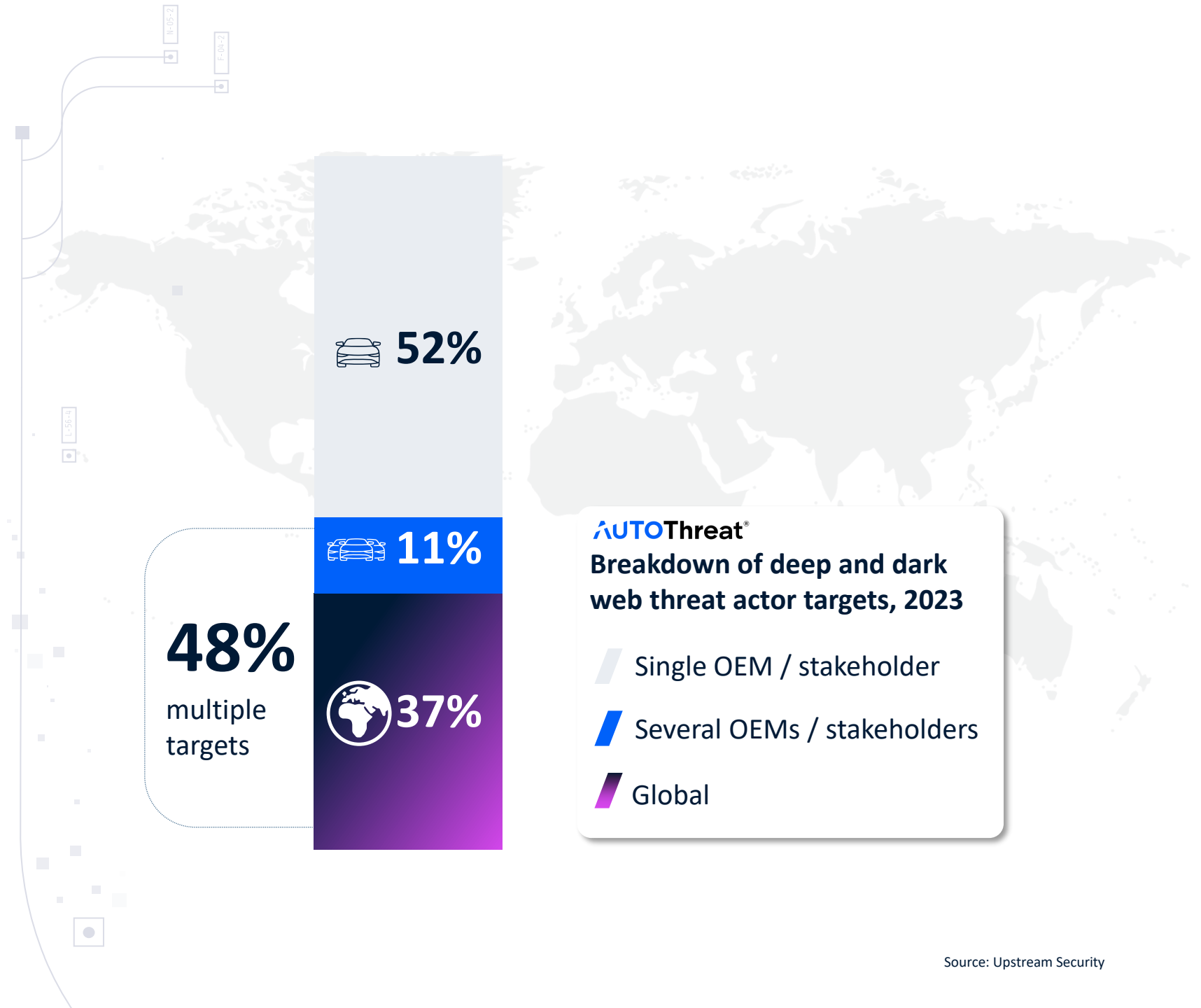
- Low**
Up to 10 mobility assets
- Medium**
Up to 1,000 mobility assets
- High**
Thousands of mobility assets
- Massive**
Millions of mobility assets

