AUTO-ISAC

MONTHLY COMMUNITY CALL

June 2020

COVID-19

Our thoughts and prayers go out to all those affected by COVID-19. We are very grateful to our Members and Partners for their continued support and engagement during these unprecedented times. If we can assist in any manner, please let us know how we might help.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why we're here ➢ Expectations for this community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC overview ➢ Heard around the community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** **Randy Sandone, Executive Director of Critical Infrastructure Resilience Institute (CIRI), Information Trust Institute (funded by DHS) at University of Illinois, Urbana.**
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! (fayefrancy@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!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

20 *OEM Members*

❖ 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

36 *Supplier & Commercial Vehicle Members*

Membership represents **99%** *of cars on the road in North America*

Coordination with **23** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

AUTO ISAC – 2020 WAY FORWARD

[redacted]

RE-EVALUATION OF STRATEGY & MISSION

Who We Are & Why We Are Here

MISSION: *To strengthen the global automotive industry against cyber threats and enhance cyber attack resilience and response.* ***An attack on one is an attack on all.***

Timely Sharing of Threat & Vulnerability Information

Building Strong Relationships

Developing Effective Response Plans

Ensuring & Maturing Consistent Cyber Capability

Each Member is expected to: Trust, Share, Teach, Learn, Act

We are a **technical organization**, serving membership by enabling **cyber learning and capability development**. As members, we are expected to both **share and learn**, and continue to strengthen capabilities to protect our customers. ***We will hold ourselves accountable.***

Auto ISAC – 2020 Way Forward

[redacted]

ROLES, RESPONSIBILITIES & METRICS | *Measuring Success*

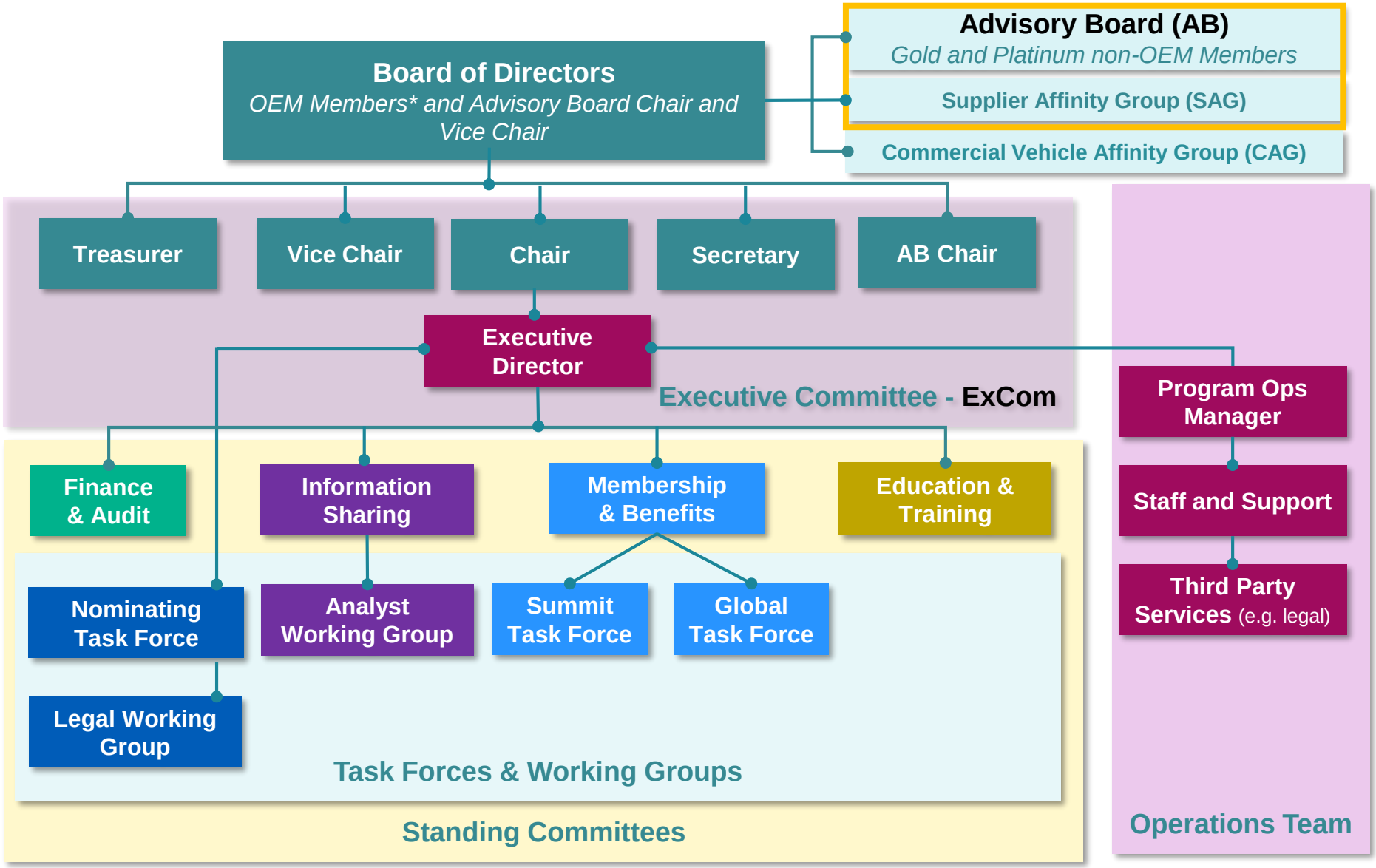
VALUE STREAMS & PERFORMANCE INDICATORS

Top Line Goal: Zero safety related cyber events in the industry

INFO SHARING & AWARENESS	EDUCATION	RELATIONSHIPS
% Participation Sharing / Platform / Attendance	% Taking Educational Offerings Maturity Surveys	% Member Satisfaction with value added relationships

Bottom Line Goal: ***Automotive Cybersecurity Resiliency Across Industry!***

Auto-ISAC Operating Model



2020 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

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

2020 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Kevin Walker
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of June 2, 2020

