



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

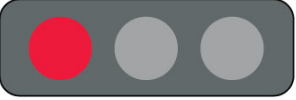



August 3, 2022

This Session will be recorded.

TLP:WHITE



DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants organizations.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>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.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

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

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ Gilad Bandel, Business Development, Cymotive▪ Title: "Continuously automated vulnerability management for safer cars and regulatory compliance"
11:45	Around the Room <ul style="list-style-type: none">➤ 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!

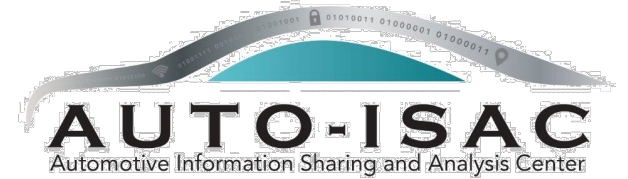
(sharmilakhadka@automotiveisac.com)



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!

22
OEM Members

21
Navigator Partners

❖ 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

46 *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

MEMBER ROSTER

AS OF AUGUST 1, 2022

Highlight = Change

68 Members, 8 in Progress

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

Eight Pending: Thyssenkrupp; Cymotive; AAM, Flex, Ferrari, ChargePoint; Nuspire, KTM

UPCOMING EVENTS

➤ Upcoming Meetings

➤ **Community Call:**

- **Wednesday, September 14** – **Speaker:** Tim Weisenberger, SAE International **Title:** “SAE EV Charging Public Key Infrastructure Program ” **Time:** 11 – 12:00 p.m. **TLP:WHITE**

- **Joint AWG & IT/OT Workshop:** Tuesday, September 6th 9 a.m. - 4 p.m. at the Henry in Dearborn, MI. [Click here for registration.](#) **TLP:AMBER// Members Only**

➤ **Members Teaching Members:**

- **Wednesday, August 17** **Speaker:** Moritz Minzlaff, Escript **Title:** “Benefits of an automotive security maturity model” **Time:** 10 – 11:30 a.m. **TLP:AMBER**

➤ Announcements

- **Auto-ISAC Cybersecurity Summit – Registration is Open!** Both in-person and virtual venue. Dates: September 7-8, 2022 in Dearborn, MI at The Henry Hotel. Your Company PoC has the “free passes” please check with them!

2022 AUTO-ISAC CYBERSECURITY SUMMIT

DRIVING A SECURE FUTURE

Hybrid Event • Dearborn, MI and Virtual • September 7-8, 2022



[More information here](#)

EVENT HOST & TITANIUM SPONSOR





AUTO-ISAC INTELLIGENCE

TLP:WHITE



AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; know our strategic view of the cyber threat environment: read the **TLP:GREEN** Threat Assessment in our 2021 Annual Report
 - **Send feedback**, contributions, or questions to analyst@automotiveisac.com
- Intelligence Notes
 - Geopolitical tensions are: **extremely high** in and around Ukraine ([PBS](#)) and between Russia and the West ([The Telegraph](#)); **high** around the Taiwan Strait ([The Hill](#)); and appear to be **building** around the Korean Peninsula ([The Associated Press](#)) and the Middle East ([The Times of Israel](#)). Such developments could add to an already heightened cyber threat environment. Organizations within the automotive community should be routinely looking for indications that their business networks, industrial systems, or products may be compromised ([CISA-Technical Approaches to Uncovering and Remediating Malicious Activity](#), [CISA Shields Up](#)).
 - We continue to see ransomware groups attacking automotive companies' business networks (Active Groups: [Cuba](#), [Hive](#), [Lockbit 3.0](#), [Black Basta](#)).
 - We continue to see and internally discuss technology-enabled vehicle theft research and incidents. **Notable open-source reports are included in the Auto-ISAC DRIVEN.**
 - Notable Tactics Techniques and Procedures: Deploying Malware via ISO Container Files ([Proofpoint](#)); Follina-Based Phishing ([Security Affairs](#)); Bug Bounties Offered by Threat Actors ([BleepingComputer](#)); Threat Actor Use of Pen Testing Tools ([Trend Micro](#)).

CISA RESOURCE HIGHLIGHTS



Case Study: Apple Releases Security Updates for Multiple Products

Regardless of industry, service providers need to monitor threats.

Apple has released security updates to address vulnerabilities in multiple products. These updates address vulnerabilities attackers could exploit to take control of affected systems.

CISA encourages users and administrators to review the Apple security updates and apply necessary releases.

[Read more here: Apple Releases Security Updates for Multiple Products | CISA](#)



Think about it: What are potential cyber threats to your organization today?



North Korean State-Sponsored Cyber Actors Use Maui Ransomware

CISA, the Federal Bureau of Investigation (FBI), and the Department of the Treasury (Treasury) have released a joint Cybersecurity Advisory (CSA), North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector, to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

CISA, FBI and Treasury urge network defenders, regardless of industry, to examine their current cybersecurity posture and apply the recommended mitigations in this joint CSA, which include:



Train users to recognize and report phishing attempts.



Enable and enforce multifactor authentication.



Install and regularly update antivirus and antimalware software on all hosts.

[North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA](#)



Case Study: Atlassian Releases Security Advisory for Questions for Confluence App, CVE-2022-26138

Regardless of industry, service providers need to monitor threats.

Atlassian has released a security advisory to address a vulnerability (CVE-2022-26138) affecting Questions for Confluence App. An attacker could exploit this vulnerability to obtain sensitive information. Atlassian reports that the vulnerability is likely to be exploited in the wild.

