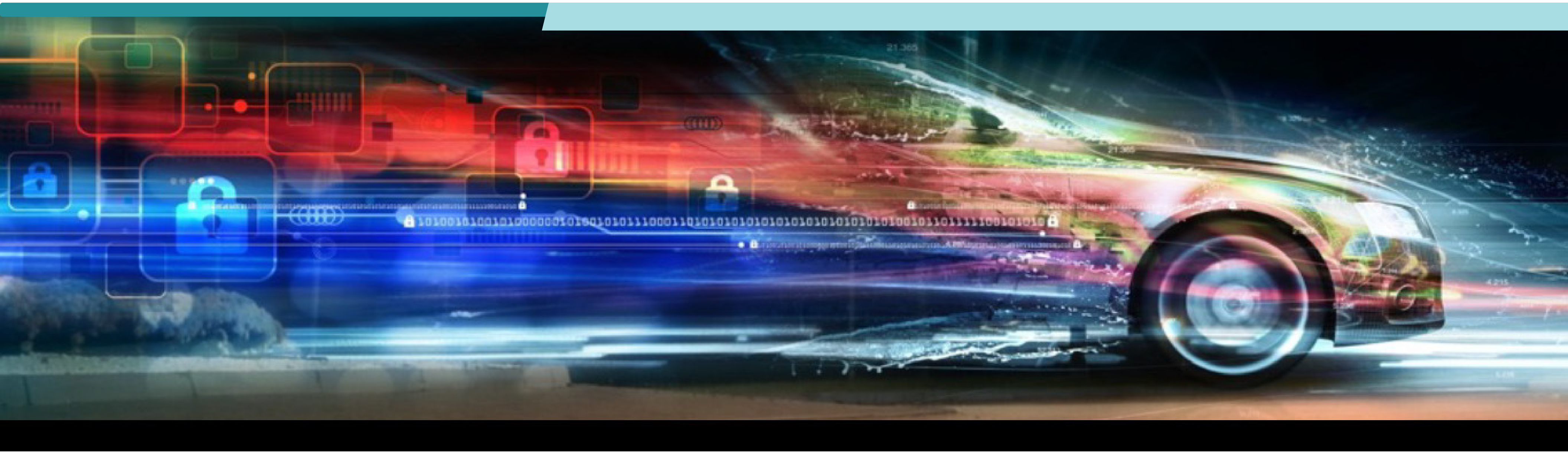


Transport Canada's Vehicle Cybersecurity Virtual workshop

Auto-ISAC: The Importance of Collaboration

Faye Francy, Auto-ISAC Executive Director

March 24, 2022
11:25 a.m. - 12:00 p.m. EST

This document is Auto-ISAC Sensitive and Confidential.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

TRANSPORT CANADA'S VEHICLE CYBER SECURITY STRATEGY

Forward-looking **vehicle cyber security goals and priorities** with a view to **strengthening** road transportation **cyber resilience** in Canada.

- *Goal 1:* **Incorporate vehicle cyber security considerations into policy and regulatory frameworks**
- *Goal 2:* **Promote awareness and foster a modernized, innovative approach to vehicle cyber security**
- *Goal 3:* **Address emerging and adjacent issues in the vehicle cyber security landscape**

- The **complex and interconnected nature** of automotive cyber security **requires collaboration and cooperation** among a broad range of stakeholders, and TC will continue to explore opportunities to address **cyber security risk** in the broader ecosystem of road transportation technology…

TRANSPORT CANADA'S VEHICLE CYBER SECURITY STRATEGY

Transport Canada Transports Canada

Canada

Legal/regulatory

In 1998, PDD-63 emphasized that 90% of the nation's **critical infrastructure** is owned and operated by the private sector.

It asked each industry to create a sector-specific organization to **share information about physical and cyber threats, vulnerabilities, and incidents**.

Today, there are 24 ISACs that serve this role.

ISACs provide trusted information exchanges through five cornerstones:

Submission anonymity ● Authenticated information sharing ● Industry driven and operated Limitation on the use of information ● Compliance with all U.S. legal requirements and antitrust law

Other policies enabling ISACs include:

National Security Policy Directive (2001)	**Comprehensive National Cybersecurity Initiative** (**CNCI**) (2008)	**Executive Order (EO) 13636:** Improving Critical Infrastructure Cybersecurity (2014)
Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2014)	**EO 13691:** Promoting Private Sector Cybersecurity Information Sharing (2015)	**Cybersecurity Act of 2015** (2015)