Highlighted = Change

Aisin	Honda	Oshkosh Corp
Allison Transmission	Hyundai	PACCAR
Aptiv	Infineon	Panasonic
AT&T	Intel	Qualcomm
Blackberry Limited	Kia	Renesas Electronics
BMW Group	Knorr Bremse	Subaru
Bosch	Lear	Sumitomo Electric
Continental	LGE	Tokai Rika
Cummins	Magna	Toyota
Denso	MARELLI	TuSimple
Delphi Technologies	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Navistar	Waymo
Google	Nexteer Automotive Corp	Yamaha Motors
Harman	Nissan	ZF
Hitachi	NXP	TOTAL: 56

2020 Auto-ISAC Staff

Faye Francy (ED)

Josh Poster (PoM)

Ricky Brooks, II (IO)

Jake Walker (CIA)

Lisa D. Scheffenacker (BA)

Sharmila Khadka (EoS)

Julie Kirk (BK)

Linda Rhodes (LC)

Callen Mackey (CPA)

Paul Hart (IT)

External Support Staff

Auto-ISAC Activities

Auto-ISAC

- Automotive industry retooling for critical COVID19 work *Thank you!*
- Advisory Board & Board of Directors Meeting To Be Held Virtually June 25
- Auto-ISAC Member Incident Response Plan (IRP) Reviews *Completed!*
- Auto-ISAC Member IRP Drills *Month of June*
- Auto-ISAC Member TableTop Exercise (TTX) *Going Virtual*
- CyberStorm 2020 postponed
- We are *cautiously optimistic* we'll hold Auto-ISAC Summit – registration, call for papers, and sponsorships on website – www.automotiveisac.com

Stay safe, secure and well!

Auto-ISAC Summit – Oct 14-15

AUTO-ISAC SUMMIT

GM

Oct. 14-15, 2020

Detroit, MI

2 days

400 attendees

ABOUT THE AUTO-ISAC SUMMIT:
The 2020 Auto-ISAC Summit hosted by General Motors connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.

Registration is Open | Call for Papers (due 6/30) | Sponsor Prospectus

Researchers Analyze Entry Points, Vectors for Manufacturing System Attacks Researchers from cybersecurity firm Trend Micro and the Polytechnic University of Milan have analyzed the possible entry points and vectors for attacks targeting smart manufacturing environments, and they discovered several new vulnerabilities in the process. The study, which resulted in a 60-page report, looked at three main points of entry: engineering workstations, custom industrial internet-of-things (IIoT) devices, and manufacturing execution systems (MES).

Mercedes-Benz Onboard Logic Unit (OLU) Source Code Leaks Online The source code for "smart car" components installed in Mercedez-Benz vans has been leaked online over the weekend, ZDNet has learned. The leak occurred after Till Kottmann, a Swiss-based software engineer, discovered a Git web portal belonging to Daimler AG, the German automotive company behind the Mercedes-Benz car brand. Kottmann told ZDNet that he was able to register an account on Daimler's code-hosting portal, and then download more than 580 Git repositories containing the source code of onboard logic units (OLUs) installed in Mercedez vans.

Memory Corruption Vulnerability in GNU Glibc Leaves Smart Vehicles Open to Attack During some recent research, Cisco's Customer Experience Assessment & Penetration Team (CX APT) discovered a memory corruption vulnerability in GNU libc for ARMv7, which leaves Linux ARMv7 systems open to exploitation. This vulnerability is identified as TALOS-2020-1019/CVE-2020-6096. In this case, Cisco uncovered a vulnerability in the ARMv7 implementation of memcpy() that was able to cause the program to enter an undefined state and allow for the conditions of remote code execution in the target application. Ultimately, this vulnerability in memcpy() causes program execution to continue in scenarios where a segmentation fault or crash should have occurred. This unexpected behavior can result in a scenario where program execution continues with corrupted runtime state leading to exploitation opportunities.

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS

Upcoming CISA Events:

- ESF-14 COVID-19 Conference Calls:
  - Tuesdays from 3:00PM-4:15PM EST **until further notice**
  - Participant dial-in is 1-800-593-7177, Participant PIN is 7963614#
- ICSJWG 2020 Virtual Spring Meeting – June 9-10, 2020
  - Registration closes on Friday June 5, 2020
  - Registration site: https://gateway[.]on24[.]com/wcc/gateway/eliteCSRALLCamanagedaffiliate/2360375

TLP: WHITE - Version 3.1 - Guidance on Essential Critical Infrastructure Workers During COVID-19

- Released on May 19, 2020 and is intended to support state, local, tribal, territorial and industry partners in identifying the critical infrastructure sectors and the essential workers needed to maintain the services and functions Americans depend on daily and that need to be able to operate resiliently during the COVID-19 pandemic response.
- This update provides clarity around many individual worker categories and updated language to better reflect terminology used in food and agriculture industries.
- As with previous versions, the guidance intended to support decision makers in communities and jurisdictions across the country during the COVID-19 emergency and it is non-binding
- Available at https://www[.]cisa[.]gov/publication/guidance-essential-critical-infrastructure-workforce

TLP: WHITE - CISA Current Activities - Hurricane-Related Scams

- June 1, 2020 marks the official start of the 2020 Atlantic hurricane season
- CISA is warning people to remain on alert for malicious cyber activity targeting potential disaster victims and charitable donors following hurricane season-related storms.
- Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events.
- More details and other resources are available at https://www[.]us-cert[.]gov/ncas/current-activity/2020/06/01/hurricane-related-scams

TLP: WHITE - CISA Current Activity: CISA, DOE, and UK's NCSC Issue Guidance on Protecting Industrial Control Systems

