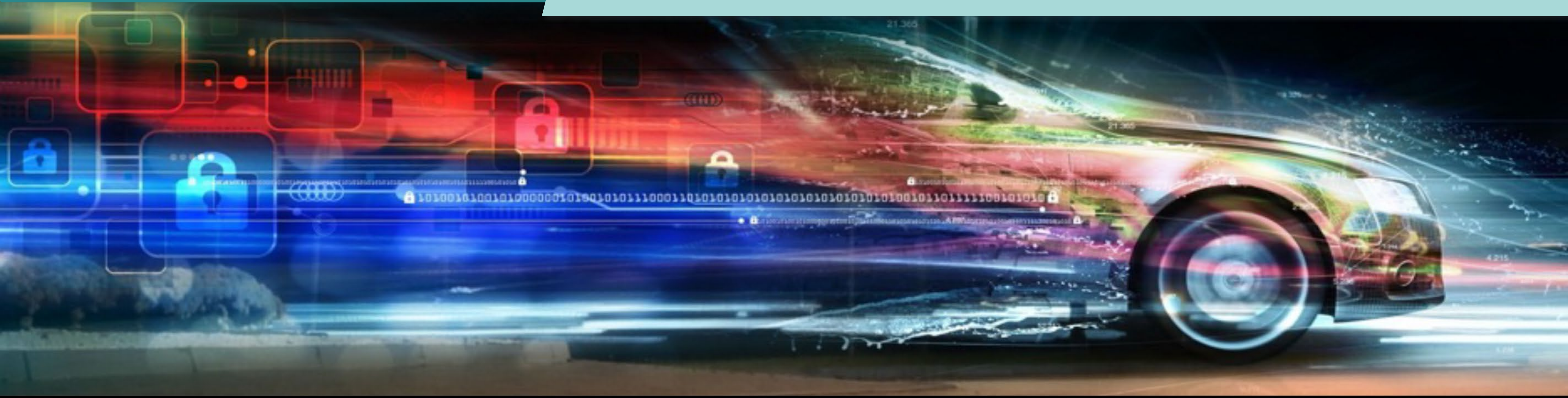


Welcome to Auto-ISAC!

Monthly Virtual Community Call

March 2, 2022

This Session will be recorded.

TLP:WHITE

AUTO-ISAC

Automotive Information Sharing and Analysis Center

DHS Traffic Light Protocol (TLP) Chart

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
TLP:RED 🔴 ● ● Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	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.
TLP:AMBER ● 🟡 ● Limited disclosure, restricted to participants organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.
TLP:GREEN ● ● 🟢 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ○ ○ ○ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

From: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We’re Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ What’s Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ▪ **Tamara Shoemaker, *Cybersecurity Training Leader, Auto-ISAC***
11:45	**Around the Room** ➢ 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!

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

22 *OEM Members*

21 *Navigator Partners*

43 *Supplier & Commercial Vehicle Members*

17 *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)*

2022 - 2023 Board of Directors

Executive Committee (ExCom)

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

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

Jenny Gilger
Secretary *of the*
Board of the Directors
Honda

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

Todd Lawless
Chair *of the*
Advisory Board
Continental

2022-2023 Advisory Board (AB) Leadership

Todd Lawless
Chair *of the*
Advisory Board
Continental

Bob Kaster
Vice Chair *of the*
Advisory Board
Bosch

Allen Houck
Chair *of the SAG*
NXP

Larry Hilkene
Chair *of the CAG*
Cummins

TLP:WHITE

Member Roster

as of March 2022

Highlight = Change

65 Members, 3 in Progress

Aisin	Hyundai	NXP
Allison Transmission	Infineon	Oshkosh Corp
Aptiv	Intel	PACCAR
Argo AI, LLC	John Deere Electronic	Panasonic
AT&T	Kia	Polaris
AVL List GmbH	Knorr Bremse	Qualcomm
Blackberry Limited	Lear	Renesas Electronics
BMW Group	LGE	Stellantis
BorgWarner	Luminar	Subaru
Bosch (Escrypt-Affiliate)	Magna	Sumitomo Electric
Continental (Argus-Affiliate)	MARELLI	Tokai Rika
Cummins	Mazda	Toyota
Denso	Mercedes-Benz	TuSimple
Faurecia	Meritor	Valeo
Ford	Mitsubishi Motors	Veoneer
Garrett	Mitsubishi Electric	Volkswagen
General Motors (Cruise-Affiliate)	Mobis	Volvo Cars
Geotab	Motional	Volvo Group
Google	Navistar	Waymo
Harman	Nexteer Automotive Corp	Yamaha Motors
Hitachi	Nissan	ZF
Honda	Nuro	

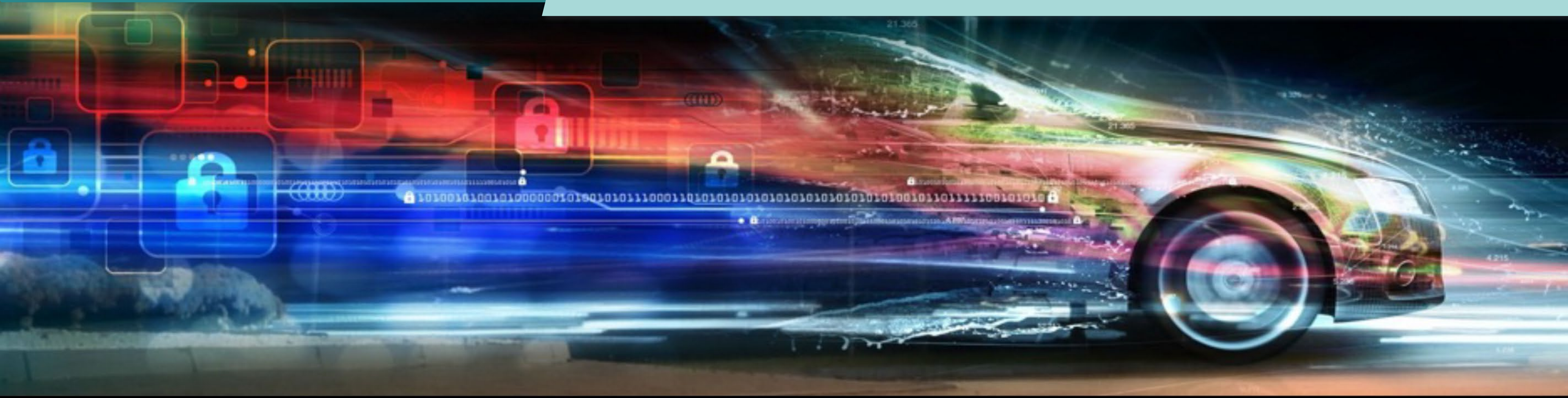
TLP:WHITE

Upcoming Events

- **Community Call:**
  - **Wednesday, April 6 - Speaker: Tara Hairston**, ***Alliance for Automotive Innovation*** **Title: *"Public Policy Affecting Automotive Cybersecurity"*** **Time:** *11 – 12:00 p.m.* **TLP:WHITE**

- **Special Announcement *for Auto-ISAC Members Only*: TLP:AMBER**
  - The **EuWG's workshop** is coming up on March 30th will concentrate on the theme ***"Make Information Sharing Easy!"*** and other topics of special interest to our European participants.

