



# WELCOME TO AUTO-ISAC!

## *MONTHLY VIRTUAL COMMUNITY CALL*

May 01, 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?
<p><b>TLP:RED</b></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><b>TLP:AMBER+STRICT</b></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><b>TLP:AMBER</b></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><b>TLP:GREEN</b></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><b>TLP:CLEAR</b></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	<b>Welcome</b> <ul style="list-style-type: none"><li>➤ Why We're Here</li><li>➤ Expectations for This Community</li></ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"><li>➤ Auto-ISAC Activities</li><li>➤ Heard Around the Community</li><li>➤ Intelligence Highlights</li></ul>
11:15	<b>DHS CISA Community Update</b> <ul style="list-style-type: none"><li>➤ <b>Jeff Terra, Joint Cyber Defense Collaborative (JCDC)</b></li></ul>
11:20	<b>Featured Speaker:</b> <ul style="list-style-type: none"><li>➤ <b>Walter Capitani, Director of Technical Product Management, Organization: CodeSecure</b></li><li>➤ <b>Title: State-of-the-Art Automotive SBOM Monitoring</b></li></ul>
11:55	<b>Q&amp;A &amp; Closing Remarks</b>

# 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](mailto: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 (1<sup>st</sup> Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions! *“Cybersecurity is a Team Sport!”*

**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

**49** 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

MAY 1, 2024

Highlight = New Active Members

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

79 MEMBERS



This document is Auto-ISAC Sensitive and Confidential.

TLP: CLEAR

1 May 2024

# AUTO-ISAC BUSINESS UPDATES AND EVENTS

- **Community Call:** Wednesday, June 5, 2024 **Time:** 11:00 – 12:00 p.m. ET **TLP:GREEN** **Speaker:** Justin Maltibano, Car Hacking Village **Title:** TBA
- **ACT Fundamental Course:** On-Demand, **Cybersecurity Basics** (32 hrs.) | **Security Engineering** (28 hrs.) | **Security Operations/Management** (22.5 hrs.)
- **CAPEX:** *Capability Exam is scheduled for **May 22, 2024**.* If interested in taking the exam, please complete the [information form](#) by May 10<sup>th</sup>. The proctored exam will be made available in multiple time zones.
- **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!](#)
- **Auto-ISAC's TLP:CLEAR 2nd Annual Auto-ISAC European Cybersecurity Summit** will be held June 12 – 13, 2024 at [BMW Welt](#) in Munich, Germany. Agenda details and registration can be found [here!](#)



# 2024 AUTO-ISAC EUROPEAN CYBERSECURITY SUMMIT

SUSTAINING THE PRESENT – SECURING THE FUTURE

# AUTO-ISAC SUMMIT

2024 Auto-ISAC Cybersecurity Summit

October 22-23 | Detroit, MI

In-person & Virtual

[Information and registration](#)







# **AUTO-ISAC INTELLIGENCE HIGHLIGHT**

## **RICKY BROOKS, INTELLIGENCE OFFICER**

*This document is Auto-ISAC Sensitive and Confidential.*

**TLP: CLEAR**



# AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; **TLP:GREEN** Auto-ISAC 2024 Threat Assessment was released March 21; we welcome your feedback.
  - **Send feedback**, intelligence, or questions to [analyst@automotiveisac.com](mailto: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](#) <sup>1</sup>, [Israel-Hamas](#) <sup>2 3</sup>, [Iran](#), [China](#) <sup>4 5 6 7 8\*</sup>, [North Korea](#)).
  - Ransomware <sup>9 10</sup> Groups Targeting Automotive: [8Base](#), [Akira](#), [Black Basta](#), [BlackSuit](#), [LockBit 3.0](#), [Medusa](#), [Hunters International](#), [Play](#), [Qilin](#), [Qiulong](#), [RA World](#), [RansomHub](#), [Red Ransomware](#)
  - **Consider Technical Debt**: “Technical debt is the accumulation of sub-optimal or expedient solutions in software development that can slow future progress and increase costs...” ([DigitalOcean](#))
  - **Notable Vehicle Research**: Gaining SSH Access to Infotainment Systems ([CANBUSHACK](#)); Bypassing Authentication on ECUs ([Link](#)).
  - **Notable TTPs**: Using social engineering to inject backdoor in open-source xz Utils ([arsTECHNICA](#)); AI-enhanced spear-phishing ([The Hacker News](#)); spear-phishing via free IP scanning tool lure ([BlackBerry](#)); exploiting vulnerabilities in firewall platforms ([CISA](#)); exploiting zero-day vulnerability in file transfer system server ([Darkreading](#)); integrating espionage, attack, and influence into combined operations ([Google](#)); business/vendor email compromise ([Abnormal](#)); **Notable Tools**: xzbot ([GitHub](#)); Jia Tan’s SSH Agent ([GitHub](#)); Pupy RAT ([Cybersecurity News](#)); LightSpy ([BlackBerry](#)); Dredge ([GitHub](#)); Ridbrute ([GitHub](#)).