- ICS/OT security best practices at https://www[.]us-cert[.]gov/ncas/current-activity/2020/05/22/cisa-doe-and-uks-ncsc-issue-guidance-protecting-industrial-control
- Resources cited:
  - Best practices infographic at https://www[.]cisa[.]gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf
  - CISA ICS Recommended practices at https://www[.]us-cert.gov/ics/Recommended-Practices
  - DOE C2M2 - https://www[.]energy[.]gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0
  - NCSC Secure Design Principles and Operational Technology at https://www[.]ncsc.gov[.]uk/blog-post/studies-in-secure-system-design

TLP: WHITE – CISA/FBI Joint Announcement on PRC Targeting of COVID-19

- Public Service Announcement released on May 13, 2020 and intended to raise awareness of the threat to COVID-19-related research.
- Cited at:
  - https://www[.]us-cert[.]gov/ncas/current-activity/2020/05/13/cisa-fbi-joint-announcement-prc-targeting-covid-19-research
  - https://www[.]cisa[.]gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations
  - https://www[.]cisa[.]gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf

TLP: WHITE - North Korean Malicious Cyber Activity

- Released on May 12, highlighted at https://www[.]us-cert[.]gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity
- Provides details on the three (3) malware variants, COPPERHEDGE, TAINTEDSCRIBE and PEBBLEDASH, identified by CISA, FBI, and DoD
- Includes links to analysis reports and DoD's VirusTotal pages for these malware variants is also provided.

TLP: WHITE - Activity Alert AA20-133A - Top 10 Routinely Exploited Vulnerabilities

- Activity Alert developed through a joint effort by CISA, the FBI, and the broader U.S. Government, available at https://www[.]us-cert[.]gov/ncas/alerts/AA20-133a
- Intended to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors
- Highlights details on vulnerabilities routinely exploited by foreign cyber actors—primarily Common Vulnerabilities and Exposures (CVEs)
- Highlights mitigation of the noted vulnerabilities and CISA resources that can be leveraged in that effort, which include:
  - CISA Cyber Resource Hub - https://www[.]cisa[.]gov/cyber-resource-hub
  - Vulnerability Management - https://www[.]us-cert[.]gov/resources/ncats

For more information:
cisa.gov

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

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*

7 *Best Practice Guides available on website*

2000+ *Community Participants*

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!

Community Speakers

Example of Previous Community Speakers

- **Urban Jonson, NMFTA, Heavy Vehicle Cybersecurity Working Group (April 2018)**
- **Ross Froat, American Trucking Association, ATA Cyberwatch Program (Oct 2018)**
- **Katherine Hartman, Chief – Research, Evaluation and Program Management, ITS Joint Program Office, US DOT (August 2019)**
- **Joe Fabbre, Global Technology Director, Green Hills Software (October 2019)**
- **Oscar Marcia, CISSP, Eonti, Device Authentication in Auto-ISAC as a Foundation to Secure Communications (November 2019)**
- **Amy Smith, the Manager of Pre-College Educational Programming at SAE International (January 2020)**

Community Call Slides are located at: *www.automotiveisac.com/communitycalls/*

Welcome to Today's Speaker

Featured Speaker

Randy Sandone, CCISO, Executive Director
Critical Infrastructure Resilience Institute (CIRI)

- ***CIRI*** is a DHS University Center of Excellence housed at the University of Illinois at Urbana-Champaign. As Executive Director, Randy is responsible for the operational, administrative and financial management of the Institute.
- Comprehensive career guiding research and technology projects in settings ranging form start-ups to Fortune 100 companies with strengths in strategy-development, business development, and project management.
- Over thirty years experience in development, testing and certification of cyber security products used by customers from Federal Agencies such as the DoD, the Intelligence Community, and private sector companies.
- MBA from University of Utah.

CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Randall Sandone, CCISO
Executive Director
Critical Infrastructure Resilience Institute
rsandone@Illinois.edu

Process, People, and Products

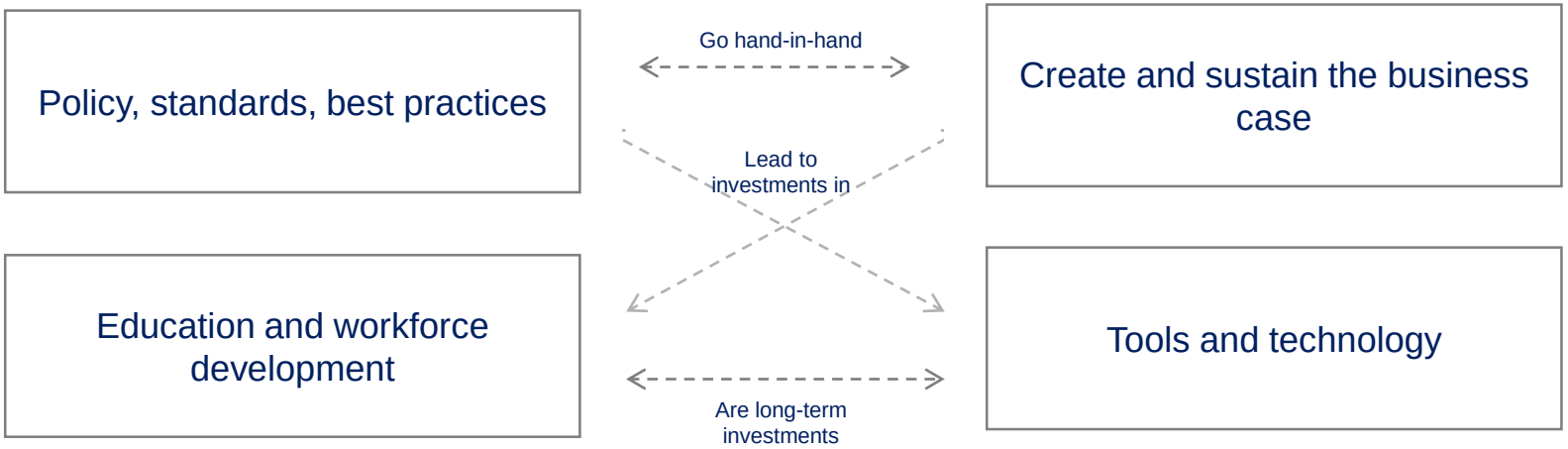
Building Cyber Resilience for the Long-Term

