Cybersecurity Preparedness Through Collaboration:

Strengthening Automotive Resilience

Faye Francy, Auto-ISAC Executive Director
Mathew Thompson, Auto-ISAC Intelligence Officer
Carey Garback, Auto-ISAC Education and Awareness Leader

March 26, 2026

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Biography

Faye Francy
Executive Director, Auto-ISAC

Current Positions

- Executive Director of Auto-ISAC
- Member of National Council of ISACs

Past Positions

- The Boeing Company, Director; Executive Director of Aviation-ISAC
- ARINC, Director
- InterSec, President & Owner
- Aviation Security (AvSec), Senior Vice President, Owner
- Forensic / Chief Chemist

Education

- Bachelor of Science, Chemistry & Mathematics
- Master of Science, Forensic Chemistry

Biography

Mathew Thompson
Auto-ISAC

Current Positions

- Intelligence Officer
- Program Leader for the Automotive Threat Matrix (ATM)

Past Positions

- Cybersecurity Intelligence Analyst, Federal Contracting
- Signals Intelligence Analyst, U.S.M.C. / Federal Contracting
- Data Flow Manager, United States Marine Corps

Education

- M.S. Cybersecurity Technologies
- GCIH, GCIA, GSLC

Biography

Carey Garback

Auto-ISAC

Current Positions

- Education and Awareness Leader, Auto-ISAC
- Program Leader for Automotive Cybersecurity Training (ACT) program

Past Positions/Experience

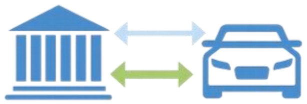
- Learning & Development Leader
- Designed and directed training programs for Fortune 500 clients. Worked in several industries including automotive, technology, insurance, & finance
- Experience with strategy, roadmaps, course design and delivery, and training program management

Education

- Bachelor of Arts, Telecommunications – Michigan State University
- Master of Arts in Teaching, English Education – Wayne State University
- Blended Learning Certification – Association for Talent Development

Thank you Transport Canada!

Why This Session Matters for Regulators



- **Shared Responsibility:** Vehicle cybersecurity resilience depends on coordinated public–private action

- **Preparedness Over Reaction:** Anticipating and mitigating risk before incidents occur

- **Scalable Impact:** Industry collaboration enables consistency, efficiency, and alignment across jurisdictions

- **Collaboration Bridge:** Auto-ISAC operationalizes collaboration and engagement. Two flagship programs demonstrate the value of collaborating