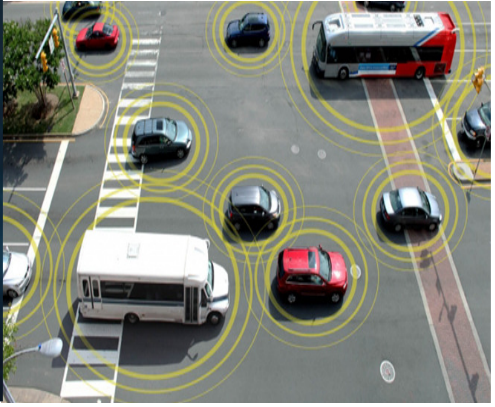
Significant Changes in Automotive World

Digital Connected Vehicles provide operational efficiencies and risks…

Cocktail napkin

⬇

100M lines of code



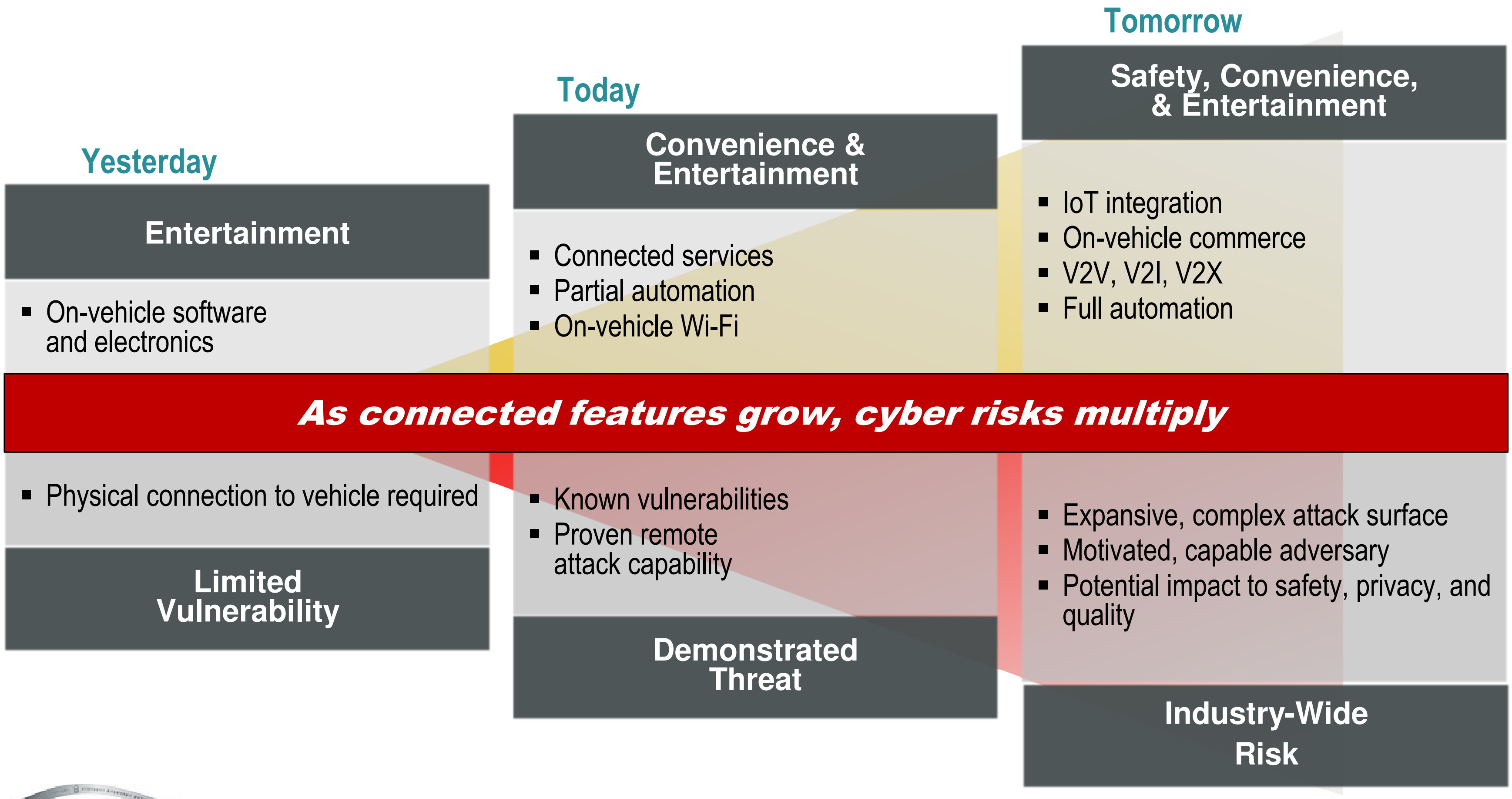
➢ Digital Age

- ✓ Customers demanding connectivity
- ✓ Automation brings efficiencies
- ✓ Increased cyber vulnerabilities within connected vehicles
- ✓ News media, congressional oversight, regulatory demands action

➢ Connected Vehicles Integrated across Systems-of-Systems (SoS)

- ✓ Connectivity provides greater efficiencies and risk
- ✓ Cyber threats and vulnerabilities growing
- ✓ Regulation, standards in varying stages
- ✓ And autonomy, V2V, V2I coming….

WITH CONNECTIVITY COMES CYBER RISK



Yesterday

Entertainment

- On-vehicle software and electronics

- Physical connection to vehicle required

Limited Vulnerability

Today

Convenience & Entertainment

- Connected services
- Partial automation
- On-vehicle Wi-Fi

- Known vulnerabilities
- Proven remote attack capability

Demonstrated Threat

Tomorrow

Safety, Convenience, & Entertainment

- IoT integration
- On-vehicle commerce
- V2V, V2I, V2X
- Full automation

- Expansive, complex attack surface
- Motivated, capable adversary
- Potential impact to safety, privacy, and quality

