



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

November 1, 2023

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



AUTO-ISAC ANTITRUST STATEMENT

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.

Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.






This meeting is being held at

TLP:CLEAR

Disclosure is not limited.

TRAFFIC LIGHT PROTOCOL (TLP)

VERSION 2.0 DEFINITIONS

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 without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.</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+STRICT</p>  <p>Limited disclosure, restricted to participants' and its organization.</p>	<p>Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.</p>	<p>Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.</p>	<p>Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.</p>
<p>TLP:CLEAR</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Recipients may share this information without restriction. Information is subject to standard copyright rules.</p>

Source: <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➤ Intelligence Highlights
11:15	DHS CISA Community Update <ul style="list-style-type: none">➤ Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Adam Robbie, Senior Staff Researcher, Palo Alto Networks➤ Title: "The Game of IT/OT Security: Unveiling New Critical Developments in Our Critical Infrastructure Threat Landscape"
11:55	Q&A & 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!

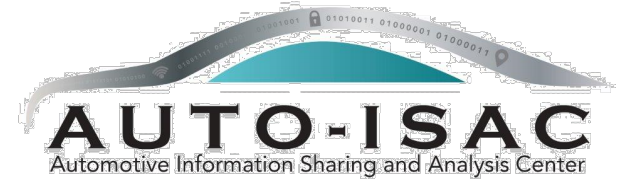
(sharmilakhadka@automotiveisac.com)



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!

30
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

47 Supplier &
Commercial
Vehicle Members

20
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)



2023 BOARD OF DIRECTORS

Thank you for your Leadership!



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



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



Stephen Roberts
*Secretary of the
Board of the Directors*
Honda



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



Andreas Ebert
Chair of the EuSC
Volkswagen



Andrew Hillery
Chair of the CAG
Cummins



Ravi Puvvala
Chair of the SAG
Fleet Defender



Monica Mitchell
Polaris



Bob Kaster
Bosch



Brian Witten
Aptiv

AUTO-ISAC MEMBER ROSTER

AS OF NOVEMBER 1, 2023

77 MEMBERS + 4 PENDING

Aisin	Fleet Defender	Luminar	Renesas Electronics
Allison Transmission	Flex	Magna	Rivian
American Axle & Manufacturing	Ford	MARELLI	Stellantis
Aptiv	Garrett	Mazda	Subaru
AT&T	General Motors (Cruise-Affiliate)	Mercedes-Benz	Sumitomo Electric
AVL List GmbH	Geotab	Mitsubishi Electric	thyssenkrupp
Blackberry Limited	Harman	Mitsubishi Motors	Tokai Rika
BMW Group	Hitachi	Mobis	Toyota (Woven-Affiliate)
BorgWarner	Honda	Motional	Valeo
Bosch (ETAS-Affiliate)	Hyundai	Navistar	Veoneer
Bose Automotive	Infineon	Nexteer Automotive Corp	Vitesco
ChargePoint	Intel	Nissan	Volkswagen (CARIAD-Affiliate)
CNH Industrial	John Deere Electronic	Nuro	Volvo Cars
Continental (Argus-Affiliate)	JTEKT	Nuspire	Volvo Group
Cummins (Meritor-Affiliate)	Kia America, Inc.	NXP	Waymo
Daimler Truck	Knorr Bremse	Oshkosh Corp	Yamaha Motors
Denso	KTM	PACCAR	ZF
e:fs TechHub GmbH	Lear	Panasonic (Ficosa-Affiliate)	
Faurecia	LG Electronics	Polaris	
Ferrari	Lucid Motors	Qualcomm	

Pending: Amazon.com, Dana Inc, Phinia Inc, Stoneridge

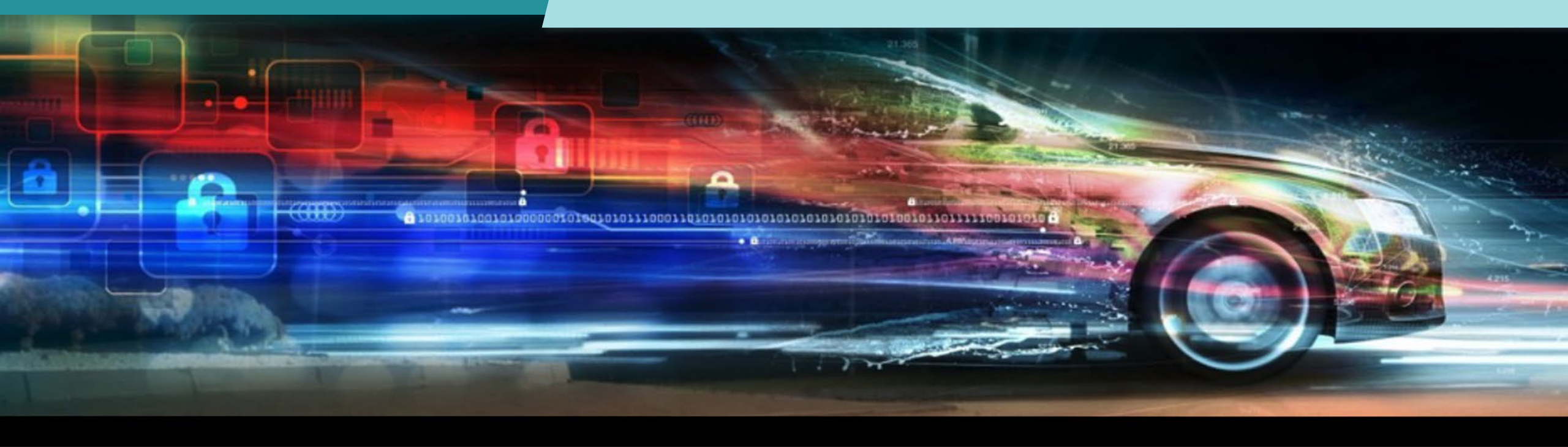
AUTO-ISAC BUSINESS UPDATES AND EVENTS

- **Community Call:** Wednesday, December 6th **Time:** 11:00am – 12:00 p.m. **TLP:GREEN** **Speaker:** Dan Barahona, Founder, APIsec University **Title:** “API Security Risks for Connected Cars”
- **Auto-ISAC 2nd European Summit** be held in Munich, Germany: June 12th – June 13th. The Titanium sponsor the 2024 event will be BMW. Stay tuned for more details.
- **Automotive Cybersecurity Training (ACT) Program:** In person ACT Advanced courses have been rescheduled to Q1/Q2 2024, but ACT Fundamental courses are available on demand. Register: <http://www.automotiveisac.com/act>! Please email ACT@automotiveisac.com with any questions.
 - **ACT Fundamental Course Block:** Online, On-Demand, Anytime, Anywhere, and by Anyone \$500/course
 - **Cybersecurity Basics** (32 hrs.) | **Security Engineering** (28 hrs.) | **Security Operations/Management** (22.5 hrs.)

☐ Advanced courses [New Dates]:

- **Advanced Engineering:** January 22 - 26, 2024
- **Wireless:** February 5 - 9, 2024
- **EV and EV Infrastructure:** March 4 - 8, 2024
- **Guided Attacks:** April 29 - May 4, 2024

NOTE: New Community Call invite for 2024 will be sent next month. Please be on a lookout. The existing 2023 invite will be discarded after December.



