



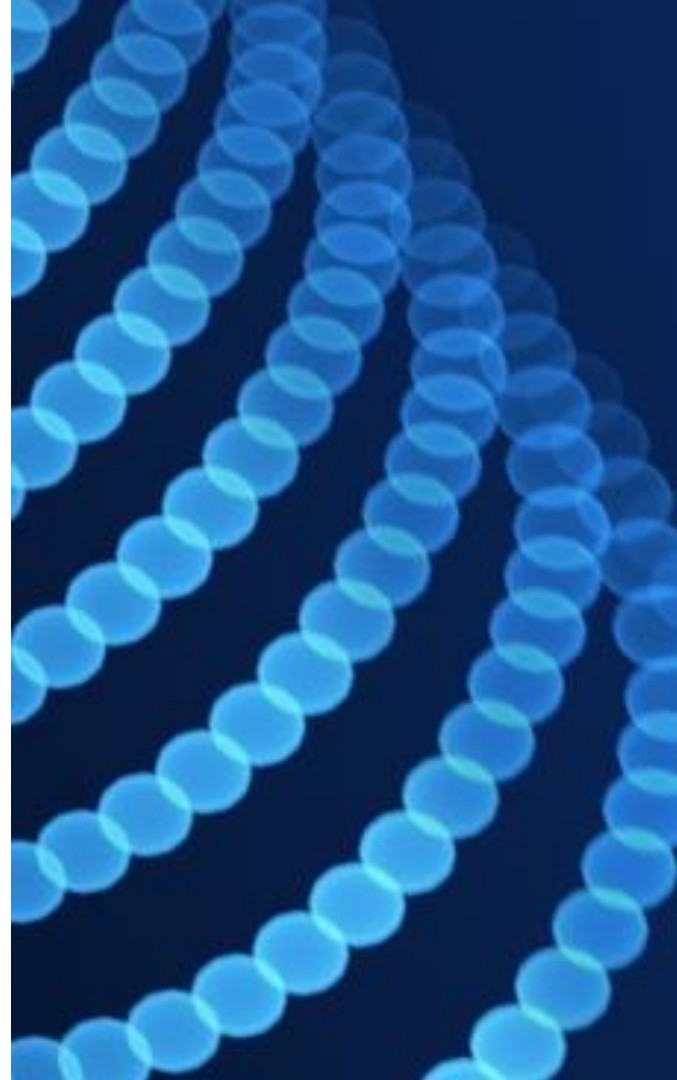
# Supply Chain Security – an Evolution

Uptane Workshop  
3/31/2023

# Discussion

---

- IR example
- GM supply chain security viewpoints
- New approach





# History: Incident Response Circa 2015

## IR Program Creation (2015)

- ▶ Build **resources** for role familiarity
  - Who does what?
- ▶ Develop **plans** for consistent execution
  - How do I do it?
- ▶ Conduct **exercises**
  - Enhance role familiarity
  - Enhance IR enterprise awareness
  - Stress-test plans

Incident Response Roles	
<b>Incident Response (IR) Lead</b>	The IR Lead coordinates GM-wide response, works across all teams, serves as the single "voice" of incident response, and is accountable for response activities.
<b>Incident Coordinator</b>	The Incident Coordinator coordinates response team actions and logistics. Manages an Incident Log, facilitates status update meetings, leads development of an after action report.
<b>Initial Assessment Team</b>	The Assessment Team provides situational awareness of incidents. <ul style="list-style-type: none"> <li>• Conducts initial analysis to understand and scope an incident after it has been detected (e.g. impact, attack vector, timeframe)</li> <li>• Small core team</li> </ul> The Initial Assessment Team is led by the Assessment Lead who oversees cross-functional engagement for the initial assessment.
<b>Business Response Team (BRT)</b>	The BRT works to contain business risk posed by the incident. <ul style="list-style-type: none"> <li>• Coordinates business response process with technical activities</li> <li>• Provides access to capabilities and resources across GM</li> <li>• Includes senior leaders from response-relevant organizations</li> </ul> The BRT is led by a Business Lead, who reports to the IR Lead, and is the central POC for business response activities.
<b>Technical Response Team (TRT)</b>	The TRT identifies the root cause and monitors the incident, and implements technical solutions to contain the incident. <ul style="list-style-type: none"> <li>• Conducts root cause analysis</li> <li>• Continuously monitors the incident</li> <li>• Identifies, builds and implements solutions to address the threat</li> <li>• Includes expertise from response-relevant technical organizations</li> </ul> Depending on the scope and impact, there may be multiple workstreams within the TRT. The TRT is led by a Technical Lead, who oversees the workstreams, and is the central POC for technical response activities.