Presentation to Auto-ISAC:
3 June 2020

Overview:

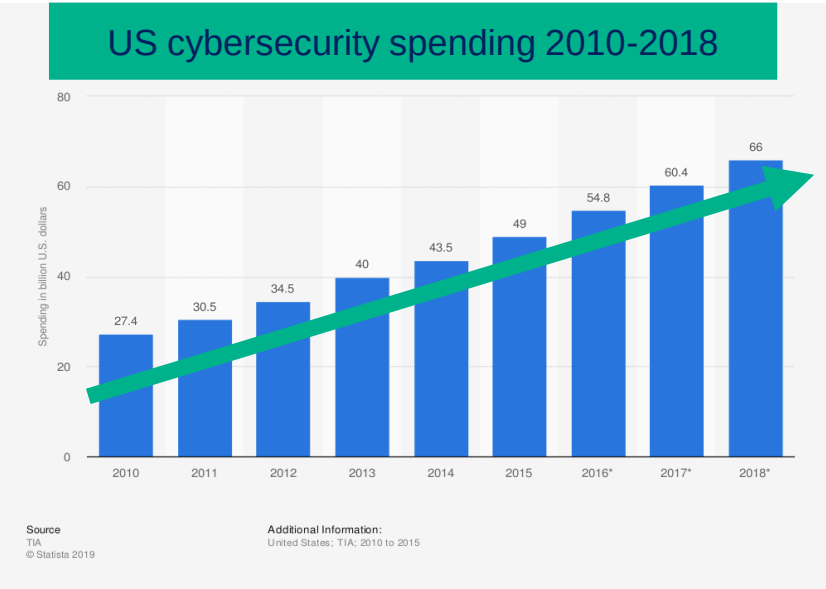
DHS Center of Excellence	• University of Illinois at Urbana-Champaign • **Practical**, **impactful** solutions to urgent problems of critical infrastructure resilience
Missions	• **Outputs-oriented** research • Tech **Transition** • Education & workforce **development**
Collaboration	• Strong end-user **engagement** in all mission areas • **Open to government and private sector**

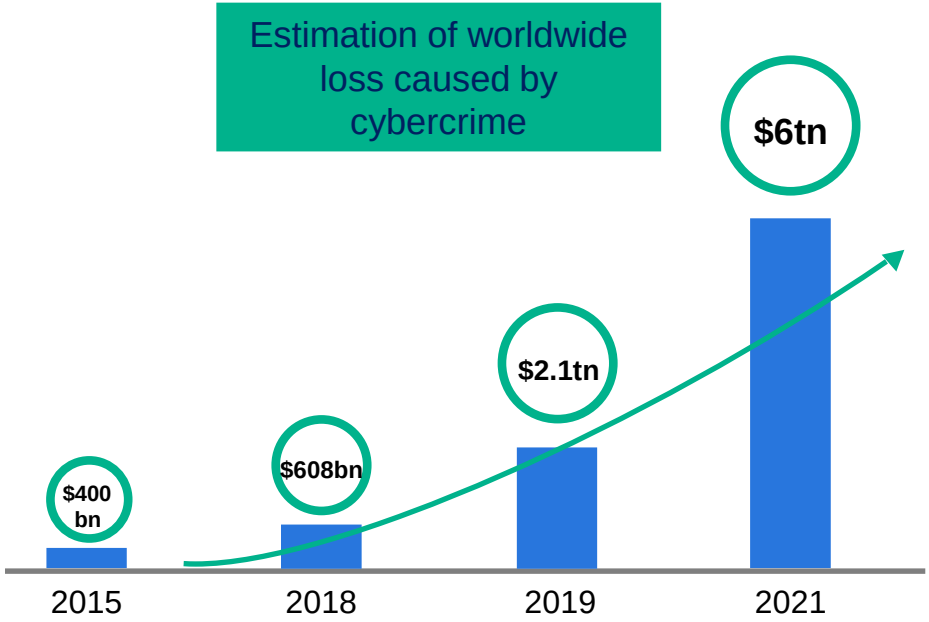
How do we attain a secure and resilient critical infrastructure?



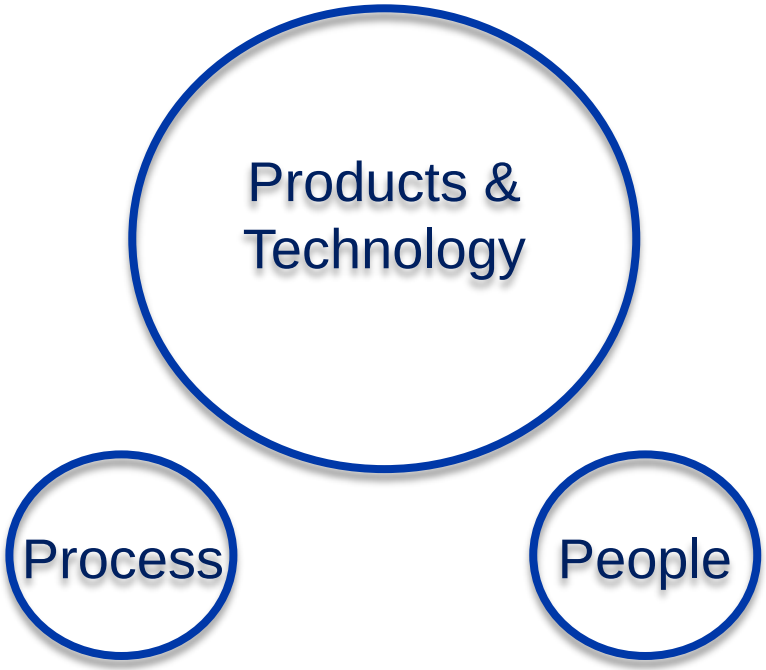
The Cybersecurity Landscape

Despite higher spending on cybersecurity, costs due to cyber attacks continue to grow exponentially