... and impact

DEEP & DARK WEB ACTIVITIES

300

threat actors, 2023



Black hats and fraud operators shift towards “massive” impact

DEEP & DARK WEB ACTIVITIES

135 (45%)

black hats and fraud operators, 2023

x1.6 vs. general threat actors



AUTOThreat[®]

Black hat and fraud activities by potential scale, 2023

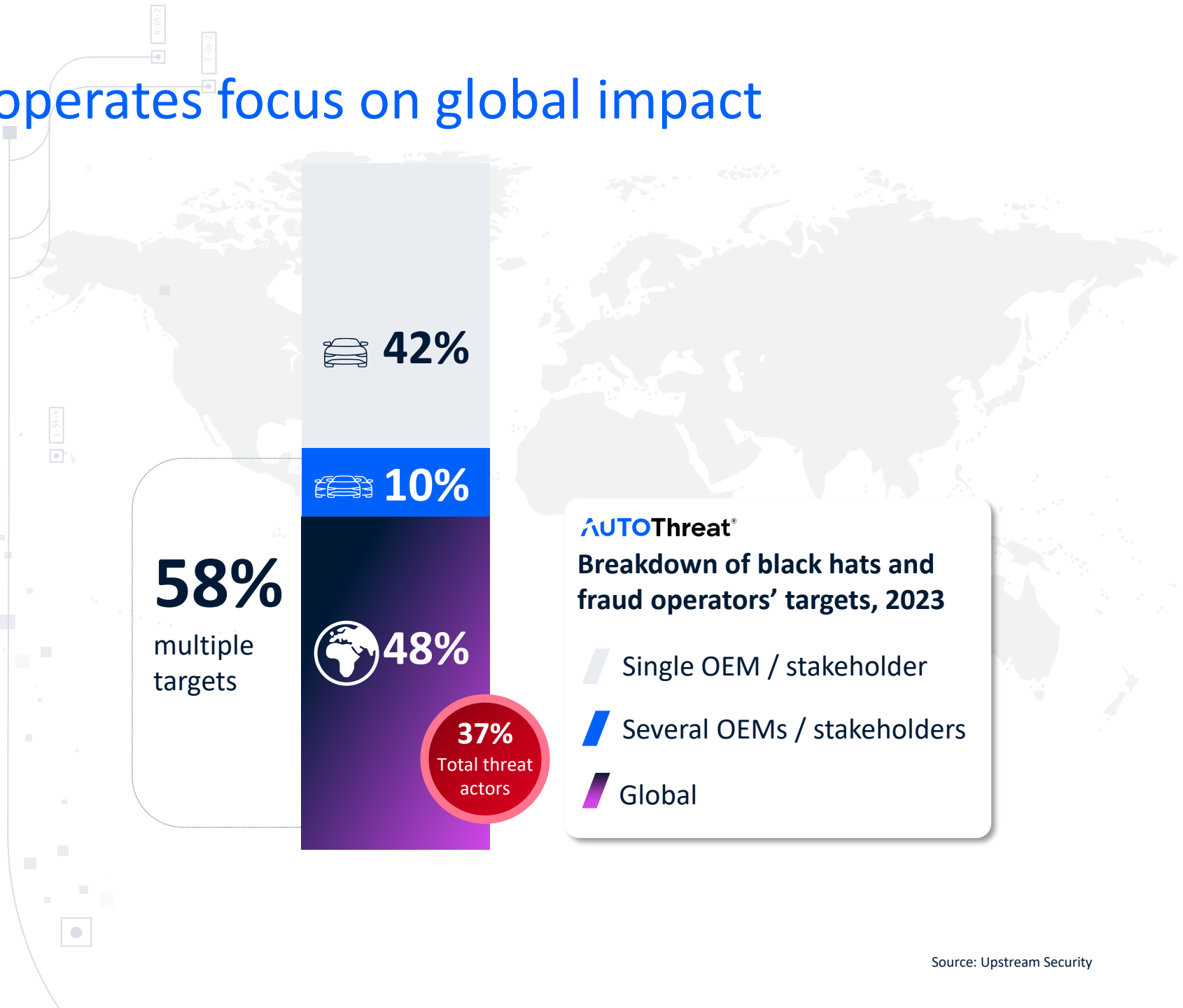
- Low**
Up to 10 mobility assets
- Medium**
Up to 1,000 mobility assets
- High**
Thousands of mobility assets
- Massive**
Millions of mobility assets