Industry-Wide Risk

As connected features grow, cyber risks multiply

AUTO-ISAC CYBERSECURITY

THE CONNECTED VEHICLE

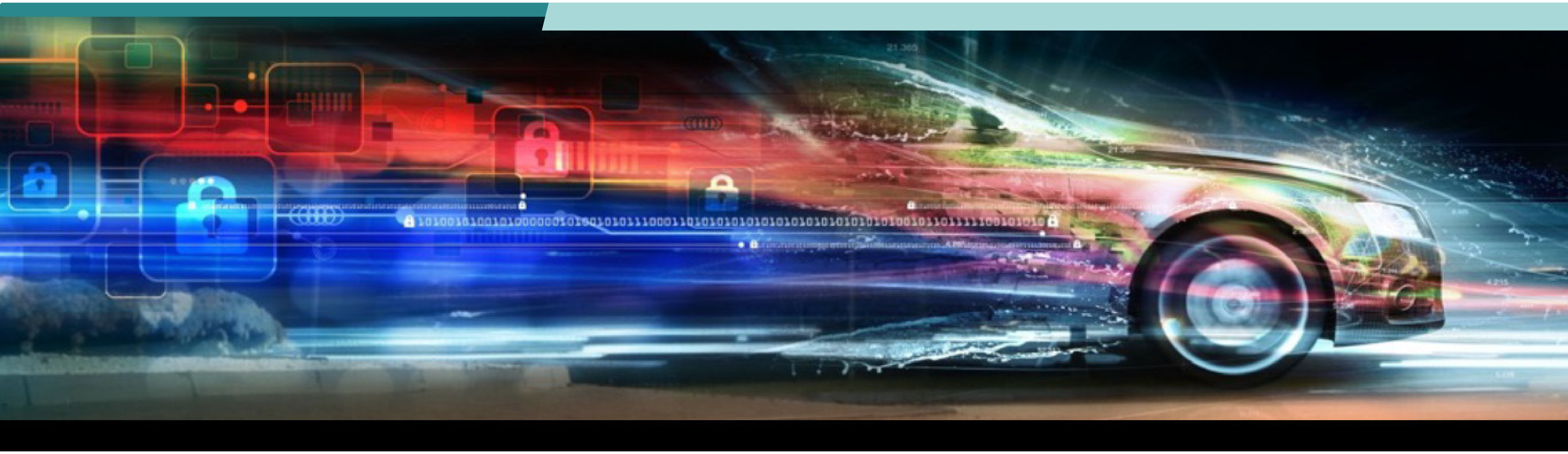
PURPOSE

- Maintain public trust
- Reduce risks and costs
- Timely, Actionable Intelligence
- Shared situational awareness
- Resiliency

BENEFITS

- Access to threat intelligence & analysis
- Detailed threat monitoring
- Sector-wide / cross sector view
- Non-attribution information sharing
- One voice

CYBERSECURITY IS EVERYONE'S RESPONSIBILITY



Auto-ISAC

What does an ISAC do?

This document is Auto-ISAC Sensitive and Confidential.

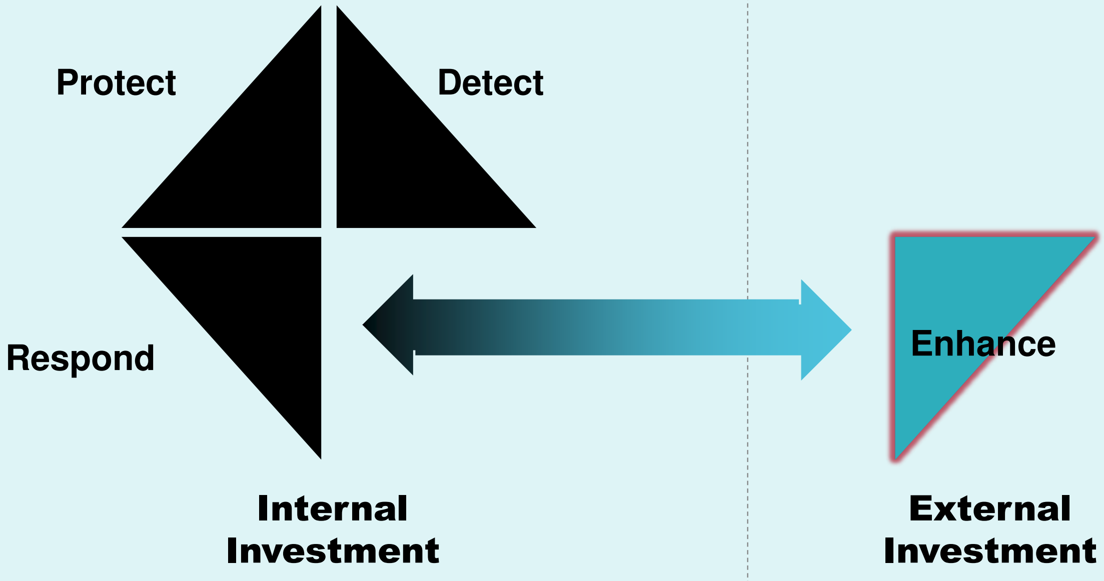
AUTO-ISAC
Automotive Information Sharing and Analysis Center

WHY AN AUTO-ISAC?

INFORMATION SHARING AND ANALYSIS CENTER (ISAC)

Organizations must act individually to manage cyber risk…

…one company's detection is another company's prevention



- ➢ Identify emerging threats and vulnerabilities earlier
- ➢ Pool limited resources to better fight your adaptive adversary
- ➢ Share incident intelligence to act more quickly
- ➢ Proactively shape industry-wide best practices
- ➢ Protect overall trust in innovation across the industry
- ➢ Build resiliency across industry