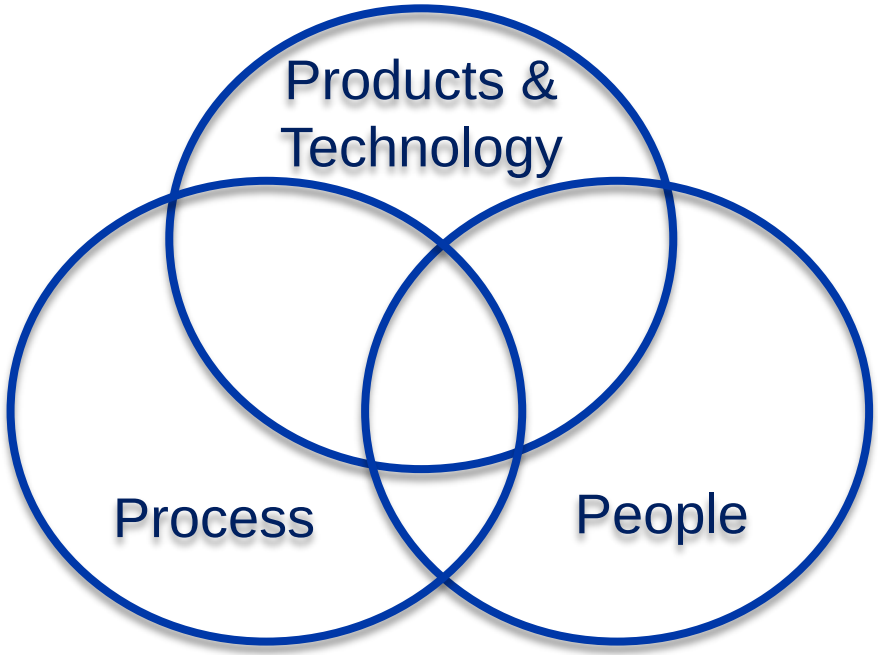




Where we are today:



Where we need to be:



Recommended Course of Action:

1. **Legislative**
   - Leverage legislative, executive, & regulatory mandates where possible
2. **Creating Conditions**
   - Create conditions for constantly improving cyber security & resilience
   - Implement sound, standardized cyber risk management process through **management, operational, and technical** controls
3. **Training**
   - Thoroughly train people in all aspects of that process
   - Match properly trained people to cyber risk management processes & tasks
4. **Data Analysis**
   - Collect and analyze progress reports & metrics on all of the above
   - Remediate as necessary

Three projects of potential interest:

National Standards: Addressing Process and People

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

Standardizing the Process: Cyber Secure Dashboard

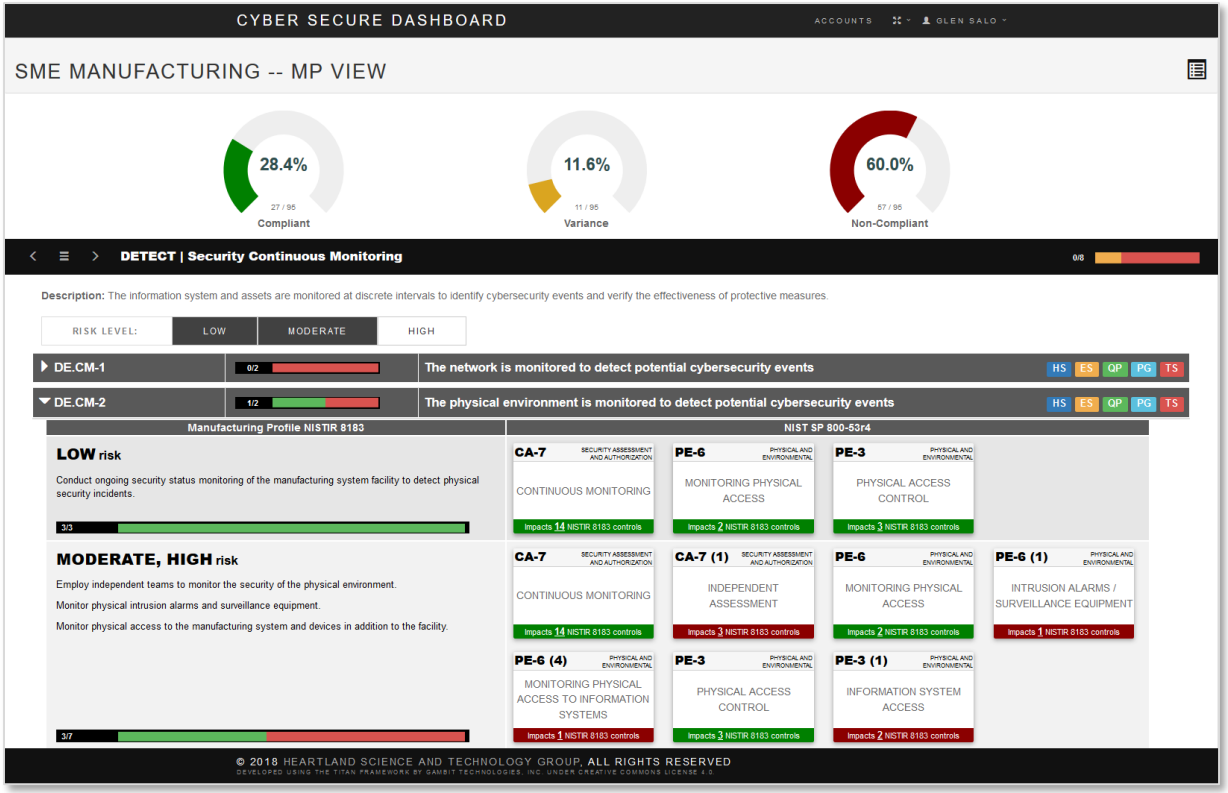
An **intuitive, cloud-based platform** that **operationalizes** a sound, standardized, effective **cyber risk management process** and **best practices**