AUTO-ISAC INTELLIGENCE HIGHLIGHT

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; Auto-ISAC 2024 Threat Assessment is in production; the **TLP:GREEN** version is expected early next year.
 - **Send feedback**, intelligence, or questions to analyst@automotiveisac.com
- Intelligence Notes
 - Geopolitical tensions involving Russia, China, North Korea, and Iran remain **high** with Russia-Ukraine and now Israel-Hamas in crisis ([Russia-Ukraine](#), [China](#) ¹, [North Korea](#), [Iran](#) ² ³).
 - Israel-Hamas War
 - Nuisance attacks and cyberespionage* have increased ([Jerusalem Post](#), [TechCrunch](#), [Cyberscoop](#))
 - No signs of state-sponsored **destructive** cyberattacks; however, the risk of **destructive** cyberattacks will increase if the war becomes regional and **directly** involves Iran. (**Note:** the likelihood of the war expanding to Iran is difficult to confidently estimate. It is at least conceivable.)
 - Ransomware ⁴ Groups Targeting Automotive: [Knight](#), [Play](#), [8Base](#), [LockBit 3.0](#), [BianLian](#)
 - Notable TTPs and Tools: Exploiting Atlassian CVE-2023-22515 ([CISA](#)); Exploiting Arm CVE-2023-4211 ([BleepingComputer](#)); Exploiting WS-FTP CVE-2023-40044 ([Assetnote](#)); Exploiting CISCO CVE-2023-20198 ([Talos](#)); Exploiting Internet-Exposed Jupyter Notebooks to Breach Servers ([BleepingComputer](#)); Employing Loader-Trojan-Stealer Combination in Attacks ([Securelist/Kaspersky](#)); Employing Fake Browser Updates ([Help Net Security](#)); Employing secure Universal Serial Bus (USB) Drives in Attacks ([The Hacker News](#))

CISA Resource Highlights

- Joint Cyber Defense Collaborative



JOINT CYBER DEFENSE
COLLABORATIVE

Jeff Terra
11/1/2023



CISA Releases Fact Sheet on Effort to Revise the National Cyber Incident Response Plan (NCIRP)

- First published in 2016, the NCIRP was developed in accordance with Presidential Policy Directive 41 (PPD-41) on U.S. Cyber Incident Coordination and describes how federal government, private sector, and state, local, tribal, territorial (SLTT) government entities will organize to manage, respond to, and mitigate the consequences of significant cyber incidents.
- NCIRP 2024 will address changes to the cyber threat landscape and in the nation's cyber defense ecosystem by incorporating principles grounded in four main areas:
 - Unification
 - Shared Responsibility
 - Learning from the Past
 - Keeping Pace with Evolutions in Cybersecurity

CISA, NSA, FBI, and MS-ISAC Release Phishing Prevention Guidance

- The joint guide outlines phishing techniques malicious actors commonly use and provides guidance for both network defenders and software manufacturers to reduce the impact of phishing techniques used in obtaining credentials and deploying malware.
- CISA and its partners encourage network defenders and software manufacturers to implement the recommendations in the guide to reduce the frequency and impact of phishing incidents.
- Malicious actors primarily leverage phishing for:
 - Obtaining login credentials
 - Malware deployment.
- Multi-factor authentication (MFA) can reduce the ability of malicious actors using compromised credentials for initial access.

CISA Releases New Resources Identifying Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware

15

- CISA launched two new resources for combating ransomware campaigns:
 - A “Known to be Used in Ransomware Campaigns” column in the KEV Catalog that identifies KEVs associated with ransomware campaigns.
 - A “Misconfigurations and Weaknesses Known to be Used in Ransomware Campaigns” table on StopRansomware.gov that identifies misconfigurations and weaknesses associated with ransomware campaigns.
- These two new resources will help organizations become more cybersecure by providing mitigations that protect against specific KEVs, misconfigurations, and weaknesses associated with ransomware.

Security/Software Updates

For October 2023:

- Apple Releases Multiple Security Updates
- Atlassian Releases Security Updates
- Oracle Releases Security Updates
- Citrix Releases Security Updates
- Microsoft Releases Security Updates
- CISCO Releases Security Updates
- VMWare Releases Security Updates
- Fortinet Releases Security Updates

- **Best practices:**
 - Leverage automatic updates for all operating systems and third-party software
 - Implement security configurations for all hardware and software assets
 - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- For the period of 10/1/23- 10/31/23 approximately 36 advisories have been issued.
- Affected systems include Sielco, Centralite Pearl Thermostat, Schneider Electric EcoStruxture, Rockwell Automation (multiple products), Santesoft Sante, Siemens (multiple products), Mitsubishi Electric, Advantech WebAccess, Hitachi Energy, and many others.
- For current ICS advisories please check [CISA.gov](https://www.cisa.gov) regularly

Please note all information provided is TLP Amber

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 added 17 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of October. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

Additional Resources from CISA

- ❑ CISA Homepage - <https://www.cisa.gov/>
- ❑ CISA NCAS – <https://cisa.gov/resources-tools/all-resources-tools>
- ❑ CISA Shields Up - <https://www.cisa.gov/shields-up>
- ❑ Free Cybersecurity Services and Tools - <https://www.cisa.gov/free-cybersecurity-services-and-tools>
- ❑ CISA News Room - <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/>



**JOINT CYBER DEFENSE
COLLABORATIVE**

For more information:

cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Jeff Terra
11/1/2023



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?

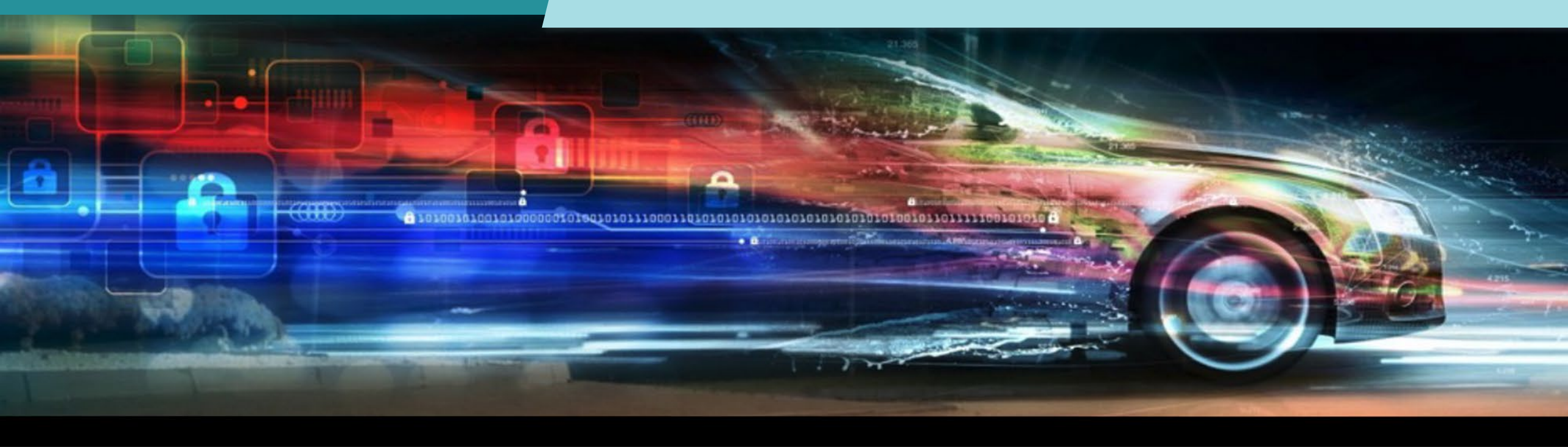
- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

30+
*Featured
Speakers to
date*

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR



MEET THE SPEAKER



Adam Robbie

Adam Robbie is an ICS/OT senior researcher at Palo Alto Networks since 2022 with over 10 years of experience in both OT and IT industries. Publisher and author with SANS, IEEE, and other journals and conferences. His ambition is about contributing to secure our critical infrastructure, search for recent vulnerabilities, develop best practices and lead new initiatives. Adam has a Bachelor and Master of Science in Electrical Engineering. Additionally, he obtained advanced certifications including the Global Industrial Cyber Security Professional (GICSP) and GIAC Response and Industrial Defense (GRID) certifications.