# 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.
- ❖ 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?

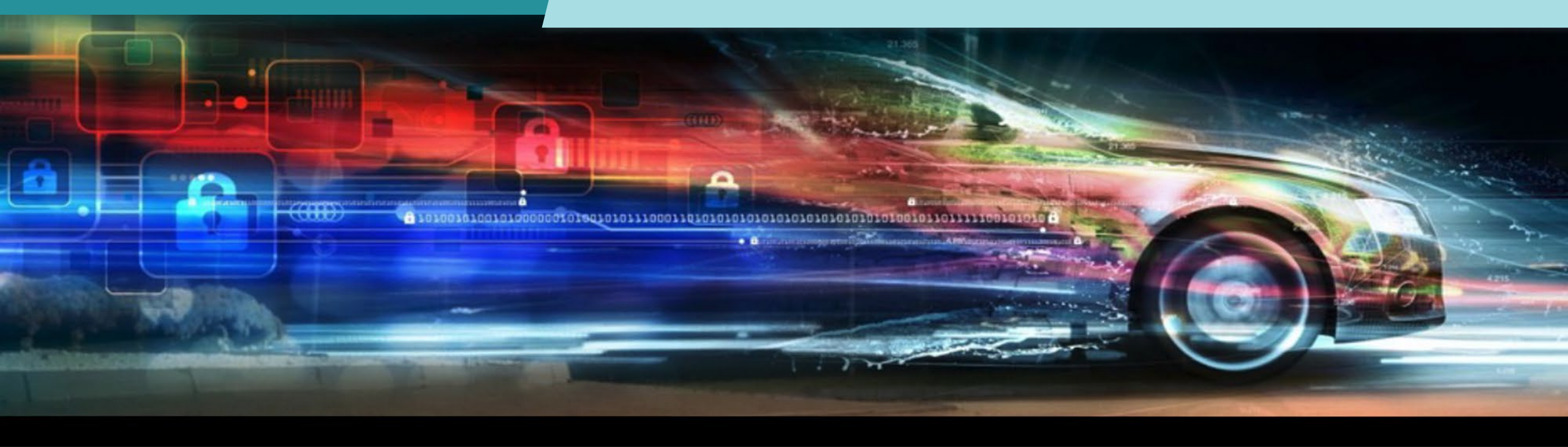
- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

**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



**Walter Capitani**

Walter Capitani, Director, Technical Product Management for CodeSecure is a recognized expert in embedded and enterprise software security.

Walter has led product teams delivering solutions to worldwide markets for automotive, safety-critical and secure software development.

Walter holds a degree in Electrical Engineering from the University of Waterloo and is an MBA graduate of the Telfer School of Management.



# State of the Art Automotive SBOM Monitoring



Walter Capitani  
Director, Technical Product Management



# Agenda



- Introduction to CodeSecure
- Software Security Workflow
  - SBOM Generation
  - Risk Analysis
  - Vulnerability Monitoring

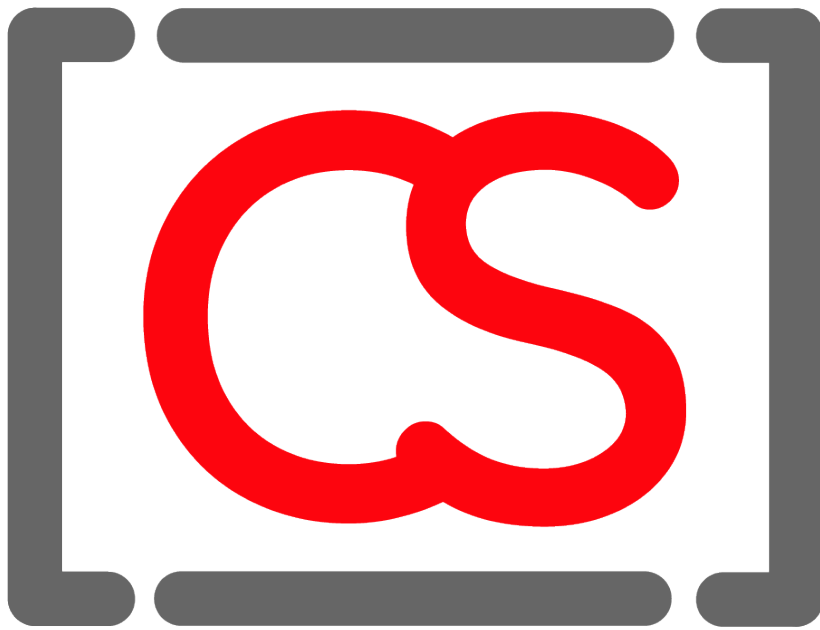


**Walter Capitani**

*Senior Director, Technical Product Management*

# CodeSecure

We protect everyone. Everywhere there's code.