CISA encourages users and administrators to review Atlassian's security advisory, Questions For Confluence Security Advisory 2022-07-20, and apply the necessary updates immediately.



Think about it: What are potential cyber threats to your organization today?

[Read more here: Atlassian Releases Security Advisory for Questions for Confluence App, CVE-2022-26138 | CISA](#)

CNMF Discloses Malware in Ukraine

The current geopolitical conflict has affected organizations all over the world, regardless of industry. Some of the greatest exploitations have resulted in financial, human resource, and other losses.



CNMF has issued warnings.

U.S. Cyber Command's Cyber National Mission Force (CNMF), in close coordination with the Security Service of Ukraine, has released a list of indicators of compromise (IOCs) of malware seen in Ukraine. According to CNMF, "Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cyber security, just as we are sharing with them."



We want to help you fight this vulnerability.

CISA encourages users and administrators to review U.S. Cyber Command's press release, Cyber National Mission Force discloses IOCs from Ukrainian networks, as well as their VirusTotal and GitHub pages for more information. See Mandiant's report, Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities, for additional information.



Read more here: [CNMF Discloses Malware in Ukraine | CISA](#)

CISA Report to NCI
August 1, 2022

KEVs Catalog

CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.



CISA has added 2 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of July. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.



Additional Resources from CISA

- ❑ CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- ❑ CISA NCAS – [https://us-cert\[.\]cisa\[.\]gov/](https://us-cert[.]cisa[.]gov/)
- ❑ CISA Shields Up - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
- ❑ Free Cybersecurity Services and Tools - [https://www\[.\]cisa\[.\]gov/free-cybersecurity-services-and-tools](https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools)
- ❑ CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- ❑ CISA Blog - [https://www\[.\]cisa\[.\]gov/blog-list](https://www[.]cisa[.]gov/blog-list)
- ❑ CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- ❑ CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- ❑ CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)





For more information:
[cisa.gov](https://www.cisa.gov)

Questions?
Central@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*

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!

30+
*Featured
Speakers to
date*

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

TLP:WHITE



GILAD BANDEL, CYMOTIVE

BUSINESS DEVELOPMENT AND MARKETING



Gilad drives CYMOTIVE's automotive cybersecurity business development and product marketing. His focus is on delivering to the market state-of-the-art, unique and innovative solutions - automotive for cyber-security protection.

Gilad is an accomplished executive with over 30 years of experience in the cyber-security and networking industries. Having covered markets in Europe, America and the APAC region, Gilad is a renowned expert in conceptualizing and developing go-to-market strategies. He specializes in business development for cyber-security solutions for automotive, IoT, critical infrastructure and homeland security markets.

Prior to joining Cymotive, Gilad served as VP of Product and Marketing at Arilou Automotive Cybersecurity, as VP of Product at Radiflow and as Director of Product Management at CyberSeal (a Magal Security company). Earlier positions held include VP of R&D, and CTO at leading networking, telecommunication and homeland security companies.

Continuously automated vulnerability management for safer cars and regulatory compliance

