



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

August 7, 2024

This Session will be recorded.






This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR



TRAFFIC LIGHT PROTOCOL (TLP)

VERSION 2.0 DEFINITIONS

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<div><div>TLP:RED</div><div></div></div> <div>Not for disclosure, restricted to participants only.</div>	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.	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.
<div><div>TLP:AMBER+STRICT</div><div></div></div> <div>Limited disclosure, restricted to participants' and its organization.</div>	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.	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.
<div><div>TLP:AMBER</div><div></div></div> <div>Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.</div>	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.	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.
<div><div>TLP:GREEN</div><div></div></div> <div>Limited disclosure, restricted to the community.</div>	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	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.
<div><div>TLP:CLEAR</div><div></div></div> <div>Disclosure is not limited.</div>	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.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

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">➤ Trevor Parks, Joint Cyber Defense Collaborative (JCDC)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Dr. Anirban Banerjee, CEO and Co-founder, Riscosity➤ Title: The state of data and privacy risks in the automotive industry
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: Slides are at **TLP:CLEAR** and on our [website](#). Discussions are **TLP:GREEN** & may be shared across Auto-ISAC Community, “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! *“Cybersecurity is a Team Sport!”*

32
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

48 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)

2024 BOARD OF DIRECTORS

Thank you for your Leadership!



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



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



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



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



Oliver Creighton
Chair of the EuSC
BMW



Andrew Hillery
Chair of the CAG
Cummins



Amine Taleb
Chair of the SAG
Harman



Maryann Combs
Polaris



Bob Kaster
Bosch



Brian Witten
Aptiv

AUTO-ISAC MEMBER ROSTER

AS OF AUGUST 1, 2024

Highlight = New Active Members

80 MEMBERS + 1 PENDING

Aisin	Ferrari	Luminar	Renesas Electronics
Allison Transmission	Flex	Magna	Rivian
Amazon	Ford	MARELLI	SiFive, Inc.
American Axle & Manufacturing	General Motors	Mazda	Stellantis
Aptiv	Geotab	Mercedes-Benz	Stoneridge
AVL List GmbH	Harman	Mitsubishi Electric	Subaru
BMW Group	Hitachi (Astemo - Affiliate)	Mitsubishi Motors	Sumitomo Electric
BorgWarner	Honda	Mobis	thyssenkrupp
Bosch (ETAS - Affiliate)	Hyundai	Motional	Tokai Rika
Bose Automotive	IAV GmbH	Navistar	Toyota (Woven - Affiliate)
ChargePoint	Infineon	Nexteer Automotive Corp	Valeo
CNH Industrial	Intel	Nissan	Veoneer
Continental (Elektrobit - Affiliate)	Jaguar Land Rover	NXP	Vitesco
Cummins	JTEKT	Oshkosh Corp	Volkswagen (Cariad - Affiliate)
Daimler Truck	Kia America, Inc.	PACCAR	Volvo Cars
Dana Inc.	Knorr Bremse	Panasonic (Ficosa - Affiliate)	Volvo Group
Deere & Company	KTM	Phinia	Waymo
Denso	Lear	Polaris	WirelessCar
e:fs TechHub GmbH	LG Electronics	Qualcomm	Yamaha Motors
Faurecia	Lucid Motors	Renault SAS	ZF

Pending: Zoox

AUTO-ISAC BUSINESS UPDATES AND EVENTS

- **Community Call:** Wednesday, September 4, 2024 **Time:** 11:00 – 12:00 p.m. ET **TLP:GREEN** **Speaker:** Chen Liu, Associate Professor, Clarkson University **Title:** “Low-Level Hardware Information Assisted Approach Towards System Security ”
- **2023 Annual Report** **TLP:CLEAR** available to Auto-ISAC Community on our [website](#).
- **Auto-ISAC** **TLP:CLEAR** **8th Annual Cybersecurity Summit** will be held October 21 – 24, 2024 in Detroit, Michigan. Agenda details and registration can be found [here!](#)
- If your organization is an **Automotive OEM, Supplier, EV, & EVSE provider**, and not a current Member of the Auto-ISAC, **chat with our team today** about [Membership!](#)
- If you **discover an incident or vulnerabilities within the Automotive industry**, please submit it via our [website](#) or [Member VDP](#).
- The Auto-ISAC Community is encouraged to review the [Automotive Threat Matrix \(ATM\)](#) created and published by the Auto-ISAC and submit any examples, new techniques, and tactics.



