AUTO-ISAC

ACT

AUTOMOTIVE CYBERSECURITY TRAINING

Automotive Cybersecurity training (ACT)

Staff Leader: Tamara Shoemaker, Auto-ISAC

February 3, 2023

This document is Auto-ISAC Sensitive and Confidential.

TLP : CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

About the Speaker

Tamara Shoemaker
Auto-ISAC
Cybersecurity Training Lead

Current Positions

- Auto-ISAC Automotive Cybersecurity Training Program Lead - (ACT)
- ETSC Staff Lead

Past Positions

- Director, University of Detroit Mercy's Center for Cybersecurity & Intelligence Studies
  - **Designating a Center of Academic Excellence in Cyber Defense with Dept of Homeland Security and the National Security Agency since 2004**
- Founder of the Michigan CyberPatriot K-12 Program
- Program Coordinator, Michigan Member Alliance InfraGard
- Co-Founder of the MCISSE Coalition of Michigan CAEs
- Licensed Private Investigator for 12 years

Drive

- 2019 Ford Taurus Sho and 2004 Ford T-Bird

AUTO-ISAC MISSION

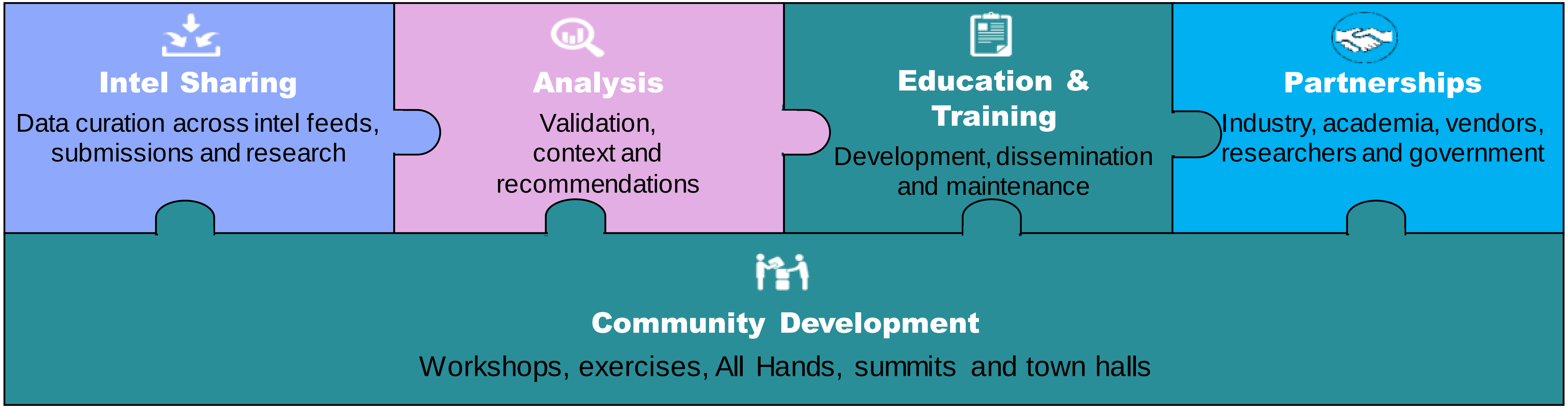
Mission

Serve as an unbiased information broker to provide 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

Light- and heavy-duty vehicles, suppliers, commercial vehicle fleets and carriers. Currently, we **are focused on *vehicle* cyber security** and have expanded into IT/OT security related to the vehicle (4Q20).

What We Do



Intel Sharing

Data curation across intel feeds, submissions and research

Analysis

Validation, context and recommendations

Education & Training

Development, dissemination and maintenance

Partnerships

Industry, academia, vendors, researchers and government

Community Development

Workshops, exercises, All Hands, summits and town halls

Auto-ISAC and National Highway Traffic & Safety Administration

Cybersecurity is an essential component of motor vehicle safety due to the increased connectivity of motor vehicles. The motor vehicle industry faces growing challenges in managing cybersecurity threats and enhancing cybersecurity resiliency to ensure motor vehicle safety. Addressing these challenges requires specialized skills and training different from traditional enterprise/information systems-focused cybersecurity educational programs.