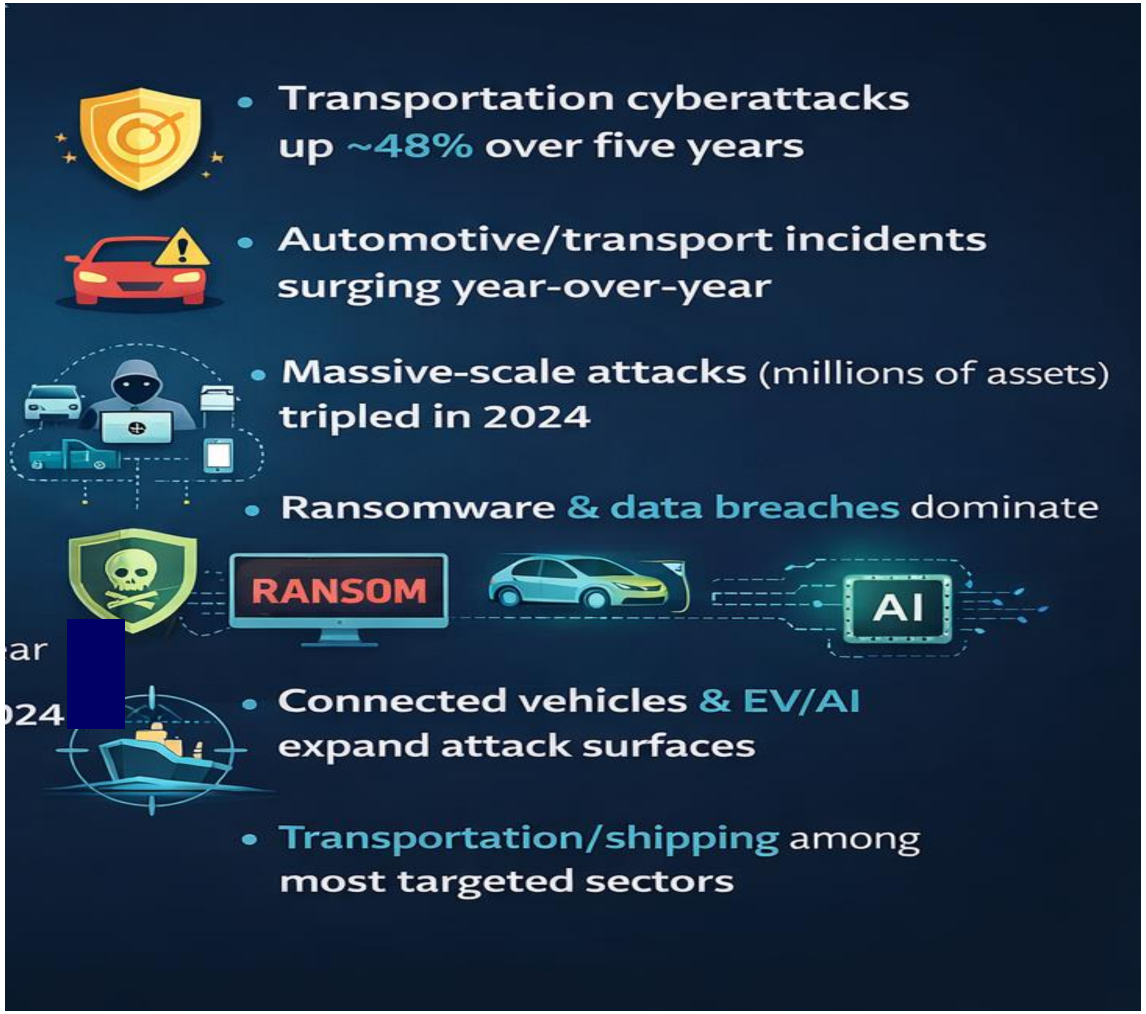
- **System Interdependence:** Vehicles rely on complex, interconnected hardware, software, and infrastructure across the supply chain

- **Shared Risk Exposure:** Vulnerabilities in one area can cascade across manufacturers, suppliers, and operators

- **Collective Defense:** Collaboration enables earlier visibility, faster response, and more consistent risk mitigation

The Threat Landscape

Transportation & Automotive Cyber Risk Drivers



Auto-ISAC Mission | Goal: *Zero Safety Related Cybersecurity Incidents*

Umbrella Cyber Defense

The Auto-ISAC functions as an impartial information broker, delivering umbrella coverage that ***connects and coordinates*** the global automotive community to ***enhance automotive cybersecurity*** through ***trusted collaboration***

Reduce Business Risk

Mitigation of business risks across ***light- and heavy-duty vehicles, suppliers, and commercial fleets and carriers.*** Initial focus on in-vehicle security has expanded to include product-related IT/OT security

What We Do

Intel Sharing

Data curation across intel feeds, submissions & research

Analysis

Validation, context, & recommendations

Education & Training

Advancing cyber maturity through knowledge sharing, training, & awareness

Partnerships

Industry, academia, vendors, researchers & government engagements

Sharing Across the Automotive Community & Beyond Membership

Monthly Town Halls, Daily DRIVEN, training and awareness sharing

Auto ISAC – Collaboration Platform with Defined Value Streams

How do we meet Strategy & Mission → *Defined Value Streams*

INFO SHARING & AWARENESS
avoid or reduce impact of cybersecurity events, growing into automotive industry

+

EDUCATION
enable effective industry response & resilience, and demonstrate commitment to stakeholders

+

RELATIONSHIPS
ensure industry readiness; working together with partners and the greater community

=

VALUE STREAMS
providing knowledge sharing, awareness, & resilience

GLOBAL SCOPE	DOMAIN SCOPE	EDUCATION
Consistent processes and policies to support Global Automotive Industry Membership	Automotive relevant information in scope. Focus on information sharing and mitigation of business risks	ATM, ACT Program, Cyber Awareness Month, Best Practice Guide Updates, and Member-Teaching-Members