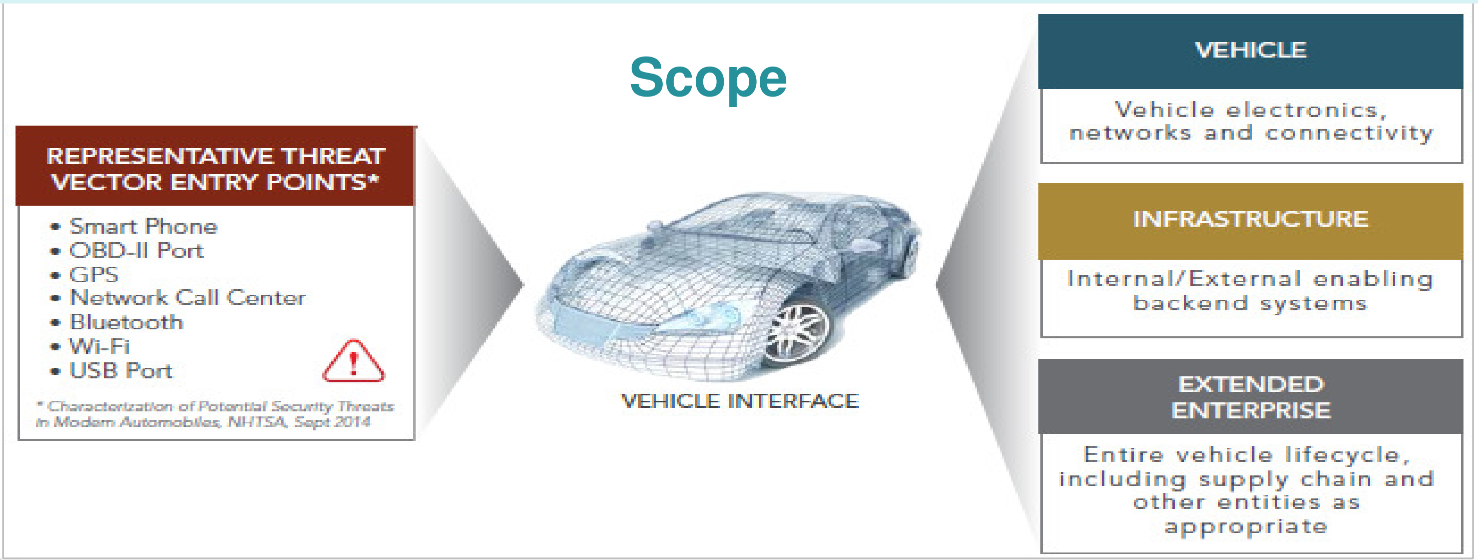
AUTO-ISAC: *CENTRAL POINT OF CYBERSECURITY COORDINATION AND COMMUNICATION* FOR THE GLOBAL AUTOMOTIVE INDUSTRY

Purpose

- Serve as an **unbiased** information broker
- Increase the **timeliness, quality, and quantity** of information shared
- Conduct threat **analysis**
- Maintain **agility and flexibility** to adapt to change (new threats, tactics, etc.)

Mission

Serve as a **central point of coordination and communication** for the global automotive industry through the analysis and sharing of trusted and timely cyber threat information



Scope

REPRESENTATIVE THREAT VECTOR ENTRY POINTS*

- Smart Phone
- OBD-II Port
- GPS
- Network Call Center
- Bluetooth
- Wi-Fi
- USB Port

Characterization of Potential Security Threats in Modern Automobiles, NHTSA, Sept 2014

VEHICLE INTERFACE

VEHICLE

Vehicle electronics, networks and connectivity

INFRASTRUCTURE

Internal/External enabling backend systems

EXTENDED ENTERPRISE

Entire vehicle lifecycle, including supply chain and other entities as appropriate

AUTO-ISAC = LEARNING ENVIRONMENT

➢Analytic Products & Assessments

- ✓ Collaboration and early detection | Crowd Sourcing
- ✓ Best in Industry (Members!)

➢Tabletops Exercises

- ✓ Executive C-suite Tabletop, Legal TTX
- ✓ Analyst Table-Tops | Drills

➢Quarterly Workshops

- ✓ Analyst & Executive F2F Engagement
- ✓ Webinars – Strategic Partnerships

➢Work Groups

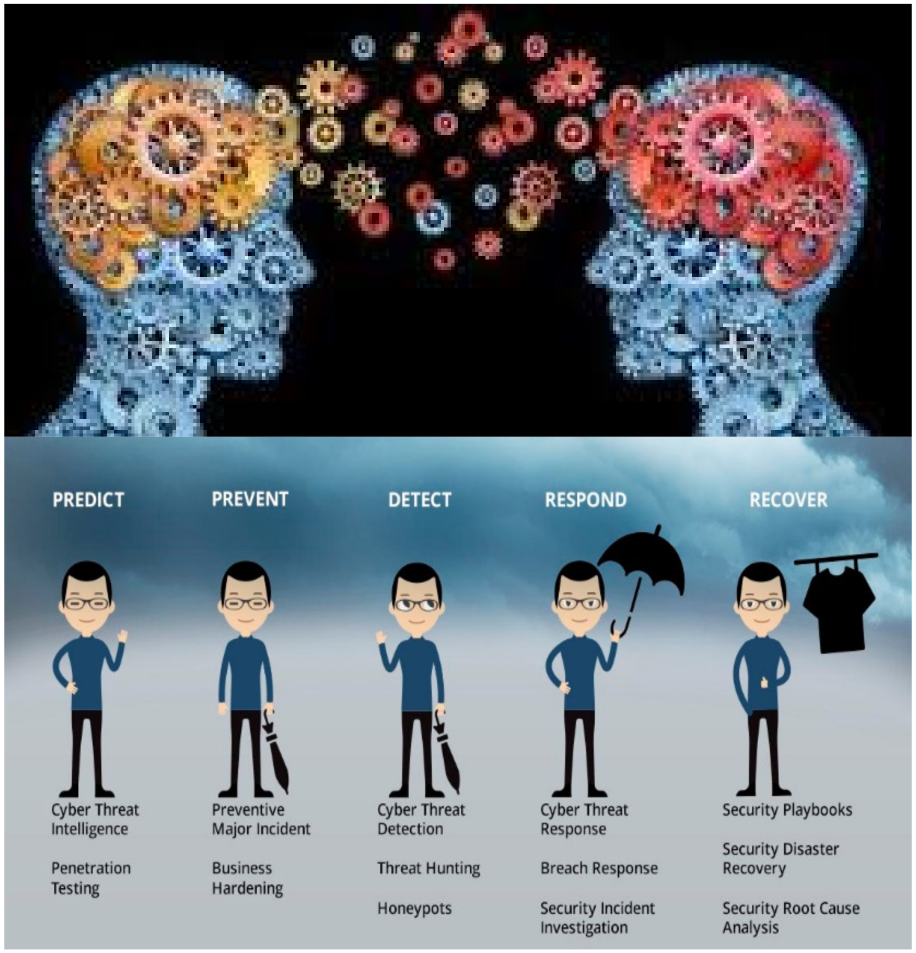
- ✓ Member-driven, Real-time Challenges
- ✓ Develop Best Practices | Members-Teaching-Members