## Security

- 35 years of experience with the DoD research division
- Cutting-edge source and binary analysis finds the most vulnerabilities



## Safety

- Software that's safer and less prone to failure or bugs than the competition
- Trusted by large, global organizations with their reputations on the line



## Speed

- Products built for a modern day development and DevSecOps environment
- Intuitive solutions integrate with existing tools and don't disrupt workflow



## Support

- Concierge-style customer service around the world
- Hundreds of global organizations depend on our collaborative team of problem solvers

# How We Power Your Success

Go deeper than ever before.



**CODESonar**<sup>®</sup>  
CODESECURE

**CODESentry**<sup>®</sup>  
CODESECURE

**Purpose**

DevSecOps with security, safety, and quality

Secure third-party code and deliver SBOMs at the end of the process

**Detection abilities**

Detect unknown defects (zero-day)

Detect components, known (N-day) and unknown (zero-day) defects

**Detection method**

Static Application Security Testing (SAST) – Source code

Software composition analysis (SCA) – Binaries



# Software Security Workflow





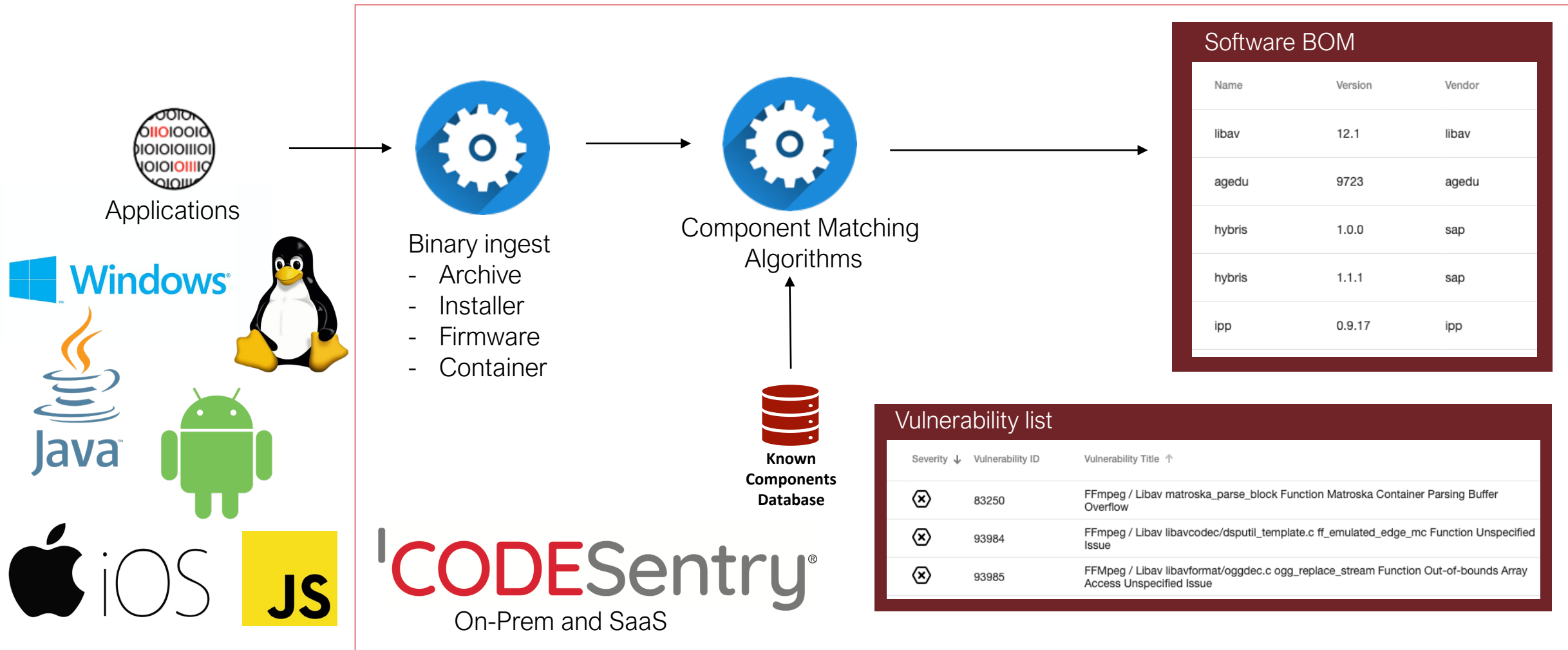
# Software Security Workflow



# Software Security Workflow



# SBOM Generation



# Generated SBOM



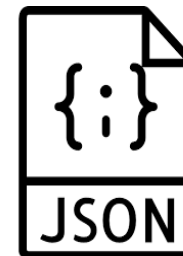
Pass/Fail	Security Score	Name	Version	Vendor	Match ↑	Vulnerabilities by Severity	Target	License	Annotate