In addition to his technical expertise, He has a strong background in leadership and education. As an Adjunct Professor, I have been teaching cybersecurity bootcamp at The George Washington University, University of Michigan, University of Wisconsin, and other universities. Through these roles, he has successfully mentored and guided students, encouraging them to excel in the field of cybersecurity. Additionally, he served as an advisor for cybersecurity curriculum development.

During his tenure as a Senior Cyber Security Consultant at Deloitte, he gained extensive experience in performing ICS/IoT penetration testing, threat hunting, risk assessment, and vulnerability research. He is proficient in utilizing various SIEM tools like Qradar, LogRhythm, and Splunk for network and host analysis. Furthermore, he has actively contributed to enhancing detection systems through the creation of security use cases.

Auto-ISAC

Briefing on OT Threat Landscape

Adam Robbie
Senior Security Researcher

November 2023



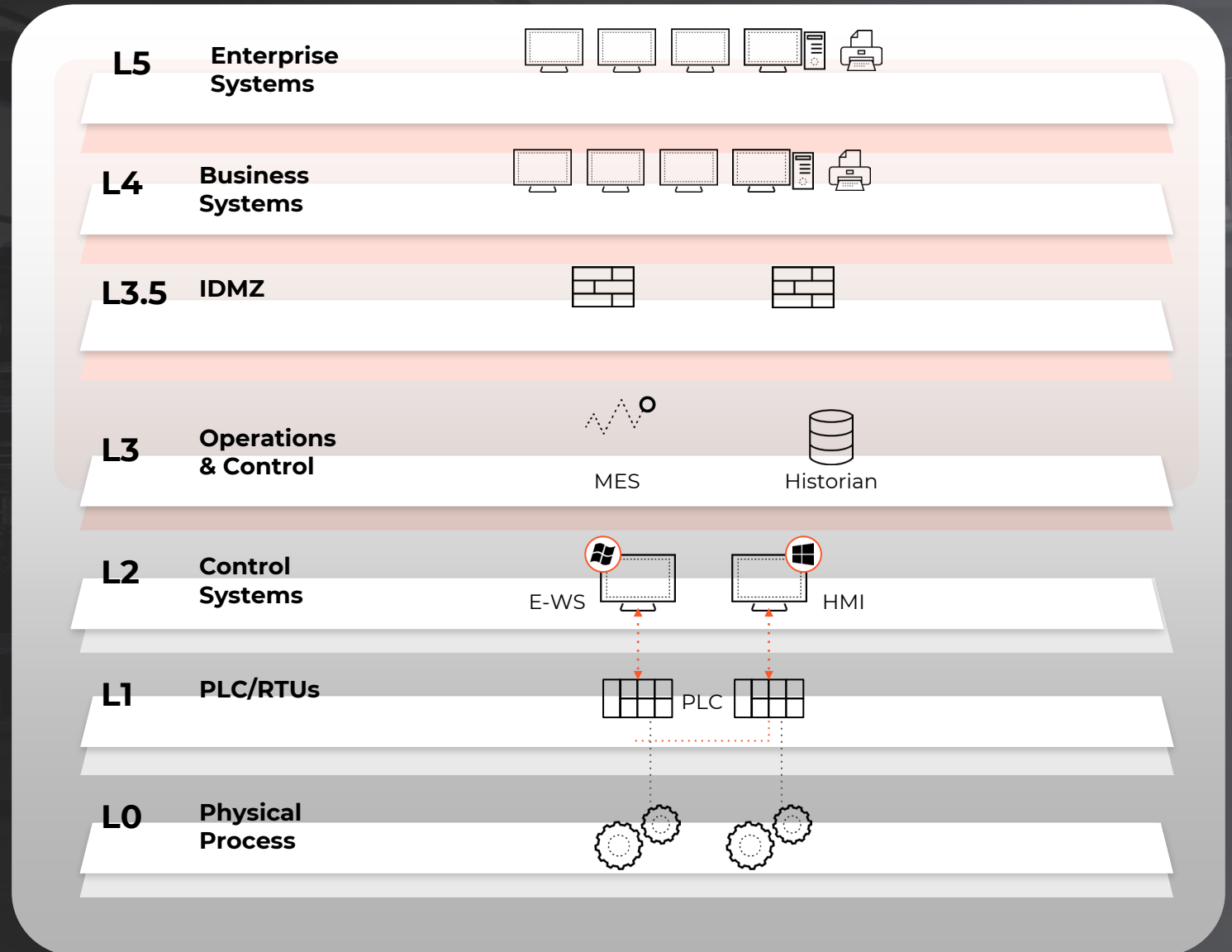
Data Source and Methodology

Data collected from 10 k industrial companies across 50 countries over the past three years:

- Threat Prevention logs in Cortex Data Lake (CDL)
 - Out of a total of 578 million malicious sessions, over 129 million were associated with OT/ICS industries.
- *Malware samples and session by Advanced WildFire*
 - Over 147 million malicious samples from different regions, including the United States, Singapore, Japan, Australia, and the European Union, were inspected and analyzed for this study.