- **Announcements:**
  - **Call for Community Call Speakers:** Might you want to speak on the topics related to Automotive and Cybersecurity? Please send your ideas to Sharmila Khadka.
  - **SAG's SBoM Working Group** is finalizing proposed **SBoM Best Practice Guide.** SBoM will brief the Board Q1.
  - **Auto-ISAC Annual Report:** In work for BoD Review/Approval in Q1 '22.
  - **ACT Program Advanced Courses** begin on April 11th. Beta signup is open for Members ***now***. Contact **Tamara Shoemaker**.



Auto-ISAC Intelligence

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- Know what we track daily by subscribing to the DRIVEN
  - Send feedback, contributions or questions to analyst@automotiveisac.com
- Expect the Auto-ISAC 2021 Annual Report and Threat Assessment this quarter.
- Intelligence Notes
  - The geopolitical landscape has dramatically changed after Russia pivoted from military exercises with Belarus and launched a full-scale military invasion of Ukraine (CNN). The Auto-ISAC will closely track and report the short- and long-run cyber threat implications.
  - Maintain heightened vigilance of your business networks, industrial systems, and products for the foreseeable future, including after the war ends.
  - Be on lookout for advanced persistent threat (APT) groups conducting attacks on Russia's behalf as well as other APT groups and cybercriminals seeking to exploit fixation on the war and its global impacts to steal sensitive data, extort victims, or disrupt systems/operations (CISA, The Hacker News, Dark Reading).
    - In January and February 2022, threat actors attacked Ukrainian organizations using destructive malware, WhisperGate, HermeticWiper, IsaacWiper, as well as distributed denial-of-service (DDoS) attacks. Minimal spillover has occurred thus far (NPR).

CISA RESOURCE HIGHLIGHTS

TLP: WHITE – CISA Industrial Control Systems Working Group (ICSJWG) Spring Virtual Event

- **ICSJWG Spring 2022 – Virtual Event – Tuesday and Wednesday April 26-27, 2022**
- **Save-the-date and registration links at:**
  - **https://www[.]cisa[.]gov/uscert/ics/icsjwg-meetings-and-webinars**
  - **https://www[.]cisa[.]gov/uscert/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG**
- **Contact ICSJWG at ICSJWG.Communications@cisa.dhs.gov**

TLP: WHITE – CISA Shields Up Website

- Provides resources and recommendations to prepare for, respond to, and mitigate the impact of cyber attacks
- Designed to support every organization – large and small – in their preparation to respond to disruptive cyber activity
- Technical Guidance page also available that provides information for review and consideration in responding to cyber incidents
- Resources available at:
  - https://www[.]cisa[.]gov/shields-up
  - https://www[.]cisa[.]gov/uscert/shields-technical-guidance

TLP: WHITE – CISA Compiles Free Cybersecurity Services and Tools for Network Defenders

- **Non-exhaustive list of no-cost security tools and services**
- **No-cost free and services offered by private and public sector organizations across the cybersecurity community included in the list**
- **Details available at:**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/18/cisa-compiles-free-cybersecurity-services-and-tools-network
  - https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools

TLP: WHITE – CISA Current Activities – Joint Products

- **Advisory on Destructive Malware Targeting Organizations in Ukraine – CISA, FBI**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/26/cisa-releases-advisory-destructive-malware-targeting-organizations
  - https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-057a
- **Iranian Government-Sponsored MuddyWater Actors Conducting Malicious Cyber Operations – CISA, FBI, NSA, CNMF, NCSC-UK**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/24/iranian-government-sponsored-muddywater-actors-conducting
  - https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-055a

TLP: WHITE – CISA Current Activities – Joint Products - continued

- **Russian State-Sponsored Actors Target Cleared Defense Contractor Networks – CISA, FBI, NSA**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/16/russian-state-sponsored-actors-target-cleared-defense-contractor
  - https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-047a
- **2020 Trends Show Increased Globalized Threat of Ransomware – CISA, FBI, NSA, ACSC (Australia), NCSC-UK:**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/09/2021-trends-show-increased-globalized-threat-ransomware
  - https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-040a

TLP: WHITE – CISA Insights: Foreign Influence Operations Targeting Critical Infrastructure

- **Published in response to current social factors that increase the risk and potency of influence operations to U.S. critical infrastructure**
- **Provides proactive steps organizations can take to assess and mitigate risks from information manipulations**
- **See:**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/18/cisa-insights-foreign-influence-operations-targeting-critical
  - https://www[.]cisa[.]gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf

TLP: WHITE – Thirty-Two (32) Known Exploited Vulnerabilities added in February 2022

- **The following CISA Current Activities highlight added KEVs:**
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/25/cisa-adds-four-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/22/cisa-adds-two-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/15/cisa-adds-nine-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/11/cisa-adds-one-known-exploited-vulnerability-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/10/cisa-adds-15-known-exploited-vulnerabilities-catalog
  - https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/02/04/cisa-adds-one-known-exploited-vulnerability-catalog

- **KEV Catalog:**
  - https://www[.]cisa[.]gov/known-exploited-vulnerabilities-catalog

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA NCAS – https://us-cert[.]cisa[.]gov/
- CISA Newsroom - 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/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus
- CISA Webinar Series on YouTube: https://www[.]youtube[.]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy

For more information:
cisa.gov

Questions?
Central@cisa.dhs.gov
1-888-282-0870

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

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*

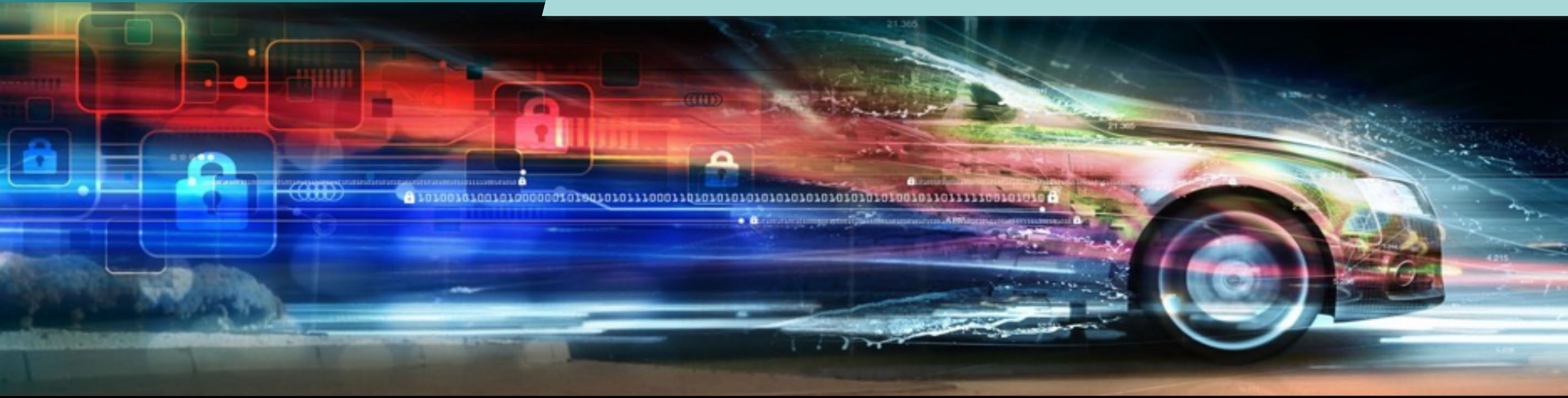
30+ ***Featured Speakers to date***

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

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Tamara Shoemaker - Auto-ISAC, Infragard

Cyber Training Leader

Tamara Shoemaker began her professional career as Lead Investigator in the states first women owned private investigative firm. She spent the last 17 years at the Center for Cyber Security and Intelligence Studies at the University of Detroit Mercy. Under her leadership the Center's projects have received over 2 million in funding. She is also President of the Michigan Midwest Regional Chapter of CISSE (MCISSE) a coalition of businesses and institutions of higher learning.

Her primary mission has been to address the critical shortage of specifically educated and trained Cyber Security professionals and to increase the diversity in that workforce.

Tamara Shoemaker has become an evangelist for the ***CyberPatriot Program,*** founding **the Michigan CyberPatriot** program to grow the number of teams participating across Michigan in 2015. In 2017 MCISSE was honored to become the 12th Center of Academic Excellence with the US CyberPatriot program for the work Tamara spearheaded.

www.micyberpatriot.com

Michigan CyberPatriot

Become A CyberPatriot Youth Mentor: Validate your Leadership Skills and Give Back to Your Community!

MIDWEST CISSE CHAPTER
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM
CENTER OF EXCELLENCE

Why CyberPatriot

Supporting CyberPatriot teams across our country will only strengthen the knowledge and awareness of our constituency and increase the number of digitally aware people in our community. Which in the end will help protect our critical infrastructure and seed the pipeline with a STEM-educated population.

- CyberPatriot also allows us to show K-12 students the wealth of career opportunities in this exciting field.

- CyberPatriot engages K-12 in cybersecurity activities that are fun, Real-world challenges

Michigan’s Why CyberPatriot

Recently release **Computer Science standards** can be 3/4 fulfilled with hands-on experiences with this afterschool program. Many teachers/coaches take the CyberPatiot training materials and integrate them into their classroom curriculum.

The CyberPatriot program is a natural fit for the **MiSTEM program. MiSTEM** is a system that will produce STEM-equipped students and educators.

Their pillars are creating a STEM culture, empower STEM teachers, integrate business and education, and ensure high-quality STEM experiences.

Connection to MiTECS and CompSci

MiTECS

- **Digital Citizen** - Rights, responsibilities, and opportunities of engaging in an interconnected digital world and are safe, legal, and ethical.
- **Computational Thinker** - Strategies for understanding and solving problems that leverage the power of technology.

Computer Science

- **Core Concepts** - Networks and the Internet
- **Core Practices** - Rational for all practices, but Michigan's K-12 CS Standards highlights: *Recognizing and Defining Computational Problems, Developing and Using Abstracts, and Communication About Computers*

Short Video:

https://www.youtube.com/watch?v=nGX1ju2jlaM&t=33s

What is CyberPatriot

CyberPatriot is the National Youth Cyber Education Program created by the Air Force Association (AFA) to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.

The CyberPatriot Programs are: The Middle School and High School Competition, the K-5 Game Program, the Cybergenerations Program, and the Literature Series

COMPETITION DIVISIONS

Open Division

Open to high school age groups:

- Public schools
- Private schools
- Parochial schools
- Magnet or charter schools
- Home school groups
- 4H clubs
- Boys and Girls clubs
- Scouting units
- Other youth programs

All Service Division

Open to:

- Air Force JROTC units
- Army JROTC units
- Marine Corps JROT units
- Navy JROTC units
- Civil Air Patrol squadrons
- U.S. Naval Sea Cadet Corps units

Middle School Division

Open to middle school age groups:

- Public schools
- Private schools
- Parochial schools
- Magnet or charter schools
- Home school groups
- 4H clubs
- Boys and Girls clubs
- Scouting units
- Other youth programs

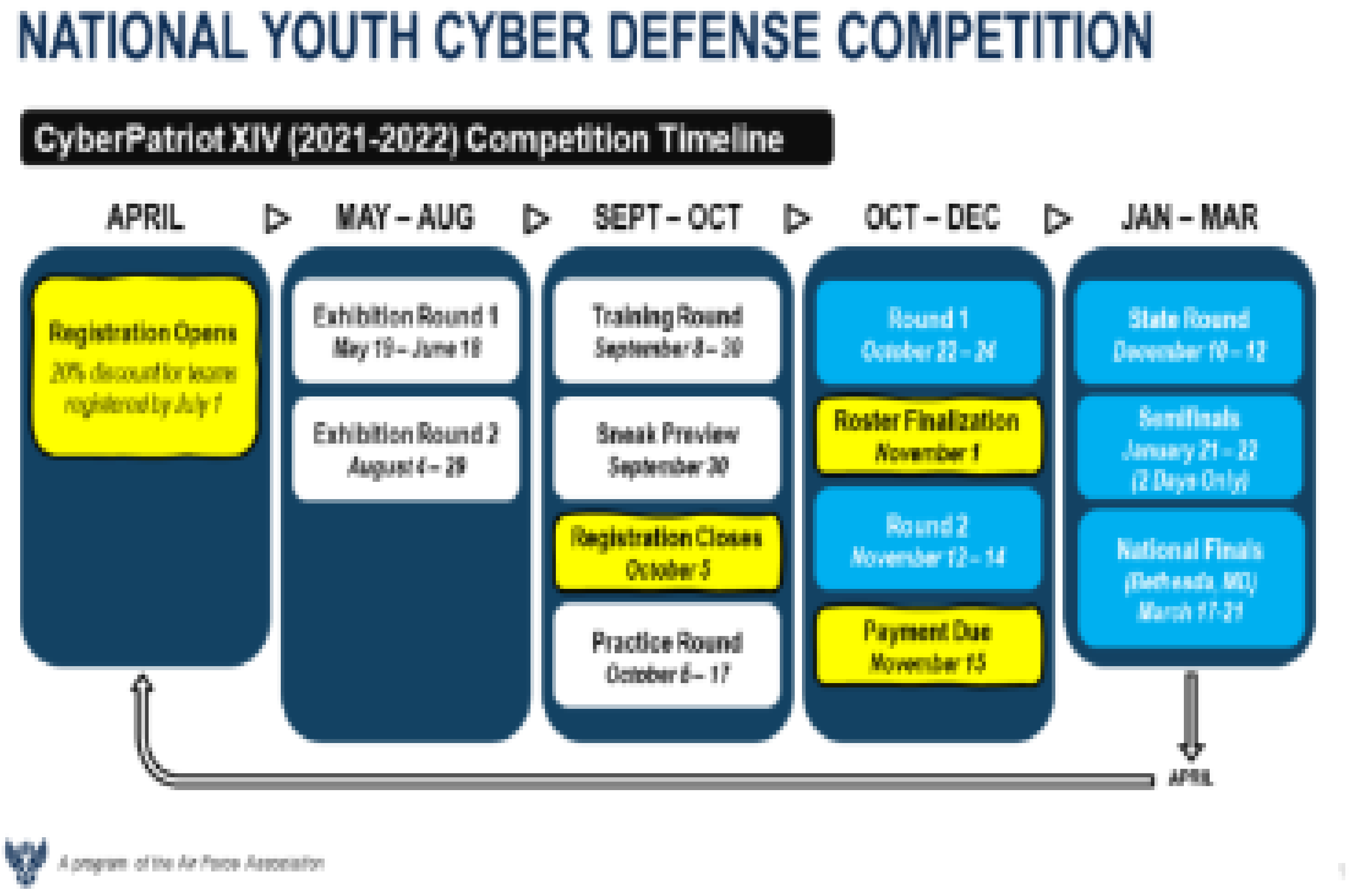
Low barrier to enter, $205 reg for HS, $165 for Middle School, all-girl team FREE, Title 1 schools FREE! All virtual rounds and finals when necessary!