➢Standing Committees

- ✓ Advise the Board on key projects
- ✓ Member-driven | Work products

➢Annual Summit | Community Calls

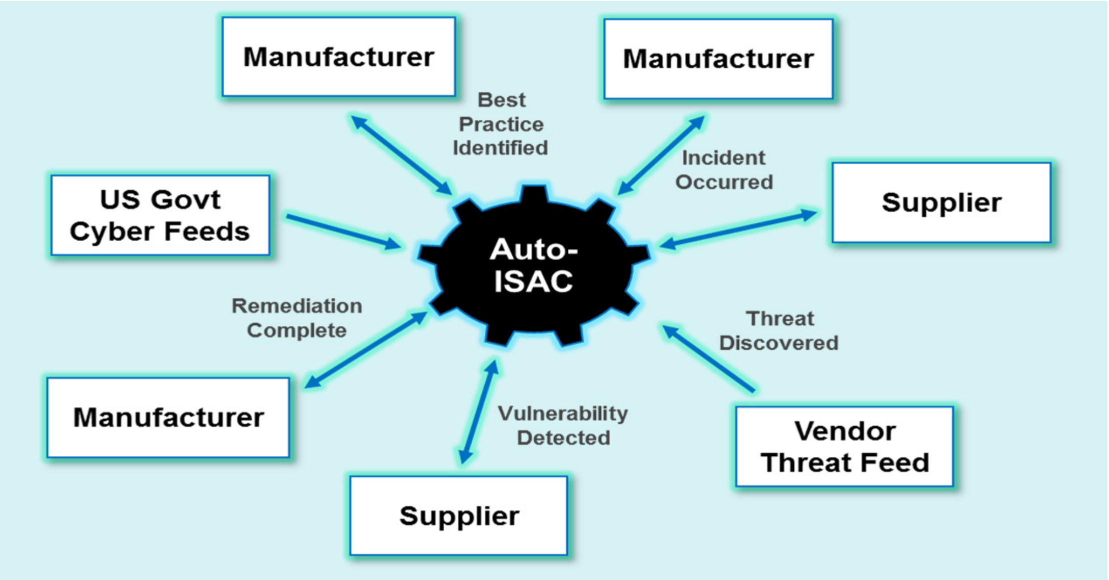
- ✓ Members, Partners / Vendors / Community
- ✓ Academia and leaders in cybersecurity



Auto-ISAC Enables Trusted Sharing and Analysis

Cyber Threat and Vulnerability Information

Central Hub for Intelligence and Analysis



Auto-ISAC

Manufacturer

Manufacturer

US Govt Cyber Feeds

Supplier

Manufacturer

Supplier

Vendor Threat Feed

Best Practice Identified

Incident Occurred

Remediation Complete

Threat Discovered

Vulnerability Detected

Aggregate, analyze and share auto-specific cyber information across the industry's attack surface

Benefits

Efficiently identify threats by supplementing internal intelligence with external feeds

Detect vulnerabilities faster with cross-industry vulnerability information sharing

Validate risk analysis with reliable industry-level findings and best practices

MS0

What To Share: Types of Intelligence

Access & Distribution Classification

What We Share

Incidents

Vulnerabilities

Threats

Situational Awareness

Scope

Share **cyber** intelligence related to consumer or commercial **vehicles** that could **impact or be used by other members.**

IT and OT are included.

You can share anonymously or with attribution; access is controlled by traffic light protocol and we will distribute intelligence according to criticality

TRAFFIC LIGHT PROTOCOL (TLP)

TLP indicates access restrictions based on intelligence sensitivity

TLP Color	Description
RED	Restricted to a limited, defined group (e.g. only those present at a meeting) due to high impact potential.
AMBER	May be shared with only Auto-ISAC Members. Information requires support, but also carries risk if released.
GREEN	May be shared with Auto-ISAC Members and Partners as determined by Auto-ISAC.
WHITE	May be shared freely and is subject to copyright rules. Information carries minimal or no foreseeable risk.

CRITICALITY

Criticality indicates how quickly intelligence will be shared.