REVVING UP RESILIENCE: *SECURITY MEETS INNOVATION*

2024 Auto-ISAC Cybersecurity Summit

October 22-23 Detroit, MI

Titanium Sponsor

**Booz
Allen.**



AUTO-ISAC INTELLIGENCE HIGHLIGHT

RICKY BROOKS II, INTELLIGENCE OFFICER

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR



AUTO-ISAC INTELLIGENCE

➤ Know what we track daily: [subscribe](#) to the DRIVEN; Auto-ISAC 2025 Threat Assessment in production.

- **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 Israel-Hamas in crises (**Russia-Ukraine** ^{1 2 3}, **Israel-Hamas/Israel-Hezbollah** ^{4 5 6}, **Iran**, **China** ^{7 8*}, **North Korea**)
- Ransomware ^{9 10} Groups Targeting Automotive: [Arcus Media](#), [Black Basta](#), [Cactus](#), [Embargo](#), [LockBit](#), [Medusa](#), [Meow](#), [Play](#), [RansomHub](#), [Space Bears](#) (**New:** [Nevermore](#))
- **CrowdStrike Cyber Incident:**
 - Non-malicious; recent unconfirmed CrowdStrike data breach does not appear related ([Link](#))
 - CrowdStrike course corrections for software updates ([Link](#))
 - Real-world operational disruptions ([Link](#))
 - Incident response **and** continuity of operations plans are critical in case orgs' endpoints are rendered inoperable/inaccessible in mass (e.g., ransomware, faulty update, state-sponsored cyberattack).
- **No reports of malicious cyberattacks on vehicles other than tech-enabled theft and fraud; vehicle hacking research continues to be shared publicly; some road users continue to tinker with in-vehicle systems.**
- **Notable TTPs:** Hacking internet service providers to deliver malicious updates ([Link](#)); distributed denial-of-service attack on cloud provider ([Link](#)); watering hole attack coupled with supply chain attack ([Link](#)).



FEATURED SPEAKER

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR



MEET THE SPEAKER



Dr. Anirban Banerjee

Dr. Anirban Banerjee is the CEO and Co-founder of Riscosity, a data flow security platform.

Prior to founding Riscosity, he founded two security startups that exited successfully (StopTheHacker and Onion ID), authored 15 scientific papers, has 8 patents, and received 3 SBIR grants from the National Science Foundation.

Dr. Banerjee is an industry expert in security and compliance, web malware analysis and third-party



You can't protect your data if you don't know where it's going. Let us help.

Agenda For Presentation

- How the surge of supply chain attacks impact regulatory requirements & concerns for the mobile industry
- Preventing & mitigating supply chain attacks
- How to improve security and meet regulatory compliance via 3rd party data observability



**The connected car market is expected to grow by
\$246.24 billion by 2027.**



As cars and fleets become more connected, APIs are the glue that allows users and companies to track, manage, and operate their vehicles.



Carmakers are responsible for API security.

Car manufacturers must know all of the APIs within their environment and accurately have visibility into all of the API traffic transporting data back and forth through their applications.