Gilad Bandel

Cymotive Technologies

CYMO TIVE
TECHNOLOGIES

About



Founded in 2016 by leaders of
Israel's National Security Services



Selected cyber partner of
the Volkswagen Group

Financially Strong & Profitable

**A full lifecycle
smart mobility
platform**

**A growing
workforce**

~200 employees
85% cyber experts

**A global
footprint**

Israel, North
America, Europe &
Asia

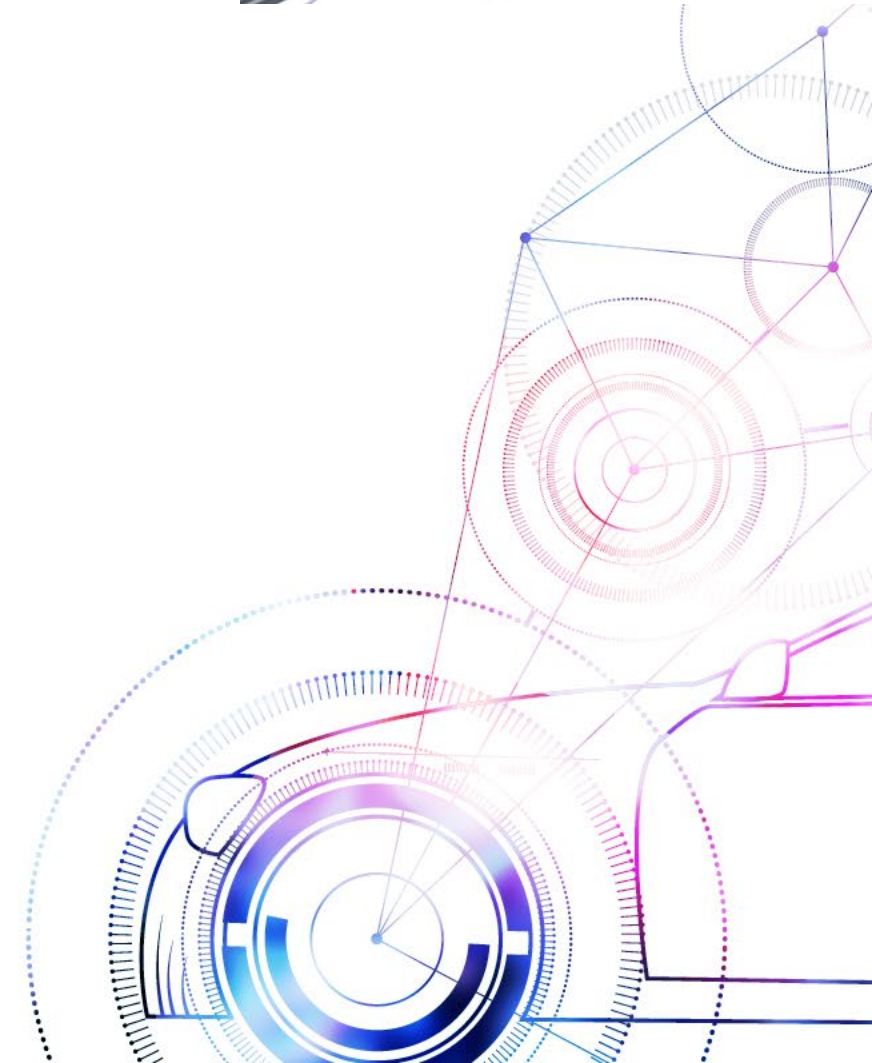
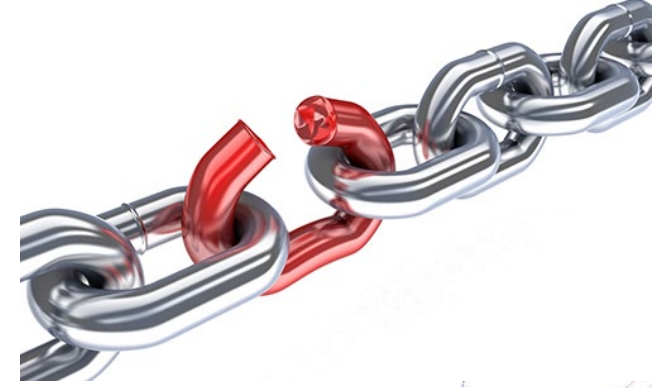
**Industry
certifications**

ISO 9001, ISO/IEC 90003,
TISAX, A-SPICE® Level 2

Automotive vulnerability management – why?

OEMs, Fleet owners/operation and Tier 1/2s must address and manage **risks** emerging from embedded **software** running in the vehicle

1. Comply with the process regulation required for **homologation**
2. Perform a documented **intrinsic secured** development



Challenges and motivation

	Development	Type approval	Postproduction	
OEM/ Fleet owner/ operator	Identify and manage cybersecurity risks during software development	Provide evidence for cybersecurity type approval certification	Continuously monitor cybersecurity risks during fleet lifespan	Protect against brand damage and recovery costs due to cyber attacks
Tier 1/2		Provide OEM with evidence necessary for cybersecurity type approval	Continuously monitor cybersecurity risks during the ECU lifespan	Protect against impact due to cybersecurity cases detected by OEM

Brand Damage

THE DRIVE THE WAR ZONE REVIEWS CAR WARRANTIES DEALS NEWSLETTER SIGNUP

Researchers Used a Drone and a WiFi Dongle to Break Into a Tesla

A hardcoded password was just the start.

BY ROB STUMPF MAY 4, 2021

TECH

AP—COPYRIGHT 2017 THE ASSOCIATED PRESS. ALL RIGHTS RESERVED.

Home > Wireless Security

Tesla Car Hacked Remotely From Drone via Zero-Click Exploit

By Eduard Kovacs on May 03, 2021

Share Tweet Recommend 450 RSS

THE BYTE.

LONG-RANGE HACKING

HACKERS BROKE INTO TESLA USING A DRONE

A ZERO-CLICK EXPLOITS LET HACKERS UNLOCK AND PARTIALLY CONTROL A NEARBY TESLA.



Technologie / #Drone #IA #Intelligenceartificielle #AirForce

Comment cette Tesla a été piratée par un drone en quelques minutes ! Démonstration