**PRODUCT CYBERSECURITY INITIAL ASSESSMENT STATUS UPDATE**

Incident Name: \_\_\_\_\_ Incident Type: \_\_\_\_\_ Priority: Enter Select  
 Incident Manager: \_\_\_\_\_ @ Email: \_\_\_\_\_ @ Email  
 @ Email: \_\_\_\_\_ @ Email: \_\_\_\_\_ @ Email: \_\_\_\_\_ @ Email: \_\_\_\_\_

Date: \_\_\_\_\_ Time: \_\_\_\_\_

Classification: \_\_\_\_\_

Impact: \_\_\_\_\_

System: \_\_\_\_\_

Severity: \_\_\_\_\_

Business Impact: \_\_\_\_\_

Technical Impact: \_\_\_\_\_

Operational Impact: \_\_\_\_\_

Reputation Impact: \_\_\_\_\_

Legal Impact: \_\_\_\_\_

Financial Impact: \_\_\_\_\_

Other Impact: \_\_\_\_\_

Overall Status: \_\_\_\_\_

Initial Assessment Status: \_\_\_\_\_

Business Response Status: \_\_\_\_\_

Technical Response Status: \_\_\_\_\_

Resolution Status: \_\_\_\_\_

After Action Review Status: \_\_\_\_\_

Incident Log Status: \_\_\_\_\_

Incident Report Status: \_\_\_\_\_

Incident Review Status: \_\_\_\_\_

Incident Closure Status: \_\_\_\_\_

Incident Escalation Status: \_\_\_\_\_

Incident Escalation Reason: \_\_\_\_\_

Incident Escalation Action: \_\_\_\_\_

Incident Escalation Date: \_\_\_\_\_

Incident Escalation Time: \_\_\_\_\_

Incident Escalation Location: \_\_\_\_\_

Incident Escalation Contact: \_\_\_\_\_

Incident Escalation Status: \_\_\_\_\_

Incident Escalation Reason: \_\_\_\_\_

Incident Escalation Action: \_\_\_\_\_

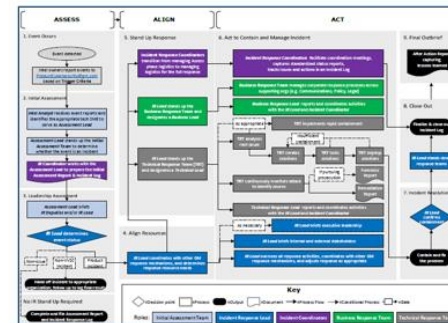
Incident Escalation Date: \_\_\_\_\_

Incident Escalation Time: \_\_\_\_\_

Incident Escalation Location: \_\_\_\_\_

Incident Escalation Contact: \_\_\_\_\_

Incident Escalation Status: \_\_\_\_\_





# History: Incident Response Circa 2015

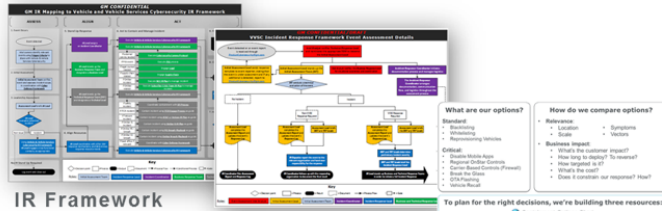
## PROCESS MAKES PERFECT...OR DOES IT?