Credible
Standardize
RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
RESPOND
PROTECT
DETECT
Mature
Flexible

Cyber Secure Dashboard

Features

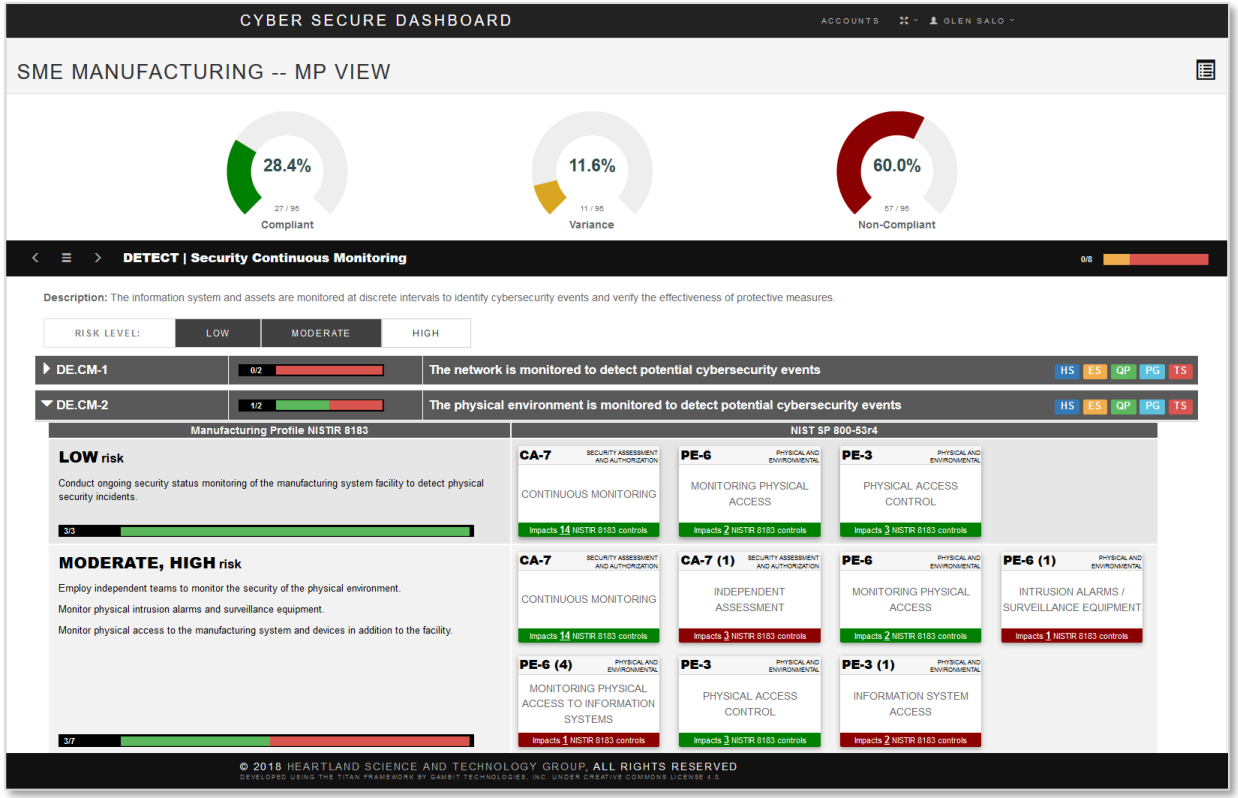
- NIST CSF + profiles + CMMC
- All-of-Company
- “Learn by Doing”
- Internal & External Communications
- One stop:
  - Requirements
  - References
  - Templates & best practices
  - POAM
  - Reporting
  - Embedded Training
- SMEs…prime contractors…entire supply chains



Cyber Secure Dashboard

Manufacturing Profile

- Status-at-a-glance
- Requirements mapped to controls
- Varying risk levels
- Includes business objectives



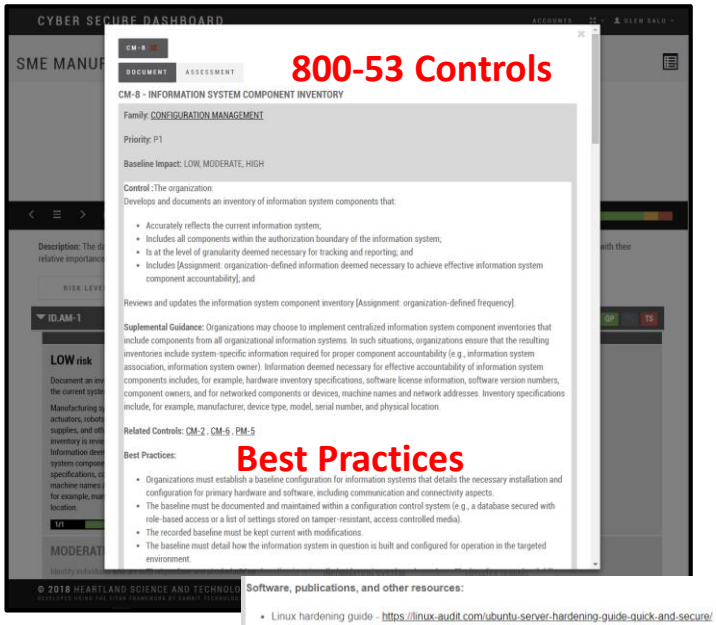
Who needs it?... Small and Medium Businesses