8 mai 2021

f t in e



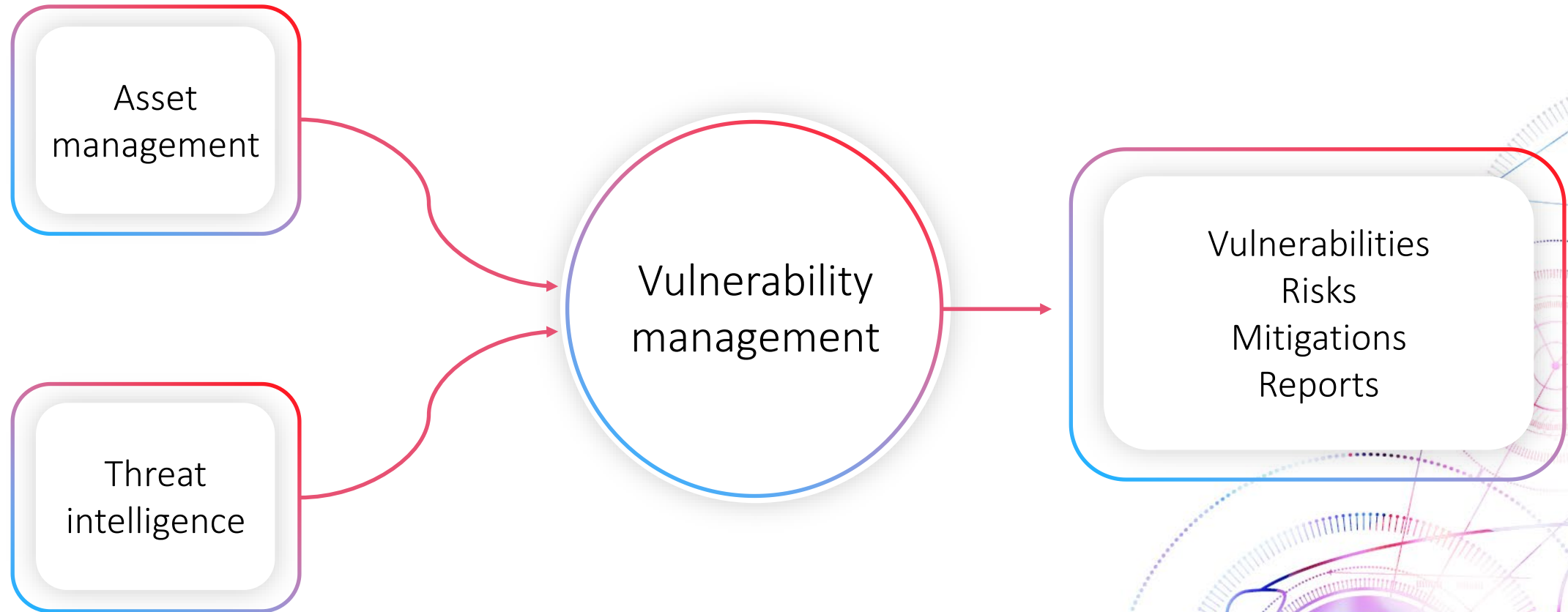
Audencia
executive.audencia.com

MBA COMMUNITY :
UNE COMMUNAUTÉ MULTICULTURELLE ET MULTIGÉNÉRATIONNELLE D'APPRENTISSAGE

- 6 MBAs en France et à l'internationale : Executive MBA & Full Time MBA
- + de 150 dirigeants formés par ans à travers le monde

CLASSEMENT CEO MAGAZINE
• #3 EMBA

Vulnerability management overview



Gained values of proper vulnerability management

- Reduced costs of development, certification and maintenance while strengthening the vehicle's security protection
- Fulfills regulation requirements - UNR 155 following ISO/SAE 21434
- Manages the risks and provides recommended mitigation
- Provides ongoing visibility and insight of the critical vulnerabilities



Automated vulnerability management process

User

Assets

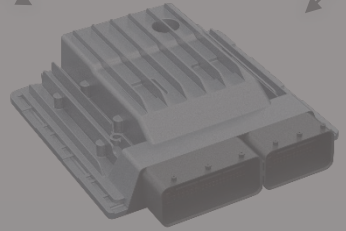
In-Vehicle Network Architecture

Review by Business Owner



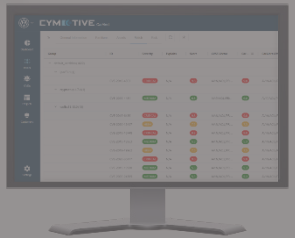
Risk Severities
Safety, Law,
Financial,
Quality