**IR Plan** defines and documents GM approach to incident response

**Capability Roadmap and Exercise Program Plan** provides plan to mature GM IR capabilities

### Resources



**IR Framework** outlines how GM deals with IR across the enterprise

**Event Assessment Flowchart** shows how to determine if an issue is a cyber event

**Containment Options Chart** details options for rapid response



**Incident Response Log** used by team to report actions

**Incident Response Report** used by team to consistently report status

Severity	Why? What the Impact to Customers/Staff?	How? What type of data breach?	How? What type of data breach?	How? What type of data breach?
Critical	Major impact to all vehicles, significant compromise of Vehicle Services, Critical vehicle safety violation	N/A	N/A	N/A
High	Major impact to all vehicles, significant compromise of Vehicle Services, Potential safety violation	Potential compromise of Personal Information	Potential compromise of Personal Information	Potential compromise of Personal Information
Medium	Normal to moderate impact to all vehicles	Potential compromise of Personal Information	Potential compromise of Personal Information	Potential compromise of Personal Information
Low	Normal to moderate impact to all vehicles	Potential compromise of Personal Information	Potential compromise of Personal Information	Potential compromise of Personal Information

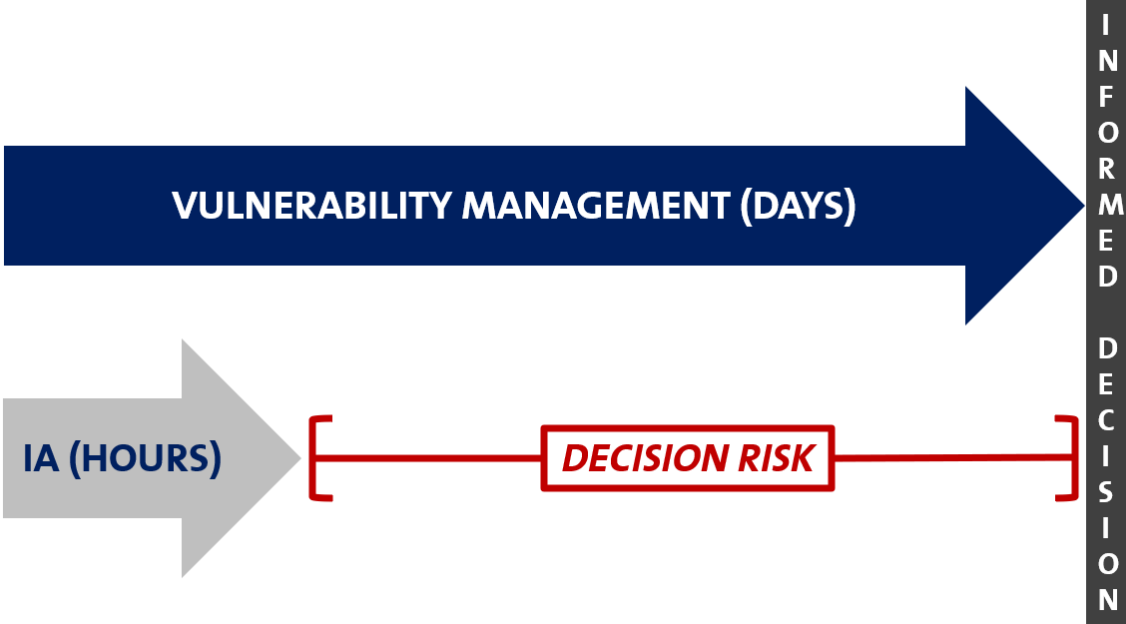
**Severity Criteria** provides guidance on how response should be tailored to scale and potential impact of incidents