How’s it Work?

- Find and fix cybersecurity vulnerabilities in virtual operating systems.
- Using a proprietary competition system, teams are scored on how secure they make the system.
- Top teams advance through the online round of competition, and the best of the best advance to the in-person National Finals Competition.

CYBERPATRIOT
SECURITY, SERVICE, EXCELLENCE
NATIONAL YOUTH CYBER EDUCATION PROGRAM
Cybersecurity
CYBERCAMP

Competition Schedule



NATIONAL YOUTH CYBER DEFENSE COMPETITION

CyberPatriot XIV (2021-2022) Competition Timeline

APRIL

- Registration Opens
  20% discount for teams registered by July 1

MAY – AUG

- Exhibition Round 1
  May 19 – June 18
- Exhibition Round 2
  August 4 – 28

SEPT – OCT

- Training Round
  September 8 – 30
- Sneak Preview
  September 30
- Registration Closes
  October 5
- Practice Round
  October 6 – 17

OCT – DEC

- Round 1
  October 22 – 24
- Roster Finalization
  November 1
- Round 2
  November 12 – 14
- Payment Due
  November 15

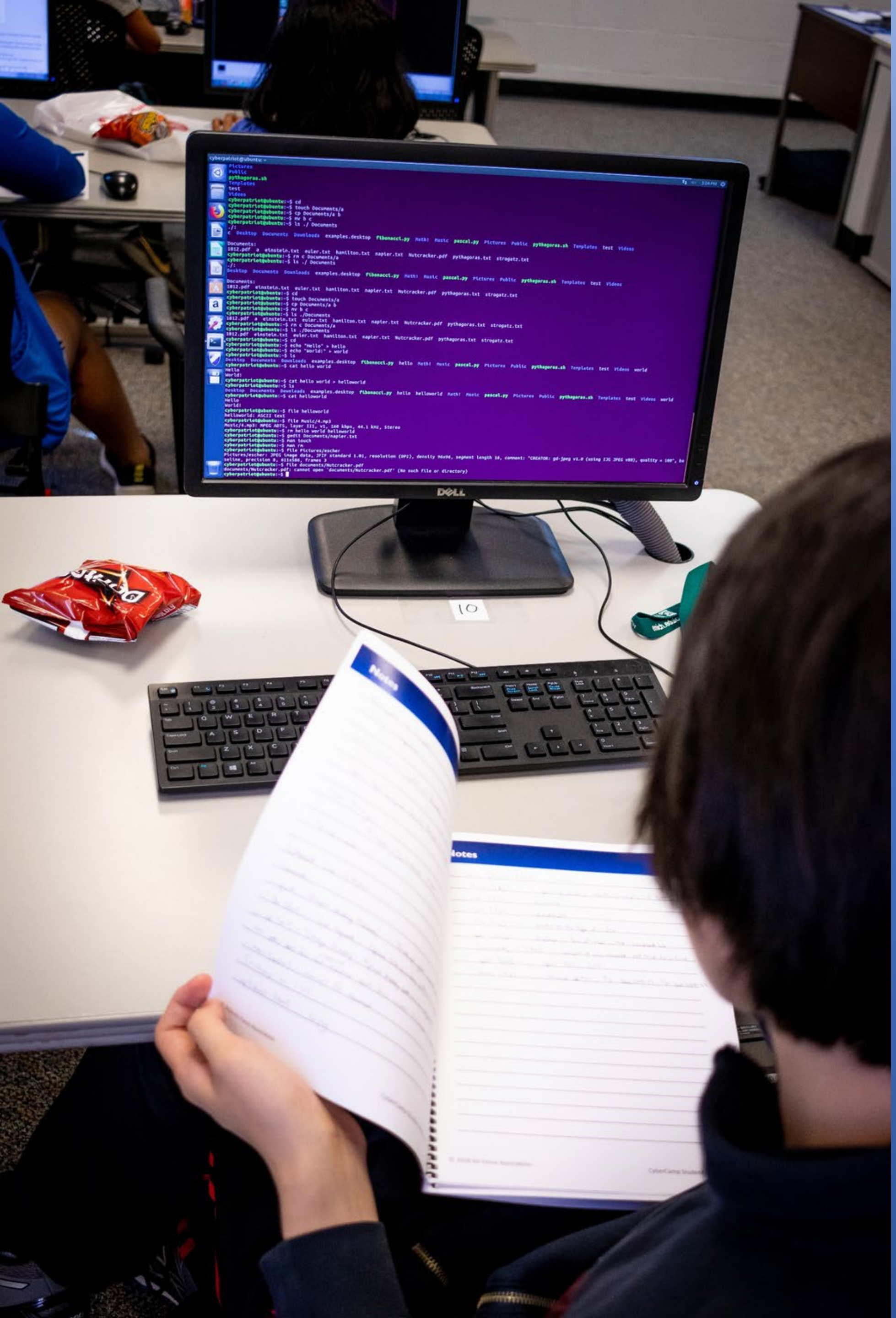
JAN – MAR

- State Round
  December 10 – 12
- Semifinals
  January 21 – 22
  (2 Days Only)
- National Finals
  (Bethesda, MD)
  March 17-21

A program of the Air Force Association

What does it take?