Threat Intelligence



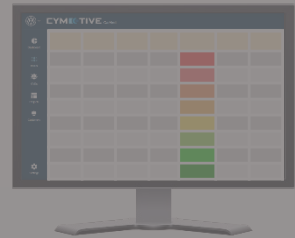
Profiling

ECU Details
Partitions
Functions
Software Packages
Risk Tags



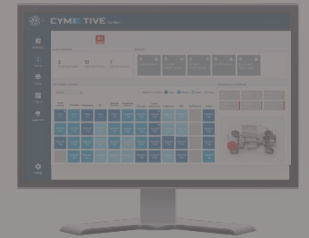
Analyzing

CVE Scores
Attack Types
Exploits



Assessment

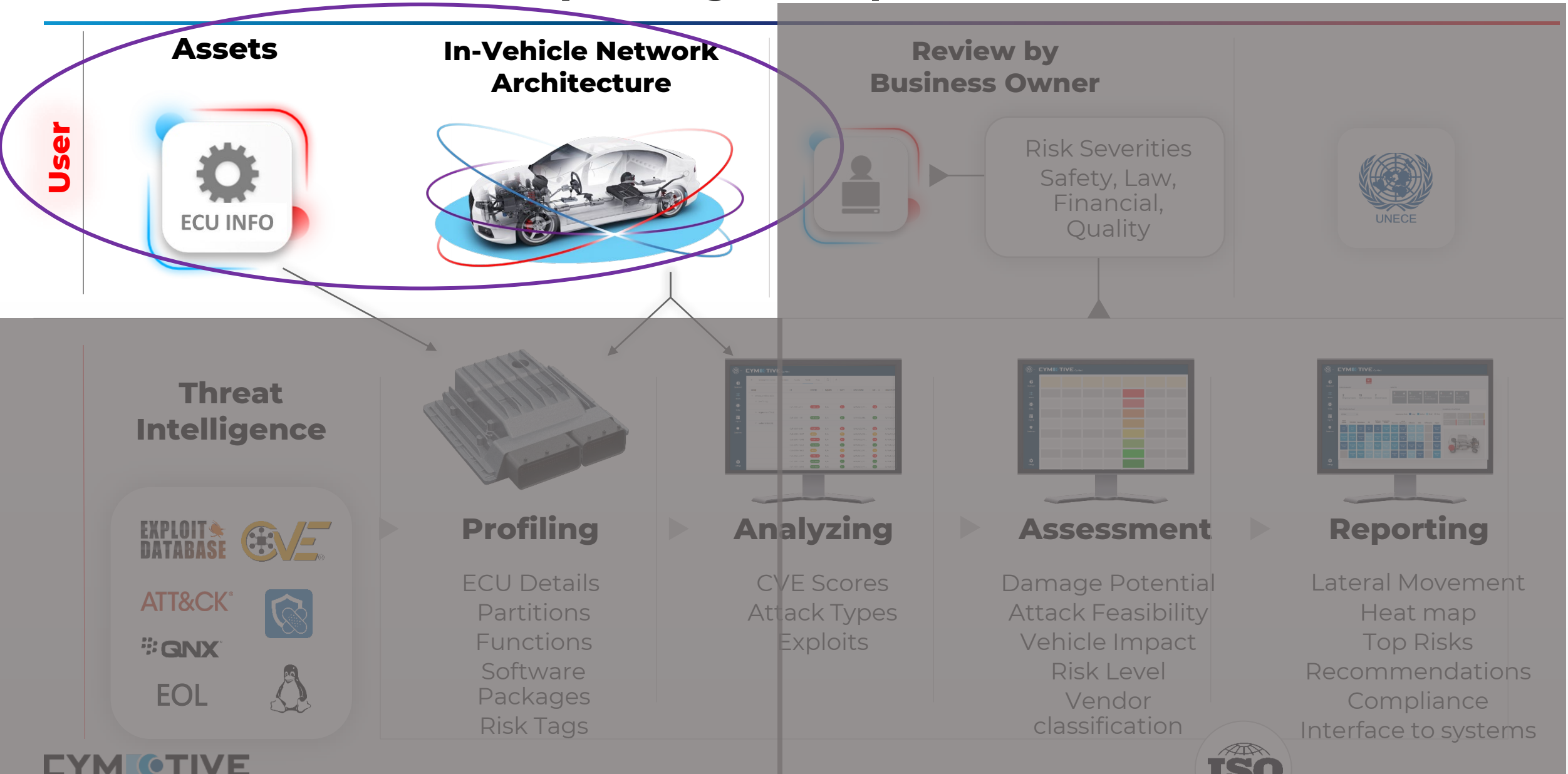
Damage Potential
Attack Feasibility
Vehicle Impact
Risk Level
Vendor classification



Reporting

Lateral Movement
Heat map
Top Risks
Recommendations
Compliance
Interface to systems

Automated vulnerability management process



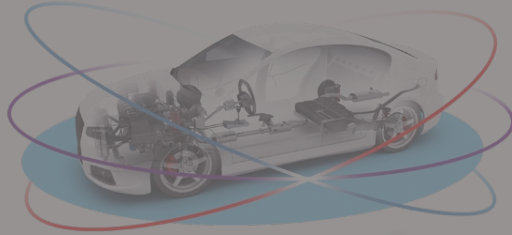
Automated vulnerability management process

User

Assets



In-Vehicle Network Architecture



Review by Business Owner



Risk Severities
Safety, Law,
Financial,
Quality

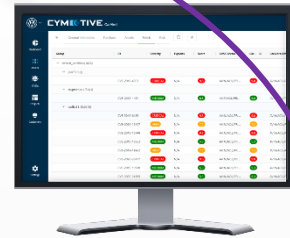


Threat Intelligence



Profiling

ECU Details
Partitions
Functions
Software
Packages
Risk Tags



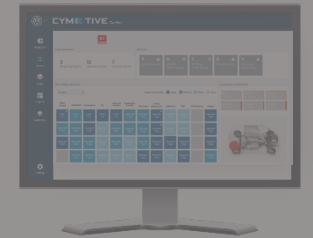
Analyzing

CVE Scores
Attack Types
Exploits



Assessment

Damage Potential
Attack Feasibility
Vehicle Impact
Risk Level
Vendor
classification