Companies share sensitive data with 3rd parties every day

AI



Payments



Messaging



Payroll



Analytics



BaaS



Security



Data Management

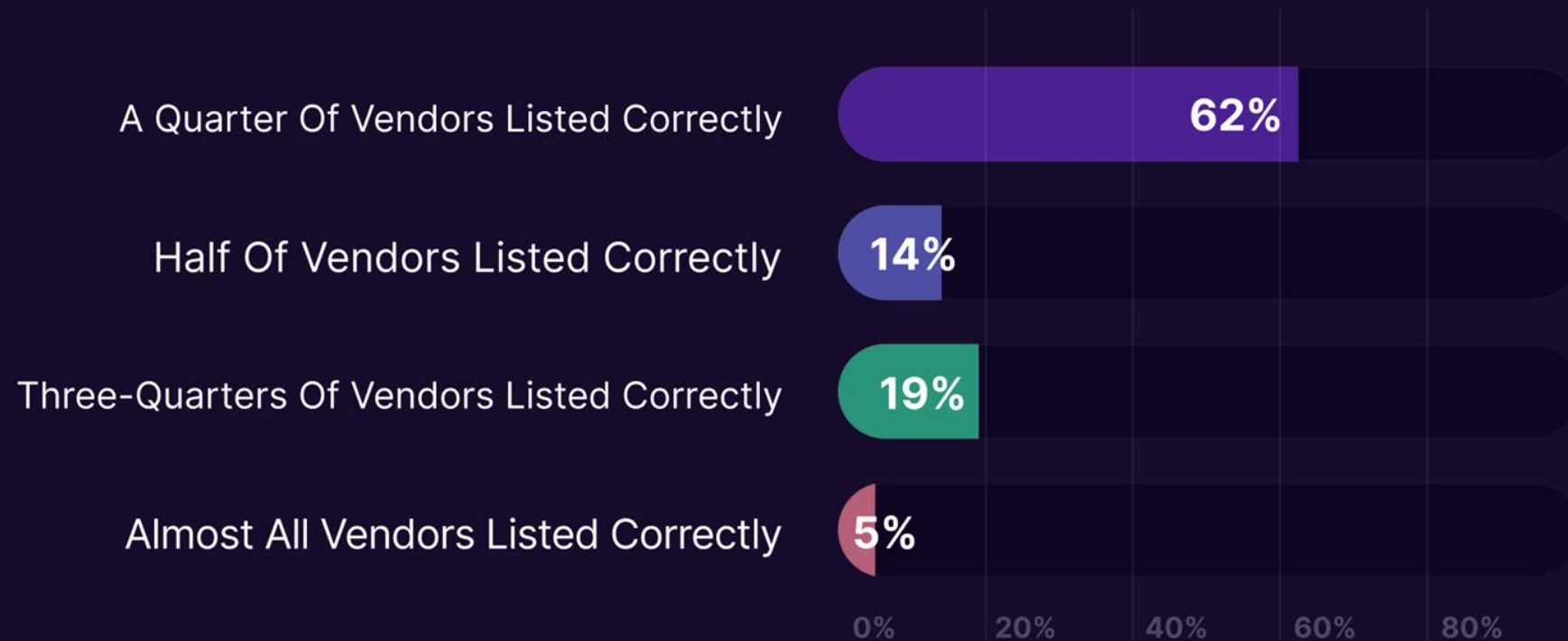


- Consider GDPR, CCPA, PIPL, DPDP Act, CPS234... etc.
- Enterprises often focus on securing their own APIs, but need visibility into data flowing to 3rd parties