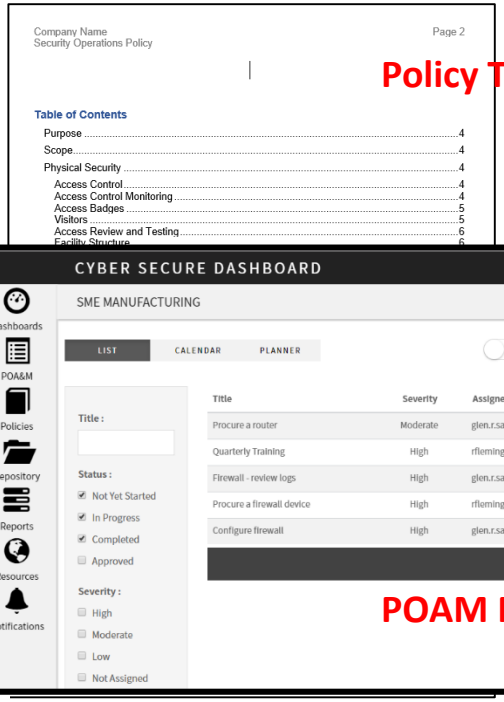
- Are the **prime targets** for attackers
- **Learn by doing** design
- **Embedded training** – including “just-in-time” and classroom
- Process and task **management**
- **Complements** outsourced cybersecurity services

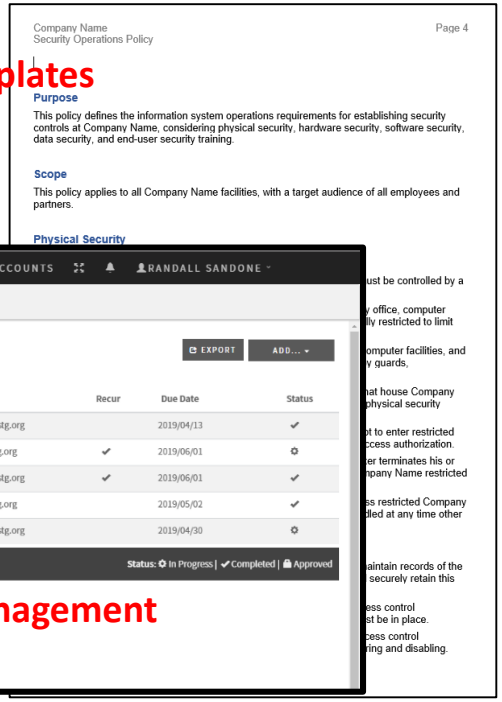
Who needs it?... Large Businesses

- **Increasingly responsible** for supply chain risks – including cyber
- **Standardize** policies, processes, requirements **across supply chains**
- View **aggregated status** of supply chain + drill down on pain points
- **Plan of Action & Milestones**, **centralized** artifact repository, **automated reports**
- Embedded training and **talent management**

Requirements, best practices, resources, and policies





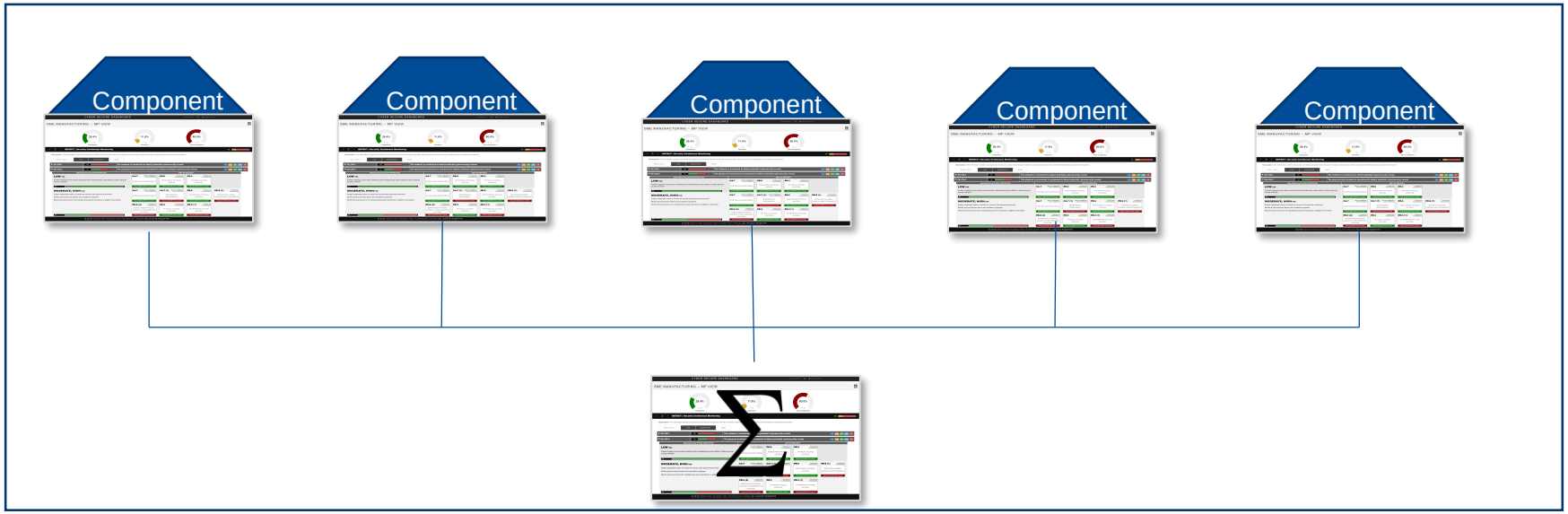


Policy Templates

POAM Management

Resources including Embedded Training Modules

Increase transparency and communication within the supply chain

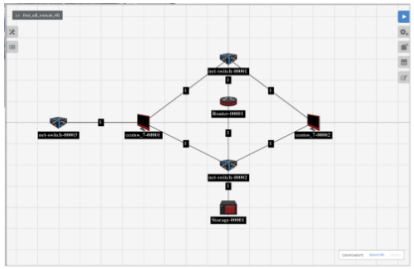


Training the people: National-Scale Delivery of Cyber Security Education

Training-Augmented Dashboard

In-Context Training

- Security Requirements
- Risk & Vulnerability Assessment
- Controls Implementation
- Monitoring & Mitigation
- Hands-on Training & Testing