2030 Strategy — Auto-ISAC: The Automotive Cybersecurity CoE

AUTO-ISAC TWENTY (20) WORKING GROUPS

MEETING THE NEEDS OF TECHNICAL SMEs, MANAGERS & EXECUTIVES

Executive Working Groups (ExWG) - 4

1. Board of Directors (BoD)
2. CISO Executive Working Group (CISO XWG) [BoD/ED]
3. Legal Executive Working Group (LWG) [BoD/ED]
4. European Steering Committee (EuSC) [BoD/EuD]

Standing Committees (SC) - 4

1. Education and Training Standing Committee (ETSC)
2. Finance and Audit Standing Committee (FASC)
3. Information Sharing Standing Committee (ISSC)
4. Membership and Benefit Standing Committee (MBSC)

Affinity Groups (AG) - 2

1. Commercial Vehicle Affinity Group (CAG)
2. Supplier Affinity Group (SAG)

Working Groups (WG) - 7

1. IT/OT Working Group (ITOTWG) [ISSC]
2. Product Working Group (PWG) [ISSC]
3. European Analyst Working Group (EuAWG) [ISSC]
4. European Working Group (EuWG) [EuSC] [MBSC]
5. Japan Working Group (JWG) [MBSC]
6. Third Party Enterprise Cybersecurity Working Group (ECSWG)
7. *Newly Formed* – Governance, Risk and Compliance (GRC WG) [EuWG, MBSC]

Task Forces - 3

1. Summit Task Force (STF) (STF-Europe) [MBSC]
2. Eu Summit Task Force (EuSTF) [MBSC]
3. Nominating Task Force (NTF) [Board C/VC/ED]

Value to Industry and Public-Sector Stakeholders

Industry
Fewer disruptions and lower costs through proactive risk management.

Public Sector
Enhanced safety, security, and public confidence

Society
More resilient, reliable, and secure transportation

Auto-ISAC Automotive Threat Matrix (ATM)

https://atm.automotiveisac.com/home

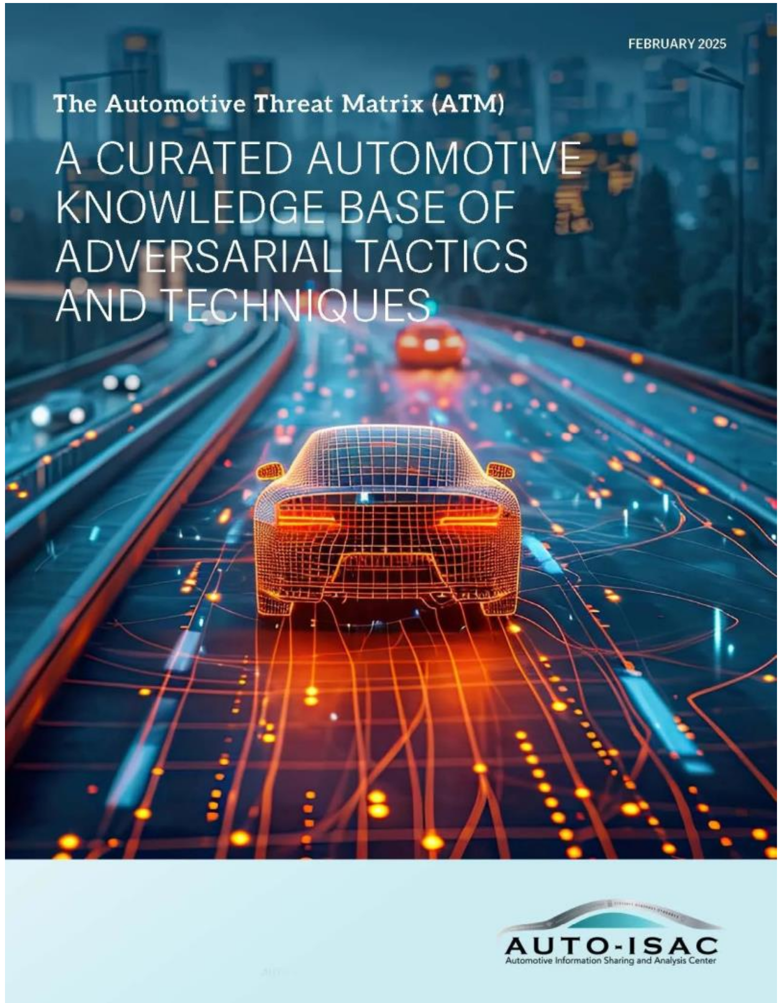
➢ What is the ATM ?