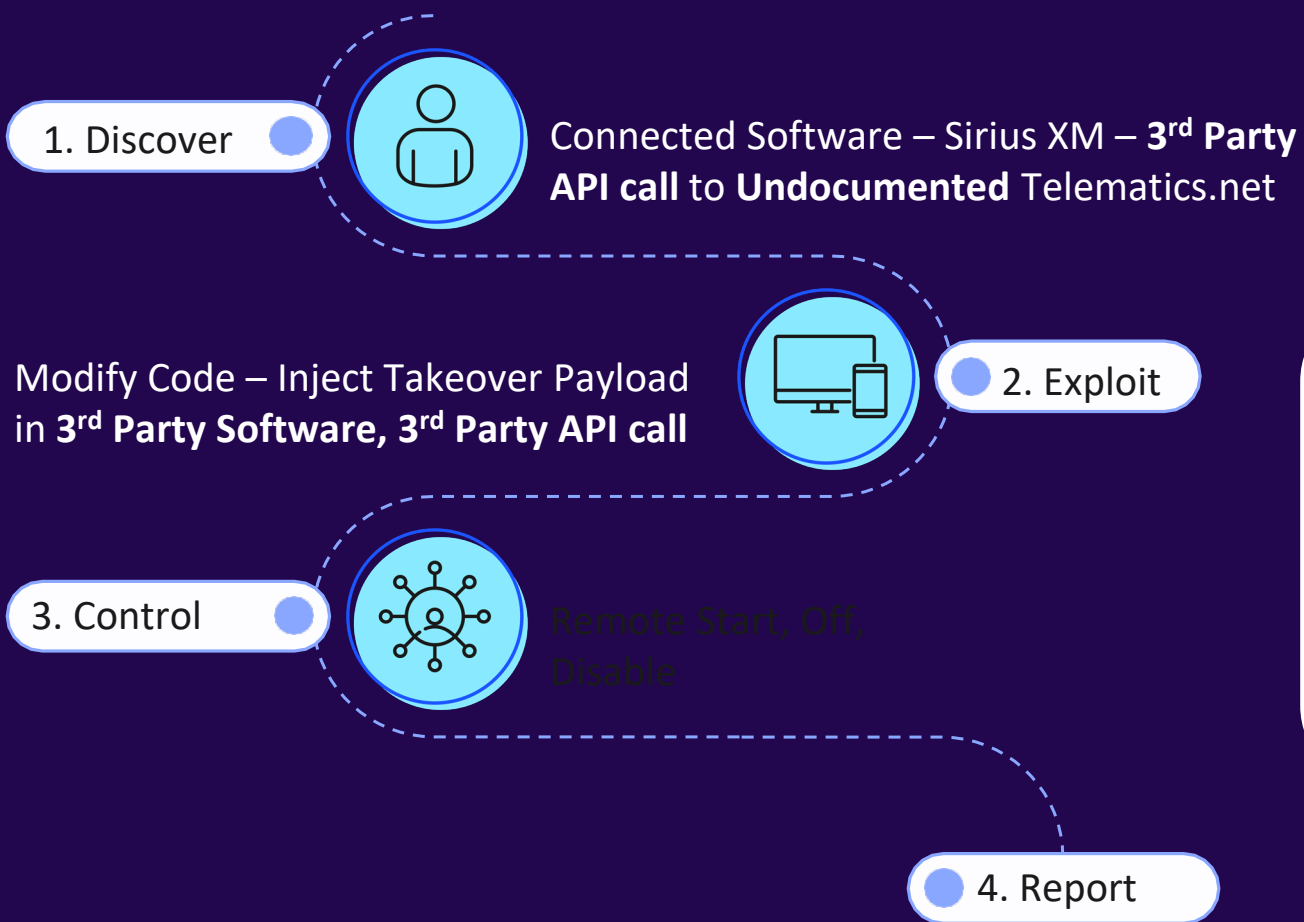


Security teams don't have control of 3rd party vendors

Over 100 Security leaders were asked to select the percentage of their software/SaaS vendors that they believed were properly listed in their procurement system. Their options were 25%, 50%, 75% or almost all vendors.



HANI ATTACK – ‘22 Honda, Acura, Nissan, and Infiniti Hack



Simplified HTTP Request

```
POST /ha/exchangeToken HTTP/2
Host: mobile.telematics.net
Cv-Tsp: NISSAN_17MY
Authorization: Bearer {JWT}

{"customerId":"nissancust:129383573", "vin":"5FNRL6H82NB044273"}
```

Simplified HTTP Response

```
HTTP/2 200 OK
Content-type: application/json

{
  "access_token":"BEARER",
  "CV-APIKey":"CLIENT-ID",
  "Expires_in":299,
  "token_type":"Bearer",
  "refresh_token":"REFRESH-TOKEN"
}
```