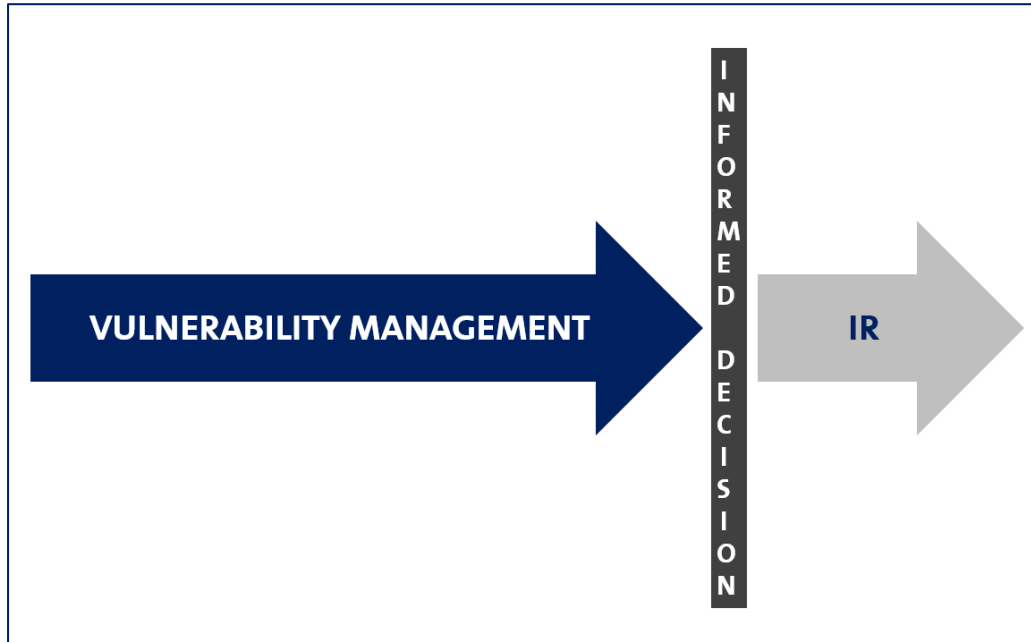
**Playbooks** provides details on how to respond by role



# VM and IR Viewed Separately Circa 2015

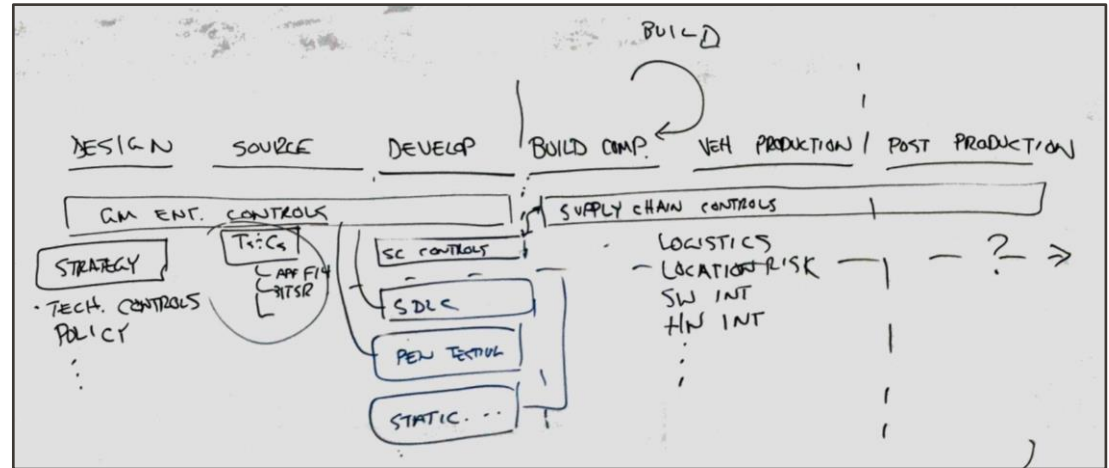
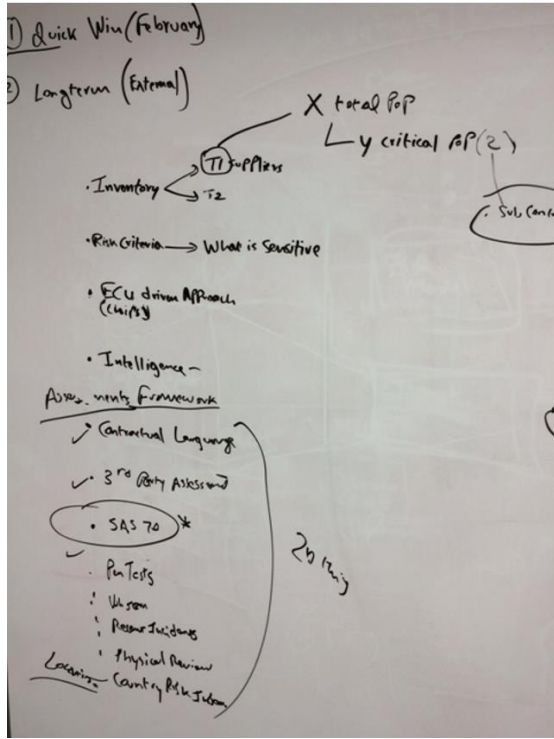


# Holistic VM View



***IR IS INSEPARABLE FROM VM***

# C-SCRM Focus Circa 2015



# 3<sup>rd</sup> Party Audit Focus Circa 2015



SOC 2 Reports cover controls relevant to a system's...