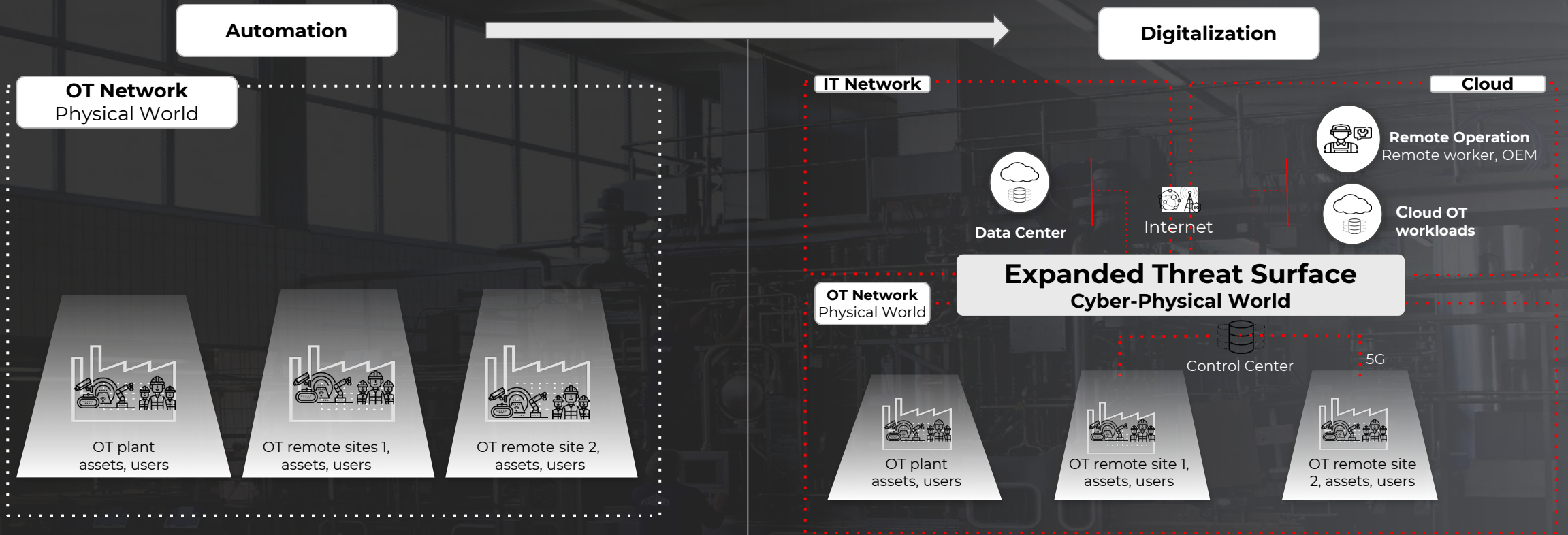
Data Source and Methodology

Based on both Unit 42's data and dark web leak site data, the manufacturing industry was the most impacted by extortion attacks in 2022.



Holistic Overview of threats in Manufacturing Industry

From 3.0 to 4.0 framework



BEFORE

- Siloed operations with isolated networks
- Little connectivity between plants, remote sites, with control centers, IT, cloud and internet

NOW

- **IT/OT convergence and cloud connectivity** - Legacy & new OT assets connecting to IT & cloud. 400% expected increase in manufacturing
- **5G connects new types of assets** - 15B 5G industrial assets by 2026
- **Remote operation is on the rise** - 70% of the ICS/SCADA assets have external connections

Overview on OT Threat Landscape

Malware observed in OT/ICS industries grew rapidly.

- An increase of 27.5% in the ratio of OT/ICS malware over all sessions
- The average number of attacks per customer increased by 238% over the last year

Exploit attacks against the OT/ICS industries tripled.

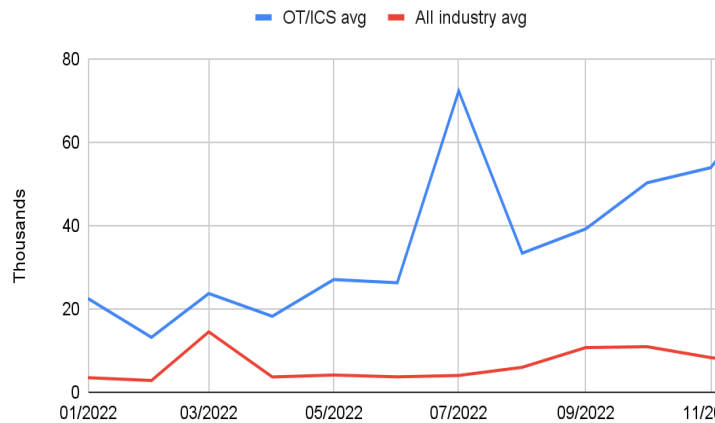
- Monthly average attacks per customer for OT/ICS industry increased from 22,000 to 72,000 during the last year.
- The average number of exploits targeting the OT/ICS industry surpassed the average for all other industries in both quantity in general and its growth trend.

Compromised devices in the OT/ICS industry increased

- Observed increment by 81% in 2022,
- and 23.2% of these incidents weren't promptly handled within one week, with a median recovery time of one hour.

Threats Surrounding OT Network Perimeters

OT/ICS Industries vs. All Industries

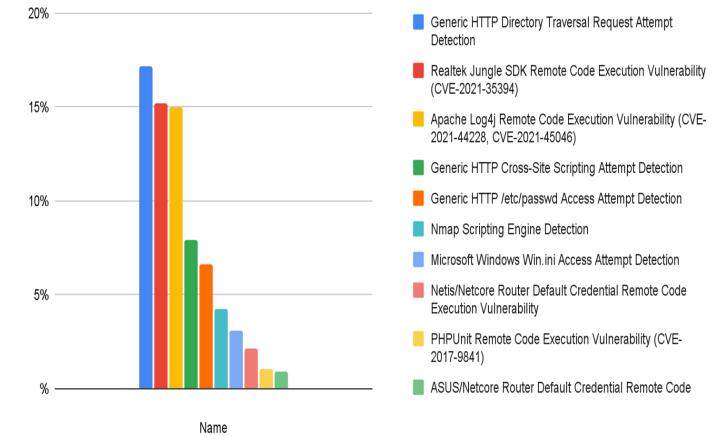


OT organizations face 3x as many threats as other organizations

Year	Malware Sessions	Per Customer
2021	31 million	816
2022	115 million	2759

The average attack detected per customer in OT organizations increased exponentially in one year

Top Exploits Identified in 2022



Based on the top 10 exploits we detected, the most targeted vulnerabilities and threats are:
Supply Chain
Remote Access
Lateral movement