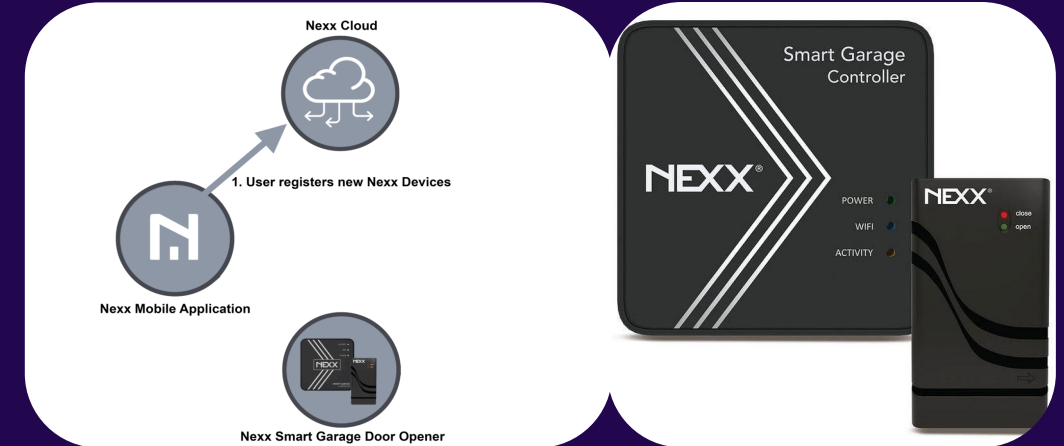


IDOR ATTACK – '23 Garage Door Openers

1. Discover



Connected Software – NexxCloud–API call with cleartext credentials



Modify Code – Inject Takeover Payload in API call



2. Exploit

3. Control



Open/Close Garage door – for anyone

4. Report

```
"statusCode":200,
"Status":0,
"Result":[
{
  "DeviceType":"NexxGarage",
  "ProductCode":"NGX-100",
  "DeviceName":"NexxGarage",
  "DeviceImageUrl":
  "https://nexx-domain.simpaltek.com/Products/NGX-100.png",
  "DeviceInfoUrl": "",
  "DeviceDescription":"NexxGarage 100",
  "DeviceConfig":
  {
    "mqtt":{"host":"","port":443,"use
    rname":"sptmqttadmin","password":"","
    ssl":true,"base_topic":"devices/","auth":true,"finge
    rprint":""},
    "ota":{"host":"","port":80,"path":"/ota","enabled":true},"accountId":"","
    "accessToken":""
  }
},
"ComingSoon":false,
"ReleaseFirmwareVersion":"0",
"ReleaseFirmwareDownloadPath":null,
"ProductNameHtml":null,
"DeviceId":null,
"Model":null,
"ActivityTimeStamp":null
}
```



CAN INJECTION – ‘23 Toyota Hack

1. Discover



CAN bus controller assumes fault when DTC floods the wires and gets physical access to bus.

While Controller resets flood Key.Auth OK messages.