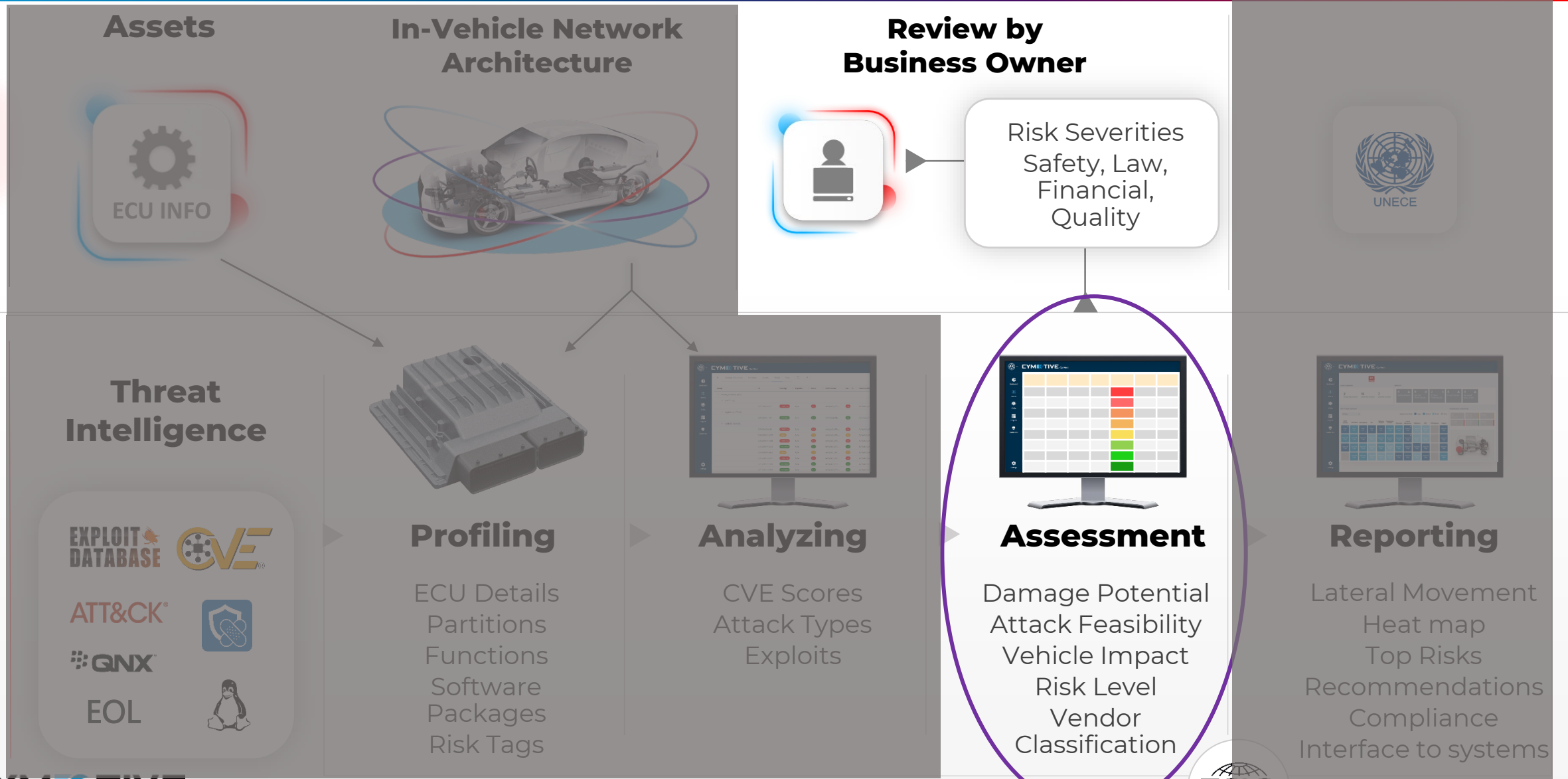


Reporting

Lateral Movement
Heat map
Top Risks
Recommendations
Compliance
Interface to systems

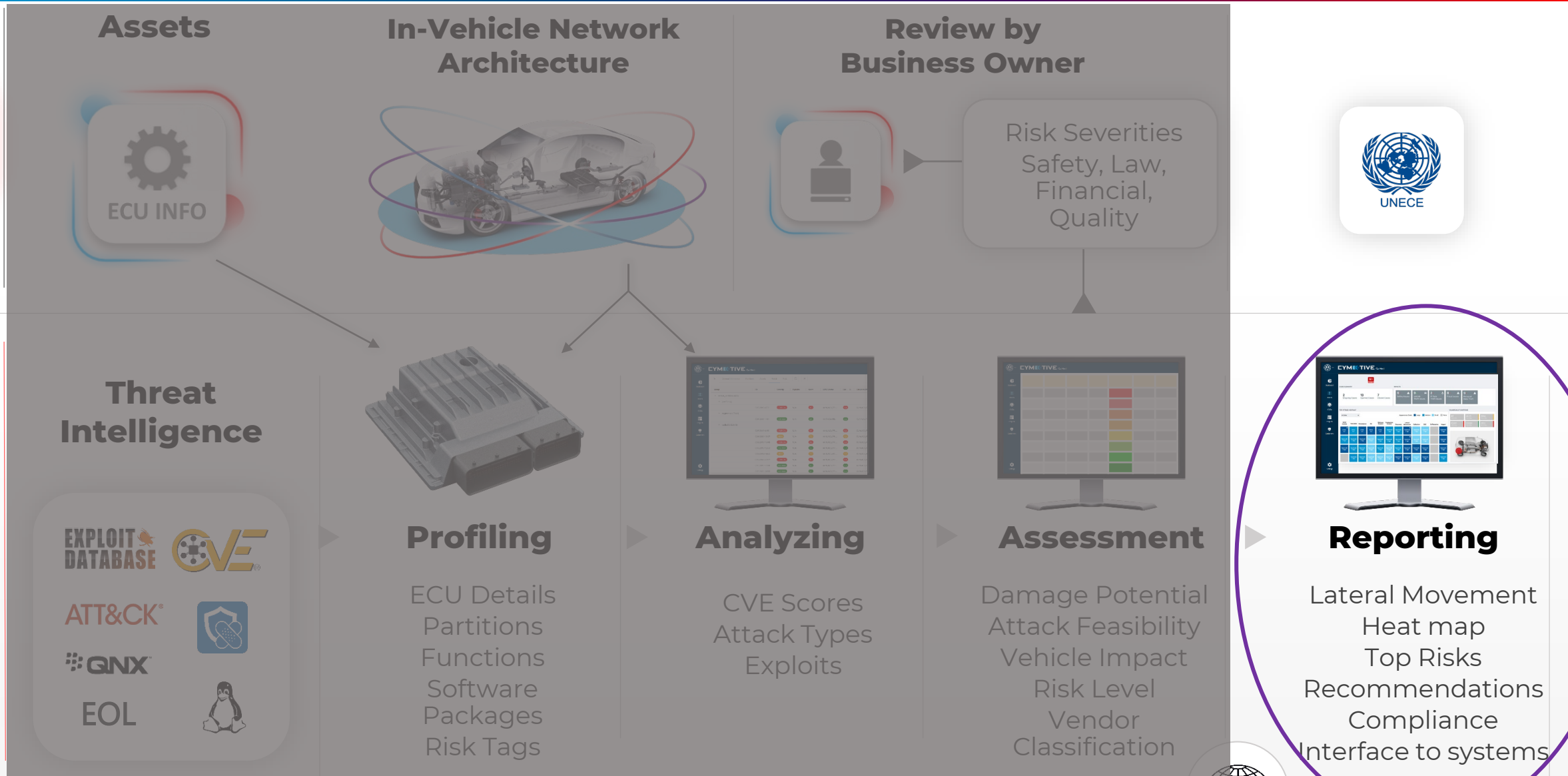
Automated vulnerability management process