Criticality	Description
URGENT	Critical; recommend immediate attention from the submitter and/or Members of Auto-ISAC.
ELEVATED	Important; recommend that Members review and determine if a response is needed in a timely manner.
NORMAL	All other information. No immediate response needed from the submitter or Auto-ISAC membership recommended.

Slide 12

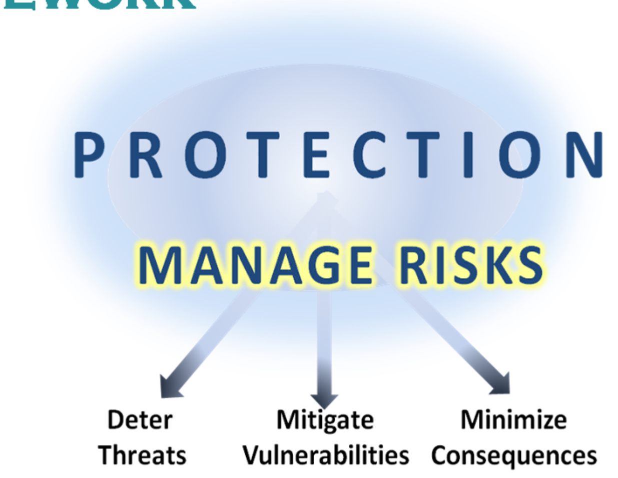
MS0 Too detailed, could drop?

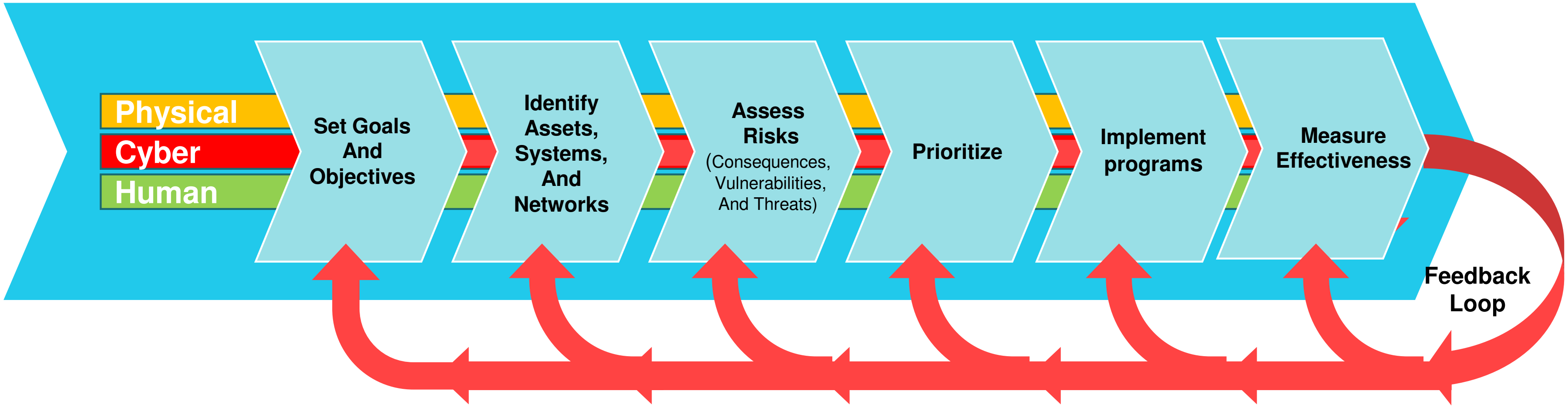
Michael Shokouhi, 2022-03-09T16:43:54.829

Connected Vehicle Cybersecurity Framework

Strategy: Managing Risk

- ✓**Risk** = threat + vulnerabilities and resultant consequences
- ✓**Framework** focuses on risk-informed decision-making
- ✓**Operational goal** = mitigate the threat by using prevent, detect and respond techniques

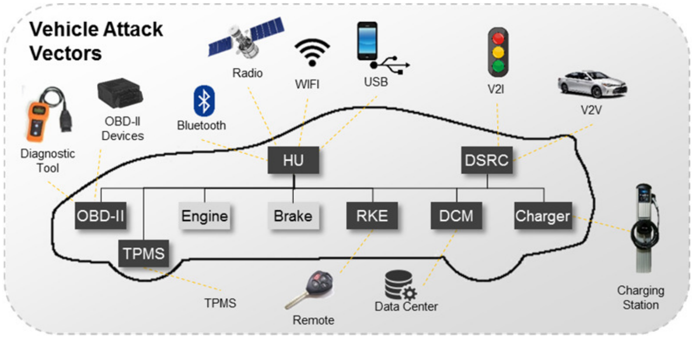




Continuous Improvement to enhance protection

A Framework for Automotive Cybersecurity

1. Establish common cybersecurity best practices for automotive
2. Establish a cybersecurity culture
3. Understand the threat
4. Understand the risk
5. Communicate the threats and assure situational awareness
6. Provide incident response
7. Strengthen the defensive system
8. Define design principles
9. Define operational principles
10. Conduct necessary research and development
11. Ensure that private sector, government and partners work together



Building Resiliency Across Automotive Industry

Interesting Stats…

- **Global Connected Vehicles** will jump **134%** from 330 million in 2018 to **774 million in 2023**[1]
- By 2025, a **connected car** will produce **26GB** of data per hour and **50GB if autnomous**[2]
- **2021** saw an **increase in sophisticated attacks** that brought challenges to the entire automotive ecosystem.
- In **2021**, the **majority of hacks** were carried out by **black-hat hackers** (57%), white-hats accounted for 39% and 4% others[3]
- The **segments of the automotive industry** hit was wide-spread **across all segments** – OEMs, Tier 1s, EVs, fleet management, car sharing, car rental, car dealerships, ride sharing, etc.
- **2021** saw an increase in the **use and sophistication of cyber attacks**.across various attack vectors **Advanced attack practices** are creating a heightened awareness across the industry of how any point of connectivity is **vulnerable to new threats.**