OT/ICS Malware Threat Overview

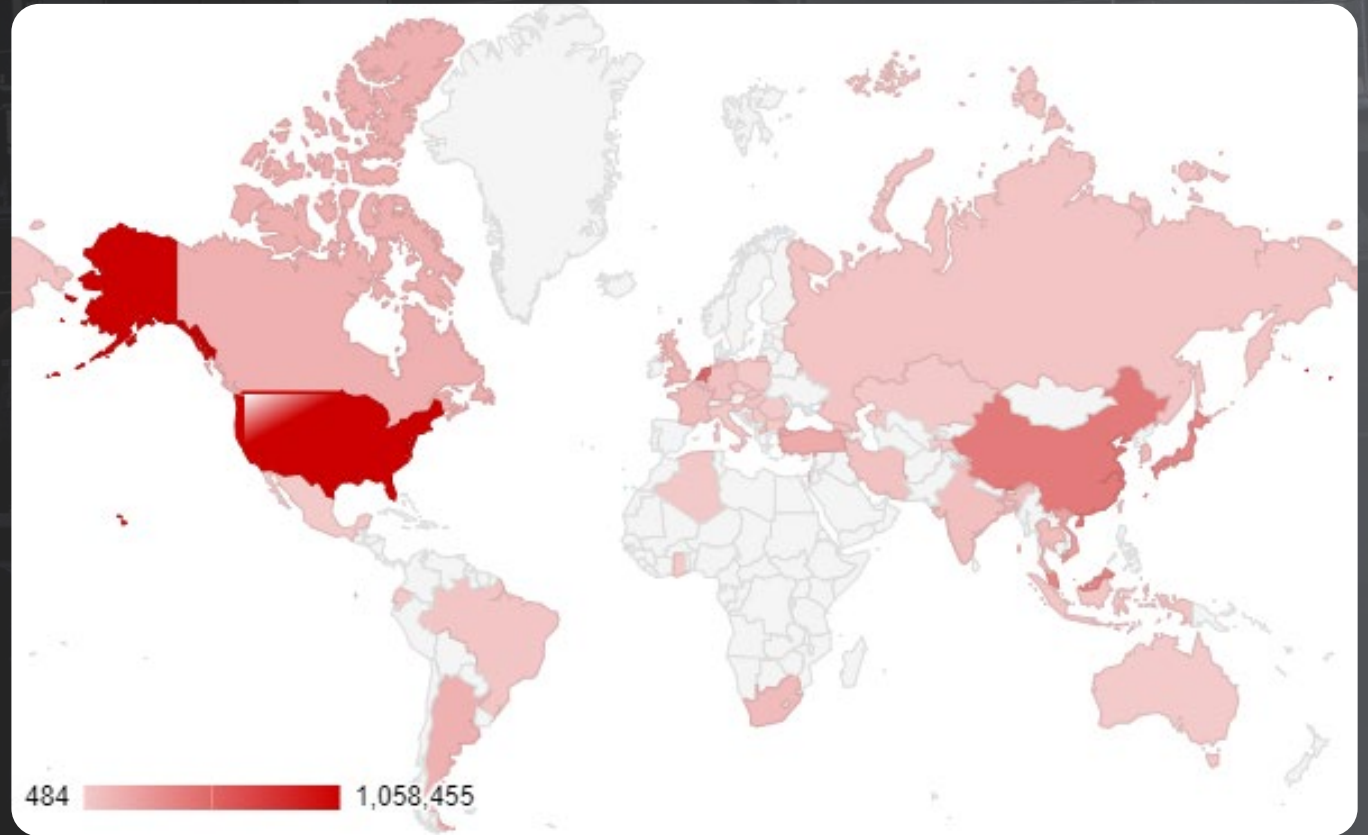
A Rising Tide of Threats - 238% increases

- Using malware sessions to represent attack attempts, each customer had an average number of 2,759 attacks detected in 2022.
- This represents an increase of 238% from the average of 816 in 2021.

Year	Malware Sessions	Malicious Ratio	Per Customer
2021	31 million	0.8%	816
2022	115 million	1.02%	2759

Malware source geolocation distribution within ICS industries.

According to our data, the United States has the highest number of reported malware incidents, with over 1 million cases, followed by China with over 400,000 cases, and Japan with over 350,000 cases.



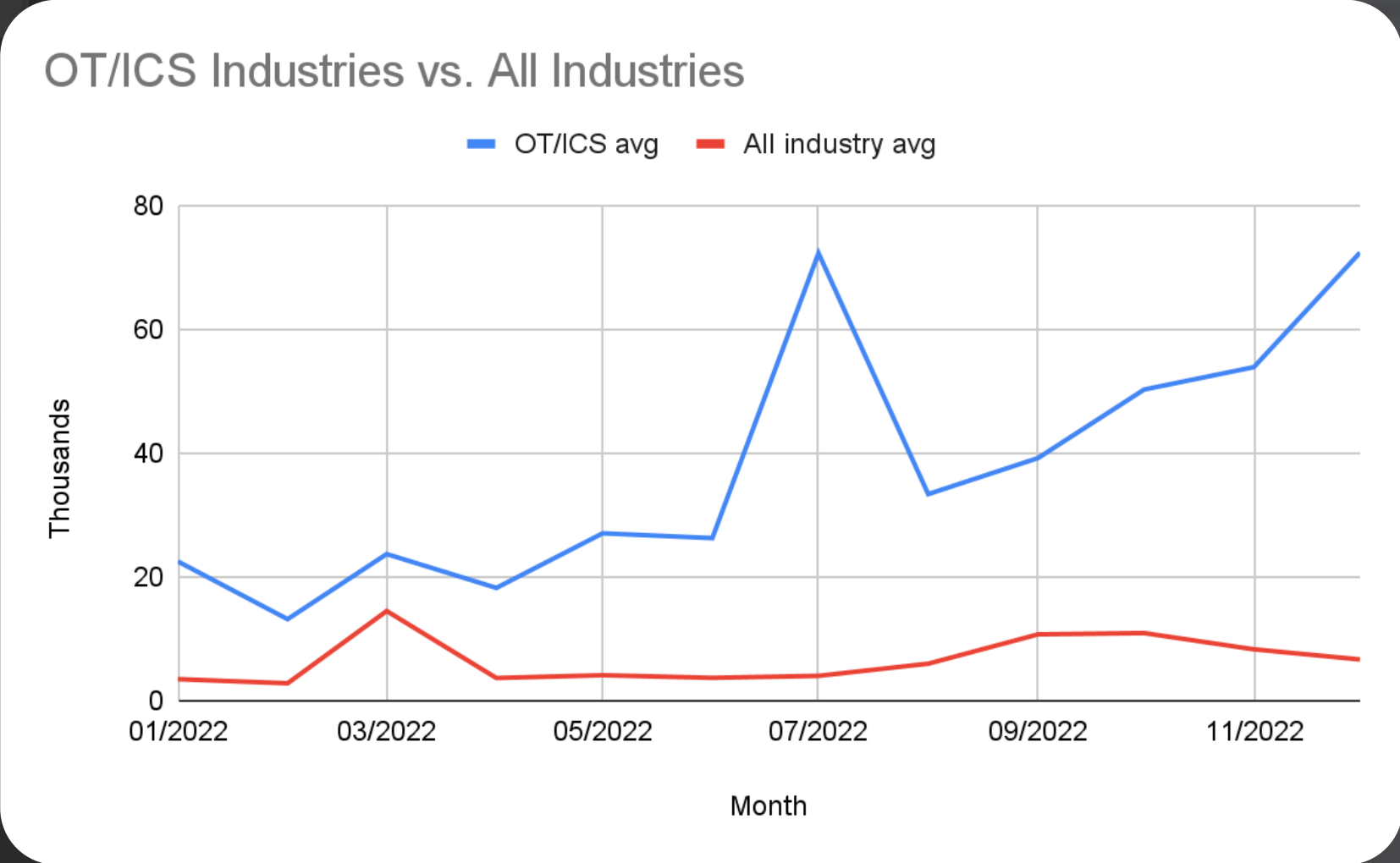
Targeted and Non-targeted Malware Threat

- Out of the 4.6 million samples that targeted the OT/ICS industry fewer than 700 samples were ICS-centric.
- These include 221 MiniFlame, 108 LockerGoga, 96 KillDisk, 68 Disttrack, 63 GreyEnergy, 43 Industroyer, plus 19 Destover, and their variations.