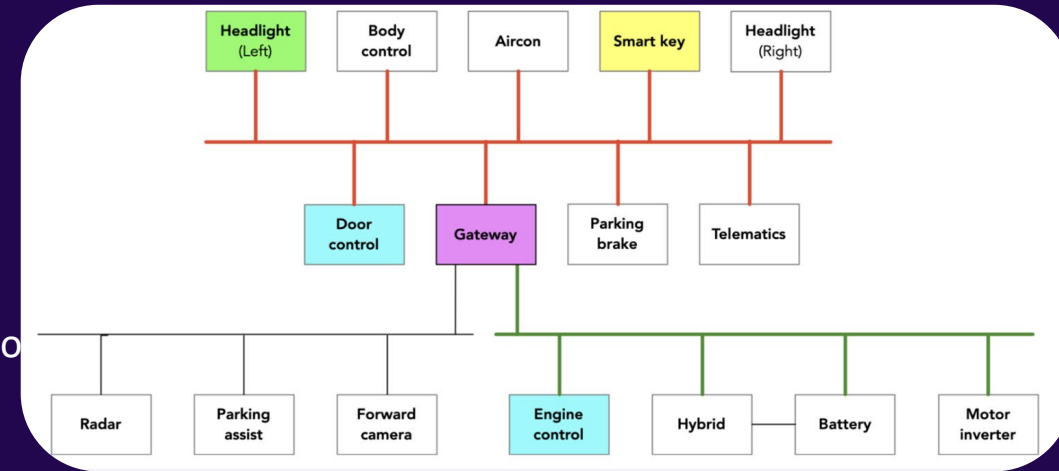
2. Exploit

3. Control



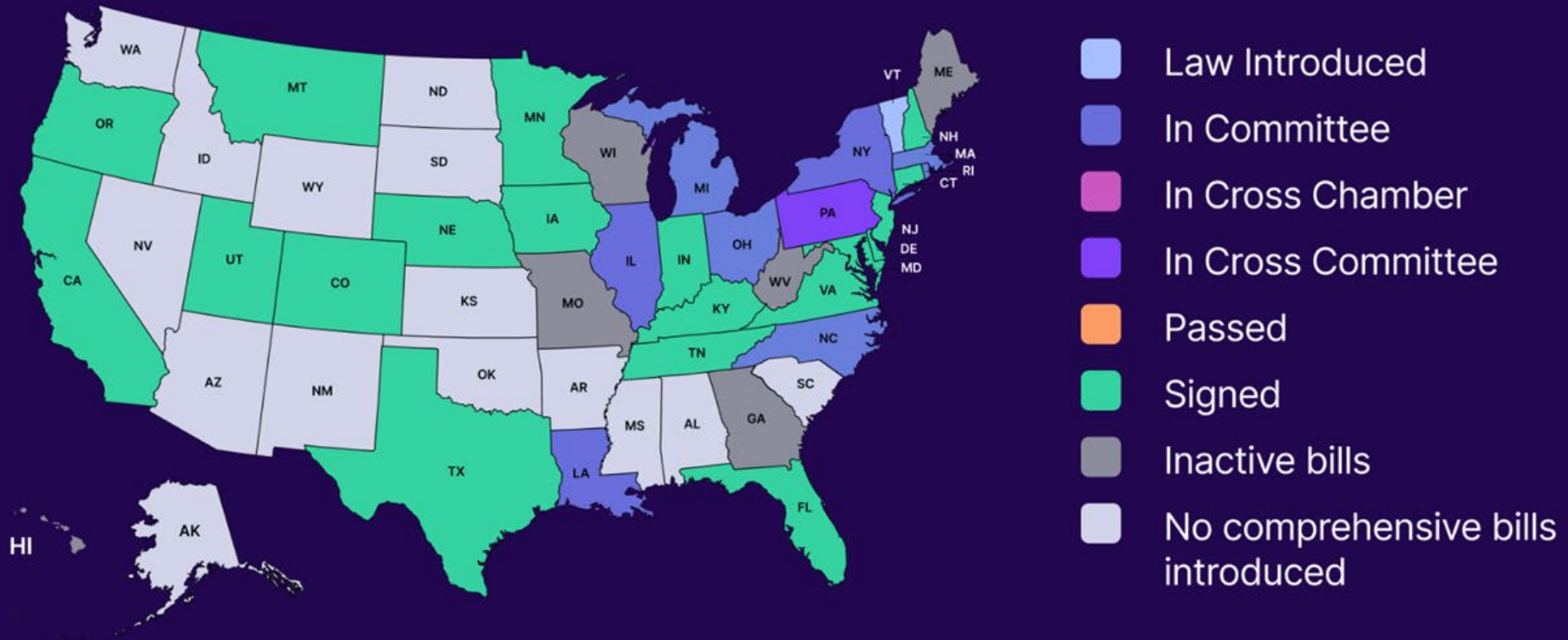
Drive away

4. Report



Status of U.S. Data Protection | Legislation by State

Last update: July 2024



The Solution



Data Flow Posture Management (DFPM)

DFPM solutions provide the tools needed to automate and centralize the identification, classification, and remediation of security risks across code, environments, and services. With a DFPM platform teams confidently gain:

1. **Real-time visibility of all 3rd parties receiving data**
2. **Real-time visibility of the data being shared with each 3rd party**
3. **Automated control of the data being shared with each 3rd party**



DFPM Maturity Phases

Gain a full picture of where data flows, with the control to redact, restrict, and redirect.

Crawl



- Scan code
- identify all data flows (read-only access)

Walk



- Scan traffic
- Validate data flow endpoints in DNS logs (read-only access)