1. https://www.juniperresearch.com/whitepapers/connected-cars-how-5g-connected-commerce-blockchain-will-disrupt-the-ecosystem
2. https://www.wevolver.com/article/high-speed-data-and-connected-cars
3. Upstream2022Report

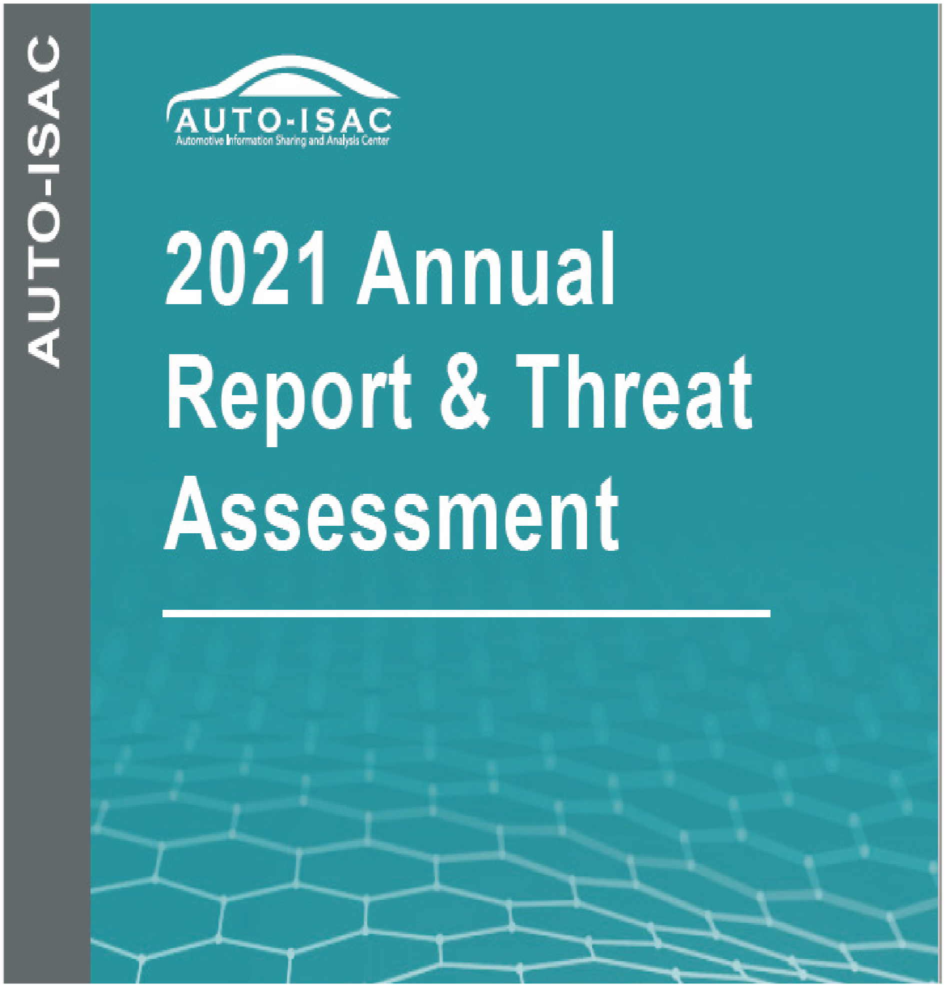
More Stats…

- There are more lines of code in the connected vehicle than a jet fighter plane or a Boeing 787!
- Keyless entry car technology accounts for nearly 50% of all vehicle thefts
- Ransomware + supply chain = *big new challenges.*
- *"Ransomware is the biggest security threat to most organizations today," says Splunk Distinguished Security Strategist Ryan Kovar. "Honestly, it's not if you're going to get hit with a ransomware attack — it's when."*

Connected Vehicles Most Common Attack Vectors[1]

Servers, Vehicles & between
Keyless entry / Key Fobs
ECUs
Mobile Apps
Infotainment
OBD Port
Sensors
Wi-Fi
In-Vehicle Networks