User



Automated vulnerability management process

User

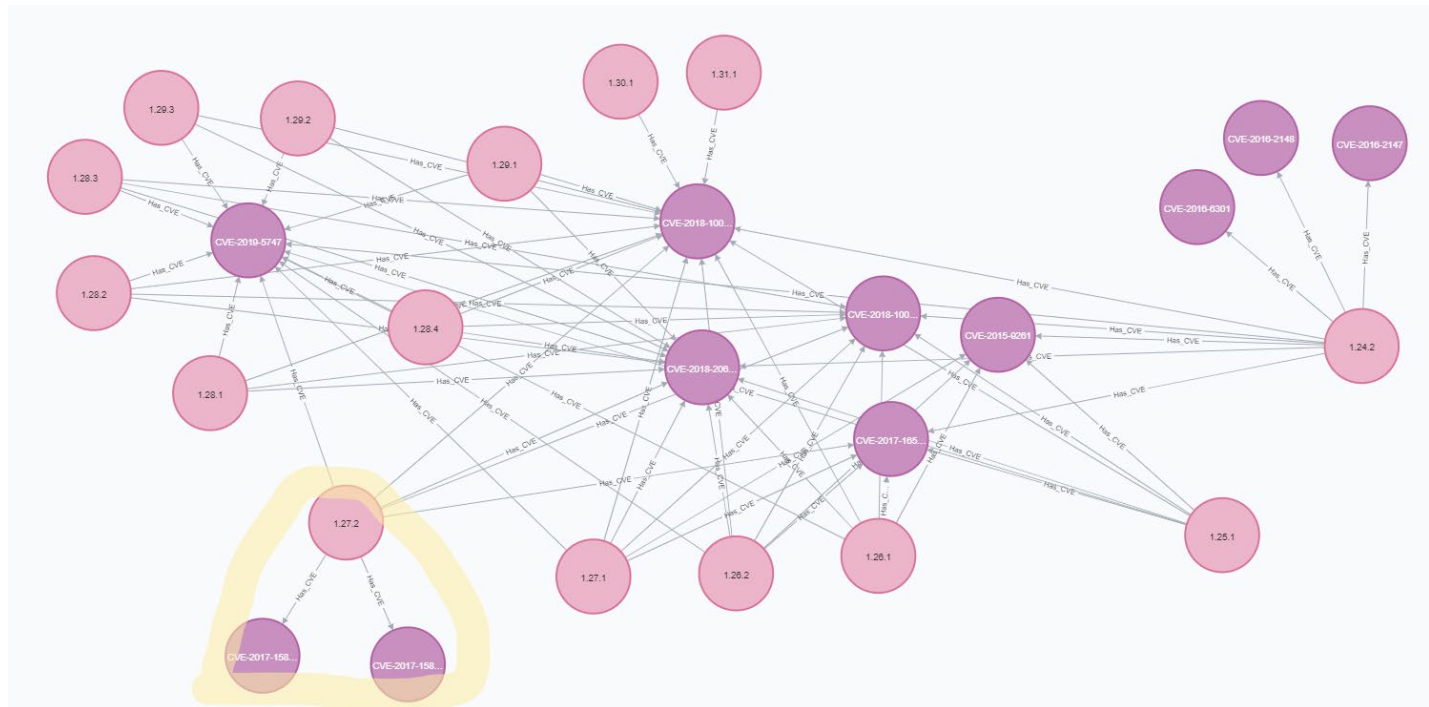


Mitigation plan for risk minimization

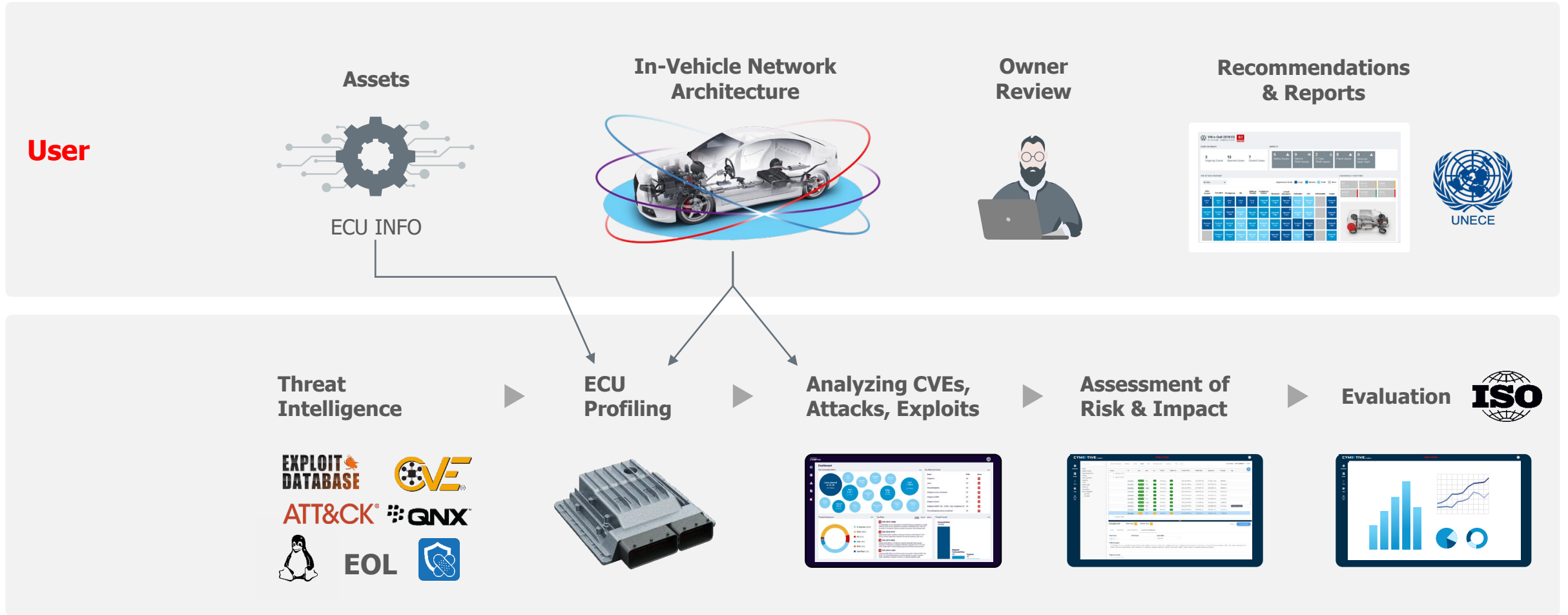
Once a vulnerability has been discovered, the ideal solution is to fix or remediate it, before it can become a security threat. For this, we must always check a few different parameters.

Customers receive a scored, prioritized list of critical vulnerabilities that require mitigation.

Vendor	Software	Current Version	Patches for Critical CVEs	Recommended Version
1	Linux Kernel	4.4	CVE-2016-10229 CVE-2016-7117 CVE-2018-20961	5.4 5.10
2	CURL	7.59.0	CVE-2019-5482 CVE-2019-5481 CVE-2018-0500 CVE-2018-16839	7.78.1 – 7.81.1



Automated Process Vulnerability Management



Things to remember

Continuous vulnerability management is a major cornerstone of the cybersecurity management system, required for regulation compliance and vehicle safety



Proper asset acquisition and supply chain management is a real challenge



All software development organizations should perform risk minimization as early as possible in the secured software development lifecycle by applying proper controls to mitigate vulnerabilities in a prioritized fashion



Product based vulnerability management such as Cymotive Car Alert increases the security while reducing the associated costs and shortens the development schedule