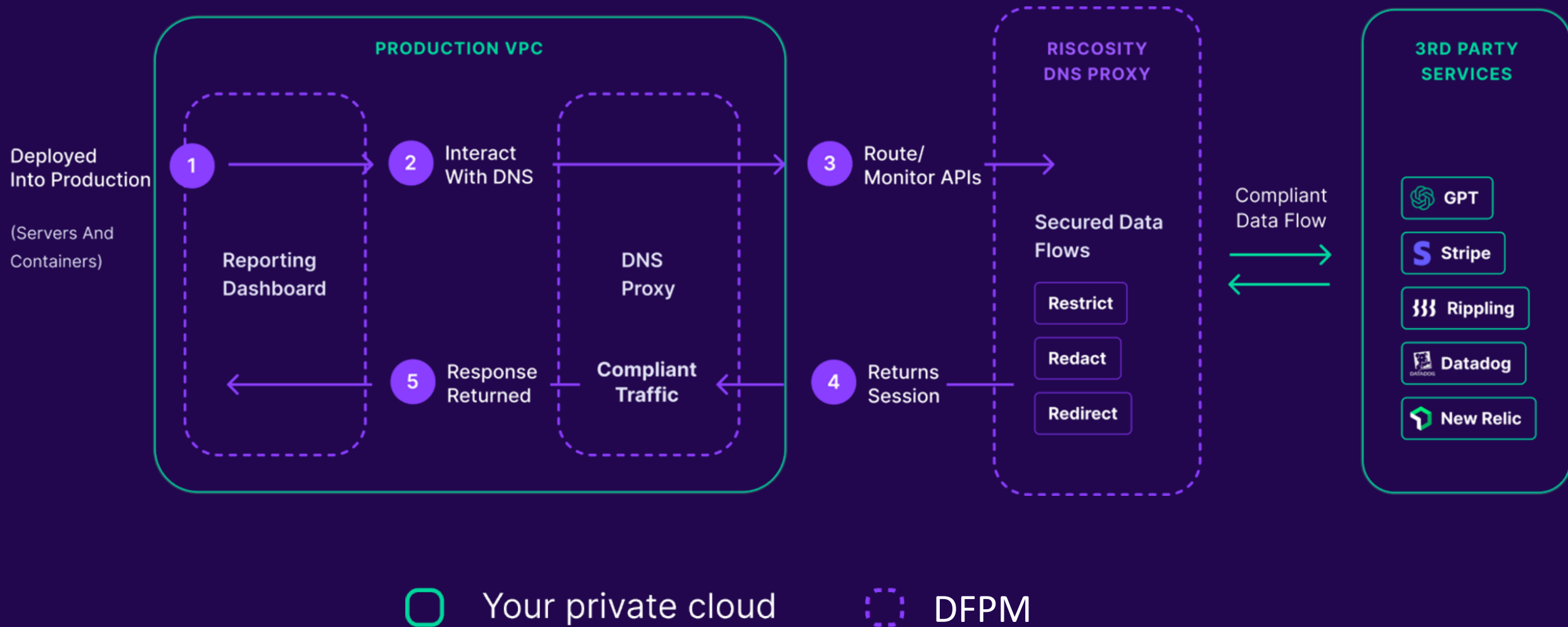
Run



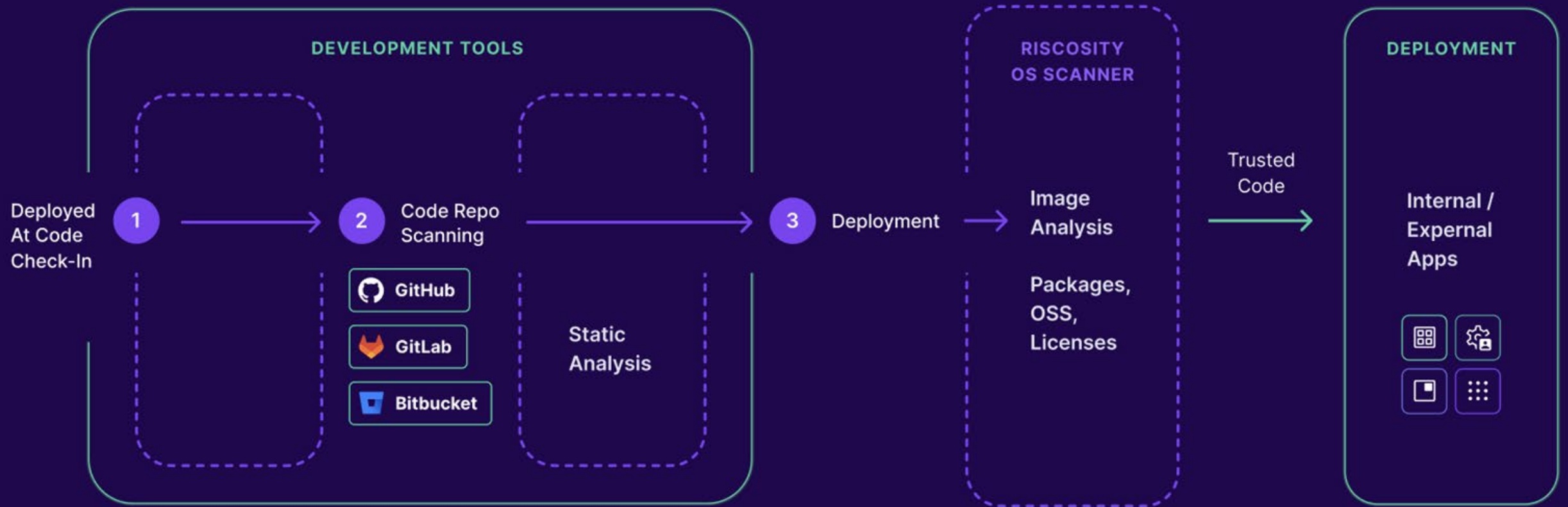
- Secure Data Flows
- Layer in active data governance
 - Implement GRC policies
 - Comprehensive cataloging
 - Privacy by design



DFPM - Network Layer Deployment



DFPM - Shift Left Deployment



Thank you!



OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE
TOPICS FOR DISCUSSION?*

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