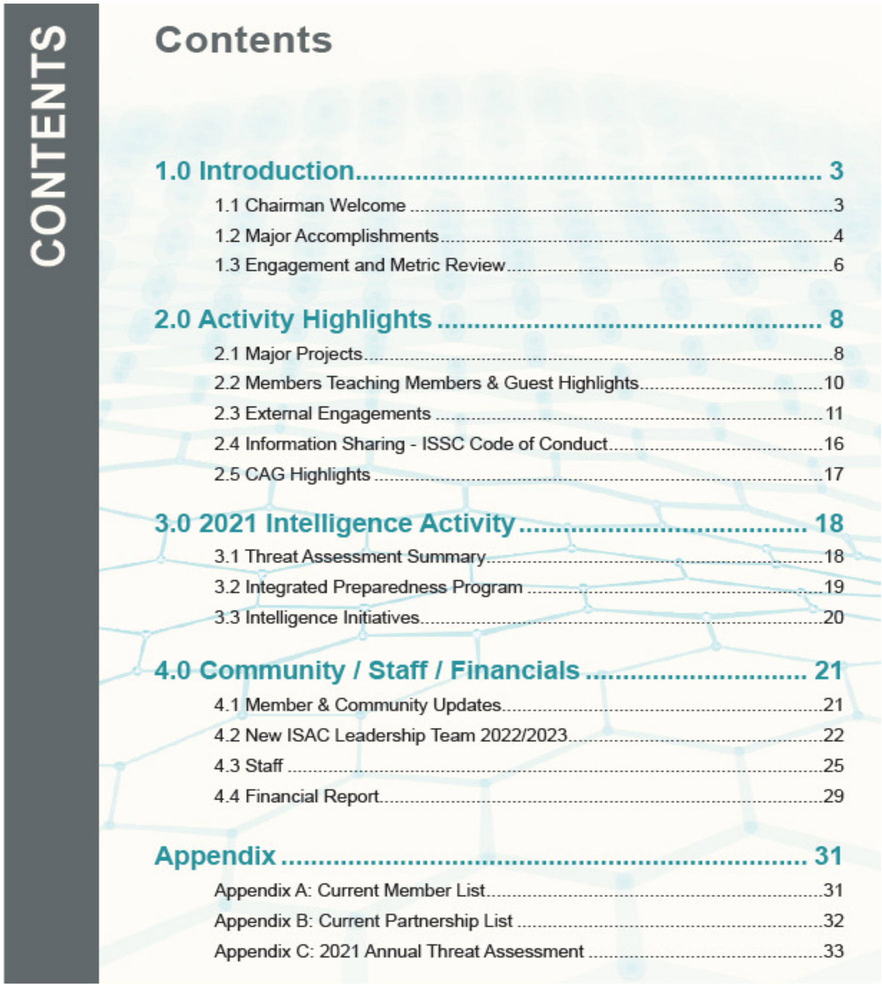
[1] *Reported in Upstream 2022 Cybersecurity Report*



AUTO-ISAC

AUTO-ISAC
Automotive Information Sharing and Analysis Center

2021 Annual Report & Threat Assessment



CONTENTS

Contents

AUTO-ISAC 2021 THREAT ASSESSMENT

7 KEY JUDGEMENTS

Anticipated Threats to the Automotive Industry in 2022

- ❑ Ransomware Groups
- ❑ Other Cybercriminal Organizations
- ❑ State-Sponsored Advanced Persistent Threat Groups
- ❑ Technology-Enabled Vehicle Theft

- ➢ In 2021 there were numerous ransomware and other cybercrime attacks on automotive companies, suppliers, and service providers resulting in disruptions of business and industrial operations and loss of sensitive information.

- ➢ Vehicle thefts in the United States decreased significantly (-4%) in 2019 and then spiked nearly 11% in 2020 (when COVID took hold), well above the previous 5-year annual trend (+/- 1-2%). Vehicle theft is expected to remain elevated in the coming year.

- ➢ The true scope of global technology-enabled vehicle theft activity is unclear due to lack of metrics on different theft tactics.

Auto-ISAC 2021 Threat Assessment

7 Key Judgements

Anticipated Potential Threats to Connected Vehicles in 2022
❑ Malware-Infected Websites, Applications, and Files Accessed via Internet-Connected Devices Synced with In-Vehicle Systems
❑ Malicious Exploitation of Vulnerabilities in Information, Communications, and/or Operational Technology
❑ Threat Actor use of Nation-State-Quality Cyberweapons

- **Barring technology-enable vehicle theft, malicious cyberattacks on connected vehicles are not occurring.**
- **Researchers are finding and reporting connected vehicle vulnerabilities to vehicle manufacturers.**
- **Proactive imagination of how new and old vulnerabilities, malware, and tools could lead to cyberattacks that threaten vehicle safety will keep the industry ahead of potential threats and the continuously evolving threat environment.**

Connected Vehicle Cybersecurity Protection

The Trajectory

- ➢ **Public-Private Partnership Essential**
  - ✓ Cybersecurity Framework for sharing information
  - ✓ Private sector working together / sharing | Government
- ➢ **Resiliency - Risk, Threat, Mitigation**
  - ✓ Shared Situational Awareness
  - ✓ *One's detection is another's prevention*
- ➢ **Working Together Framework**
  - ✓ Connected Vehicle Framework & Roadmap needed
  - ✓ International cybersecurity strategy essential
  - ✓ Coordinated policy for automotive cyber domain

Zero safety-related cyber incidents

JUSPAXAR
OBRIGADO
MATONDO
SALAMAT
KIITOS
KIA ORA
MULTUMESC
MAAKE
MOCHCHAKKERAM
TERMA KASIH
RAIBH MAITH AGAT
CHOKRANE
SALAMAT
GRAZIE
MULTUMESC
MERCI
CAM ON BAN
RAIBH MAITH AGAT
MERCI
MERCI
OBRIGADO
MOCHCHAKKERAM
MOCHCHAKKERAM
GRAZIE
THANK
ASANTE
CHOKRANE
UA TSAUG RAU KOJ
MATUR NUWUN
MOCHCHAKKERAM
MATONDO
YOU
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
OBRIGADO
DANK JE
RAIBH MAITH AGAT
SPASIBO
WELALIN
VINAKA
NIRRINGRAZZJAK
MAMANA
SPASIBO
ARIGATO
KIITOS
MAAKE
DANKON
OBRIGADO
MULTUMESC
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO

Our Contact Info

Faye Francy
Executive Director

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

http://www.automotiveisac.com