Cyber Range

In-Class Training

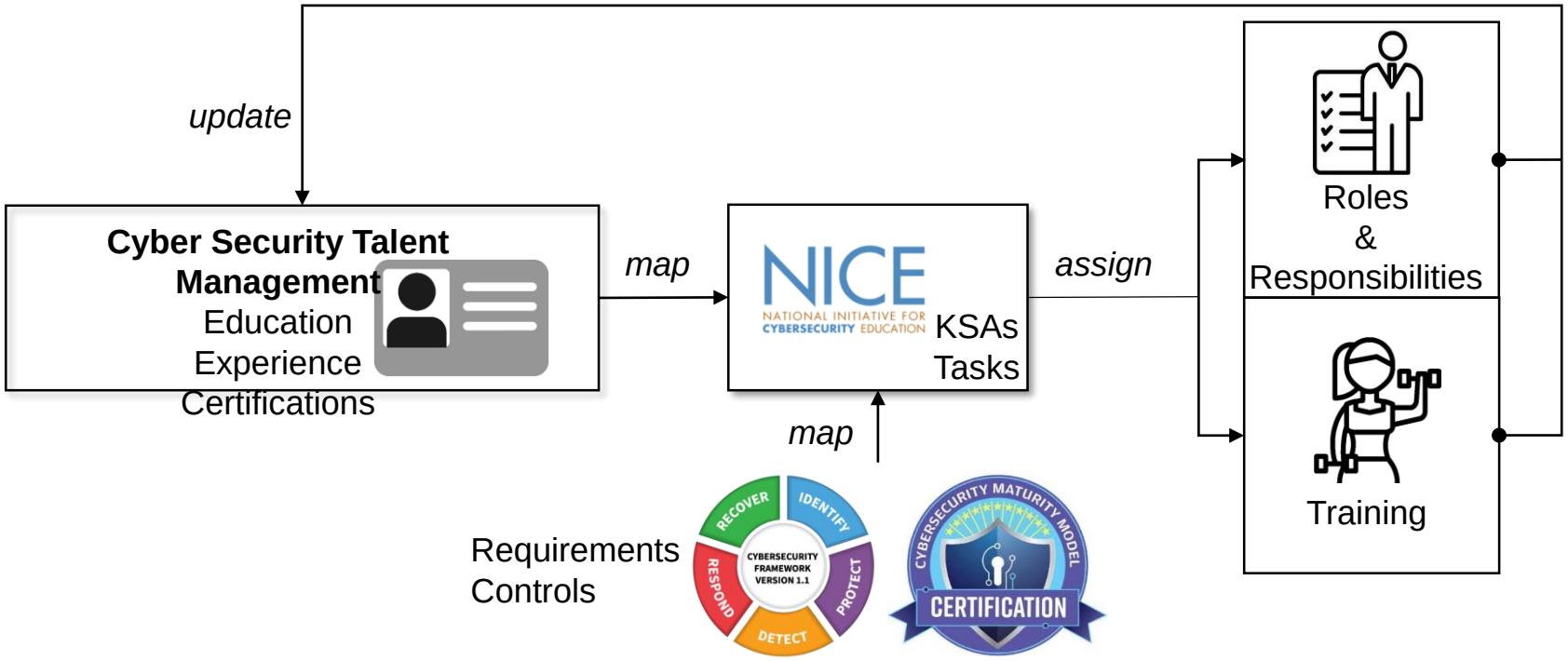
- Risk Awareness
- Risk Management Process
- Duties & Responsibilities
- Policies & Implementation

Matching people to tasks: Cyber Security Talent Management Module

Human resources tool to document, track, and manage cybersecurity knowledge, skills, and abilities of personnel based on NIST NICE Framework


NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

Matching People to Tasks:



Summary

Shift to a more **holistic approach** to products, people, and process. With a proper emphasis on the **people and process**

Implement and **train employees** to match a standard & mature **cyber risk management process**

Train to address KSA gaps, match tasks to appropriately skilled employees

Monitor performance with full **transparency** and **communicate expectations** clearly

Thank you!

Visit Us: ciri.Illinois.edu

51

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 or Partnership, please contact Auto-ISAC! contact.us@automotiveisac.com

Strategic Partnership Programs

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, SANS, IOActive, GRIMM

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Alliance, ACEA, ATA, JAMA, CLEPA

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: DHS, NHTSA, Colorado State, Johns Hopkins, NCI

Community

Companies interested in engaging the automotive ecosystem and supporting the community.

Examples: Summit sponsorship – key events

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

NAVIGATOR
Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities

COLLABORATOR
Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges- coordination activities

BENEFACTOR
Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

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!


thank you
danke
謝謝
ngiyabonga
شكراً جزيلاً
рахмат
teşekkür ederim
Баярлалаа
спасибо
faafetai lava
dank je
gracias
tapadh leat
хвала
bedankt
dziękuję
hvala
mauruuru
kiitos
dankie
vinaka
спасибі
blagodaram
misaotra
matondo
paldies
grazzi
mahalo
asante
manana
obrigada
tenki
murakoze
enkosi
gracie
köszönöm
akun
dankon
ačiū
djiere dieuf
tau
mochchakkeram
дякую
mamnun
chnorakaloutioun
gratias ago
gracies
sulpáy
go raibh maith agat
chokrane
sobodi
dēkuji
obrigado
sukriya
kop khun krap
tạiku
arigatô
takk
dakujem
trugarez
mesi
sagolun
didi madloba
kam sah hamnida
najis tuke
ありがとう
tanemirt
grazie
rahmet
terima kasih
diolch
dhanyavadagalu
shukriya
мерси
merci
rahmat
তোমাকে ধন্যবাদ
감사합니다
xiexie
ευχαριστώ

Our contact info

Faye Francy
Executive Director

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

Josh Poster
Program Operations Manager

20 F Street NW, Suite 700
Washington, DC 20001
joshposter@automotiveisac.com

automotiveisac.com
@auto-ISAC