▶	100	a2dp.vol	126	unspecified	Low	0  0  0  0  0  0	classes.dex	No data available	
▶	100	android-framework-23	6.0.1+r72-4	unspecified	Low	0  0  0  0  0  0	classes.dex	Apache 2.0	
▶	100	android-framework-23	6.0.1+r72-4	unspecified	Low	0  0  0  0  0  0	classes.dex	Apache 2.0	
▶	100	android-framework-23	6.0.1+r72-4	unspecified	Low	0  0  0  0  0  0	classes.dex	Apache 2.0	
▶	100	android-platform-art	11.0.0+r48	unspecified	Low	0  0  0  0  0  0	libartbase.so	Apache 2.0	
▶	100	android-platform-frameworks-base	10.0.0+r36	unspecified	Low	0  0  0  0  0  0	classes.dex	Apache 2.0	
▶	100	android-platform-frameworks-base	10.0.0+r36	unspecified	Low	0  0  0  0  0  0	classes.dex	Apache 2.0	
▶	100	android-platform-frameworks-native	10.0.0+r36	unspecified	Low	0  0  0  0  0  0	libgui.so	Apache 2.0	
▶	100	android-platform-frameworks-native	10.0.0+r36	unspecified	Low	0  0  0  0  0  0	libgui.so	Apache 2.0	
▶	100	android-platform-frameworks-native	10.0.0+r36	unspecified	Low	0  0  0  0  0  0	libgui.so	Apache 2.0	



# SBOM Outputs



- CycloneDX
- SPDX
- CSV Format
  - Convenient for 3<sup>rd</sup> party integrations
- VEX Exports
  - Vulnerability Export Exchange
  - Machine readable JSON format
  - Used in combination with the CycloneDX SBOM

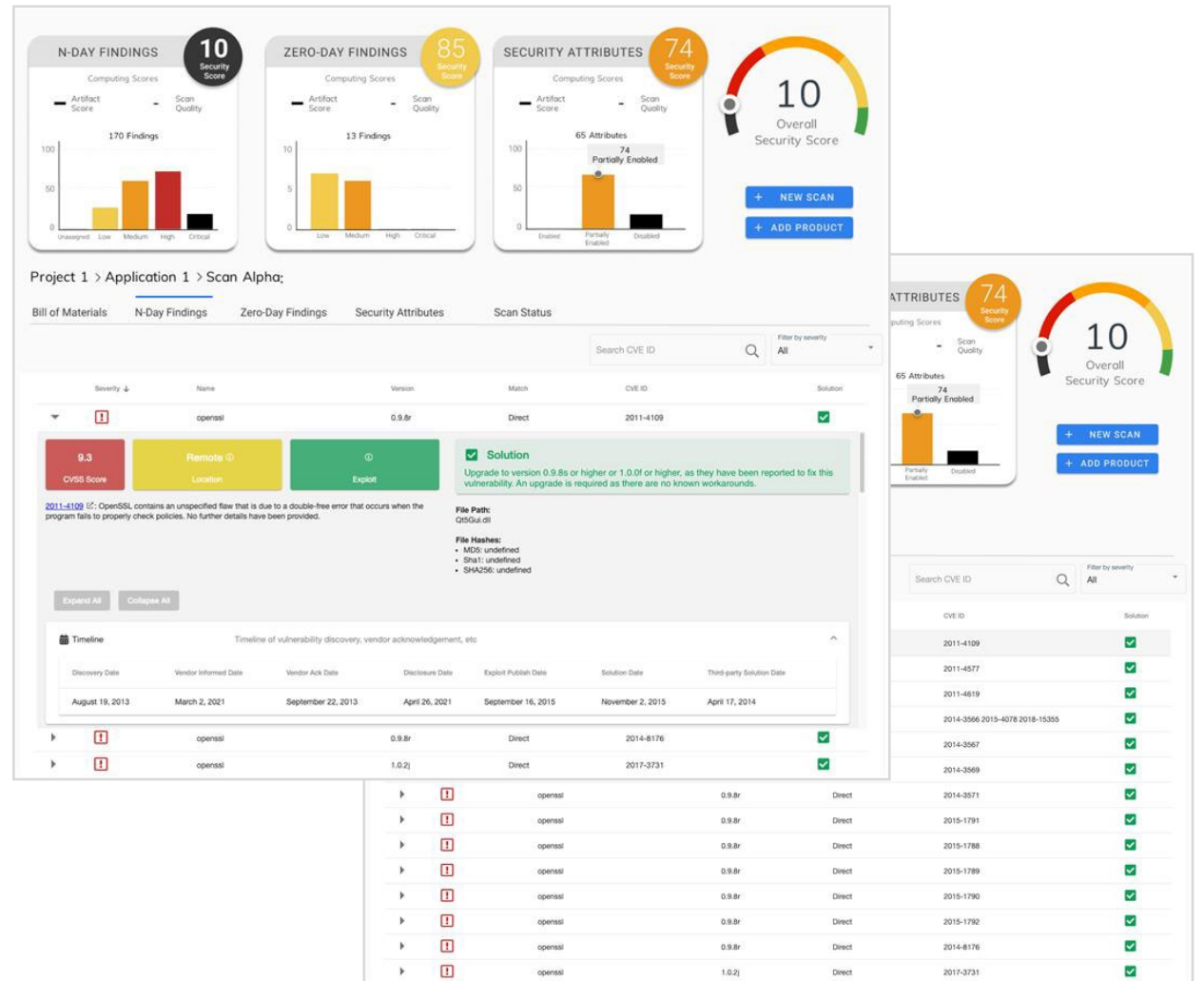


# Software Security Workflow



# Initial Risk Analysis

- Software Bill Of Materials
- Security scores
- N-Day vulnerabilities
- License Risk
- Security Attributes
- External Dependencies