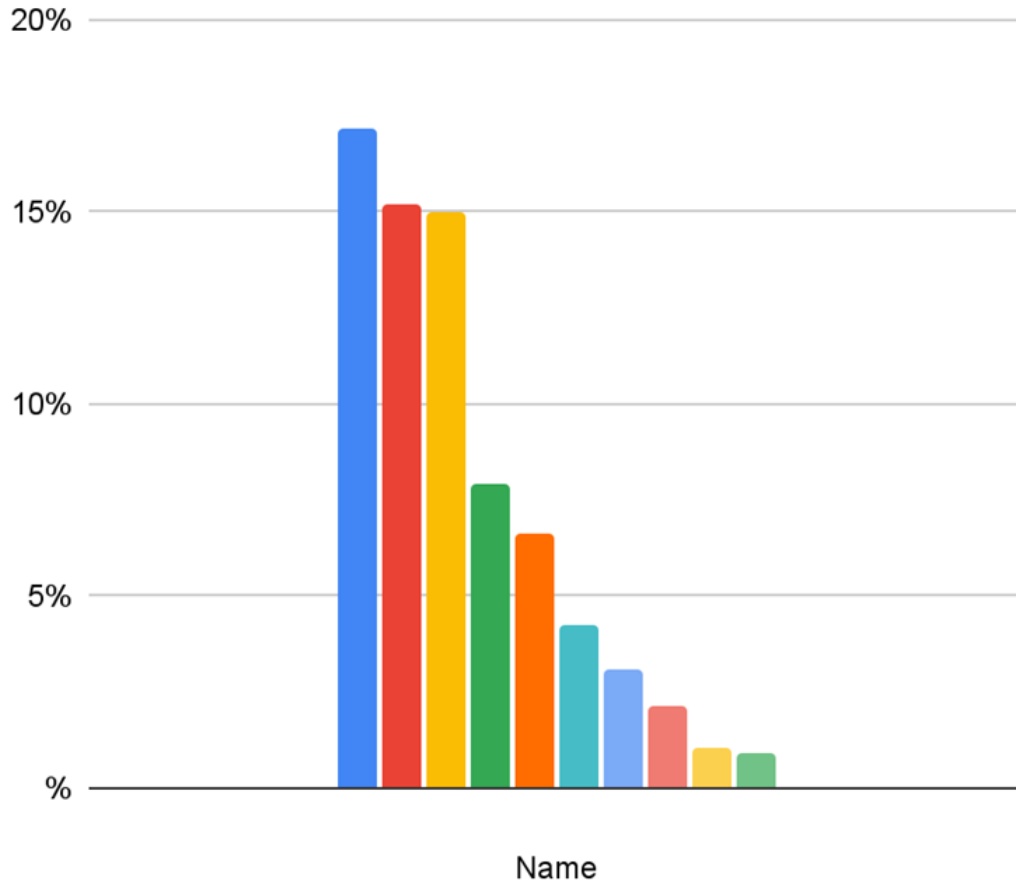
Exploits Observed Against the OT/ICS Industries

Exploits Observed Against the OT/ICS Industries



Top Exploits

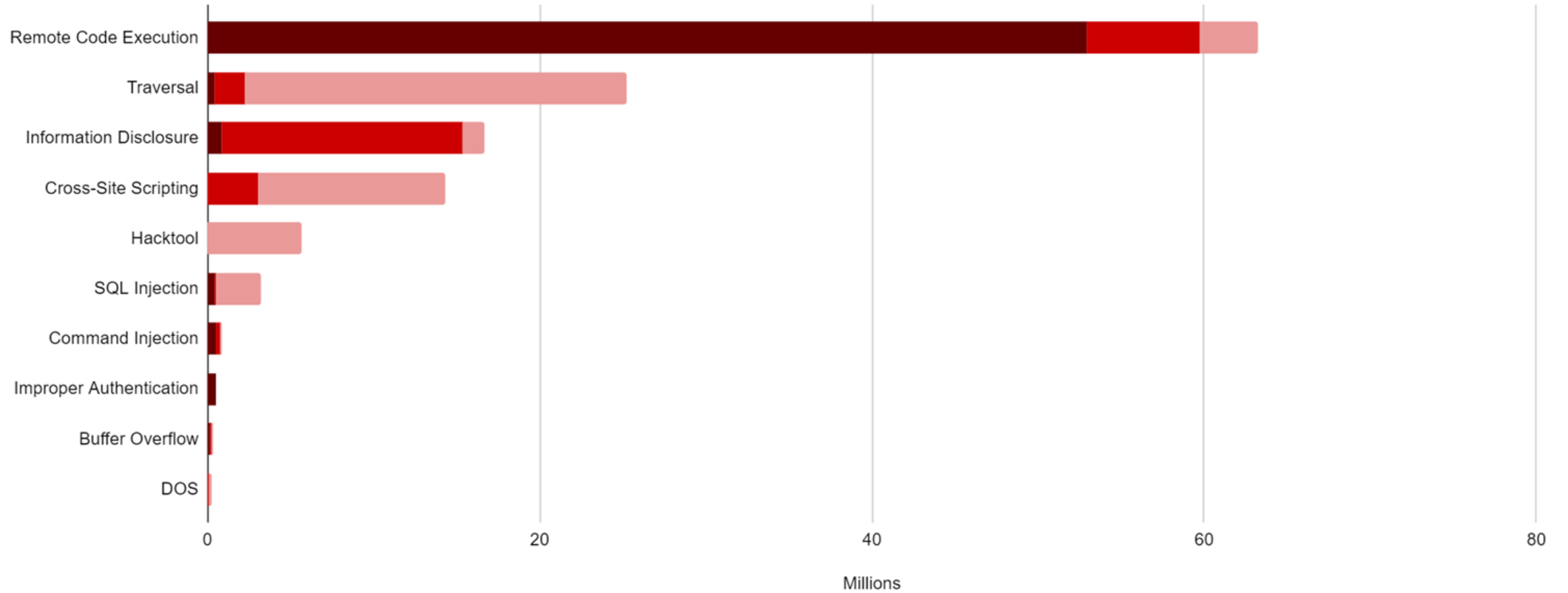
Top Exploits Identified in 2022



- Generic HTTP Directory Traversal Request Attempt Detection
- Realtek Jungle SDK Remote Code Execution Vulnerability (CVE-2021-35394)
- Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228, CVE-2021-45046)
- Generic HTTP Cross-Site Scripting Attempt Detection
- Generic HTTP /etc/passwd Access Attempt Detection
- Nmap Scripting Engine Detection
- Microsoft Windows Win.ini Access Attempt Detection
- Netis/Netcore Router Default Credential Remote Code Execution Vulnerability
- PHPUnit Remote Code Execution Vulnerability (CVE-2017-9841)
- ASUS/Netcore Router Default Credential Remote Code