- An *online tool* and dataset of practical, verified adversarial *tactics & techniques used against the vehicle*

➢ Goal: Define a *common threat taxonomy* for the automotive industry

➢ Function: Enable cross-functional cybersecurity teams tackling complex issues with common understanding, assisting in tasks:

- Threat and risk assessment modeling
- Intelligence sharing
- Attack trend analysis
- Incident response
- Compliance reporting
- Cybersecurity testing



Community-Driven Framework

The ATM is governed by the ATM User Group providing credibility to the framework through:

- **Crowd Sourcing - Diverse Input**: Contributions from a diverse group of global subject matter experts offers Industry-wide perspective.
- **Open Collaboration**: User Group is not limited to Auto-ISAC Members.
- **Peer-reviewed Updates**: Proposed changes undergo group review before adoption.

Automotive Threat Matrix

Reconnaissance	Manipulate Environment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Gather Target Information – from Other	Adversarial Machine Learning	Aftermarket, Customer, or Dealer Equipment	Command and Scripting Interpreter	Abuse Standard Diagnostic Protocol for Persistence	Abuse Elevation Control Mechanism	Bypass Code Integrity Protections	Exploit Isolated Execution Environment Vulnerability	File and Directory Discovery
Gather Target Information – from Vehicle	Analog Sensor Attacks	Browser Compromise	Native API	Disable Software Update	Exploit Co-Located Computing Device for Privilege Escalation	Bypass Network Filtering	Capture SMS Message	Location Tracking
	Downgrade to Insecure Protocols	Exploit via Radio Interface	Abuse Standard Diagnostic Protocol to Temporarily Modify Execution	Modify OS Kernel, Boot Partition, or System Partition	Exploit OS Vulnerability	Bypass UDS Security Access	Input Capture	Network Service Scanning

ATM User Guide

Why did the User Group make a guide?

- **Great interest but some confusion:**
  - *Is there a guide? How do we use the ATM?*
  - *Not sure where to begin*

- **Tactics and Techniques**
  - A large number to learn
  - Daunting if new to ATM/MITRE, even as a security professional

14 Tactics to describe the target or goal of the adversary

Techniques under every Tactic to describe the "how".

Automotive Threat Matrix

Reconnaissance	Manipulate Environment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Affect Vehicle Function
Gather Target Information – from Other	Adversarial Machine Learning	Aftermarket, Customer, or Dealer Equipment	Command and Scripting Interpreter	Abuse Standard Diagnostic Protocol for Persistence	Abuse Elevation Control Mechanism	Bypass Code Integrity Protections	Exploit Isolated Execution Environment Vulnerability	File and Directory Discovery	Abuse Standard Diagnostic Protocol for Lateral Movement	Capture SMS Message	Aftermarket, Customer, or Dealer Equipment	Aftermarket, Customer, or Dealer Equipment	Adversarial Machine Learning
Gather Target Information – from Vehicle	Analog Sensor Attacks	Browser Compromise	Native API	Disable Software Update	Exploit Co-Located Computing Device for Privilege Escalation	Bypass Network Filtering	Capture SMS Message	Location Tracking	Bridge Vehicle Networks	Input Capture	Cellular Communication	Cellular Communication	Analog Sensor Attacks
	Downgrade to Insecure Protocols	Exploit via Radio Interface	Abuse Standard Diagnostic Protocol to Temporarily Modify Execution	Modify OS Kernel, Boot Partition, or System Partition	Exploit OS Vulnerability	Bypass UDS Security Access	Input Capture	Network Service Scanning	Exploit ECU for Lateral Movement	Network Sniffing	Internet Communication	Internet Communication	Abuse Standard Diagnostic Protocol for Affecting Vehicle Function
	Jamming or Denial of Service	Exploit via Removable Media		Modify Isolated Execution Environment	Exploit Isolated Execution Environment Vulnerability	Bypass Mandatory Access Control	Input Prompt	Process Discovery	Remote Services	Location Tracking	Receive Only Communication	Short Range Wireless Communication	CAN Bus Denial of Service
	Manipulate Communications	Malicious App		Compromise Cryptographic Security	Hardware Fault Injection	Compromise Cryptographic Security	Network Sniffing	Software Discovery	Reprogram ECU for Lateral Movement	Abuse Standard Diagnostic Protocol for Collection	Short Range Wireless Communication	Standard Cryptographic Protocol	Denial of Service on Vehicle Function
	Relay Communications	Phishing			Process Injection		ECU Credential Dumping	System Information Discovery	Compromise Cryptographic Security	Capture Camera or Audio	Standard Cryptographic Protocol	Removable Media	Local Function
	Rogue Cellular Base Station	Physical Modification			Reprogram Co-Located Computing Device for Privilege Escalation		Unsecured Credentials	System Network Configuration Discovery		Data from Local System		Physical Access	Modify Bus Message
	Rogue Wi-Fi Access Point	Supply Chain Compromise			Compromise Cryptographic Security		URI Hijacking	System Network Connections Discovery		Network Information Discovery			Unintended Vehicle Network Message
										Screen Capture			