- 2-5 Students
- 1 Coach
- Mentors
- 3 PCs per team with 64 bit and enough memory to run VmWare



The Game

- Each team has two challenges during their six-hour competition period: **Network Security Challenge:** involves finding and fixing security vulnerabilities in Windows and Linux operating systems.

- **Cisco Networking Challenge:** consists of an online quiz and a virtual networking exercise based on specific training materials.

Digital Badges for Michigan CyberPatriot Students, First in the Country!

Each year completed earns your student a digital badge found on Badgr website for them to display on their digital backpack!

All criteria for the badges have been aligned or mapped to the NIST NICE Workforce Framework and the Michigan CompSci Standards.

MIDWEST CISSE CHAPTER
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
1ST YEAR
PLATINUM LEVEL
NATIONAL YOUTH CYBER EDUCATION PROGRAM
CENTER OF EXCELLENCE

MIDWEST CISSE CHAPTER
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
SEMI FINALIST
NATIONAL YOUTH CYBER EDUCATION PROGRAM
CENTER OF EXCELLENCE

MIDWEST CISSE CHAPTER
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
1ST YEAR
GOLD LEVEL
NATIONAL YOUTH CYBER EDUCATION PROGRAM
CENTER OF EXCELLENCE

CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
NATIONAL FINALIST
NATIONAL YOUTH CYBER EDUCATION PROGRAM

MIDWEST CISSE CHAPTER
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
1ST YEAR
SILVER LEVEL
NATIONAL YOUTH CYBER EDUCATION PROGRAM
CENTER OF EXCELLENCE

www.badgr.com

Summer Camps

2017 – 2 camps, Battle Creek ANG and UDM

2018 - 4 camps around 100 students

2019 – 8 camps, 250 students with 48% female

2020 - 9 virtual camps across MI with 48% female

2021 – 10 virtual and in-person camps nationally

2022 - Blended Method Planned – July 11-15

www.micyberpatriot.com

MIDWEST CISSE CHAPTER
CYBERPATRIOT
CENTER OF EXCELLENCE

www.uscyberpatriot.org

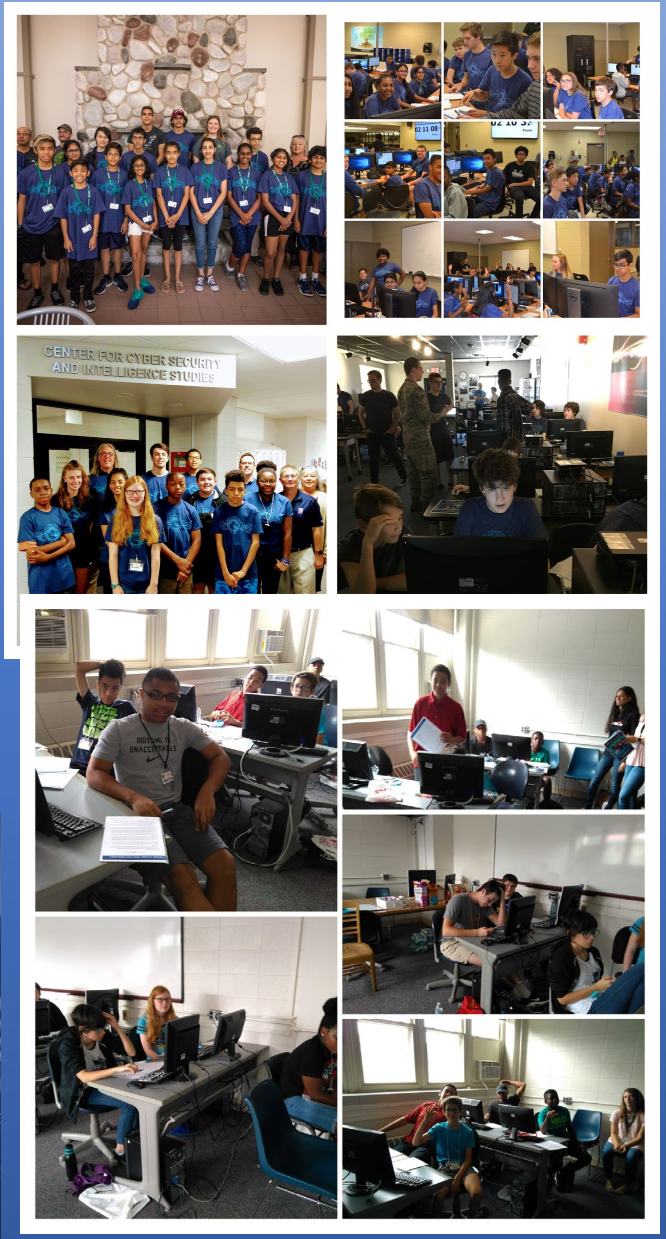
Summer Camps-We need You!

We will offer beginner Summer Camps at multiple locations across Michigan. These camps will be run using a blended method.

AFA supplies the course materials, but it costs $1500 per week plus supplies.

We can have as many camps that week as we can handle across the state.

We need locations and volunteers!



