SBOM in Automotive – Know What's in Your Car

Dennis Kengo Oka
Senior Principal Automotive Security Strategist and Executive Advisor

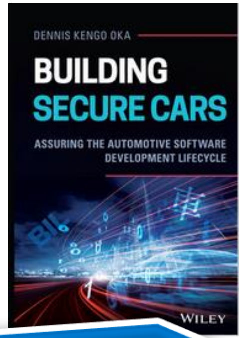
GlobalPlatform Automotive Security Roundtable
2024/10/24, Tokyo, Japan

Speaker Information: Dennis Kengo Oka

Senior Principal Automotive Security Strategist & Executive Advisor

Solutions for secure automotive software development

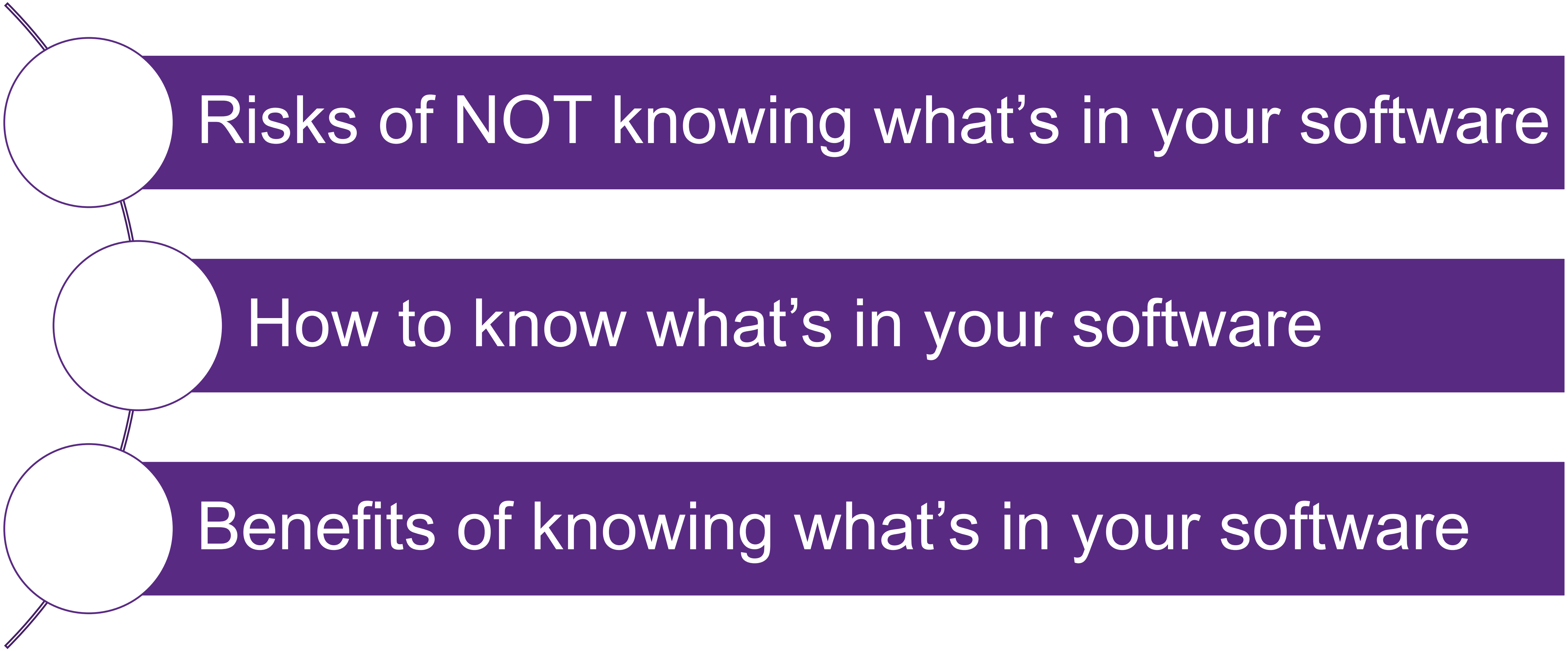
dennis.kengo.oka@blackduck.com



<packt>
Building Secure Automotive IoT Applications
Developing robust IoT solutions for next-gen automotive software
DR. DENNIS KENGO OKA | SHARANUKUMAR NADAHALLI
JEFF YOST | RAM PRASAD BOJANKI

Author of the books: “*Building Secure Cars: Assuring the Automotive Software Development Lifecycle*” *and* “*Building Secure Automotive IoT Applications: Developing Robust IoT Solutions for Next-Gen Automotive Software*”

Agenda



Risks of NOT knowing what’s in your software

How to know what’s in your software

Benefits of knowing what’s in your software

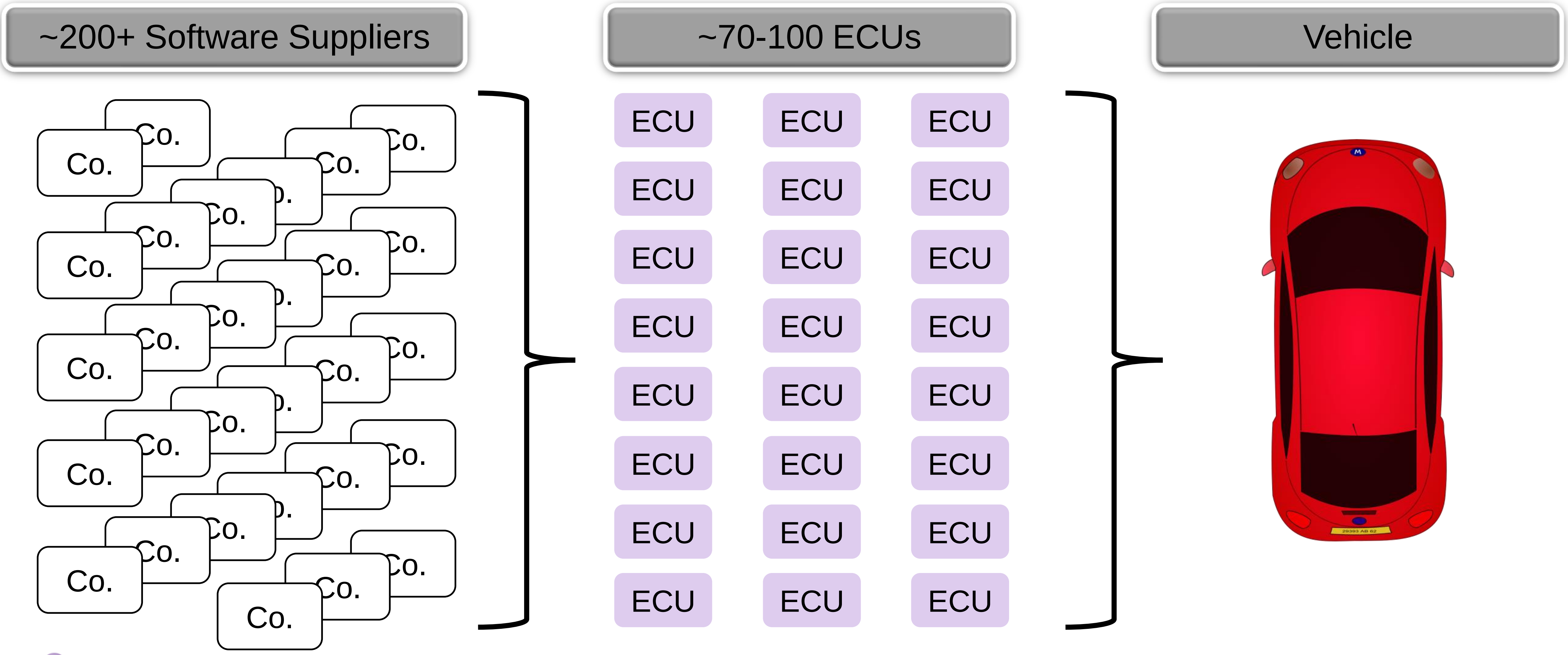
© 2024 Black Duck Software, Inc.

Agenda

- Risks of NOT knowing what’s in your software
- How to know what’s in your software
- Benefits of knowing what’s in your software

ECU: Electronic Control Unit

Automotive Supply Chain



~200+ Software Suppliers

~70-100 ECUs

Vehicle

© 2024 Black Duck Software, Inc.

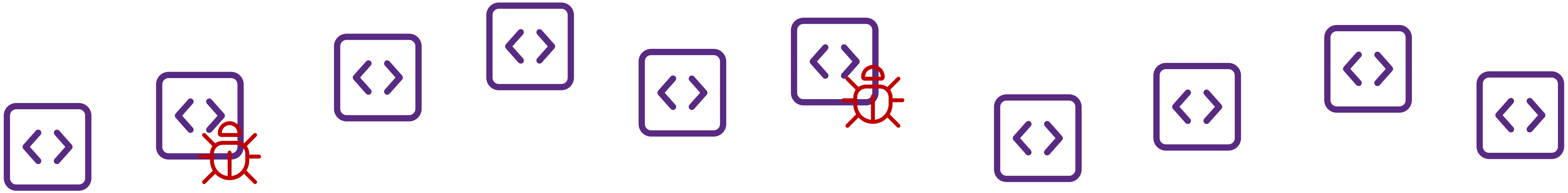
BlueBorne: Bluetooth Vulnerabilities Expose Billions of Devices to Hacking

- Estimated more than 5 billion affected devices
- Bluetooth implementations in Android, iOS, Linux and Windows

© 2024 Black Duck Software, Inc.

Is Your Car Vulnerable?

- Which vulnerabilities affect which versions of software?
- Which software versions are included in my products?
- I.e., which products are vulnerable?
- (is the vulnerability exploitable, how easy/hard is it to exploit etc.)



Need to know which software are included in our products

© 2024 Black Duck Software, Inc.

OSS Risks

Security

- Vulnerabilities in OSS that can be exploited

License

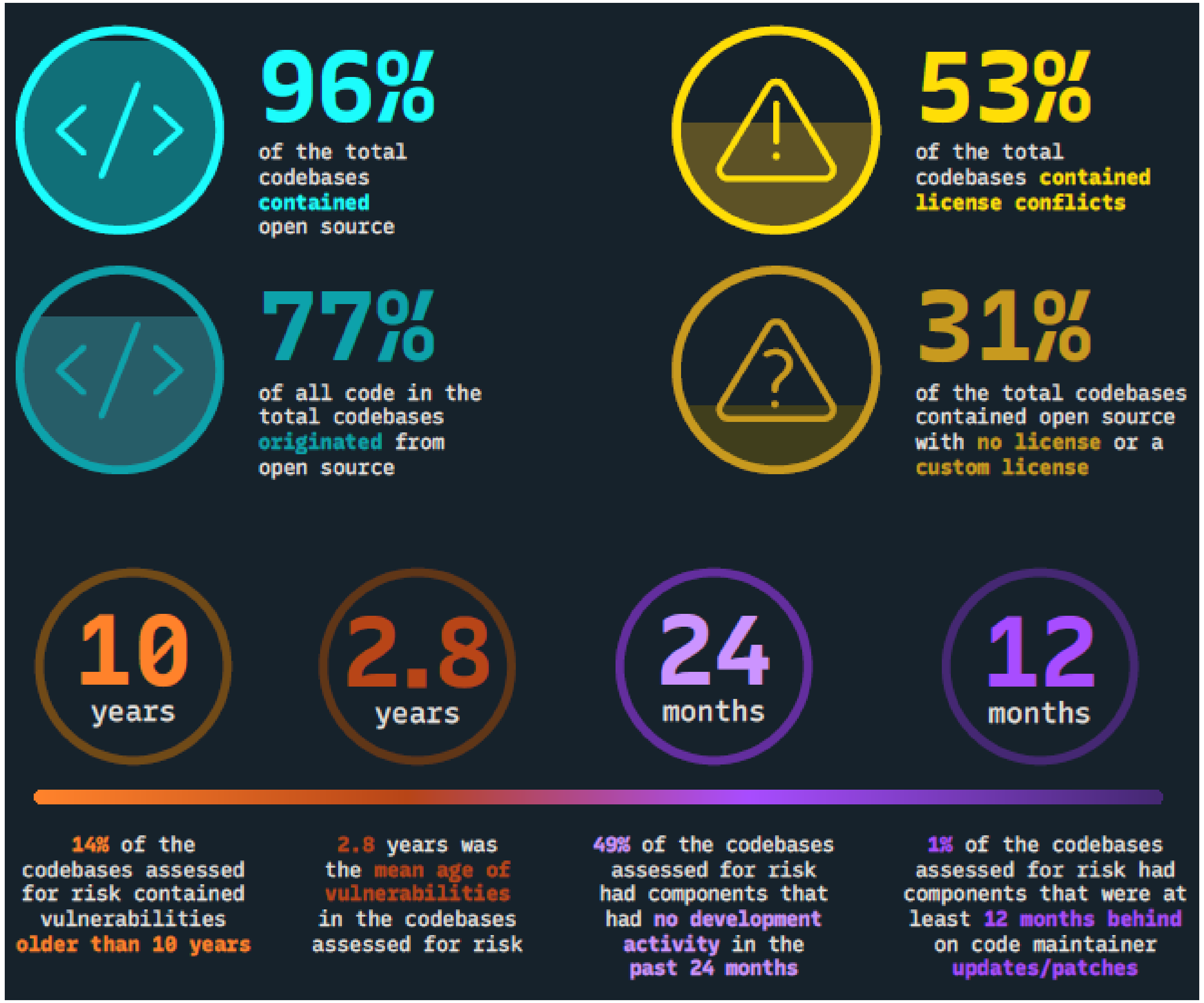
- Lawsuits due to non-compliance with license terms and conditions

Maintenance

- No timely bug fixes or addition of new functionality due to inactive OSS communities

© 2024 Black Duck Software, Inc.

Open Source Security and Risk Analysis Report 2024 (OSSRA)



96% of the total codebases **contained** open source

53% of the total codebases **contained license conflicts**

77% of all code in the total codebases **originated** from open source

31% of the total codebases contained open source with **no license** or a **custom license**

10 years

2.8 years

24 months

12 months

14% of the codebases assessed for risk contained vulnerabilities **older than 10 years**

2.8 years was the **mean age of vulnerabilities** in the codebases assessed for risk

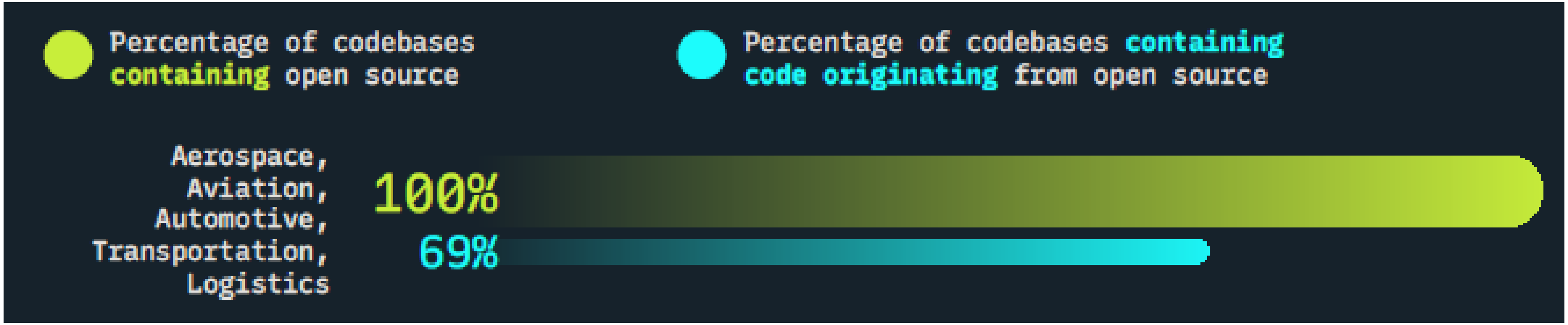
49% of the codebases assessed for risk had components that had **no development activity** in the **past 24 months**

1% of the codebases assessed for risk had components that were at least **12 months behind** on code maintainer **updates/patches**

https://www.blackduck.com/blog/open-source-trends-ossra-report.html

© 2024 Black Duck Software, Inc.

OSSRA 2024 - Automotive



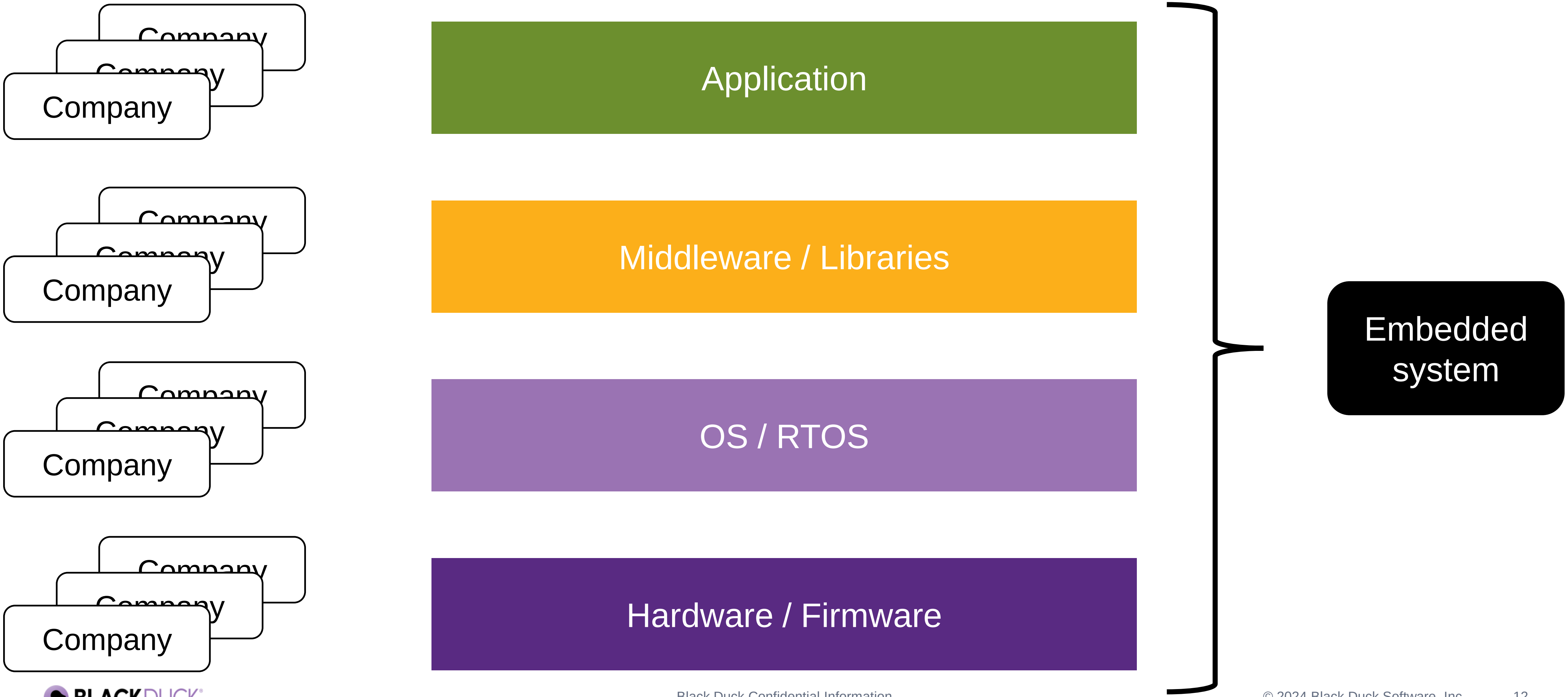
© 2024 Black Duck Software, Inc.

Agenda

- Risks of NOT knowing what’s in your software
- How to know what’s in your software
- Benefits of knowing what’s in your software

OS: Operating System
RTOS: Real Time Operating System

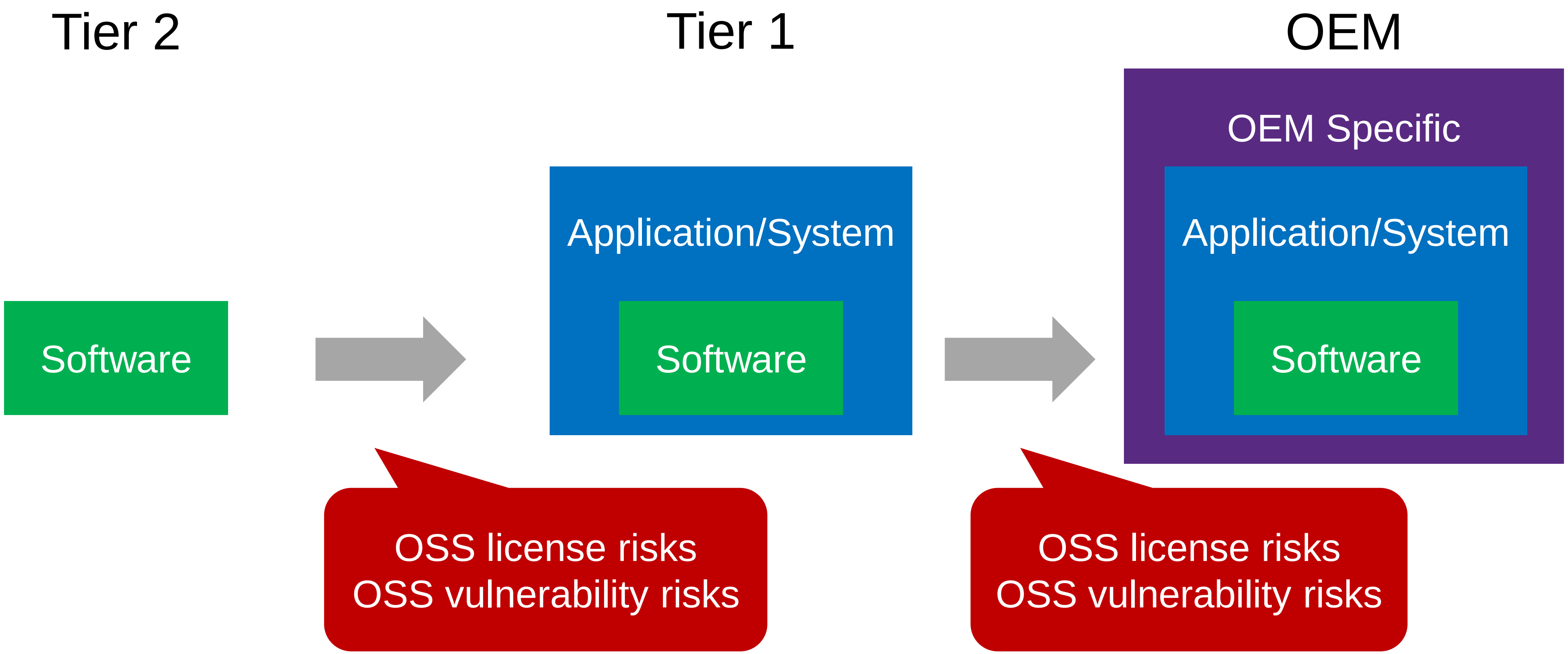
Complex Supply Chain for Embedded Systems



© 2024 Black Duck Software, Inc.

OSS: Open-Source Software
OEM: Original Equipment Manufacturer

Software Supply Chain OSS Risks



Tier 2

Software

Tier 1

Application/System

Software

OEM

OEM Specific

Application/System

Software

OSS license risks
OSS vulnerability risks

OSS license risks
OSS vulnerability risks

Binary supplied - Two options for the receiving side:

- Trust what the supplier tells you what’s in the binary
- Perform binary analysis with a software composition analysis tool

Recommendations:

- Trust but verify
- Scan both source code and binaries, if possible

Overview of OSS Processes

- **OSS whitelist**
  - List of acceptable OSS components
  - Requires periodic reviews

- **OSS policies**
  - Acceptable licenses
  - Number of vulnerabilities/criticality
  - How long OSS project has existed
  - Number of active developers

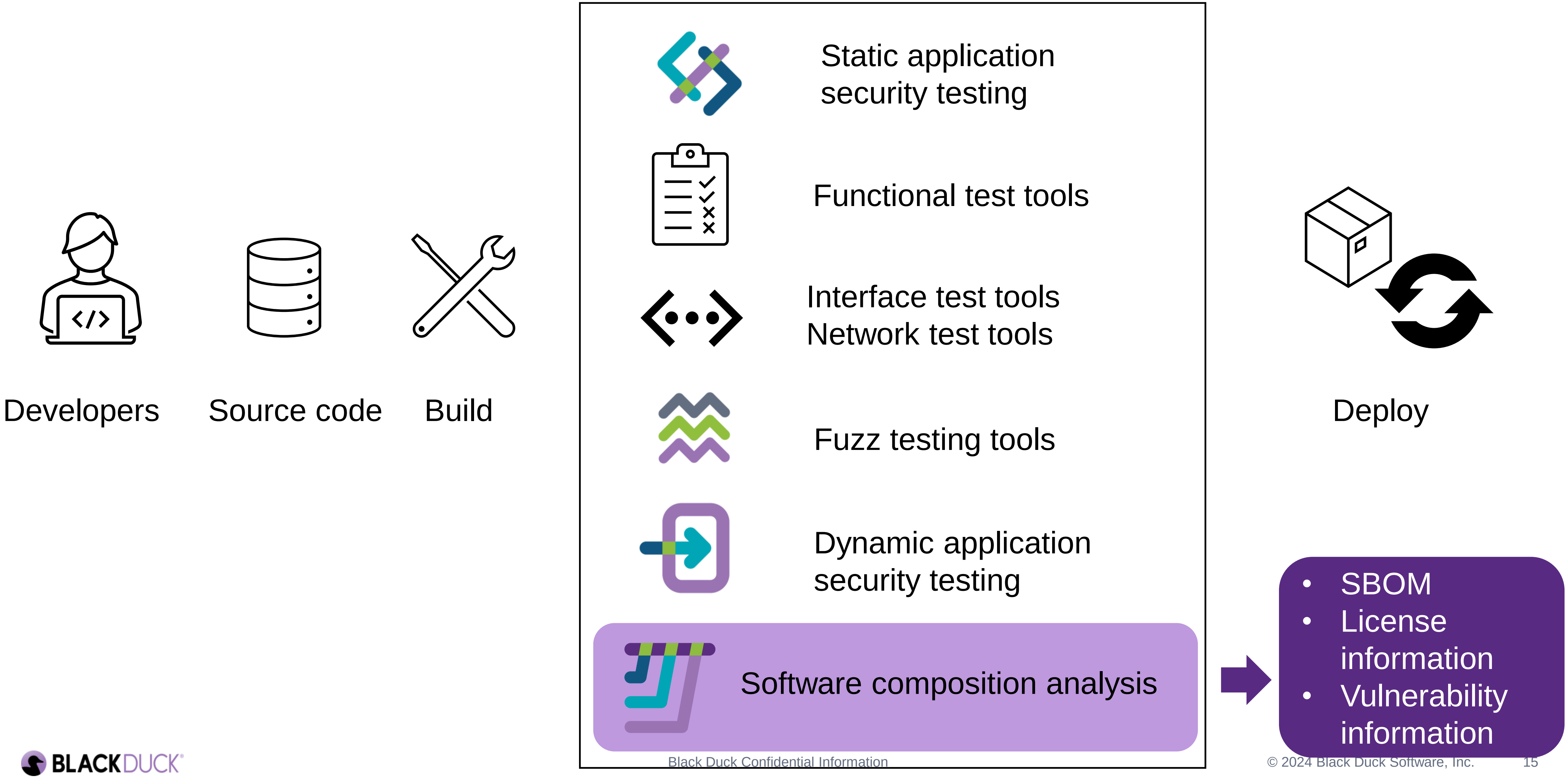
- **Process for adding OSS to the whitelist**
  - Evaluation criteria
  - Approver

- **OSS utilization process**
  - Store OSS component information
  - Cybersecurity monitoring of OSS components

- **OSS vulnerability process**
  - Addressing OSS vulnerabilities

© 2024 Black Duck Software, Inc.

Development Process and Tools



Developers

Source code

Build

Static application security testing

Functional test tools

Interface test tools
Network test tools

Fuzz testing tools

Dynamic application security testing

Software composition analysis

- SBOM
- License information
- Vulnerability information

Deploy

Software Composition Analysis is the Foundation

Visibility
Know what components are entering your code

Security
Be alerted to vulnerabilities in development and production

Compliance
Avoid IP and legal risks due to OSS license violations

Control
Automate policies to govern what components enter your code

Know what's in your code
Establish visibility & control of your software supply chain

Software Composition Analysis (SCA)

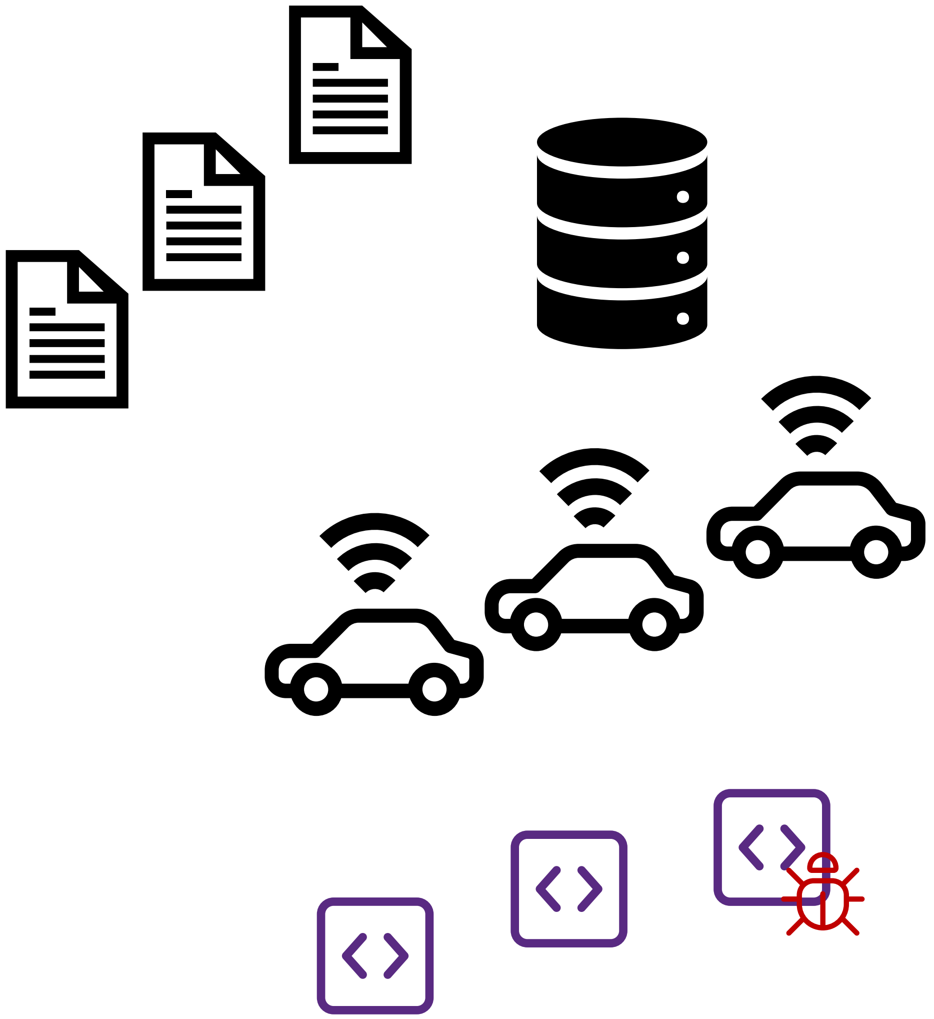
Agenda

- Risks of NOT knowing what’s in your software
- How to know what’s in your software
- Benefits of knowing what’s in your software

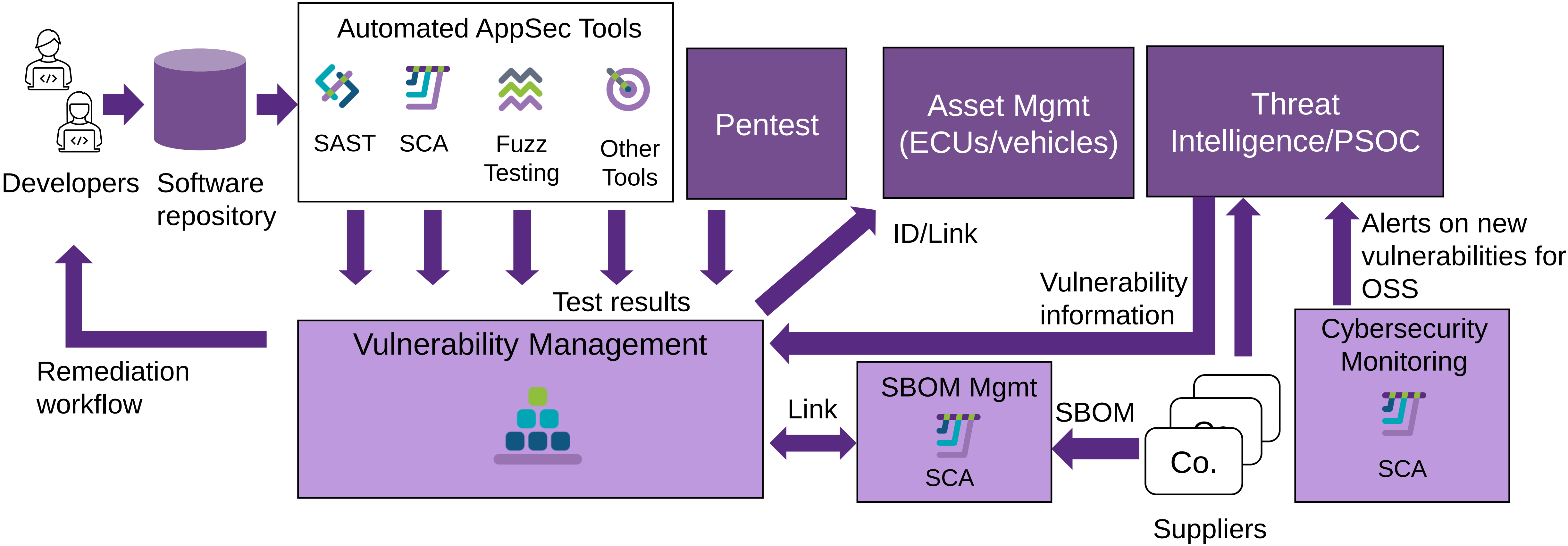
SBOM: Software Bill Of Material

Use Cases for SBOM

- SBOM Management
  - Create, import and aggregate SBOM
- Asset Management
  - Map SBOM to products (ECUs/vehicles)
- Vulnerability Management
  - Import supplier or OSS vulnerability information
  - Map vulnerabilities to software/SBOM
  - (manage vulnerabilities found during development)

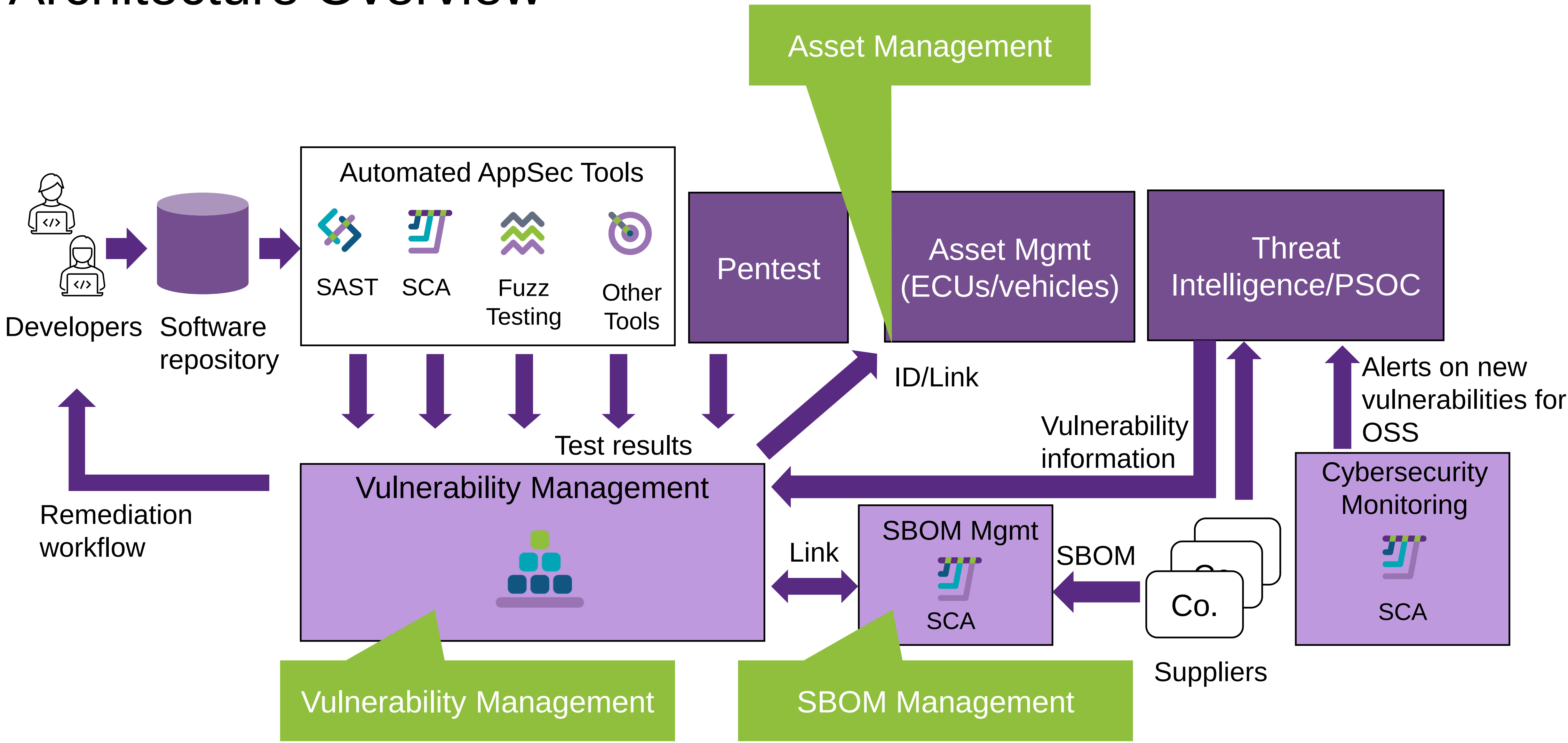


Architecture Overview



© 2024 Black Duck Software, Inc.

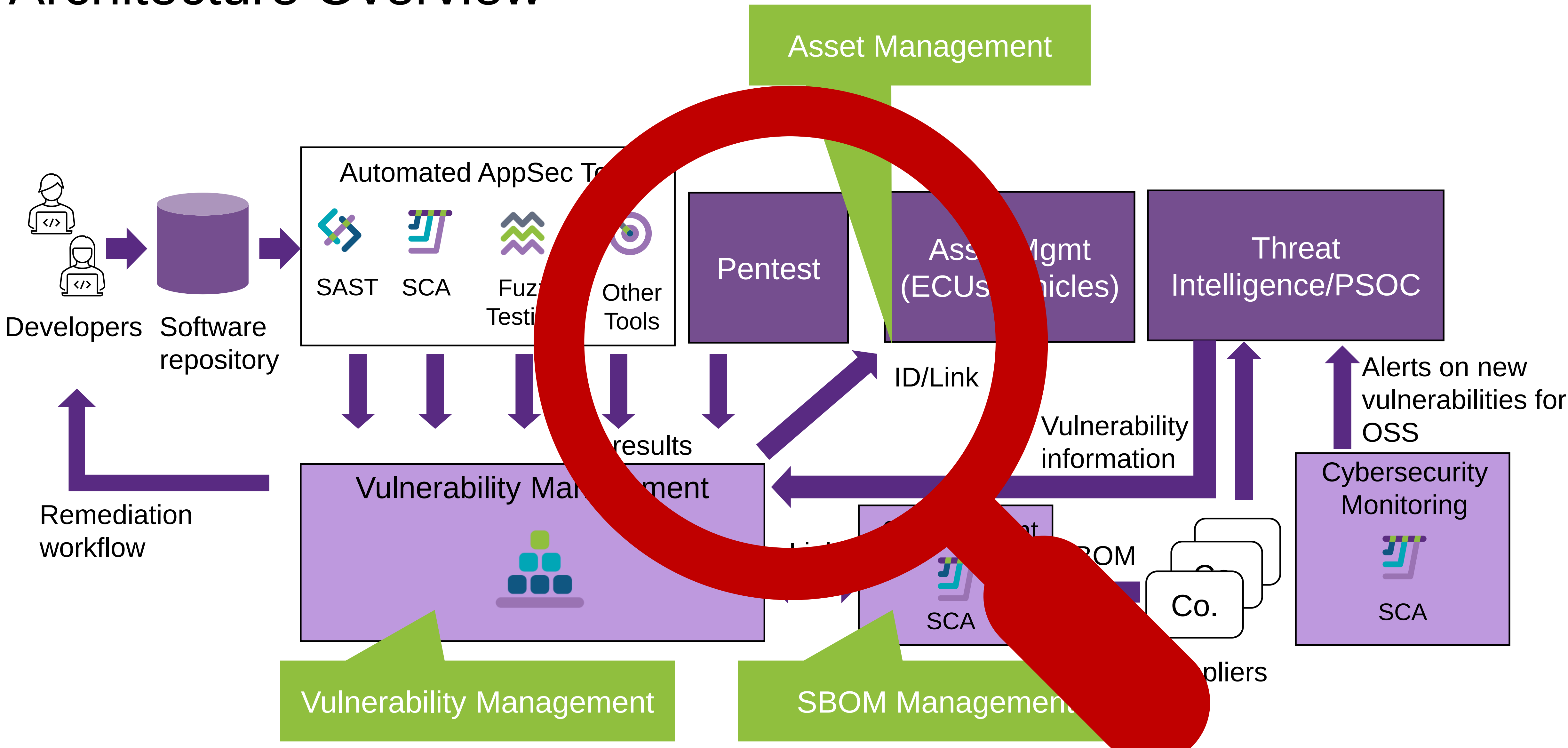
Architecture Overview



© 2024 Black Duck Software, Inc.

SBOM: Software Bill Of Material

Architecture Overview



Asset Management

Automated AppSec To

SAST

SCA

Fuz
Testi

Other
Tools

Developers

Software
repository

Pentest

Ass Mgmt
(ECUs hicles)

Threat
Intelligence/PSOC

ID/Link

Alerts on new
vulnerabilities for
OSS

results

Vulnerability
information

Vulnerability Ma ment

Remediation
workflow

SCA

OM

Co.

pliers

Cybersecurity
Monitoring

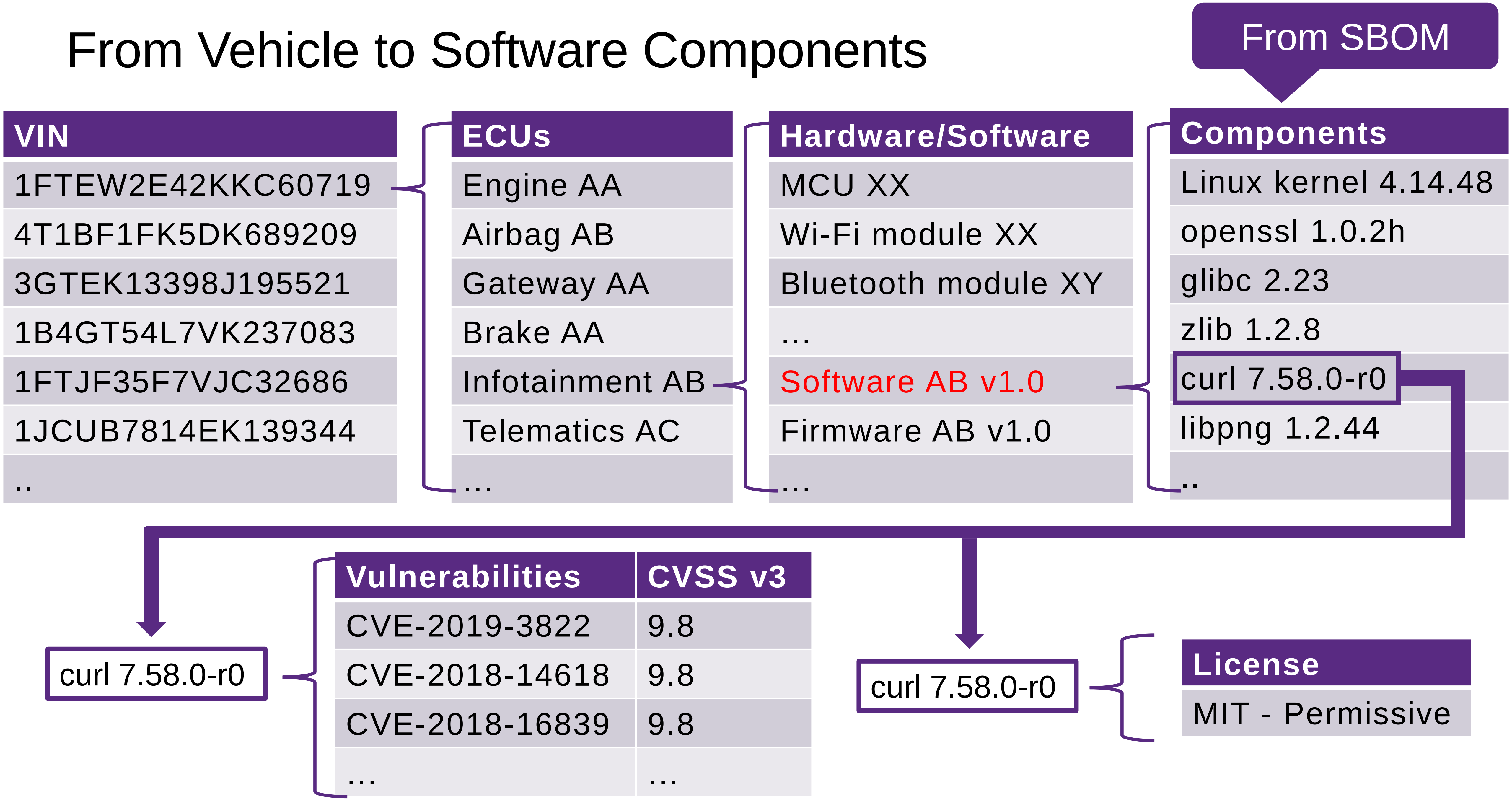
SCA

Vulnerability Management

SBOM Managemen

© 2024 Black Duck Software, Inc.

From Vehicle to Software Components



From SBOM

VIN
1FTEW2E42KKC60719
4T1BF1FK5DK689209
3GTEK13398J195521
1B4GT54L7VK237083
1FTJF35F7VJC32686
1JCUB7814EK139344
..

ECUs
Engine AA
Airbag AB
Gateway AA
Brake AA
Infotainment AB
Telematics AC
…

Hardware/Software
MCU XX
Wi-Fi module XX
Bluetooth module XY
…
Software AB v1.0
Firmware AB v1.0
…

Components
Linux kernel 4.14.48
openssl 1.0.2h
glibc 2.23
zlib 1.2.8
curl 7.58.0-r0
libpng 1.2.44
..

curl 7.58.0-r0

Vulnerabilities	CVSS v3
CVE-2019-3822	9.8
CVE-2018-14618	9.8
CVE-2018-16839	9.8
…	…

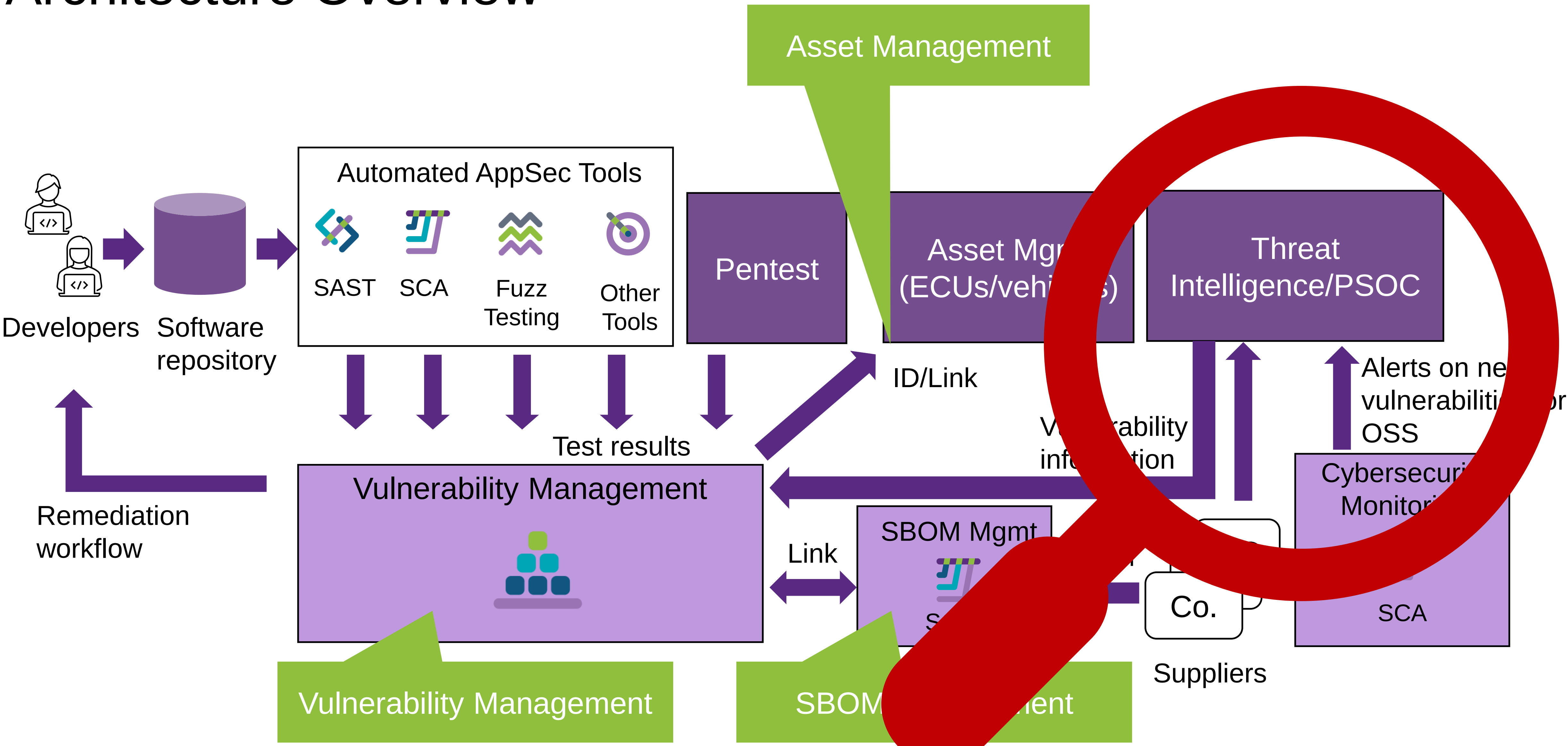
curl 7.58.0-r0

License
MIT - Permissive

VIN: Vehicle Identification Number CVSS: Common Vulnerability Scoring System

SBOM: Software Bill Of Material

Architecture Overview



Asset Management

Developers

Software repository

Automated AppSec Tools

SAST

SCA

Fuzz Testing

Other Tools

Pentest

Asset Mgr (ECUs/vehi s)

Threat Intelligence/PSOC

ID/Link

Test results

V rability inf tion

Alerts on ne vulnerabiliti or OSS

Remediation workflow

Vulnerability Management

Link

SBOM Mgmt

S

Co.

Cybersecuri Monitori

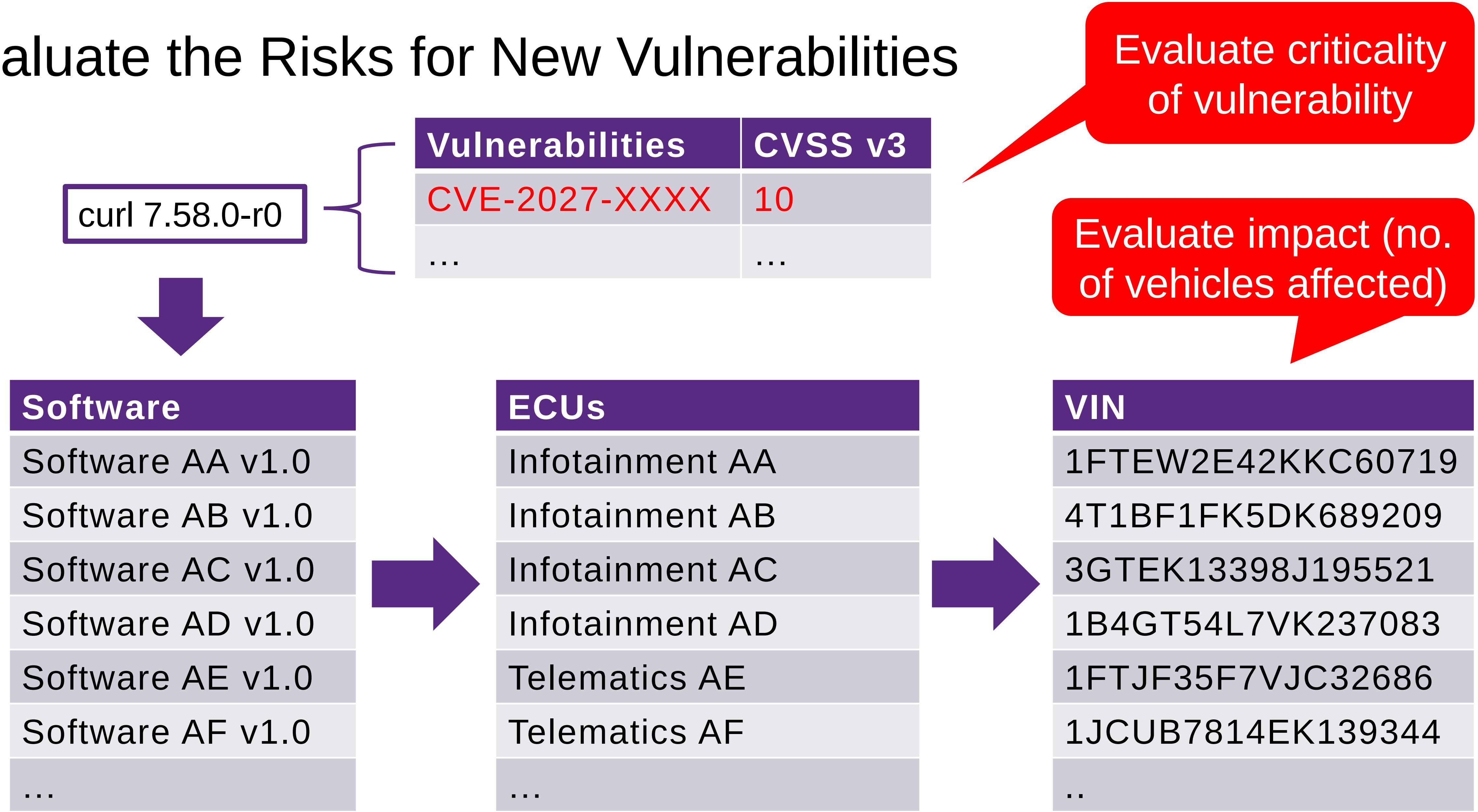
SCA

Suppliers

Vulnerability Management

SBOM ent

Evaluate the Risks for New Vulnerabilities



Evaluate criticality of vulnerability

curl 7.58.0-r0

Vulnerabilities	CVSS v3
CVE-2027-XXXX	10
…	…

Evaluate impact (no. of vehicles affected)

Software
Software AA v1.0
Software AB v1.0
Software AC v1.0
Software AD v1.0
Software AE v1.0
Software AF v1.0
…

ECUs
Infotainment AA
Infotainment AB
Infotainment AC
Infotainment AD
Telematics AE
Telematics AF
…

VIN
1FTEW2E42KKC60719
4T1BF1FK5DK689209
3GTEK13398J195521
1B4GT54L7VK237083
1FTJF35F7VJC32686
1JCUB7814EK139344
..

CVSS: Common Vulnerability Scoring System

Black Duck Confidential Information

© 2024 Black Duck Software, Inc.

Software Repository

Software
Software AA v1.0
Software AB v1.0
Software AC v1.0
Software AD v1.0
Software AE v1.0
Software AF v1.0
…

Vulnerable Software

OTA Platform:

- Secure communication
- Digital signatures
- …

Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.0
4T1BF1FK5DK689209	Software AB v1.0
3GTEK13398J195521	Software AC v1.0
1B4GT54L7VK237083	Software AD v1.0
1FTJF35F7VJC32686	Software AE v1.0
1JCUB7814EK139344	Software AF v1.0
..	…

OTA: Over the Air

© 2024 Black Duck Software, Inc.

Software Repository

Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.0
4T1BF1FK5DK689209	Software AB v1.0
3GTEK13398J195521	Software AC v1.0
1B4GT54L7VK237083	Software AD v1.0
1FTJF35F7VJC32686	Software AE v1.0
1JCUB7814EK139344	Software AF v1.0
..	…

OTA Platform:

- Secure communication
- Digital signatures
- …

© 2024 Black Duck Software, Inc.

Software Repository

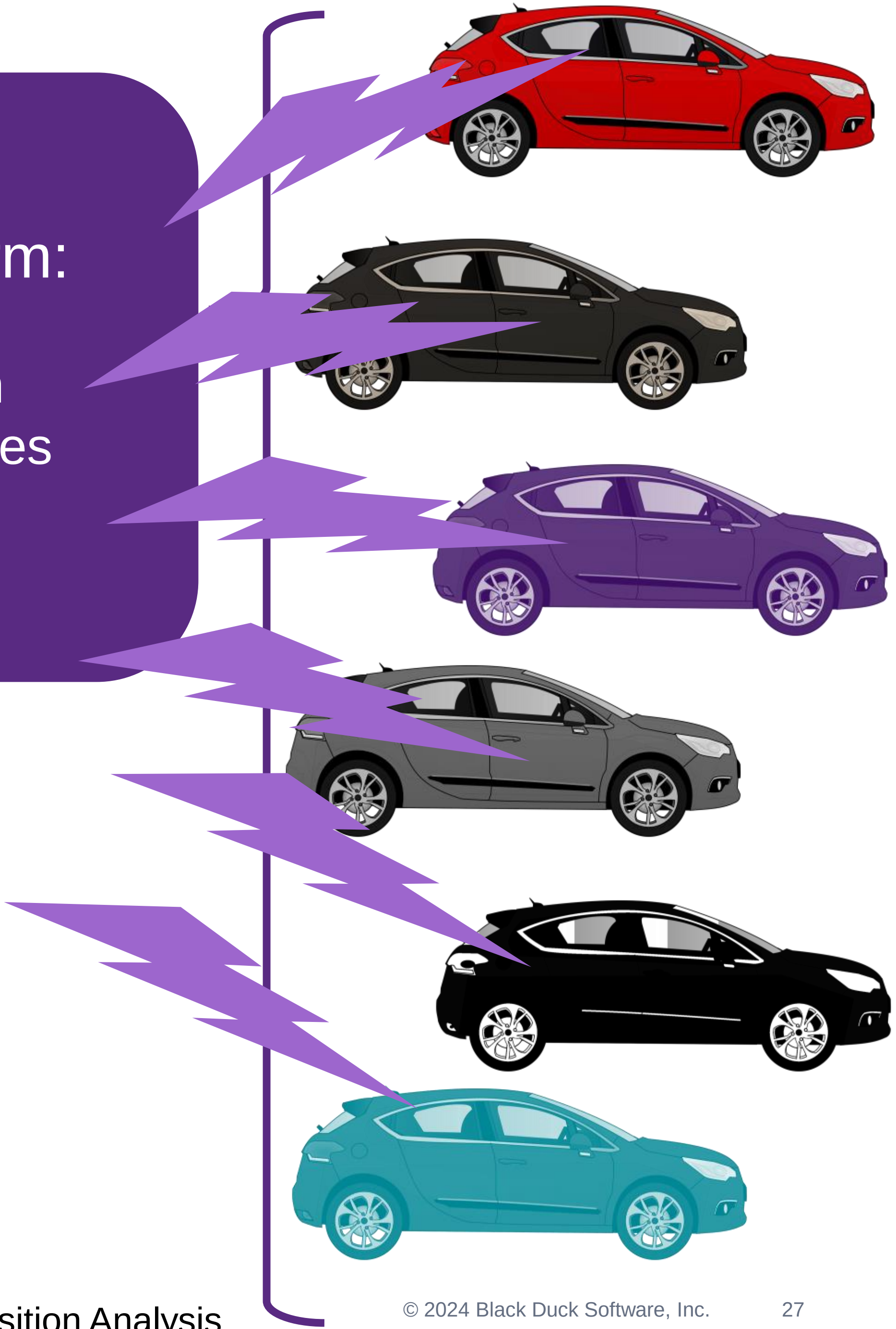
Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

AppSec testing to minimize new vulnerabilities before new software is pushed out

OTA Platform:

Secure communication

- Digital signatures
- …



Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.0
4T1BF1FK5DK689209	Software AB v1.0
3GTEK13398J195521	Software AC v1.0
1B4GT54L7VK237083	Software AD v1.0
1FTJF35F7VJC32686	Software AE v1.0
1JCUB7814EK139344	Software AF v1.0
..	…

© 2024 Black Duck Software, Inc.

Software Repository

Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

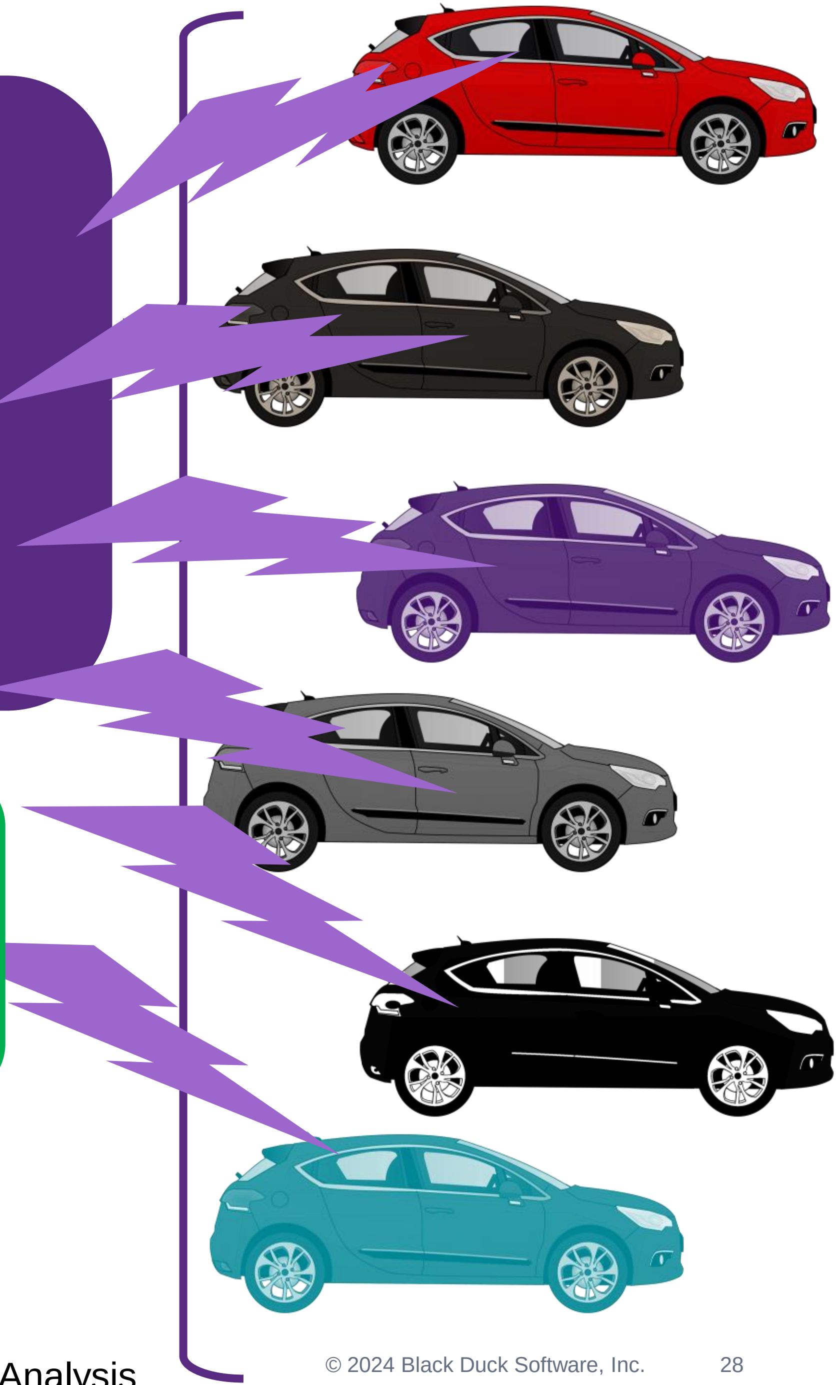
OTA Platform:

- Secure communication
- Digital signatures
- …

Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.1
4T1BF1FK5DK689209	Software AB v1.1
3GTEK13398J195521	Software AC v1.1
1B4GT54L7VK237083	Software AD v1.1
1FTJF35F7VJC32686	Software AE v1.1
1JCUB7814EK139344	Software AF v1.1
..	…

Map new SBOM to Asset Mgmt system

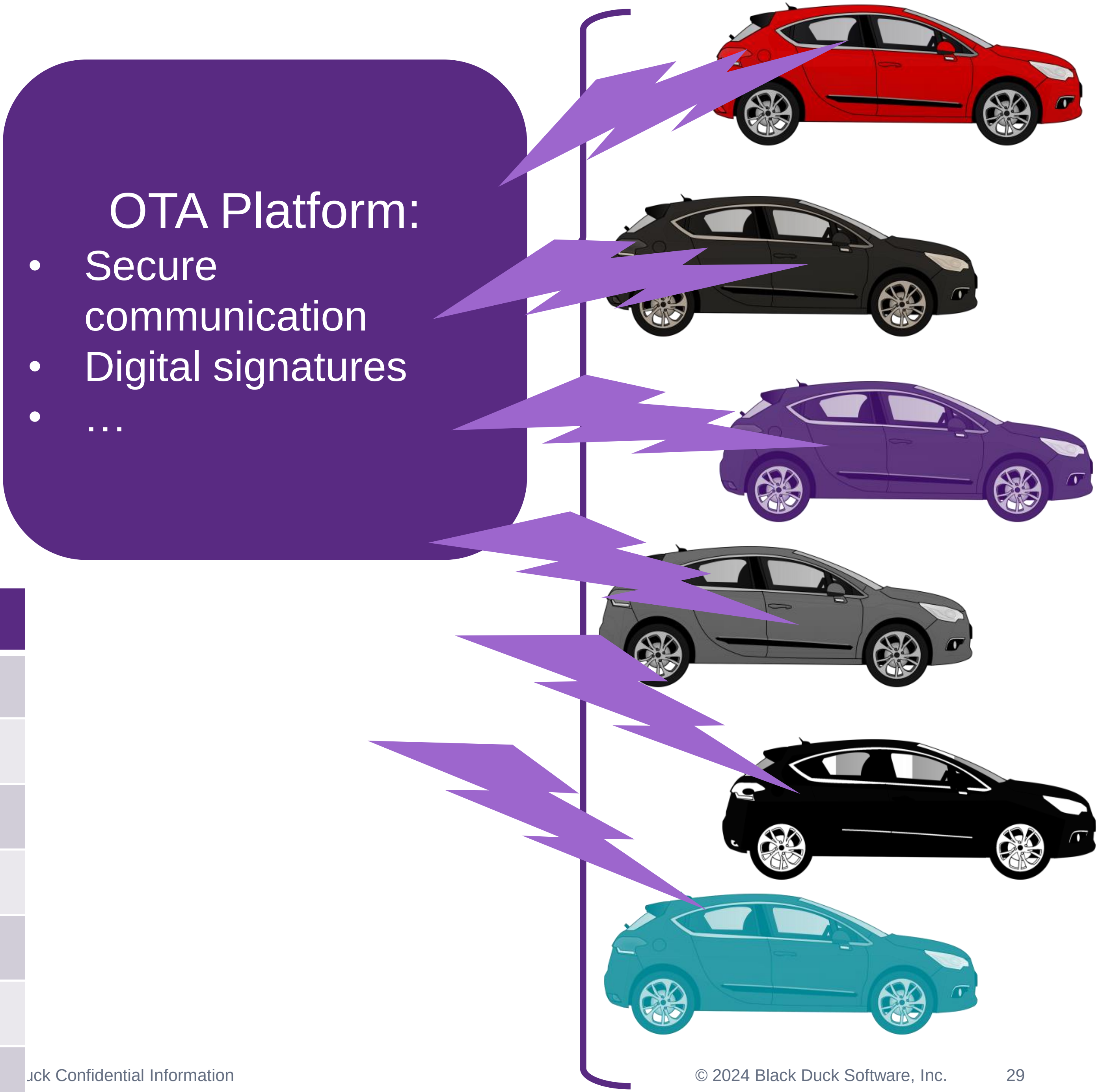


Software Repository

Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.1
4T1BF1FK5DK689209	Software AB v1.1
3GTEK13398J195521	Software AC v1.1
1B4GT54L7VK237083	Software AD v1.1
1FTJF35F7VJC32686	Software AE v1.1
1JCUB7814EK139344	Software AF v1.1
..	…



OTA Platform:

- Secure communication
- Digital signatures
- …

Call to Action

Reduce risks by knowing what’s in your software

- License risks
- Vulnerabilities
- SBOM management, Asset Management, Vulnerability Management

Consider how to collaborate on SBOM

- Auto-ISAC
- NTIA
- OpenChain
- GlobalPlatform
- …

Thank You