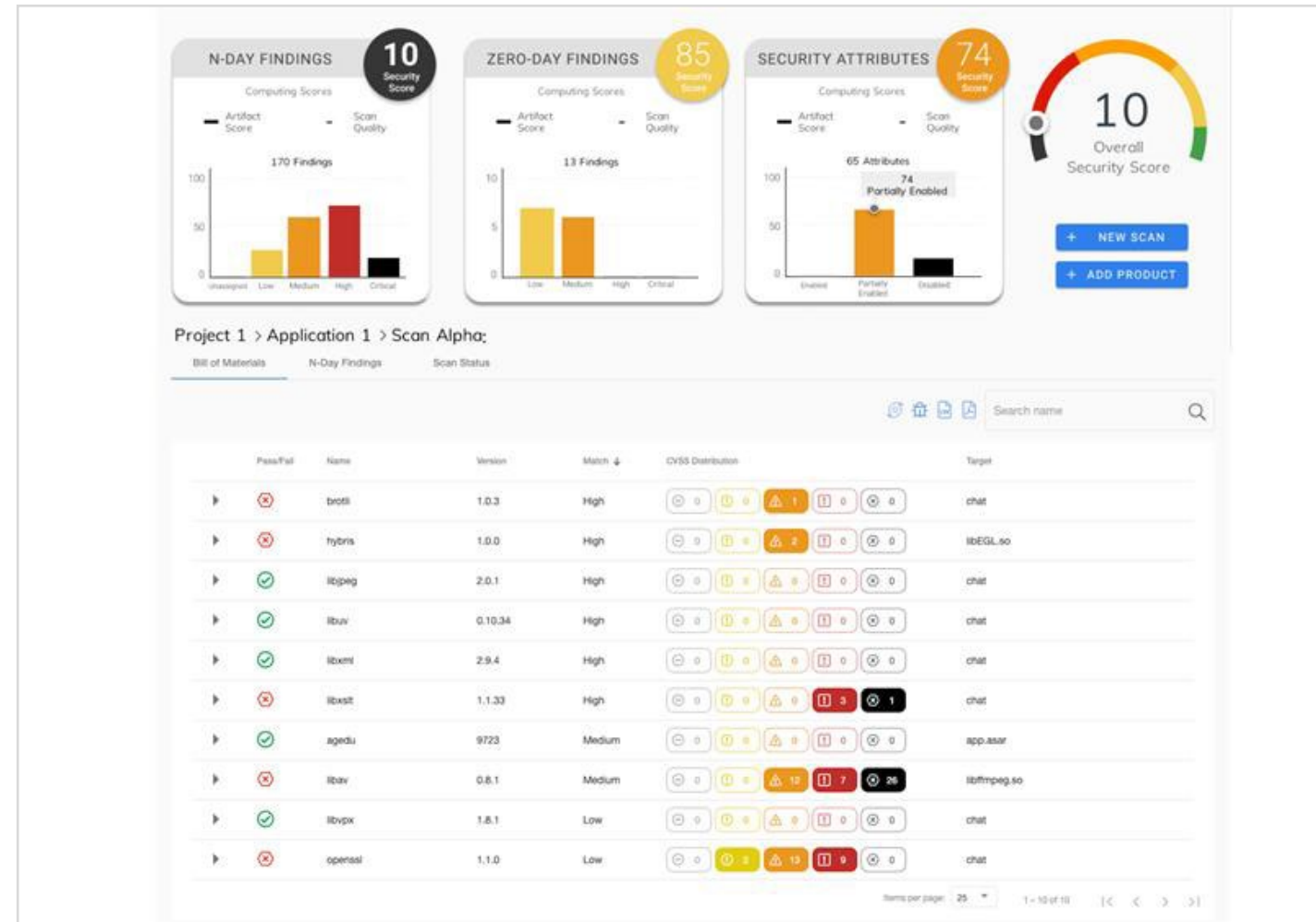
# SBOM Risk Analysis





# Software Bill of Materials (SBOM)

- Component Name
- Version
- Match
- Target
- Pass/Fail
- CVSS Distribution



# Refine SBOM Components



- Review discovered components
- Add components from 3rd party software that may not be included in scan
- The goal is to have the most accurate SBOM for monitoring

### Annotate Component ✕

Component Name: gpac  
Component Version: 2.2.1  
Vendor: gpac  
Target File Name: CoreMedia.dll

Component State:

Comment:  
  
Max 2000 characters. The previous comment will be overwritten. 0/2000

License: Open Source GNU Library or 'Lesser' General Public License (LGPL) License State:

Note: components that are excluded can be re-included if needed. When a component is excluded, the component, as well as any associated vulnerabilities, will not be included in overall metrics and reports.