ATM User Guide

Who is this for?

- **Automotive cybersecurity professionals with involvement in:**
  - SoC, Intel analysis
  - TARA/Risk management
  - Vulnerability Analysis
  - Incidence Response
- **See the Auto-ISAC ATM Whitepaper (Feb 2025) for more potential usage**

ATTACK TREND ANALYSIS

Cybersecurity at its core, is about assessing and managing risk. One of the goals during development of ISO/SAE 21434 was to define this common language and the ATM builds on that foundation. The ISO/SAE 21434 TARA process requires attack paths to be defined for each threat scenario. The ATM is a tool to help build these attack paths, as it was built upon the foundation of the MITRE ATT&CK taxonomy with modifications to support the unique automotive aspects.

The individual cells (components) of the ATM can be used to define each step of an attack path. The ATM serves as a "library" of potential steps of an attack path, and a promotes a common language within the supply chain and optimizes the process of determining the associated attack feasibility as each element (step) of the ATM can be assigned a default feasibility. Thus, after building the attack path by selecting elements of the ATM, which can be assigned a default attack feasibility by the user, the overall attack feasibility is instantly determine

(e.g., differences in architecture

THREAT ANALYSIS & RISK ASSESSMENT MODELING

Threat analysis and risk assessments (TARA), a form of threat modeling, are a required part of automotive security regulations and standards, such as UN Regulation R155, ISO/SAE 21434, and China's GB 44495-2024. These TARA models are ideally developed at the start of the design process so that later vulnerability management is as streamlined as possible. If a potential vulnerability is mitigated in the design process by adding security controls, such as enforcing encryption, or removing data channels, the overall attack surface is reduced.

The ATM can support the feasibility and analysis of damage scenarios, threat scenarios, and attack trees. The tactics and techniques outlined show a set of attack possibilities that may affect new designs. Using the information provided by the ATM serves to improve the future designs so that tomorrow's vehicles are more secure than today's vehicles.

Neither threat models nor the ATM are designed to be single-use tools. They are both continually updated

uously updated vehicle

INCIDENT RESPONSE

The ATM may be used to perform a technical analysis as part of an incident response (IR). A potential, or identified, incident may be compared to observed TTPs as part of the analysis, and to develop contextual understanding of the incident. The ATM may also be used as part of a common taxonomy for developing the IR report, including the vulnerability analysis.

The ATM, and its TTPs, may also be used to answer key questions, such as:

1. How is the adversary accessing and exploiting the environment?
2. How is the adversary maintaining command and control?
3. What are the methods of persistence (e.g. malware backdoor, remote tools, etc.)?
4. What methods are being used for reconnaissance?
5. Is lateral movement suspected or known? How is lateral movement conducted?
6. What techniques are used to exfiltrate data?

VULNERABILITY MANAGEMENT

Security experts often face the challenge of prioritizing the analysis and remediation of vulnerabilities. While it would be ideal if all vulnerabilities were remediated shortly after they are discovered (and before they can be exploited), this is often impractical for many embedded systems, including and especially automotive. Long development cycles, the need for rigorous integration and validation testing, high system complexity, and other factors result in a situation where a 'patch everything' approach is impractical or impossible. To make better use of limited resources, it is highly desirable to identify what subset of vulnerabilities are important to remediate, and in the case of zero-day vulnerabilities, an attacker has knowledge of an issue before the defender does. The ATM can be used to help with these situations.

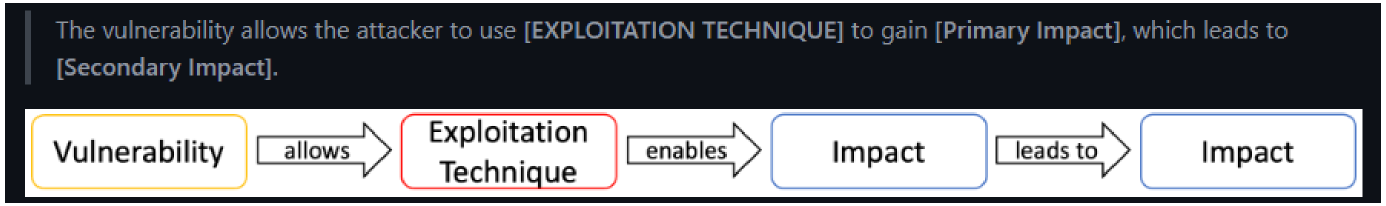
TLP:CLEAR

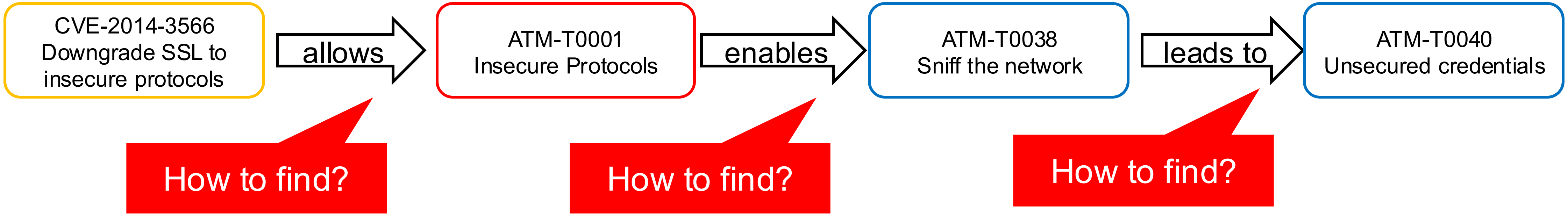
ATM User Guide

What is it?

➢ A "Quick start," how to get started

- Top-down, show how the ATM should be used
  - Referencing the *MITRE ATT&CK® Getting Started, Methodology*
- Bottom-up, show examples/use cases
  - Easy to follow, step-by-step use cases
- Section 1: Vulnerability Analysis
  - Describe how to find *Tactics* and *Techniques* in the ATM Matrix associated with a vulnerability
  - Show how to map and follow the attack chain



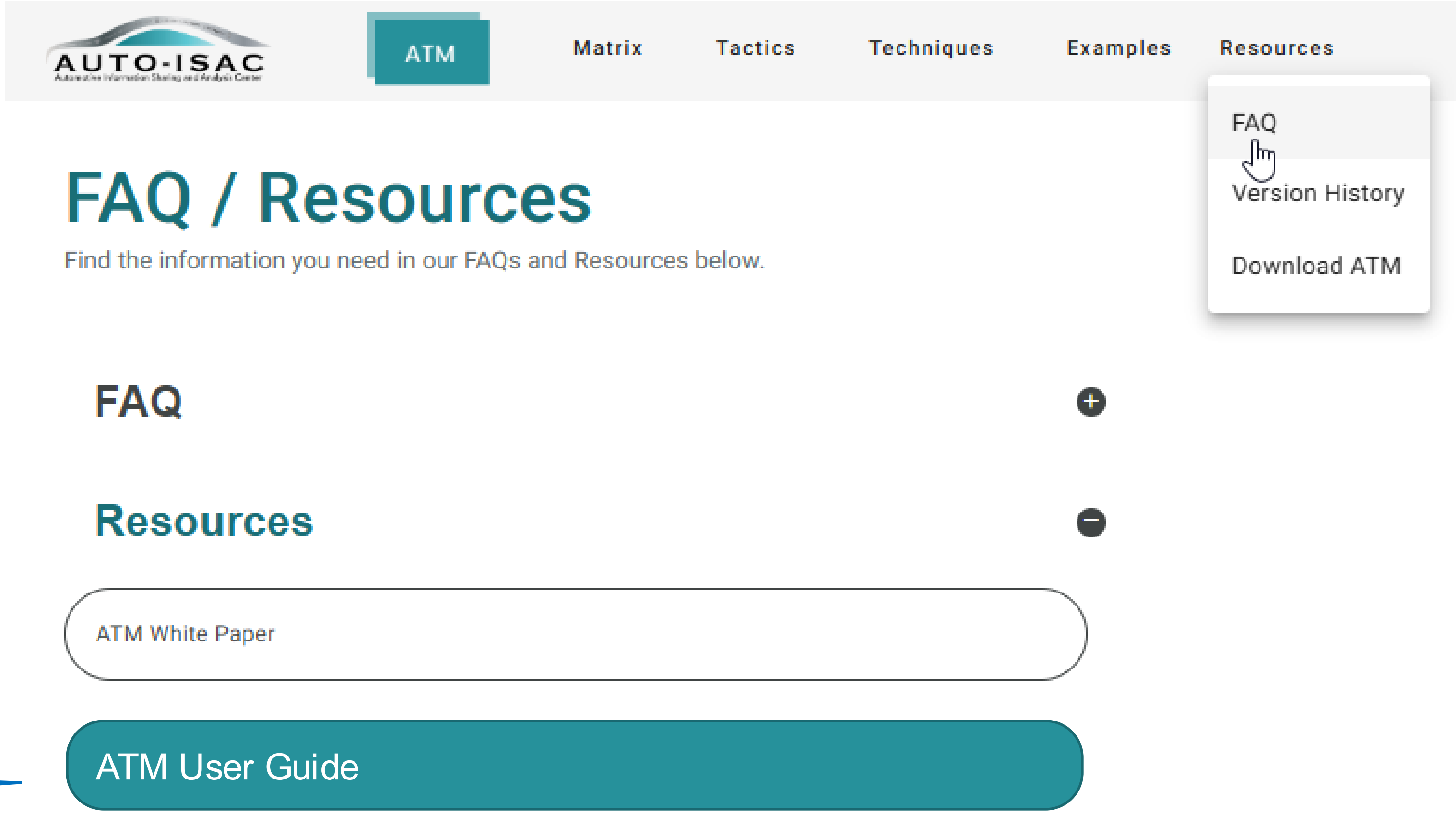


ATM User Guide

Section 1: Vulnerability Analysis, Scenario 1 available online on the ATM website

- https://atm.automotiveisac.com

Here



WHY WORKFORCE PREPAREDNESS IS CRITICAL TO CYBERSECURITY RESILIENCE

Rapid Response to Threats
Prepared teams recognize, escalate, and respond more quickly when issues arise.

Empowered, Informed Staff
Shared knowledge and training improve decision-making across organizations.

Proactive Defense Capabilities
A prepared workforce enables earlier identification and mitigation of risk.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

TLP:CLEAR

What is the Automotive Cybersecurity Training (ACT) Program?

ACT is an educational training program that was developed with top global experts to produce a comprehensive curriculum based on fundamental and advanced automotive cybersecurity best practices, standards, and regulatory knowledge.

- A NHTSA grant funded the creation of the ACT Program
- Auto-ISAC sponsored a year-long, global research study to create an R-155 and R-156-compliant teaching curriculum based on ISO/SAE 21434 stipulations
  - Established a Tiger Team to review the research and support curriculum development and trainer selection
  - After running both Alpha and Beta pilots, the ACT Program is fully validated, and content is regularly updated to meet changing industry needs
- Badges and certificates are issued at the completion of each course
- Earn an automotive cybersecurity certification
- The program is available to the broader automotive community

Automotive Cybersecurity Training (ACT)

➢ Fundamental Courses

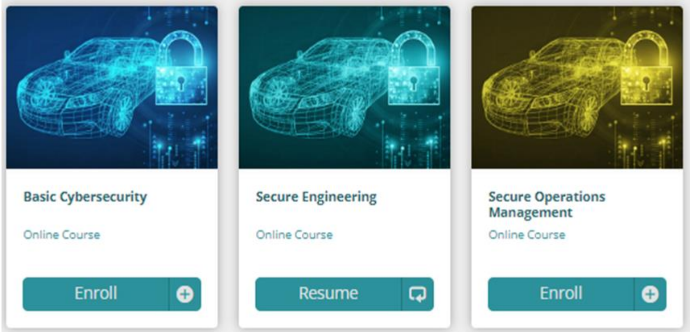
- ***Updated*** assessments
- ***New*** Secure Engineering Kali Linux Pen Testing lab
- ***New*** Test Out Exam allows learners to move to Advanced courses quicker

Basic Cybersecurity
- Engineering (with lab)
- Operations Management

Engineering
- Wireless
- EV Infrastructure
- Guided Attacks

➢ Advanced Courses

- **Originally** designed for in-person learning
- ***Now – New*** online courses created for global audience
- ***New*** live, in-person labs for each online course
  - not required, but highly recommended



➢ Learning Management System (LMS)

- ✓ **All courses are Online, On-Demand**
- ✓ **Capability Exam (CAPEX) to earn CASE**
  - o Updated and online – May 2026
- ✓ **Course, CASE and CPE transcripts**
- ✓ **Badges and Certificates – all in one place!**

AUTO-ISAC CASE CERTIFIED AUTOMOTIVE CYBERSECURITY ENGINEER

WHO SHOULD ATTEND ACT? *TARGET AUDIENCE*

ACT Fundamentals

- New hires, interns, co-op students, employees new to cybersecurity role
- Individuals with limited cybersecurity experience looking to up-skill
- Anyone with a curiosity for automotive cybersecurity interested in learning fundamental concepts of the cybersecurity field

ACT Advanced

- Mid-level IT or cyber professional, proficient but not an expert in specific course topic(s)

CASE Certification

- Pass the Capability Exam (CAPEX) offered annually
  - Open to anyone who believes they have the combined knowledge of ACT Fundamentals and Advanced courses – courses are <u>not</u> a prerequisite

How ACT Supports Different Audiences

Engineering and Technical Teams

Provides practical, applied cybersecurity training aligned to real-world vehicle systems and threats.

Operational Decision-Makers

Builds a shared understanding of risk and response, enabling more informed and timely operational decisions.

Executive and Leadership Awareness

Improves cybersecurity literacy at the leadership level, supporting oversight, accountability, and strategic alignment.

Shaping the Future
Automotive Cybersecurity

Contribute to Industry Practices
Participate in shaping automotive cybersecurity policies, frameworks, and best practices through Auto-ISAC initiatives.

Collaborate with Peers
Engage with other members to share insights, experiences, and expertise, helping to advance solutions across the sector.

Influence Cybersecurity Priorities
Join working groups to provide input on Auto-ISAC's focus areas and contribute to collective problem-solving and knowledge sharing.

Stay Engaged and Informed
Regular involvement in meetings, discussions, and activities keeps your organization connected to the latest intelligence, trends, and best practices in automotive cybersecurity.

Strategic Navigation

Building a Roadmap to Protect the Automotive Industry

➢ **Cybersecurity Management:** ***Building a Culture of Security***

✓ **Embedded Network Security Requirements across lifecycle**

✓ **Training & Awareness / New Skills (ACT Program)**

✓ **Threat Detection & Vulnerability Management**

✓ **Focus on Business Risk Management**

➢ **Collaboration is key:** ***Threat Actors do it all the time!***

➢ **Continuous Education and Awareness is a necessity**

- **Governance, Risk Management and Compliance (GRC)**
- **Security Development Lifecycle, understanding ATM+**
- **3rd Party Risk Management**
- **Institutionalize Incident Response**
  - ✓ **Intel and Information Sharing (Early and Often)**
  - ✓ **Threat Response and Recovery**
  - ✓ **Sharing within the Auto-ISAC and across industry**

An Attack on One is an Attack on All

Auto-ISAC Contact Information

Faye Francy
Executive Director

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

Carey A. Garback
Education And Awareness Leader

20 F Street Northwest
Suite 700
Washington, DC 20001
404-539-2519
careygarback@automotiveisac.com

Mathew Thompson
Sr. Cybersecurity Intelligence Analyst

20 F Street Northwest
Suite 700
Washington, DC 20001
404-539-2519
MathewThompson@automotiveisac.com

https://automotiveisac.com/contact-auto-isac

Thank you!


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