Black hats and fraud operators focus on global impact

DEEP & DARK WEB ACTIVITIES

135 (45%)

black hats and fraud operators, 2023



Black hats and fraud operators and focus on high-impact activities

DEEP & DARK WEB ACTIVITIES

135 (45%)

black hats and fraud operators, 2023



50%

Vulnerability exploits

19%

Diagnostic software

13%

Vehicle manipulation tools

12%

PII

7%

Car hacking manuals

AUTOThreat®

THE FINANCIAL PERSPECTIVE

Analyzing the financial
impact of cyber attacks

Automotive cyber inflection point

Threat actor landscape

Financial impact

Power of GenAI

2024 Predictions

Financial implications of Automotive cyber attacks

ONE OF THE BIGGEST RANSOM DEMANDS IN HISTORY

June 2023, Taiwan-based tier-2 hit by a

\$70 million

ransomware attack, threatening to expose confidential information.

Upstream Cyber Financial Framework



Vehicle safety, operations and recalls



Data and privacy breaches



Vehicle theft and break-ins



Service and business disruption



Legal and regulatory compliance



Fraud



Brand and reputation

#1

Financial impact of an EV fleet-wide vulnerability

ILLUSTRATION #1 MARCH 2023

French security researchers demonstrated a hack of EV OEM gateway energy management system. Claimed to potentially access full vehicle controls.



Lorenzo Franceschi-Bicchierai @lorenzofb / 4:05 PM GMT+3 • March 28, 2023

██████████ said we wouldn't be able to turn the steering wheel, accelerate or brake. But from our understanding of the car architecture we are not sure that this is correct, but we don't have proof of it," he said, because they don't have full access to a ██████████ at the moment.

- Severity** High
- Threat actor type** White hat
- Potential impact** Fleet-wide
- Fleet size** 3+ million vehicles

#1

Financial impact of an EV fleet-wide vulnerability



**Vehicle safety,
operations and recalls**

OTA UPDATE

\$0.39 for line-of-code update, assuming 5 large ECUs @500MB; 10 small ECUs @0.42MB (*Aurora Labs*).

Upstream

**\$1,250,000 -
\$2,000,000**



**Vehicle safety,
operations and recalls**

BATTERY RECALL

\$15,000 per battery, assuming 0.01%-0.05% impacted vehicles.

Upstream

**\$5,250,000 -
\$26,250,000**



**Legal and regulatory
compliance**

CLASS ACTION

\$600 per plaintiff, assuming 0.5%-1% of vehicles owners participating; plus \$500,000 legal fees.

Upstream

**\$11,000,000 -
\$21,500,000**

Total potential financial impact

\$17.5 - \$49.75 million

#2

Financial impact of an EV charging data breach

ILLUSTRATION #2 JUNE 2023

Security researcher discovered an online database with ~1TB of logs of thousands of EV charging points, including VINs, location, customer PII, and more.



Zack Whittaker @zackwhittaker / 10:30 AM GMT+3 • June 9, 2023
The data, seen by TechCrunch, contained names, email addresses, and phone numbers of fleet customers who use the EV charging network. The database included the names of fleet operators, which identified organizations — such as police departments — with vehicles that recharge on the network. Some of the data included vehicle identification numbers, or VINs.

Severity	High
Threat actor type	Black hat
Breach size	1TB of data
Network size	X00,000 public charging stations; 30+ countries

#2

Financial impact of an EV charging data breach



Data and privacy breach

DATA BREACH

\$36 million average cost for a data breach at this magnitude (*IBM*).

Upstream

\$30,000,000 - \$40,000,000



Legal and regulatory compliance

GDPR FINES

€864,776 average fine in the transportation sector;
€1,346,050 average fine for insufficient measures.

Upstream

\$1,000,000 - \$2,000,000

Total potential financial impact

\$31 - \$42 million

THE POWER OF GENERATIVE AI

Introducing unprecedented
capabilities to threat actors
and vSOC teams

Automotive cyber inflection point

Threat actor landscape

Financial impact

/ Power of GenAI

2024 Predictions

GenAI: the intruder's perspective

“The use of generative AI for nefarious purposes has become an increasingly popular topic on the dark web after the launch of ChatGPT”

BAIN & COMPANY 



Utilize LLM models to identify vulnerabilities



Simulate and standardize exploit tactics, methods and processes



APIs are a prime target for GenAI attacks due to public documentation, enabling to map endpoints, vulnerabilities, and lower attack barriers

The vSOC 3.0: powered by Gen AI

GenAI has the potential to transform the vSOC



Agile investigations, to automating vSOC workflows



Generate complex insights based on deep and dark web data and in-depth vulnerability & threat management



Quickly analyze massive amounts of connected vehicle and mobility data across multiple sources, detect patterns, filter incident alerts, and automate investigations

LOOKING INTO 2024

Upstream's predictions

Automotive cyber inflection point

Threat actor landscape

Financial impact

Power of GenAI

/ 2024 Predictions

APIs and Gen AI present new opportunities and challenges

Digital transformation will continue to introduce large-scale attacks

Expand vSOC coverage to monitor API threats

Regulatory fatigue, landscape is becoming overwhelmingly complex

Global regulations vary according to country, region, global initiatives; often creating overlap and conflicts; upcoming second milestone of R155 and expected expansions, regulations in China

Generative AI emerges as a double-edged sword

vSOC teams are expected to incorporate AI-based tools to support agile ops and combat emerging threat vectors

Rapid EV adoption expands cyber risks and drives regulations

Expand cyber posture to cover IoT protocols, standards and regulations; driving additional regulations

APIs and Gen AI present new opportunities and challenges

Digital transformation will continue to introduce large-scale attacks

Expand vSOC coverage to monitor API threats

Regulatory fatigue, landscape is becoming overwhelmingly complex

Global regulations vary according to country, region, global initiatives; often creating overlap and conflicts; upcoming second milestone of R155 and expected expansions, regulations in China

Generative AI emerges as a double-edged sword

vSOC teams are expected to incorporate AI-based tools to support agile ops and combat emerging threat vectors

Rapid EV adoption expands cyber risks and drives regulations

Expand cyber posture to cover IoT protocols, standards and regulations; driving additional regulations

APIs and Gen AI present new opportunities and challenges

Digital transformation will continue to introduce large-scale attacks

Expand vSOC coverage to monitor API threats

Generative AI emerges as a double-edged sword

vSOC teams are expected to incorporate AI-based tools to support agile ops and combat emerging threat vectors

Regulatory fatigue, landscape is becoming overwhelmingly complex

Global regulations vary according to country, region, global initiatives; often creating overlap and conflicts; upcoming second milestone of R155 and expected expansions, regulations in China

Rapid EV adoption expands cyber risks and drives regulations

Expand cyber posture to cover IoT protocols, standards and regulations; driving additional regulations

APIs and Gen AI present new opportunities and challenges

Digital transformation will continue to introduce large-scale attacks

Expand vSOC coverage to monitor API threats

Regulatory landscape is becoming overwhelmingly complex

Upcoming second milestone of R155 and expected expansions, as well as new regulations in China

Generative AI emerges as a double-edged sword

vSOC teams are expected to incorporate AI-based tools to support agile ops and combat emerging threat vectors

Rapid EV adoption expands cyber risks and drives regulations

Expand cyber posture to cover IoT protocols, standards and regulations; driving additional regulations

Upstream

THANK YOU!

Get insights from
2024 report!



NEW!

OPEN DISCUSSION

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

OUR CONTACT INFO

Faye Francy
Executive Director



20 F Street Northwest
Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com



AUTOMOTIVEISAC.COM