# Vulnerability Risk Analysis



# Vulnerability Risk Analysis



Bill of Materials External Dependencies N-Day Findings Security Attribute Findings Zero-Day Findings License Findings Scan Status Scan Report

INCLUDED (331) EXCLUDED (0) Choose a date Search CVE or Vuln ID Filter by severity All Filter by match High Filter by included status All Filter by remediation All Filter by location All

Severity ↓	Vulnerability ID	Vulnerability Title	Component Name	Component Version	Match	CVE ID(s)	Status	Remediation Available	Annotate	
▶	⊗	152287	Libxml2 Unspecified Out-of-bounds Access Issue	libxml2	2.9.14+dfsg	High	2016-9833	Under Investigation	⊗	<input type="checkbox"/>
▶	⊗	152287	Libxml2 Unspecified Out-of-bounds Access Issue	libxml2	2.9.14+dfsg	High	2016-9833	Under Investigation	⊗	<input type="checkbox"/>
▶	⊗	152287	Libxml2 Unspecified Out-of-bounds Access Issue	libxml2	2.9.14+dfsg	High	2016-9833	Under Investigation	⊗	<input type="checkbox"/>
▶	⊗	152287	Libxml2 Unspecified Out-of-bounds Access Issue	libxml2	2.9.14+dfsg	High	2016-9833	Under Investigation	⊗	<input type="checkbox"/>
▶	⊗	117589	PHP ext/opcache/zend_shared_alloc.c zend_shared_memdup() Function Use-after-free Unspecified Issue	php	8.2.7	High	2015-1351	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	129841	PHP yaml_parse() Functions php/object Extension Type Handling Unserialize Invocation Remote Code Execution	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	146959	PHP file ext/standard/math.c _php_math_number_format_ex() Function Separator String Handling Remote Memory Corruption	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	146960	PHP ext/pgsql/pgsql.c pg_escape_string() Function Integer Overflow Remote Heap Buffer Overflow	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	146961	PHP ext/bz2/bz2.c bzdecompress() Function String Handling Integer Overflow Remote Heap Buffer Overflow	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	146967	PHP ext/standard/html.c php_escape_html_entities_ex() Function Integer Overflow Remote Heap Buffer Overflow	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	146969	PHP ext/standard/math.c _php_math_number_format_ex() Function Size Value Handling Remote Memory Corruption	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	193251	Yaml Extension for PHP (php-yaml) parse.c handle_mapping() Function YAML Array Merge Handling Type Confusion Remote Code Execution	php	8.2.7	High	None	Under Investigation	✓	<input type="checkbox"/>
▶	⊗	291151	SQLite Unspecified Issue	sqlite	3.32.2	High	2021-46100	Under Investigation	⊗	<input type="checkbox"/>
▶	⊗	291151	SQLite Unspecified Issue	sqlite	3.32.3	High	2021-46100	Under Investigation	⊗	<input type="checkbox"/>
▶	⊗	291151	SQLite Unspecified Issue	sqlite	3.39.2	High	2021-46100	Under Investigation	⊗	<input type="checkbox"/>

# Vulnerability Annotations



### Annotate Vulnerability

Vulnerability ID: 152287

**Libxml2 Unspecified Out-of-bounds Access Issue**

Libxml2 contains an out-of-bounds access flaw that may allow a context-dependent attacker to have an unspecified impact. No further details have been provided by the researcher.

**10** ⓘ  
CVSS Score

Vulnerability Status ⓘ  
Under Investigation

Vulnerability Status Comment  
Enter Annotations comments - going to fix this...  
Max 2000 characters. The previous comment will be overwritten. 49/2000

CVSS Score

Keep score at its current score of 10  
 Modify score

New CVSS Score: 10

CANCEL  UPDATE

Severity	Vulnerability ID	Vulnerability Title	Component Name	Component Version	Match	CVE ID(s)	Updated At (UTC)	Target Path	Status	Link to Scan	Annotate
	152287	Libxml2 Unspecified Out-of-bounds Access Issue	libxml2	2.9.10+dfsg-6.7+deb11u1	High	2016-9833		PM/HTTP Server Container/ webserver.tar.gz/ httpd.tar/ 637803ff40f025011015fd890d7b8323f36aef705d2532f505bb2e871ef18658/layer.tar/usr/lib/x86_64-linux-gnu/libxml2.so.2.9.10	Under Investigation		<input type="checkbox"/>

Expand All Collapse All

Vulnerability Annotation This finding was last annotated on April 15, 2024, 8:55 PM GMT+1

- Current status: Under Investigation  
Status comment: Enter Annotations comments - going to fix this...
- Original CVSS score: 10  
Score comment: None

Remediation Available Annotate

Annotate (1 Finding)