- Security (physical and logical)
- Confidentiality
- Processing Integrity
- Availability
- Privacy

...and attest to a service org's ability to maintain controls (vs. snapshot in time)

Goal: achieve specific business objectives (e.g., delivery of services, production of goods) in accordance with **management-specified requirements**.

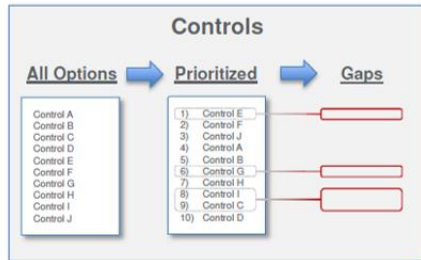
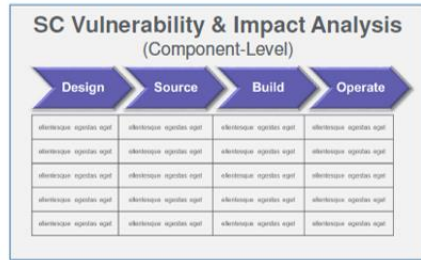
- Components
  - Infrastructure. The physical structures, IT, and other hardware (e.g., facilities, computers, equipment, mobile devices, and telecommunications networks).
  - Software.
  - People.
  - Processes.
  - Data.



# 3<sup>rd</sup> Party Compliance Focus Circa 2015

## INITIAL STRATEGY

Today



Early Fall 2015

- Repeatable method for SC risk assessment
- Ideal questions to ask of the data lake (e.g., who owns source code for Part X?)
- Optimized control plan
  - Will look at end-of-line flashing as one of many options
  - Analyzed by cost/benefit
  - Recommendation plan for foundational SC controls; advanced controls to follow

# Circa 2015: Hardware Integrity Attestation - DARPA SHIELD

## **DARPA** SHIELD: The DARPA Supply Chain Solution

- Full AES encryption engine with on-dielet key storage
- Passive sensors to detect dielet tamper attempts
- Physical fragility designed in to thwart removal
- Unique serial ID

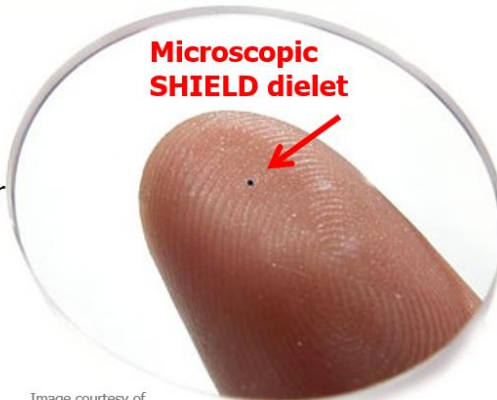


Image courtesy of <http://www.hitachi.com/New/cnews/030902.html>

- 100 $\mu$ m x 100 $\mu$ m
- 50 $\mu$ W total power
- Less than \$0.01 per-dielet cost
- Wireless power and communication (connection made through external probe)

The SHIELD dielet, installed in the package of the integrated circuit, will provide 100% assurance against many common supply chain threats. Physically fragile with on-board industry standard encryption, SHIELD will be highly resistant to cloning and spoofing attempts.