The Auto-ISAC recognized the need for a common motor vehicle cybersecurity educational program. ACT program was established because no comprehensive curriculum addressed cybersecurity in the automotive segment. NHTSA's best practices identified workforce development and continuous education as crucial steps to improve motor vehicle cybersecurity.

ACT Program - Development of Curriculum & Courses

Design of the ACT Program

- Performed global research on existing vehicle cybersecurity training and education
- Membership review and validation
- Alignment with industry needs

Dedicated **Tiger Team** to support the review development and oversight:

- Curriculum
- Courseware
- Training Staff

- Conducted **Alpha and Beta pilots** to determine any course corrections
- Selected both novice and experienced cybersecurity trainees
- Program will be sustained and updated as needed

ACT Program
Course Delivery

Fundamental courses

Delivered online using University's learning system, offered both synchronously and asynchronously, as defined tracks:

1. **Basic Cybersecurity** (36 Hours)
2. **Security Engineering** (36 Hours)
3. **Security Operations, Government, & Management** (36 Hours)

Advanced courses

Delivered hands-on at the **American Center for Mobility** in Ypsilanti, Michigan:

1. **Advanced Engineering** (36 Hours)
2. **Advanced Wireless** (40 Hours)
3. **Guided Attacks** (38 Hours)
4. **EV and EV Infrastructure** **(36-40 Hours)**

***These courses lead to certificates of completion*.**

Automotive Cybersecurity Training (ACT) Program Update

Metrics for the ACT program:

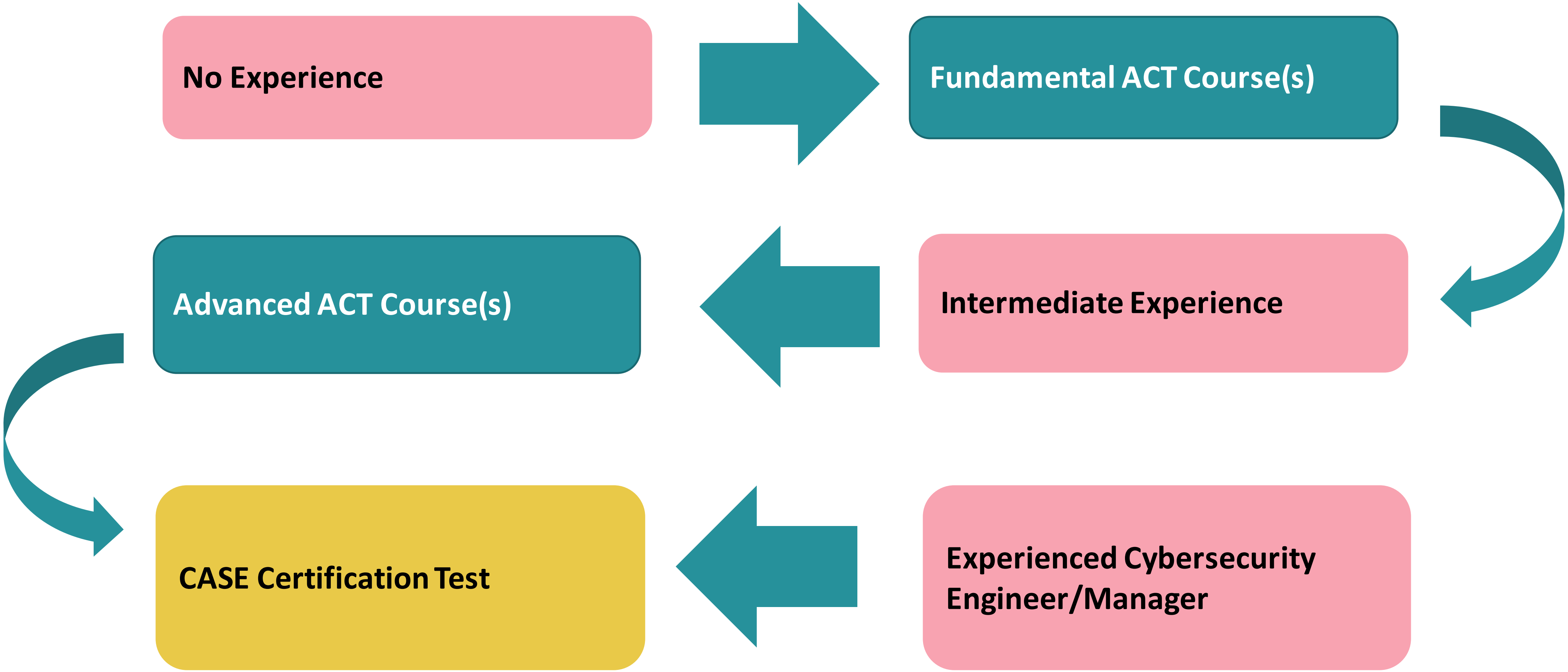
- **224** Individual members signed up for courses from **53** Member companies
- **134** Trainees attended the Fundamentals Alpha and Beta Courses
- **105** Trainees attended Advanced Alpha and Beta Courses
- **59** Members are scheduled to sit for the CAPEX (**27** on Jan 24th and **32** in March)