The process can be done internally by cybersecurity experts if available or outsourced to a professional service company



Thank You | cymotive.com

gilad.bandel@cymotive.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 michaelshokouhi@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
(17)**

ArmorText
 Cybellum
 Deloitte
 FEV
 GRIMM
 HackerOne
 Irdeto
 Itemis
 Karamba Security
 KELA
 Pen Testing Partners
 Red Balloon Security
 Regulus Cyber
 Saferide
 Security Scorecard
 Trustonic
 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-

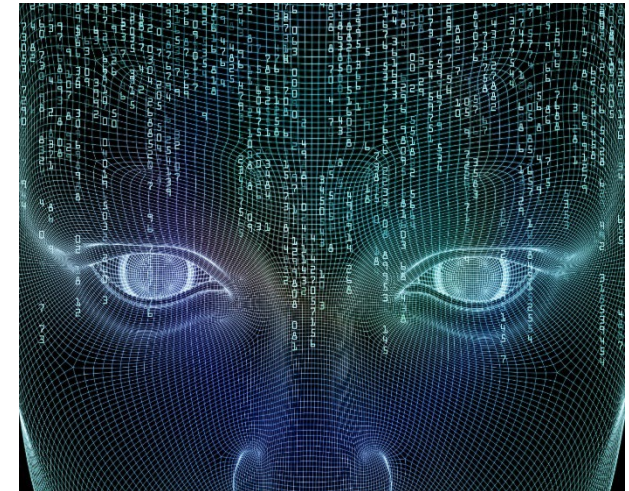
Celerium
 Cyware
 Denso
 NDIAS
 IOActive
 Claroty
 Deloitte
 Finite State
 Tanium
 Recorded Future
 PaloAlto Networks
 Upstream
 Securonix
 Zimperium
 Micron
 Block Harbor
 SecurityScorecard
 Booz Allen
 CybelAngel
 ATT
 Ford
 Cybellum

2020 Summit Sponsors-

Claroty
 Upstream
 Escrypt
 Blackberry
 Cybellum
 Blockharbor
 C2A
 Synopsis
 Intsignts
 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!



OUR CONTACT INFO

Faye Francy
Executive Director



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

Sharmila Khadka
Information Technology Executive
Coordinator



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



www.automotiveisac.com
@auto-ISAC