**SHIELD makes counterfeiting too expensive and too hard to do.**



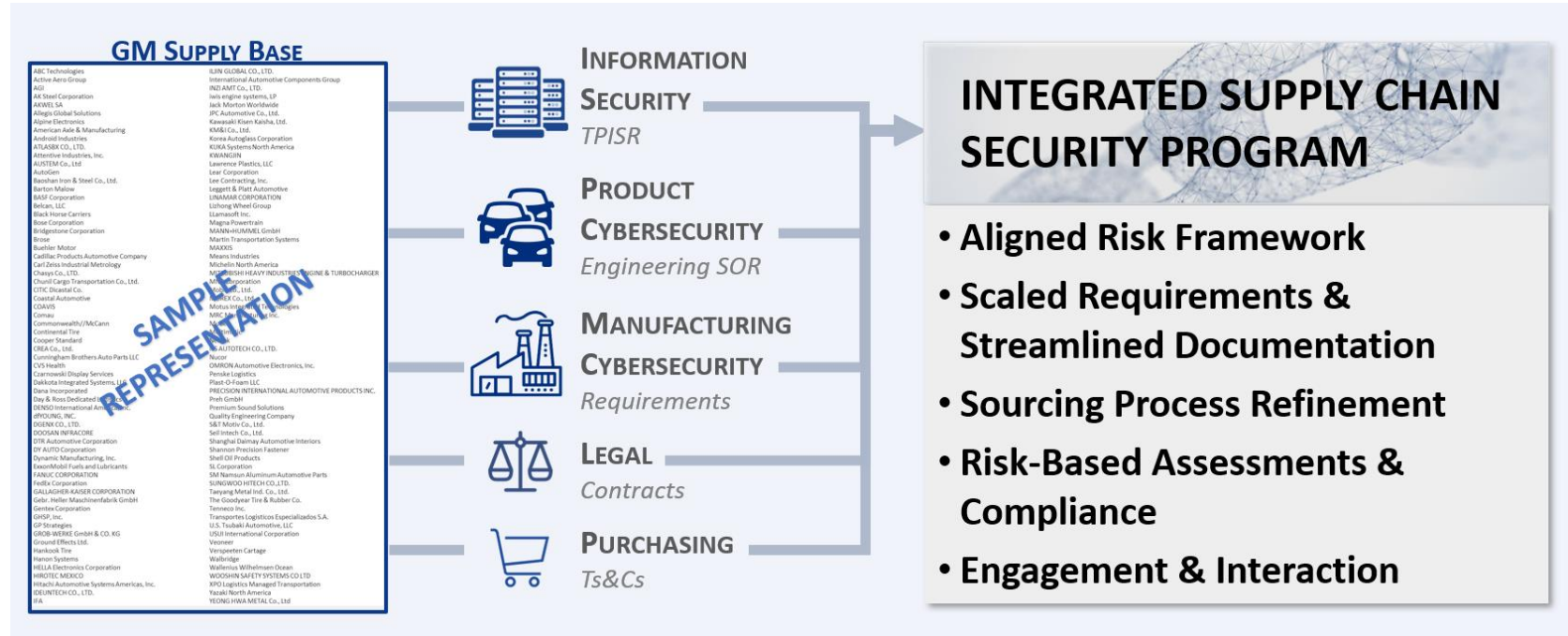
# 2015 Software Supply Chain Security Assurance Activities

---

- Suppliers write majority of the code
  - Performed binary SCA analysis
  - Required static code analysis
- OSS SBOM submission requirement for license compliance (OSS team moved to PCYS team in 2017)
  - Manual CVE mapping not ideal, but possible
- Internal and 3<sup>rd</sup>-party pentests
- Explored sub-tier hardware attestation requirements
  - Industry-wide adoption prospects were dim



# 2019 focus: Cross-functional Cyber Domain C-SCRM





# Recent: NIST CSF, log4j, NHTSA, EO 14028, SSDF, NCS ...

**ID.AM-1:** Physical devices and systems within the organization are inventoried

**ID.AM-2:** Software platforms and applications within the organization are inventoried

## 4.2.6 Inventory and Management of Software Assets on Vehicles

[G.10] Manufacturers should maintain a database of operational software components<sup>19,20</sup> used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.

[G.11] Manufacturers should track sufficient details related to software components,<sup>21</sup> such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,<sup>22</sup> manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

**Example 4:** Require third parties to provide provenance<sup>5</sup> data and integrity verification mechanisms for all components of their software.

develop and maintain their software products and services. This safe harbor will draw from current best practices for secure software development, such as the NIST Secure Software Development Framework. It also must evolve over time, incorporating new tools for secure software development, software transparency, and vulnerability discovery.