Certificates of completion and Certification

- Certification web application to track certificates of completion and CASE Certification.
- Compiled criteria for certificates of completion on current trainees.
- **CAPEX** is a Capability Exercise required to qualify for the **Certified Automotive cyberSecurity Engineer Certification (CASE).**
  - To take the CAPEX: You must be an experienced Cybersecurity Engineer or a trainee who has completed the ACT course blocks appropriate to augment your knowledge and experience.
  - To qualify for the CASE designation, you must pass this virtual scenario-based one day exercise.

ACT Training will be scheduled for the Fall of 2023 – www.automotiveisac.com.

ACT Program Target Audience



No Experience

Fundamental ACT Course(s)

Intermediate Experience

Advanced ACT Course(s)

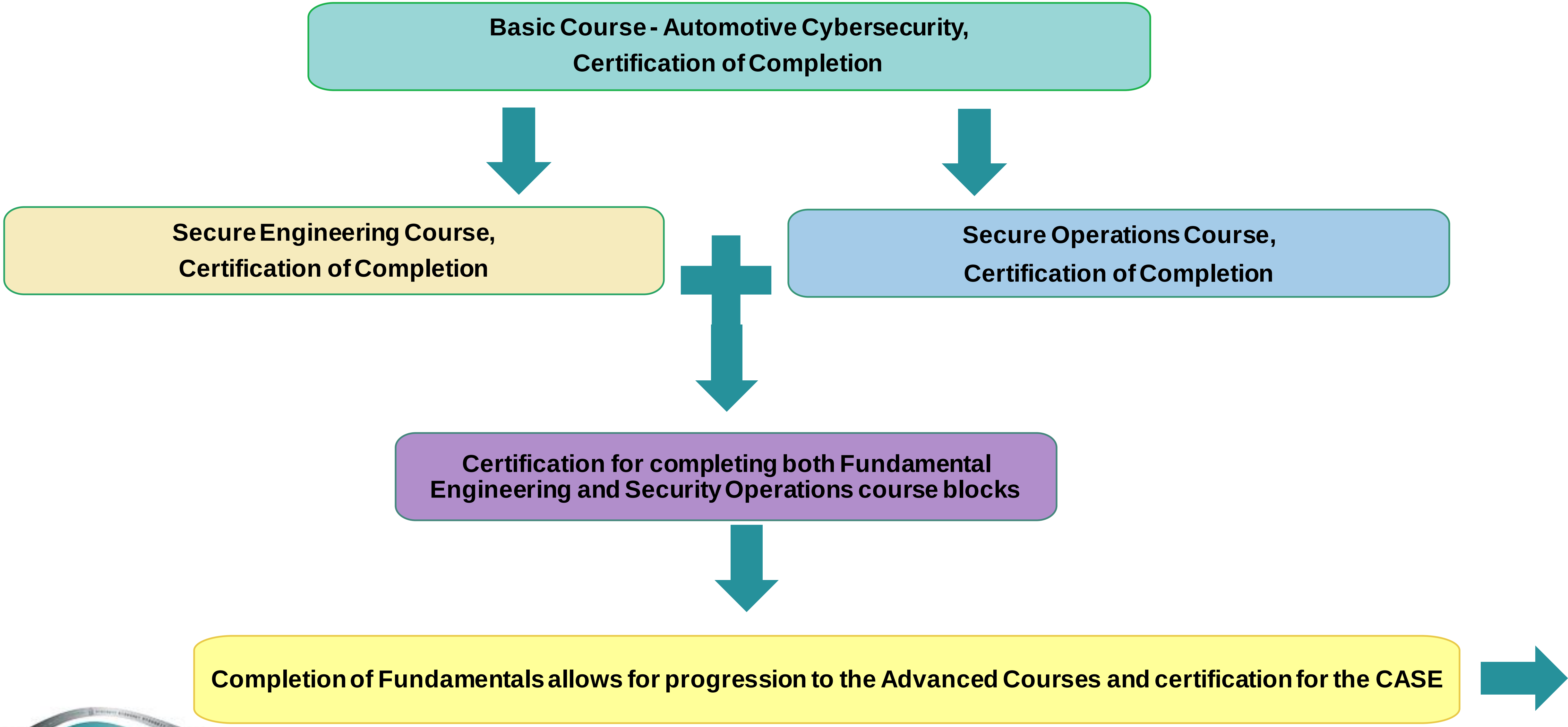
CASE Certification Test

Experienced Cybersecurity Engineer/Manager

Sustainment of the ACT Program

- **Goal:**
  - ACT Fundamental Courses available through University Partners, and
  - ACT Fundamental Courses available through Auto-ISAC via *a Learning Management System*
  - ACT Advance Course scheduled in person for the Fall of 2023
  - Certifications awarded for Course completion
  - CASE Certification awarded after passing the CAPEX
- **Fundamental Course will be shared with Partnering Universities**
  - University Partners supply their Cybersecurity curriculum (prerequisites)
  - Audit of curriculum, unless certified as an NSA/DHS Center of Academic Excellence (CAE)
  - Auto-ISAC supplies Fundamentals Courses from the ACT Program
  - Periodic Follow-ups will be required to ensure the integrity of the Program
- **Assembling of Courses to fit the University model**
  - Mapping to standards, regulations, and best practices
  - Adjusting to Tiger Team, Trainee reviews, and Expert advice
  - Membership requesting online on-demand training (LMS)
  - Standardizing of curriculum for partnering universities
- **Advance Courses**
  - Negotiate contracts with 20+ instructors
  - Choose venues and LMS
  - Purchase Equipment

Certification Stackable Pathway for fundamentals



Basic Course - Automotive Cybersecurity, Certification of Completion

Secure Engineering Course, Certification of Completion

Secure Operations Course, Certification of Completion

Certification for completing both Fundamental Engineering and Security Operations course blocks

Completion of Fundamentals allows for progression to the Advanced Courses and certification for the CASE