Attack Category

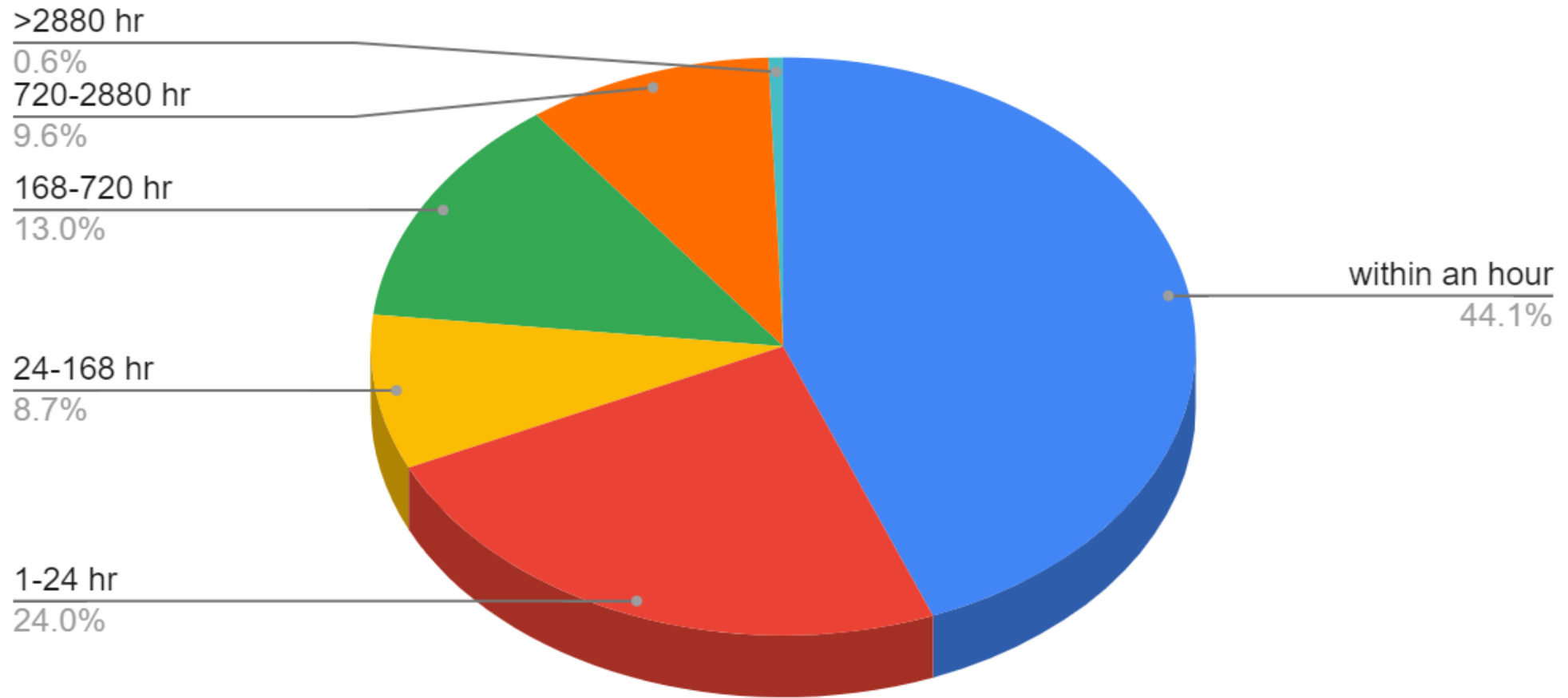
■ Critical ■ High ■ Medium





Compromised Devices in the OT/ICS Industries

2022 Recover Time of Compromised Devices





Three Steps to a Comprehensive Solution

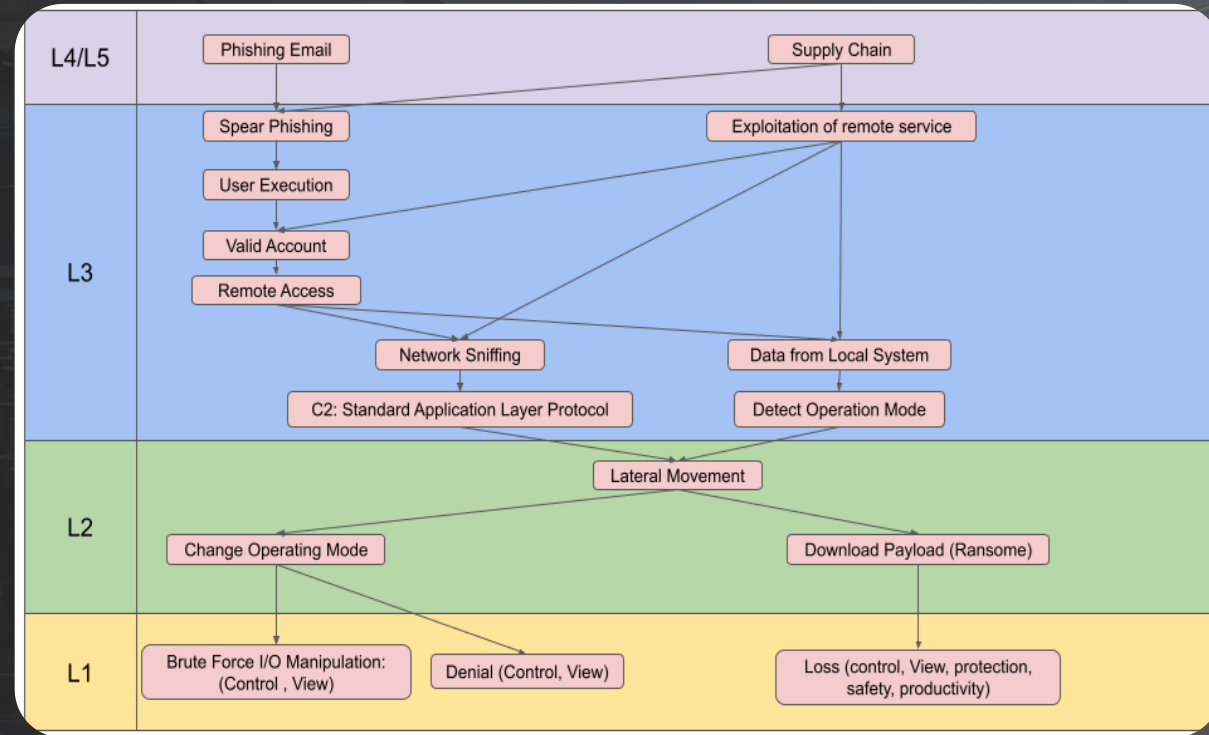
Three Steps to a Comprehensive Solution

Asset Identification	Threat Levels	Defense Levels
Group A: Critical	Advanced	Level 3: Group A
Group B: High	Medium	Level 2: Group A and B
Group C: Low	Simple	Level 1: Group A, B, and C

Threat Analysis

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Scripting	Valid Accounts	Exploitation for Privilege Escalation	Change Operating Mode	Remote System Information Discovery	Remote Services	Program Upload	Standard Application Layer Protocol	Data Destruction	Modify Parameter	Loss of Productivity and Revenue
Remote Services	Change Operating Mode	Hardcoded Credentials	Hooking	Exploitation for Evasion	Valid Accounts	Detect Operating Mode	Commonly Used Port	Activate Firmware Update Mode	System Firmware	Unauthorized Command Message	Loss of Safety
Supply Chain Compromise	User Execution	System Firmware		Indicator Removal on Host	Network Sniffing	Lateral Tool Transfer	Connection Proxy	Alarm Suppression		Brute Force I/O	Damage to Property
Spearphishing Attachment	Execution through API	Modify Program		Masquerading	Remote System Discovery	Program Download	Screen Capture	Block Command Message		Module Firmware	Denial of Control
Exploitation of Remote Services	Hooking	Module Firmware		Rootkit	Network Connection Enumeration	Exploitation of Remote Services	Adversary-in-the-Middle	Block Reporting Message		Spoof Reporting Message	Denial of View
Exploit Public-Facing Application	Modify Controller Tasking	Project File Infection		Spoof Reporting Message	Wireless Sniffing	Hardcoded Credentials	Automated Collection	Block Serial COM			Loss of Availability
External Remote Services	Native API					Default Credentials	Data from Information Repositories	Change Credential			Loss of Control
Internet Accessible Device	Command-Line Interface						Data from Local System	Denial of Service			Loss of Protection
Replication Through Removable	Graphical User Interface						I/O Image	Device Restart/Shutdown			Loss of View
							Monitor	Manipulate I/O Image			Manipulation of Control
								Modify Alarm			Manipulation of View