THE CYBERSECURITY 202

## An 'ingredients list' for software could help prevent the next log4j

CISA warns 'most serious' Log4j vulnerability likely to affect hundreds of millions of devices

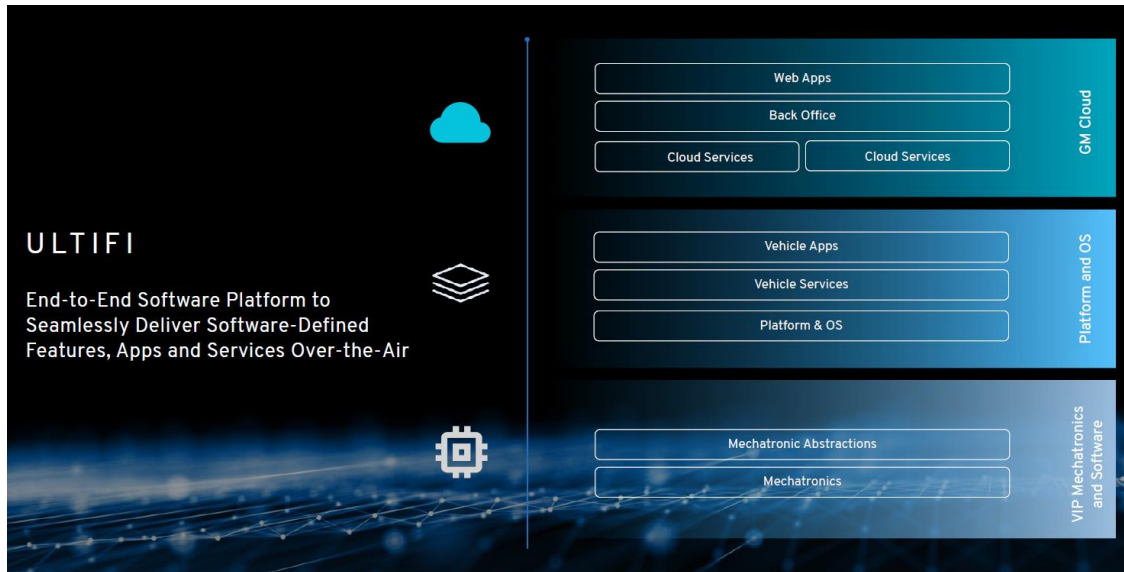
CISA's director said that the vulnerability "is one of the most serious I've seen in my entire career, if not the most serious."

## Secure Software Development Framework (SSDF) Version 1.1:

*Recommendations for Mitigating the Risk of Software Vulnerabilities*



# Today: SDV == VM Effort ↑



General Motors is now a platform company and working with Red Hat is a critical element in advancing our Ultifi software development. Incorporating the company's expertise in open source solutions and enterprise networks will pay dividends as we aim to provide the most developer-friendly software platform in the industry.

**Scott Miller**

Vice President, Software Defined Vehicle and Operating System, General Motors



# Vehicle as a Platform

- Before
  - Suppliers wrote most application code
- Now
  - GM is writing a lot of code
- A paradigm shift
  - Cultural
  - Procedural
  - Practical

The infographic features a blue background with a glowing blue car in the center. Above the car, there are several horizontal lines of glowing dots, suggesting data or connectivity. The text is arranged in a clean, modern layout with white and blue colors.

**gm | ultifi**

**END-TO-END SOFTWARE PLATFORM**  
that enables the frequent and seamless delivery of features and services to customers over the air.

**SOFTWARE-DEFINED EXPERIENCES**

- Vehicle themes
- Personalized settings
- Driver-assist features
- Performance upgrades
- New vehicle apps

**SYSTEM FEATURES**

- In-house development
- Enhanced OTA updates
- Cloud-based services
- Network integration
- Developer-friendly





# Internal Software Supply Chain Security Assurance

- DevSecOps establishment
  - Secure coding policies
  - SCA source code scans supporting multiple platform CI/CD build chains
- SBOM creation, ingestion, analysis
  - Basis for VM / threat monitoring
  - Inform pen test and TARA modeling

DevSecOps helps ensure that security is addressed as part of all DevOps practices by integrating security practices and automatically generating security and compliance artifacts throughout the processes and environments, including software development, builds, packaging, distribution, and deployment. This is important for several reasons, including:

- reducing vulnerabilities, malicious code, and other security issues in released software without slowing down code production and releases;
- mitigating the potential impact of vulnerability exploitation throughout the software lifecycle, including when the software is being developed, built, packaged, distributed, deployed, and executed on dynamic hosting platforms;
- addressing the root causes of vulnerabilities to prevent recurrences, such as strengthening test tools and methodologies in the toolchain, and improving practices for developing code and operating hosting platforms; and



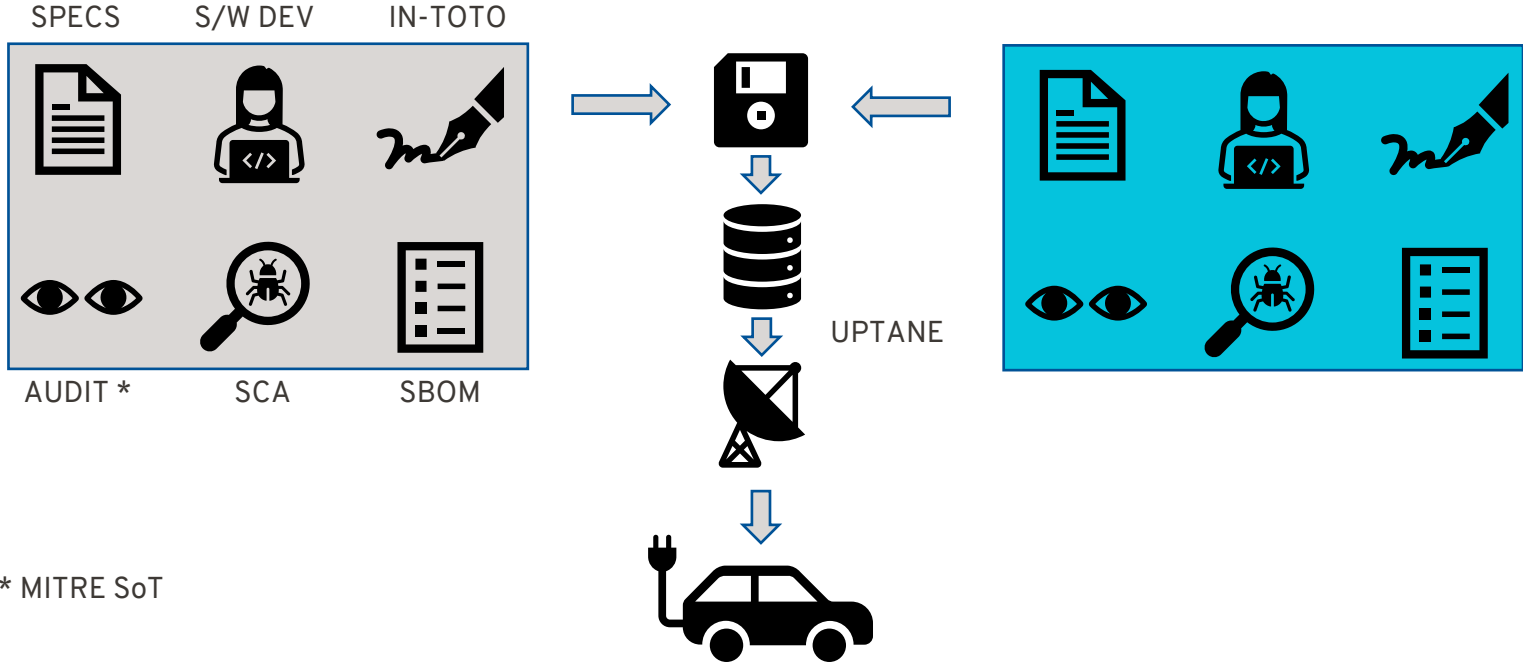


# Supply Chain Security Viewpoints

---



# Today



**SUPPLY CHAIN SECURITY IS INSEPARABLE FROM VM**