- Review CVSS Score, Exploit and Remediation Status
- Set vulnerability state appropriately to AFFECTED, NOT AFFECTED, FIXED



# License Risk Analysis





# License Risk Review



License Name (Number of Licenses)	In Review	Not Approved	Approved	License Risk Category ↓
▶ Free Software (2)	0	0	2	
▶ Open Source Other (5)	5	0	0	
▶ Open Source GNU Affero General Public License (AGPL) (1)	1	0	0	
▶ Open Source GNU General Public License (GPL) (48)	47	0	1	
▶ Open Source Eclipse Public License (EPL) (1)	1	0	0	
▶ Open Source GNU Library or 'Lesser' General Public License (LGPL) (41)				
▶ Open Source Mozilla Public License (MPL) (5)				
▶ Open Source Apache License 2.0 (10)				
▶ Open Source Boost Software License (BSL) (2)				
▶ Open Source BSD 2-Clause 'Simplified' or 'FreeBSD' license (14)				

▼ Open Source Apache License 2.0 (10) 10 0 0

Filter by license state: All
**BULK ANNOTATE**

Product Name ↑	Version	Vendor	Product Path	License State	Annotate
arangodb	3.8.9	unspecified	COTS-Software.zip/COTS-Software/JavaScriptCore.dll	In Review	
juce	7.0.2	unspecified	COTS-Software.zip/COTS-Software/CoreAudioToolbox.dll	In Review	
llvm	org-17-init	unspecified	COTS-Software.zip/COTS-Software/Admin.dll	In Review	
llvm	org-17-init	unspecified	COTS-Software.zip/COTS-Software/JavaScriptCore.dll	In Review	
swoole	5.0.3	unspecified	COTS-Software.zip/COTS-Software/JavaScriptCore.dll	In Review	
traffic_server	6.1.1	apache	COTS-Software.zip/COTS-Software/CFNetwork.dll	In Review	
webkitgtk+	safari-610.4.3.1.7	unspecified	COTS-Software.zip/COTS-Software/JavaScriptCore.dll	In Review	
webkitgtk+	safari-610.4.3.1.7	unspecified	COTS-Software.zip/COTS-Software/WebKit.dll	In Review	
webkitgtk+	webkit-611.3.10.1.17	unspecified	COTS-Software.zip/COTS-Software/WTF.dll	In Review	

# Software Security Workflow

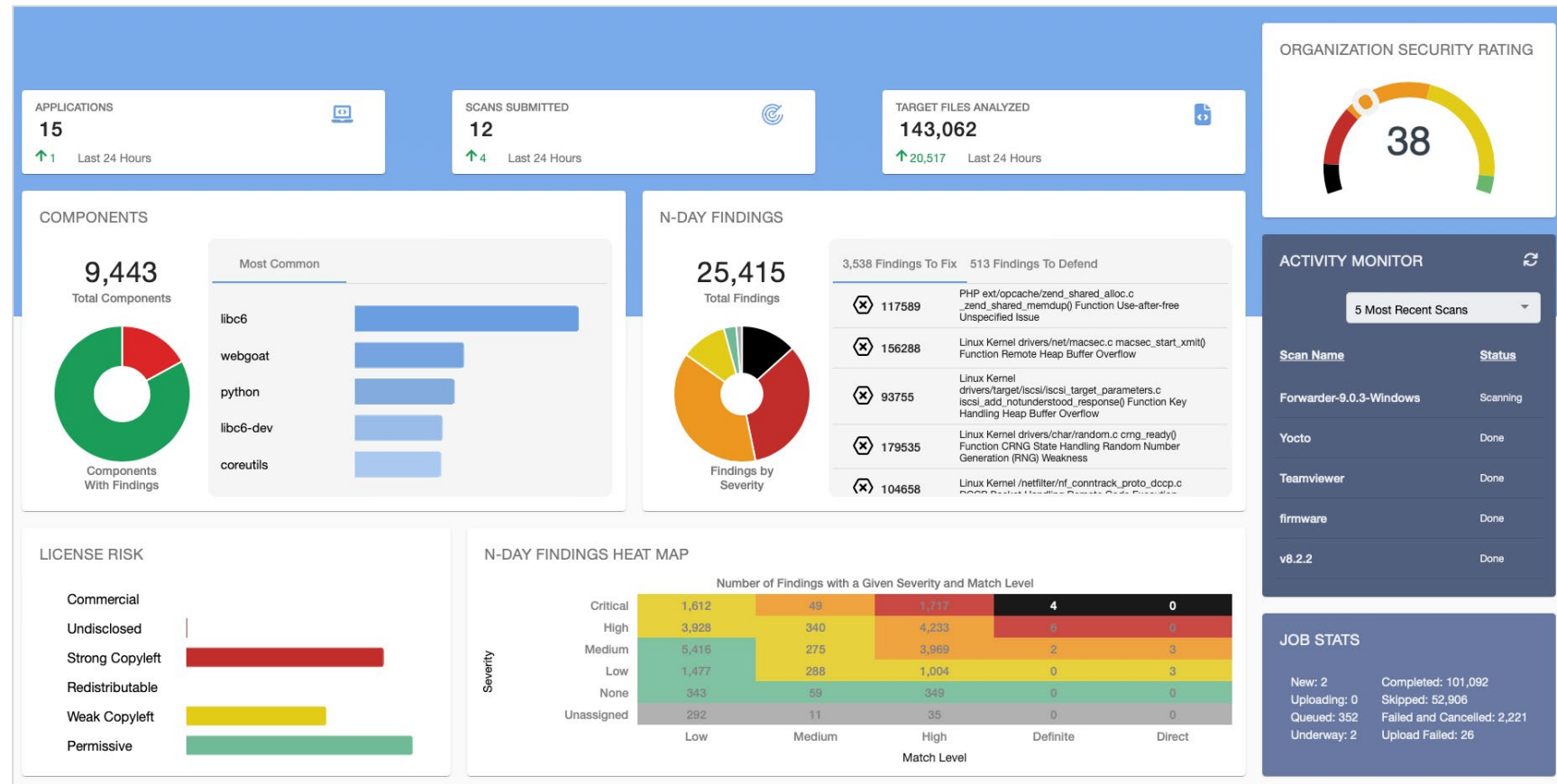


# SBOM Monitoring



# Monitor Software Portfolio

- Applications
- Scans
- File Analyzed
- Components
- License Risk
- N-Day Findings
- Heat Map
- Security Rating





# Instance-wide monitoring

- Search for components and vulnerabilities
- Filter to refine search

The screenshot displays the CODESentry web interface, which is used for instance-wide monitoring. The interface is divided into several sections:

- Dashboard:** Located at the top left, it includes a sidebar with navigation options like 'Dashboard', 'Summary', 'xDevOps', 'ROB', 'Demo', and 'PM'. A 'NEW SCAN' button is also present.
- Summary Cards:** Two cards at the top right show '4 Applications' and '9 Scans'.
- Vulnerabilities Section:** This section is active and shows a search for 'openssl'. It includes search filters for 'Search component version' and 'Search component vendor'. Below the search bar, there are filters for severity (set to 'All'), remediation (set to 'Remediation Available'), and location (set to 'Remote/Network Access').
- Vulnerability Table:** A table listing vulnerabilities with columns for Severity, Vulnerability ID, Vulnerability Title, Component Name, Component Version, CVE ID(s), Target Path, and Link to Scan. The table shows three entries for CVE-2023-0465, all with a severity of 'High' (indicated by a red triangle icon).

Severity	Vulnerability ID	Vulnerability Title	Component Name	Component Version	CVE ID(s)	Target Path	Link to Scan
High	316482	OpenSSL crypto/x509/x509_vfy.c check_policy() Function Leaf Certificate Invalid Certificate Policy Handling Remote Policy Check Bypass	openssl	1.1.1k	2023-0465	Demo/Web Conference Client/ZoomInstaller.exe	<a href="#">Link to Scan</a>
High	316482	OpenSSL crypto/x509/x509_vfy.c check_policy() Function Leaf Certificate Invalid Certificate Policy Handling Remote Policy Check Bypass	openssl	3.0.0	2023-0465	Demo/Wifi Firmware/BZ.ar7240.v4.3.28.11361.210128.2309.bin	<a href="#">Link to Scan</a>
High	316482	OpenSSL crypto/x509/x509_vfy.c check_policy() Function Leaf Certificate Invalid Certificate Policy Handling Remote Policy Check Bypass	openssl	3.0.0	2023-0465	PM/Wifi Firmware/BZ.ar7240.v4.3.28.11361.210128.2309.bin	<a href="#">Link to Scan</a>

# Continuous Monitoring

- Requires hourly or daily updates of vulnerability information
- Alert to new:
  - Vulnerabilities
  - Exploits
  - Remediations
- Triage new vulns and assign for investigation and remediation

The screenshot shows a date selection interface for May 2023. The month is displayed as 'MAY 2023' with navigation arrows. Below is a calendar grid with the 1st of May highlighted in a blue circle. Underneath the calendar, there is a section titled 'Include vulnerabilities that have all of the following changes since the selected date'. This section contains four checked checkboxes: 'Updated Vulnerability', 'Updated Remediation', 'Updated Exploit', and 'New Vulnerability'. At the bottom of the interface are three buttons: 'Cancel', 'Clear', and 'Apply'.

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Include vulnerabilities that have all of the following changes since the selected date

- Updated Vulnerability
- Updated Remediation
- Updated Exploit
- New Vulnerability

Cancel Clear Apply

# Software Security Workflow





Walter Capitani

*Senior Director, Technical Product  
Management*

For more information, visit us at  
<https://www.codesecure.com/>





# OPEN DISCUSSION

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



# OUR CONTACT INFO

**Faye Francy**  
Executive Director



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



[AUTOMOTIVEISAC.COM](http://AUTOMOTIVEISAC.COM)