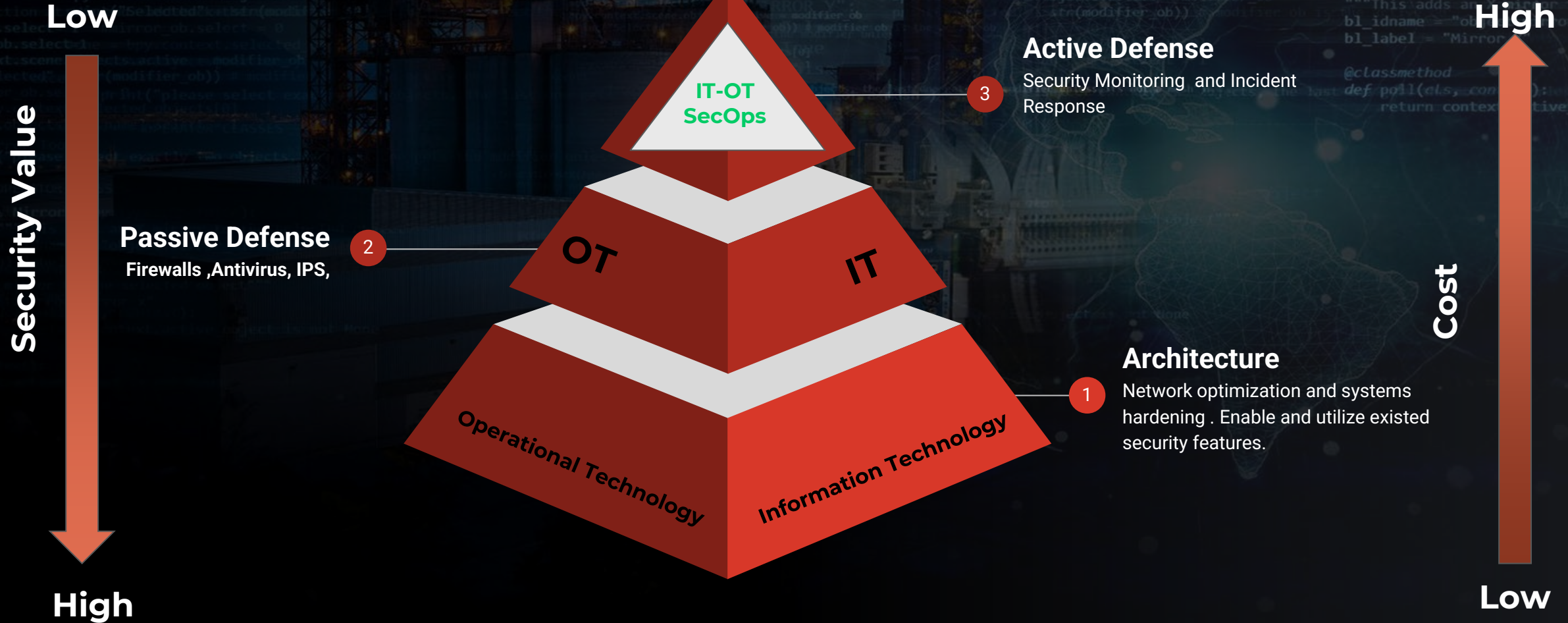
Threat Heat Map



Attack Tree

Security Monitoring & Incident Response Challenges

IT-OT technology convergence VS IT-OT security convergence



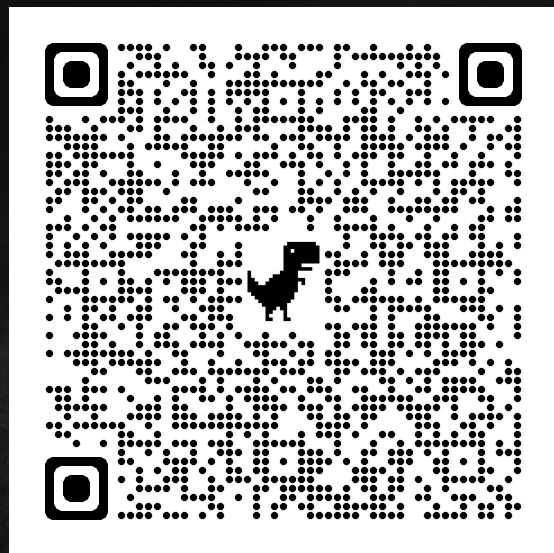
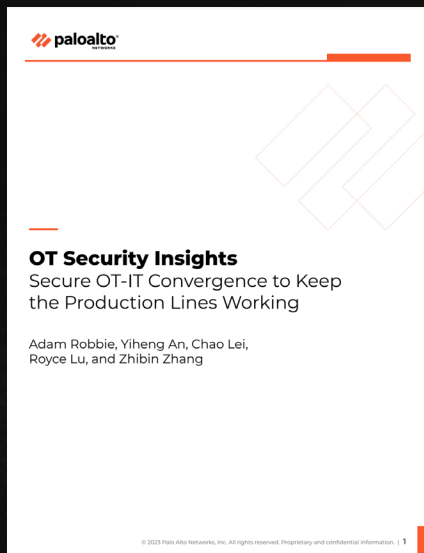


Thank you.



Questions?

Download Unit 42 OT white paper and research study



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 and Partnership, please contact melissacromack@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
(20)**

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

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

BENEFACTOR

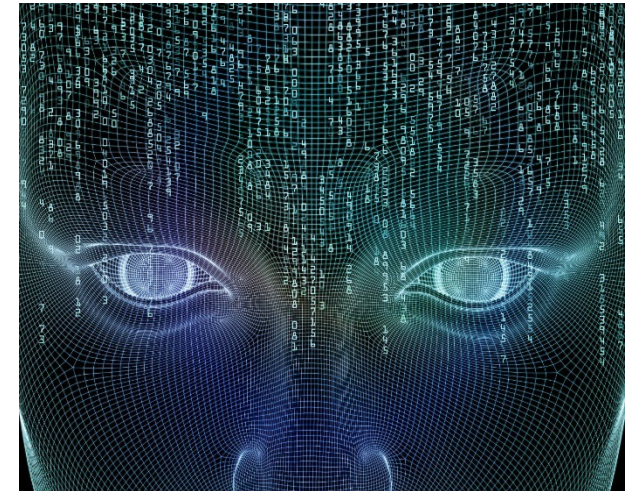
**Sponsorship
Partnership**

2022 Summit Sponsors-

Argus
BGNetworks
Bosch
Blackberry
Block Harbor
BlueVoyant
Booz Allen Hamilton
C2A
Cybellum
CyberGRX
Cyware
Deloitte
Denso
Finite State
Fortress
Itemis
Keysight Technologies
Micron
NXP
Okta
Sandia
Securonix
Tanium
UL
Upstream
VicOne

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 Northwest
Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com



AUTOMOTIVEISAC.COM