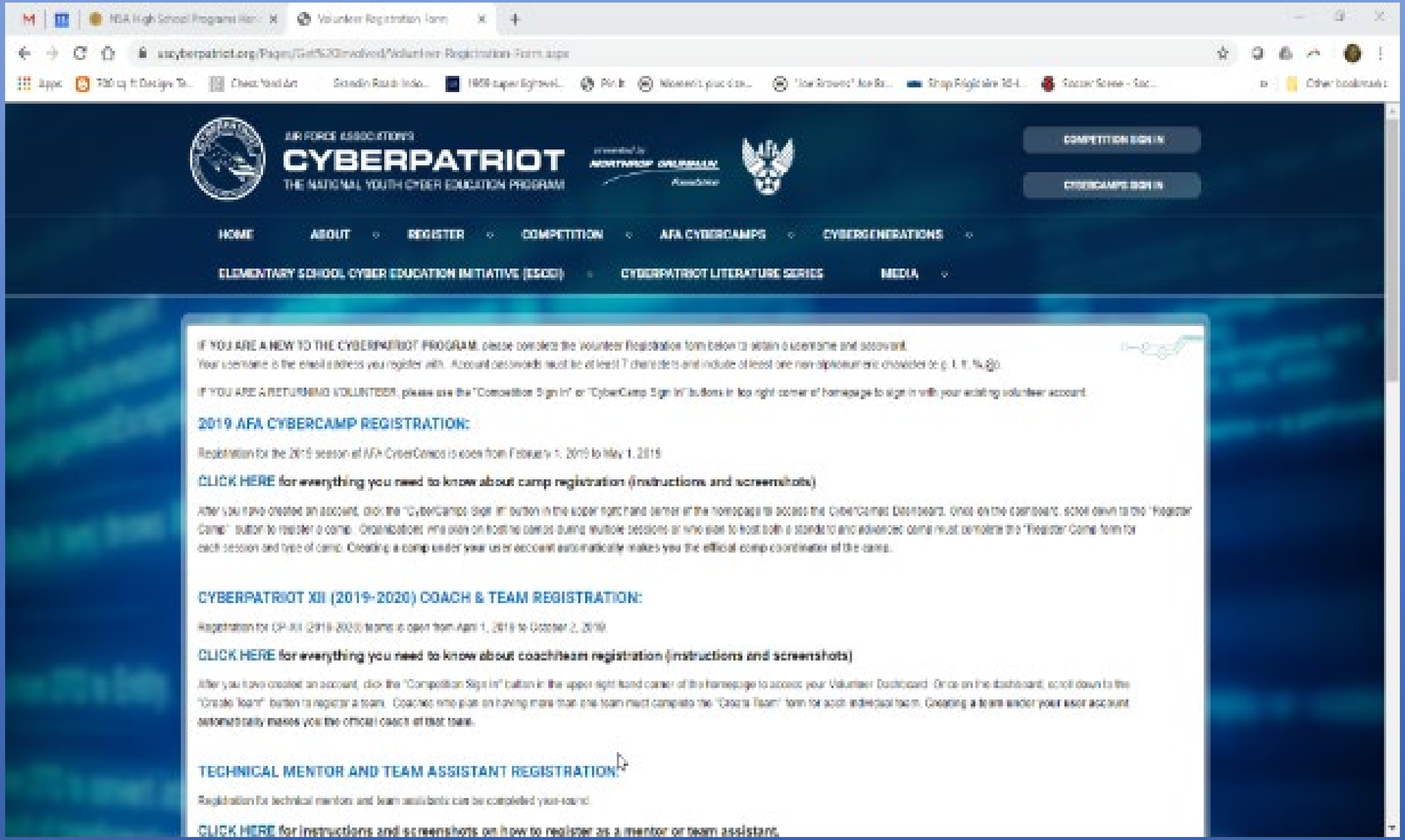
Mentors Needed

MIDWEST CISSE CHAPTER
CYBERPATRIOT
INTEGRITY, SERVICE, EXCELLENCE
COACH
NATIONAL YOUTH CYBER EDUCATION PROGRAM
CENTER OF EXCELLENCE

- Invest your time, help us fill the pipeline with these amazing innovative minds!
- IT and Cybersecurity experience a plus but not necessary
- Training materials provided

How do you sign-up ?

www.uscyberpatriot.org


uscyberpatriot.org/Pages/Get%20Involved/Volunteer-Registration-Form.aspx
AIR FORCE ASSOCIATION'S
CYBERPATRIOT
THE NATIONAL YOUTH CYBER EDUCATION PROGRAM
presented by NORTHROP GRUMMAN Foundation
COMPETITION SIGN IN
CYBERCAMPS SIGN IN
HOME
ABOUT
REGISTER
COMPETITION
AFA CYBERCAMPS
CYBERGENERATIONS
ELEMENTARY SCHOOL CYBER EDUCATION INITIATIVE (ESCEI)
CYBERPATRIOT LITERATURE SERIES
MEDIA

IF YOU ARE A NEW TO THE CYBERPATRIOT PROGRAM, please complete the Volunteer Registration form below to obtain a username and account.
Your username is the email address you register with. Account passwords must be at least 7 characters and include at least one non-alphanumeric character (e.g. !, #, %, @).

IF YOU ARE A RETURNING VOLUNTEER, please use the "Competition Sign In" or "CyberCamp Sign In" buttons in top right corner of homepage to sign in with your existing volunteer account.

2019 AFA CYBERCAMP REGISTRATION:

Registration for the 2019 season of AFA CyberCamps is open from February 1, 2019 to May 1, 2019.

CLICK HERE for everything you need to know about camp registration (instructions and screenshots)

After you have created an account, click the "CyberCamps Sign In" button in the upper right hand corner of the homepage to access the CyberCamps Dashboard. Once on the dashboard, scroll down to the "Register Camp" button to register a camp. Organizations who plan on hosting camps during multiple sessions or who plan to host both a standard and advanced camp must complete the "Register Camp" form for each session and type of camp. Creating a camp under your user account automatically makes you the official camp coordinator of the camp.

CYBERPATRIOT XII (2019-2020) COACH & TEAM REGISTRATION:

Registration for CP-XII (2019-2020) teams is open from April 1, 2019 to October 2, 2019.

CLICK HERE for everything you need to know about coach/team registration (instructions and screenshots)

After you have created an account, click the "Competition Sign In" button in the upper right hand corner of the homepage to access your Volunteer Dashboard. Once on the dashboard, scroll down to the "Create Team" button to register a team. Coaches who plan on having more than one team must complete the "Create Team" form for each individual team. Creating a team under your user account automatically makes you the official coach of that team.

TECHNICAL MENTOR AND TEAM ASSISTANT REGISTRATION:

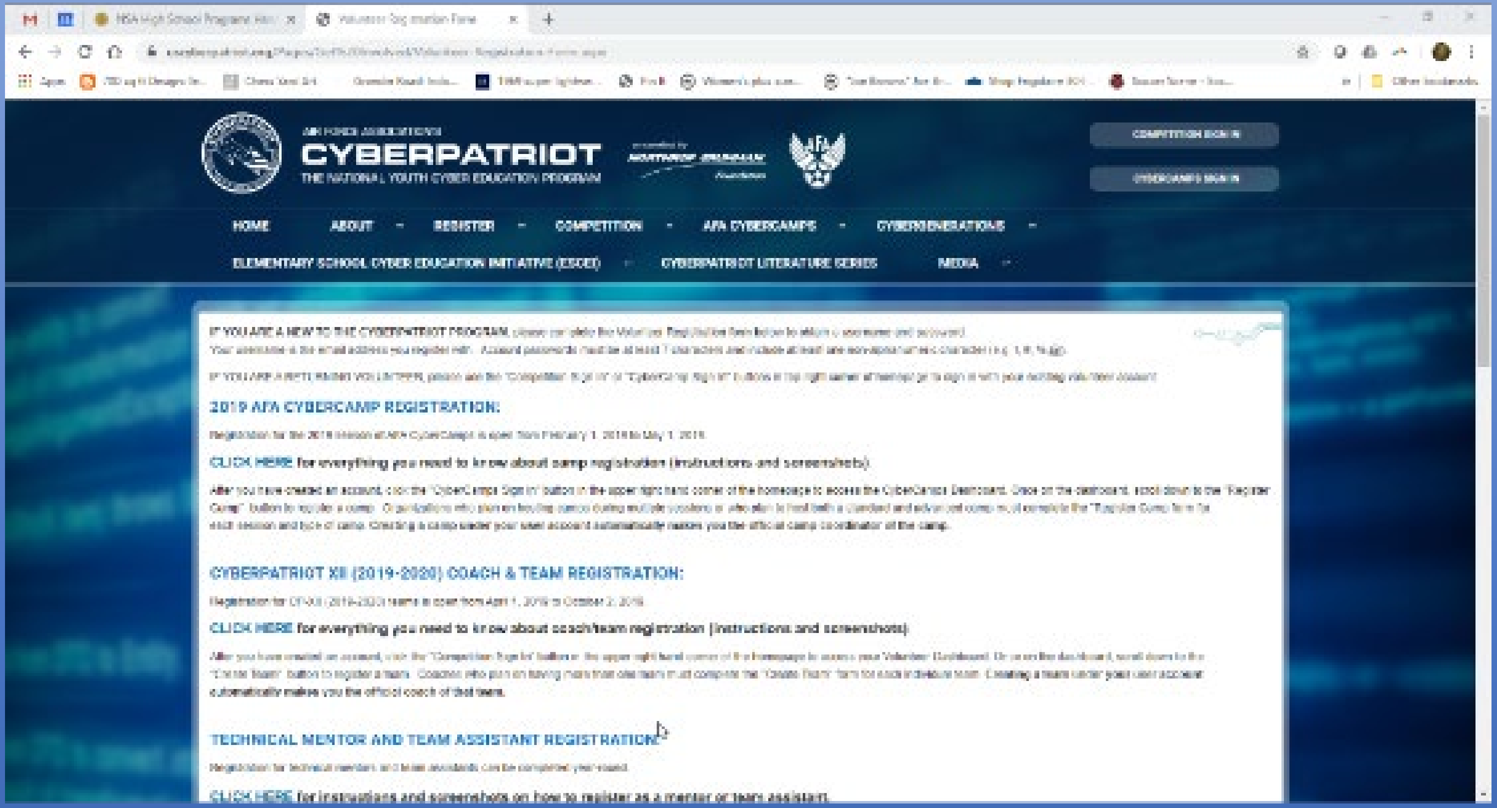
Registration for technical mentors and team assistants can be completed year-round.

CLICK HERE for instructions and screenshots on how to register as a mentor or team assistant.

www.edupaths.org you will find a course on how to sign-up and run a team!

Training website materials
Training web-conferences
Training with MCISSE
Training with Microsoft
Training with Linux
Training with CISCO

All available once you sign-up as a coach or mentor!


AIR FORCE ASSOCIATION'S
CYBERPATRIOT
THE NATIONAL YOUTH CYBER EDUCATION PROGRAM
presented by NORTHROP GRUMMAN Foundation
COMPETITION SIGN IN
CYBERCAMPS SIGN IN
HOME
ABOUT
REGISTER
COMPETITION
AFA CYBERCAMPS
CYBERGENERATIONS
ELEMENTARY SCHOOL CYBER EDUCATION INITIATIVE (ESCEI)
CYBERPATRIOT LITERATURE SERIES
MEDIA

IF YOU ARE A NEW TO THE CYBERPATRIOT PROGRAM, please complete the Volunteer Registration form below to obtain a username and password. Your username is the email address you register with. Account passwords must be at least 7 characters and include at least one non-alphanumeric character (e.g. !, #, %, @).

IF YOU ARE A RETURNING VOLUNTEER, please use the "Competition Sign In" or "CyberCamp Sign In" buttons in top right corner of homepage to sign in with your existing volunteer account.

2019 AFA CYBERCAMP REGISTRATION:

Registration for the 2019 season of AFA CyberCamps is open from February 1, 2019 to May 1, 2019.

CLICK HERE for everything you need to know about camp registration (instructions and screenshots).

After you have created an account, click the "CyberCamps Sign In" button in the upper right hand corner of the homepage to access the CyberCamps Dashboard. Once on the dashboard, scroll down to the "Register Camp" button to register a camp. Organizations who plan on hosting camps during multiple sessions or who plan to host both a standard and advanced camp must complete the "Register Camp" form for each session and type of camp. Creating a camp under your user account automatically makes you the official camp coordinator of the camp.

CYBERPATRIOT XII (2019-2020) COACH & TEAM REGISTRATION:

Registration for CP-XII (2019-2020) teams is open from April 1, 2019 to October 2, 2019.

CLICK HERE for everything you need to know about coach/team registration (instructions and screenshots).

After you have created an account, click the "Competition Sign In" button in the upper right hand corner of the homepage to access your Volunteer Dashboard. Once on the dashboard, scroll down to the "Create Team" button to register a team. Coaches who plan on having more than one team must complete the "Create Team" form for each individual team. Creating a team under your user account automatically makes you the official coach of that team.

TECHNICAL MENTOR AND TEAM ASSISTANT REGISTRATION:

Registration for technical mentors and team assistants can be completed year-round.

CLICK HERE for instructions and screenshots on how to register as a mentor or team assistant.

www.uscyberpatriot.org to sign up as a volunteer, if you are in Michigan then reach-out to Tamara to be assigned a team near you!
tamarashoemaker@automotiveisac.com

Our Growth in Michigan

1st Year we supported the program from 4-25 teams, 125 students served

2nd year we supported the program 52 teams, 260 students served

3rd year we supported the program 80 teams, 400 students served

4th year we supported the program 142 teams, 710 students served

5th year we supported the program 182 teams, 900-1000 students

6th year we supported 156 teams, around 800 students –COVID yr. 1

7th year we supported 152 teams, around 750 students – COVID yr. 2

Getting started resources

www.micyberpatriot.com	*All things Michigan CyberPatriot*
www.edupaths.org	*Cybersecurity modules for Continuing Ed Credits*
www.uscyberpatriot.org	*The National CyberPatriot Program and Sign-up*
www.badgr.com	*To register for free account and see the Michigan CyberPatriot Badges*

CyberPatriot for Elementary School (ESCEI)

FREE Three games to download

Security Showdown 2: Learn the basics of sharing personal information with family, friends, and strangers in this simple point-and-click game. Key Topics: Personal Information **Grade Levels: K-2**

JeffOS: Join Jeff, your helpful sidekick, as he guides you through his operating system and covers everything from basic computer skills to dealing with complex issues like phishing and malware. Key Topics: Phishing, Malware, Firewalls **Grade Levels: 3-6**

Packet Protector: Build a computer network to mine for cryptocurrency and use this money to expand and secure your network! Key Topics: Malware, Defenses, Passwords **Grade Levels: Grades 3-6**

MIDWEST CIESE CHAPTER CYBERPATRIOT CENTER OF EXCELLENCE

www.uscyberpatriot.org

CyberGenerations: teaching Seniors about Cyber Safety

- **Introduction - Cybersecurity 101:** Helps learn the basics of cybersecurity, including physical t to cyber safety and the importance of personally identifiable information.