ACT Beta re-aligned Curriculum

Fundamentals – Online instructor led training

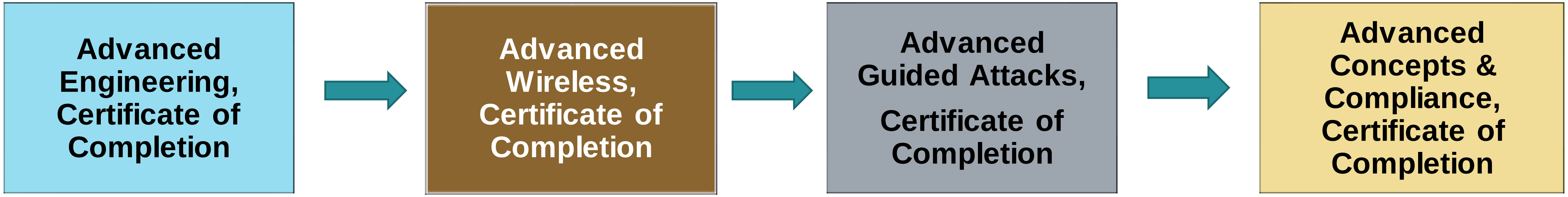
- **Basics – 30-36 Hours**
  - Cybersecurity Basics (NIST Workforce Framework, CSEC 2017, NIST 800)
  - Automotive Threat Management (Clause 15)
  - Risk Management (RMF)
  - UNECE Regulatory Compliance (R155-21434, R156-24089)
  - Security Operations
  - Data Privacy and Protection (GDPR, PCI . .)

- **Security Engineering – 36 Hours**
  - System Security Engineering Process (24089)
  - CANbus and Protocols
  - Crypto Applications
  - Intro to Communication Security/OSI
  - Metrics & Measurements Process
  - Operating Systems Security

- **Security Operations, Government, & Management – 36 Hours**
  - Cybersecurity Policies (Clause 5)
  - Cybersecurity Policy Implementation (clause 8)
  - Cybersecurity Control Models (Clause8(
  - Product Vulnerability Management/CM (Clause 7)
    - Build IR Playbook
    - Incident Response Process
    - Supply Chain Woes
  - Other, Fleets, Off Road, Military . . .

Advanced Courses & Certification for CASE

Those without experience should take the courses in this order.



Advanced Engineering, Certificate of Completion

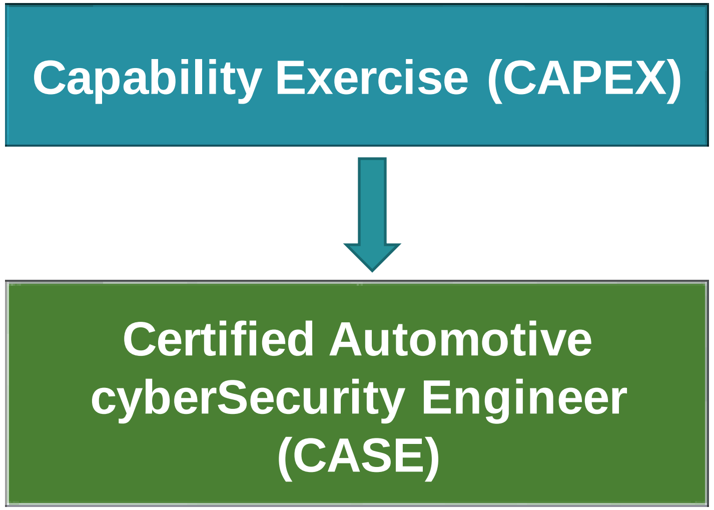
Advanced Wireless, Certificate of Completion

Advanced Guided Attacks, Certificate of Completion

Advanced Concepts & Compliance, Certificate of Completion

Intermediate experienced may take courses that fulfill their needs.

Experts may go straight to the CAPEX.



Capability Exercise (CAPEX)

Certified Automotive cyberSecurity Engineer (CASE)

Advanced EV in place of C&C coming soon!

ACT Beta Curriculum

Advanced – Collaborative in-person hands-on training

- Advanced Engineering – 36 Hours
  - Approaches to Secure Design Thinking
  - CAN Tools & Low-Level Interactions
  - Overview of Sec Hardware Design Principals
  - ISO-TP Details
  - Interactive UDS
  - Software Updates
  - Infotainment Flaws and Remedies
  - Forensics
  - Automotive Risk Assessment
  - Intro to Hardware Reverse Engineering
  - Intro to Software Reverse Engineering
- Advanced Intelligence Analyst – 36 Hours
  - Bluetooth
  - WiFi
  - Nearfield
  - Cellular & Telematics
  - Protocols & Diagnostics
  - SDR & GPS
  - V2X
  - Ultra Wide Band
- Guided Attacks – 40 Hours
  - Remote Keyless Entry
  - Side Chanel Analysis and Fault Injection
  - Relay Hardware Attacks
  - RF Attacks
  - Phone App Attacks
  - ARM/Intel/etc. Exploitation
  - ISO 21434 – Advanced Attacks
  - Sensor Fusion, Adversarial AI
  - TMPS
- Future EV Session 36 Hours
  - EV Security & GRID Interactions
  - Courses for this section TBD

Certification scheme

Certifications of Completion

- One certification per course block completed
- One certification for completing all Fundamentals and Advance

Certified Automotive Security Engineer (CASE)

- Completion of Courses plus CAPEX for beginners
- Completion of Advanced course plus CAPEX for intermediate level of experience
- CAPEX for cybersecurity professionals

Sustainment of the ACT Program

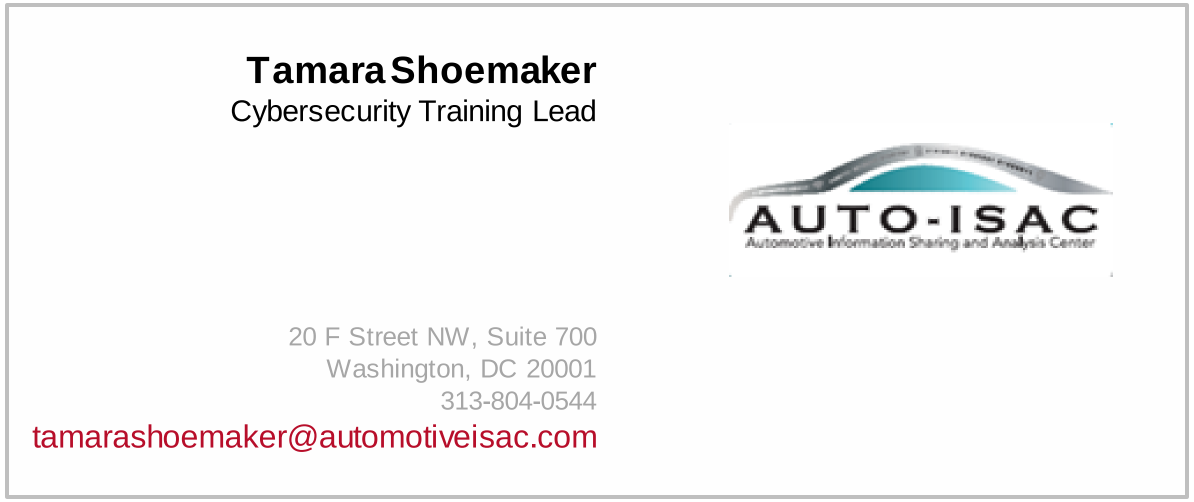
➢Fall 2023 – *visit our website for updates*

- Fundamental Basic, Secure Engineering and Secure Operations, Government, and Management online via Learning Management System and partnering universities
- Advanced: Engineering, Wireless, Guided Attack, and EV offered in the Metro-Detroit Michigan area
- Capability Exercise (CAPEX) for Certified Automotive Cybersecurity Engineer (CASE) offered as needed

www.automotiveisac.com

WWW.AUTOMOTIVEISAC.COM

Our Contact Info



Tamara Shoemaker
Cybersecurity Training Lead

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street NW, Suite 700
Washington, DC 20001
313-804-0544
tamarashoemaker@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com