- **Module 1 - Password Management:** The importance of maintaining good password hygiene and tips on creating strong, unique passwords.
- **Module 2 - Common Internet Threats:** Raise awareness about malware, social engineering methods (phishing, vishing, etc.) and public Wi-Fi tips to avoid becoming victims of cybercrime.
- **Module 3 - Internet Scams and Fraud:** Different types of scams targeting seniors, how to recognize false customer service calls, identity theft, and online shopping tips.
- **Module 4 - Social Media Safety:** Understanding privacy settings, becoming mindful of the various social media scams, and information about social media etiquette.
- **Self-Help Resources:** Direct contact information for government and local resources

Middle School, High School and College students' volunteers needed!

www.micyberpatriot.com

TECH CAREGIVERS

NEW PROGRAM LAUNCH

Engaging student and adult volunteers to give back to their communities

Want to give back and make a difference in your community?

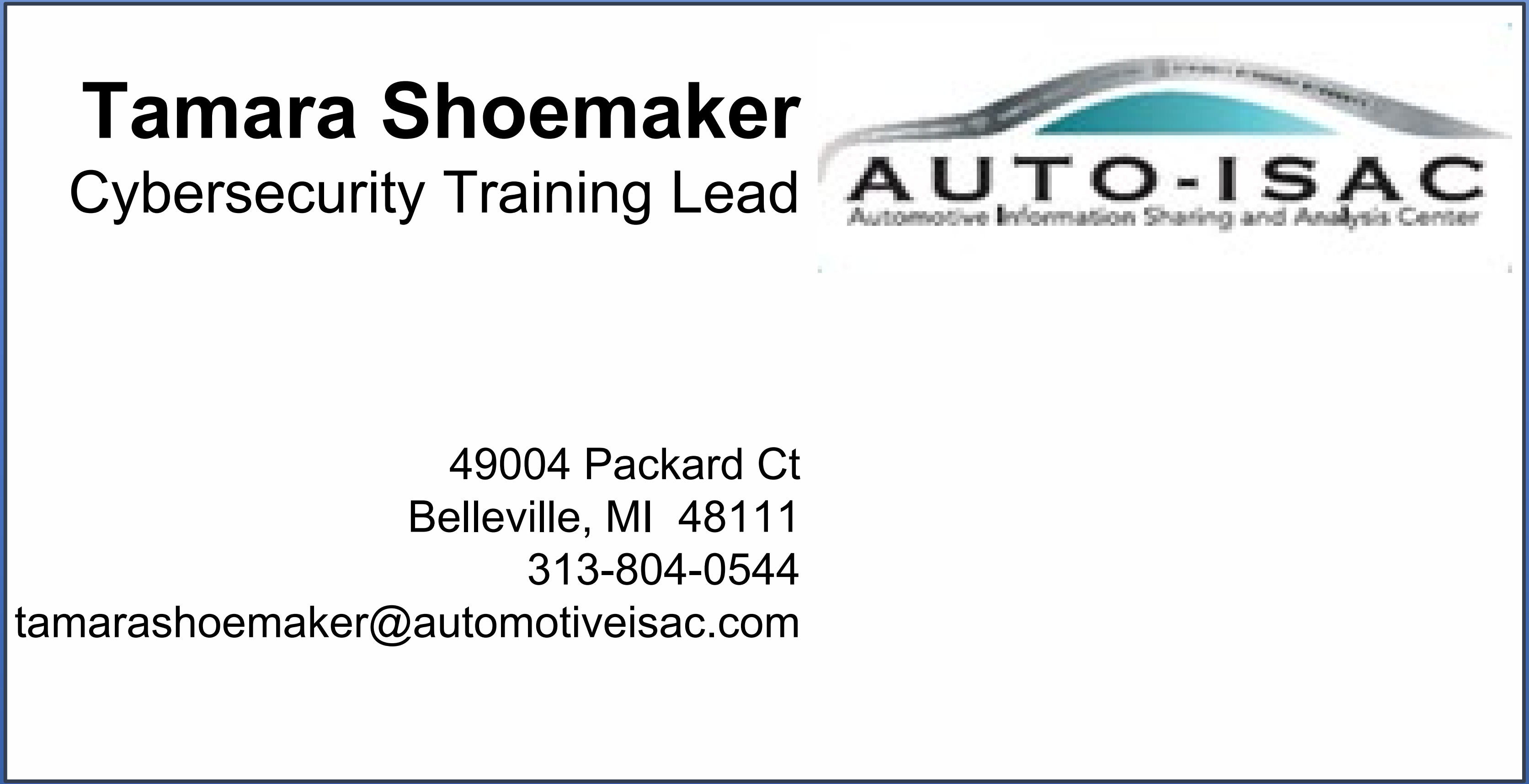
Want to help people gain confidence to safely navigate online?

Want to add value to your academic or career life and have a sense of accomplishment?

Volunteer to become a Tech Caregiver for FREE!

Student and adult volunteers can receive a certification to offer cybersecurity support to those adults who are often vulnerable to cyber threats due to a lack of technological experience and knowledge.

Contact Info



Tamara Shoemaker
Cybersecurity Training Lead

AUTO-ISAC
Automotive Information Sharing and Analysis Center

49004 Packard Ct
Belleville, MI 48111
313-804-0544
tamarashoemaker@automotiveisac.com

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 andreaschunn@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 (12)

Cybellum

Deloitte

FEV

GRIMM

HackerOne

Karamba Security

Pen Testing Partners

Red Balloon Security

Regulus Cyber

Saferide

Security Scorecard

Upstream

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 - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

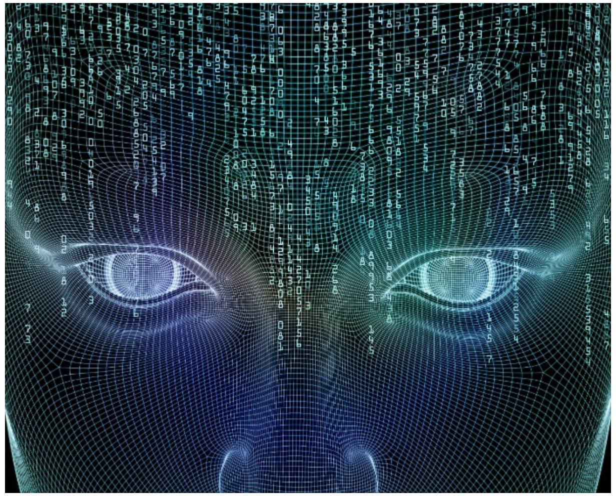
BENEFACTOR

Sponsorship Partnership

2021 Summit Sponsors-
Celerium
Cyware
Denso
NDIAS
IOActive
Claroty
Deloitte
Finite State
Tanium
Recorded Future
PaloAlto Networks
Upstream
Securonix
Zimperium
Micron
Block Harbor
SecurityScorecard
Booz Allen
CybelAngel
ATT
Ford
Cybellum
2020 Summit Sponsors-
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsights
ValiMail

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!

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

Our Contact Info

Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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

Sharmila Khadka
Information Technology Executive Coordinator

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC