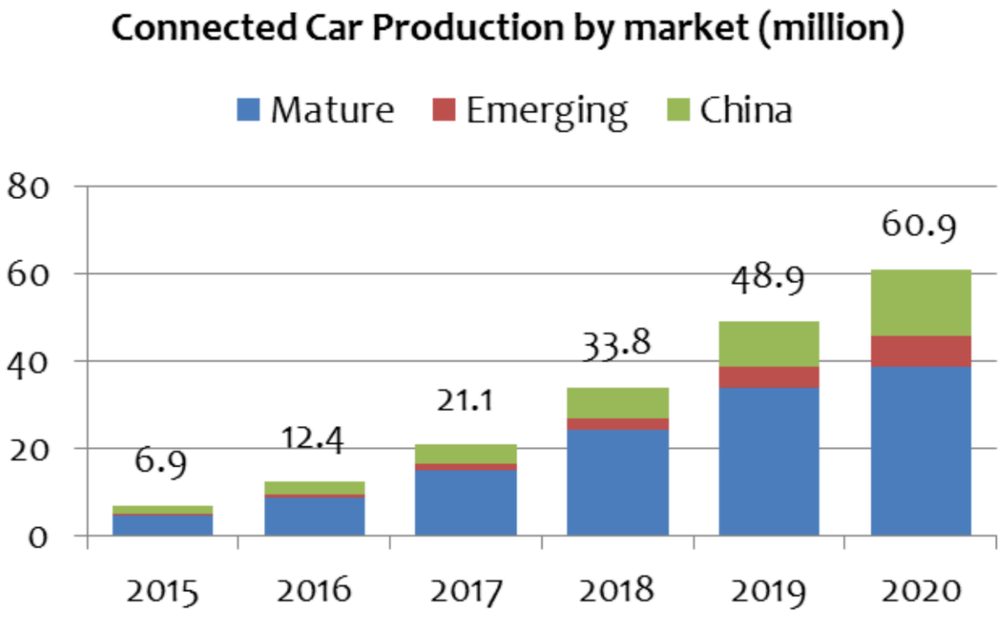
Binary Scanning: The First Line of Defense Against Security Breaches

Tae-Jin (TJ) Kang

President & CEO, Insignary

taejin@insignary.com

Connected car market

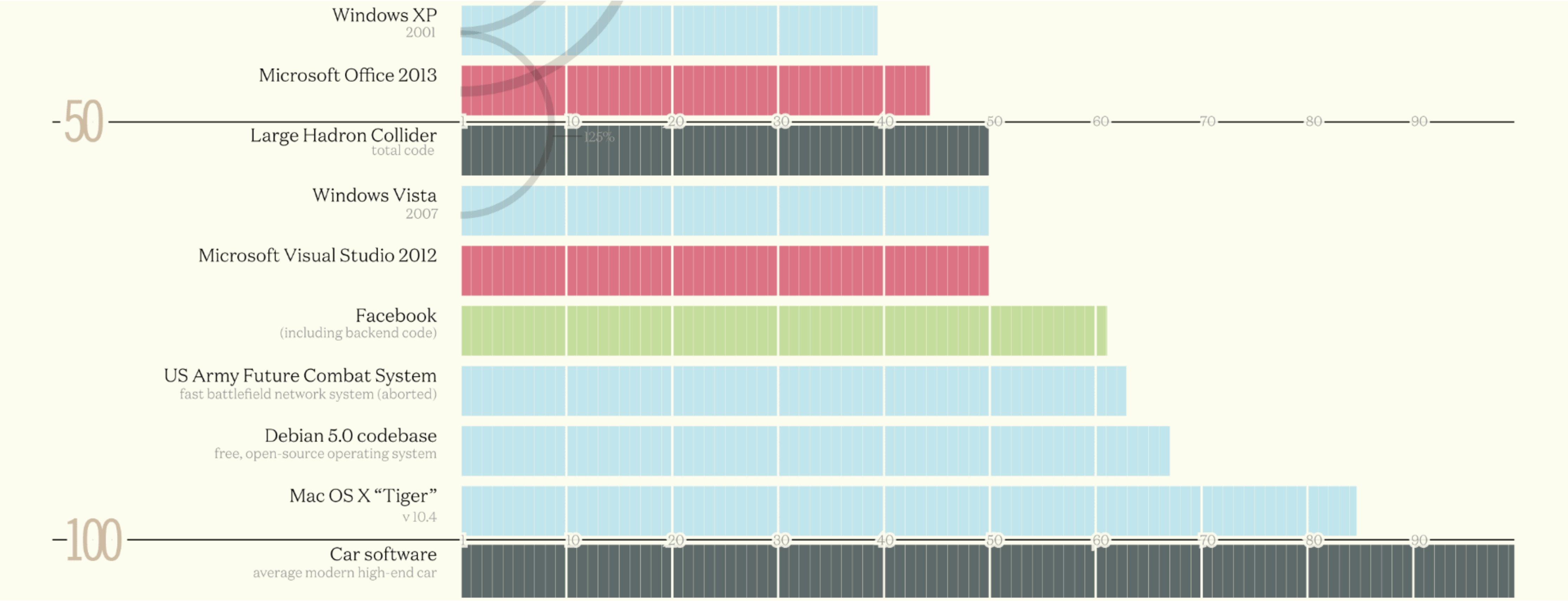


Source: Gartner via Linked Motion

- 152 million actively connected cars on global roads by 2020
- Technology companies are targeting automobile market for bigger revenues
- Automotive industry needs to be prepared for 4 terabytes of data being generated by every car every day (Brian Krzanich, CEO of Intel Corporation)

insignary

100 million lines of code



Source: Information is Beautiful

insignary

> “As vehicles get smarter, cyber security in the automotive industry is becoming an increasing concern. Whether we’re turning cars into Wi-Fi connected hotspots or equipping them with millions of lines of code to create fully autonomous vehicles, cars are more vulnerable than ever to hacking and data theft.”

- The key principles of vehicle cyber security for connected and automated vehicles

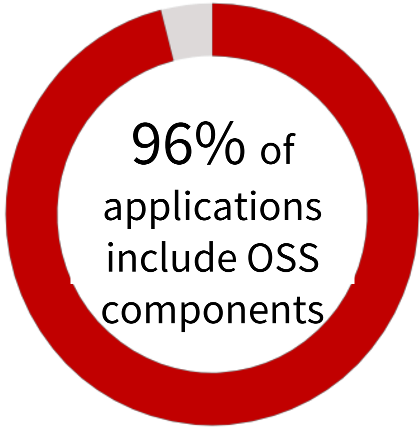
insignary

Focusing on open source software security

insignary

Open source software trends

OSS is ubiquitous



96% of applications include OSS components

In 2017, the average app contained 147 unique OSS components

In 2018, the average app contains 257 unique OSS components

OSS comprises, on average, 23% of automotive commercial applications

OSS adoption is growing

In 2017, OSS comprised an average of 36% of codebase

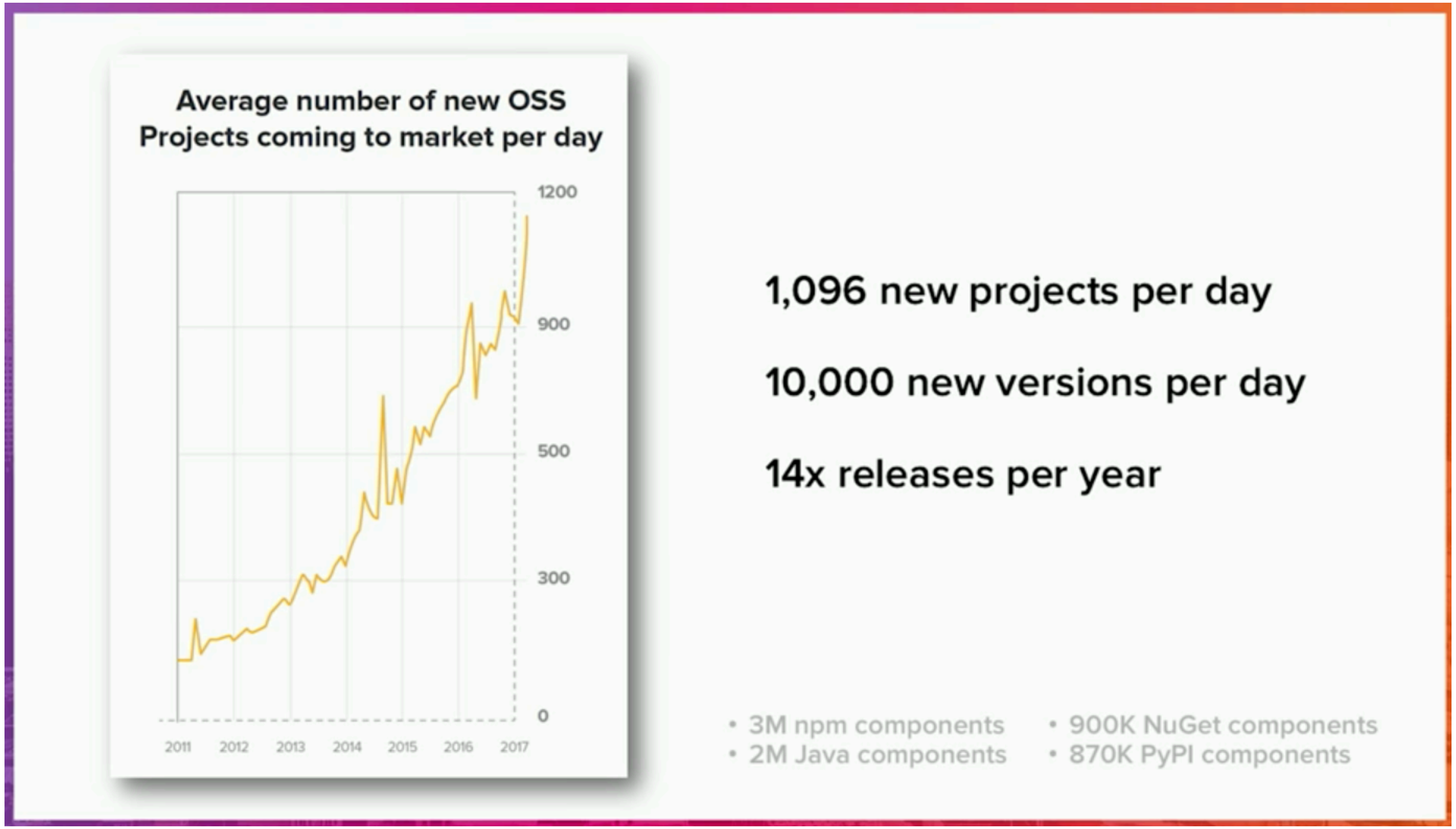
In 2018, OSS comprises an average of 57% of codebase

Many applications now contain more open source code than proprietary code

Source: Synposys

insignary

Open source software trends



Average number of new OSS Projects coming to market per day

1,096 new projects per day

10,000 new versions per day

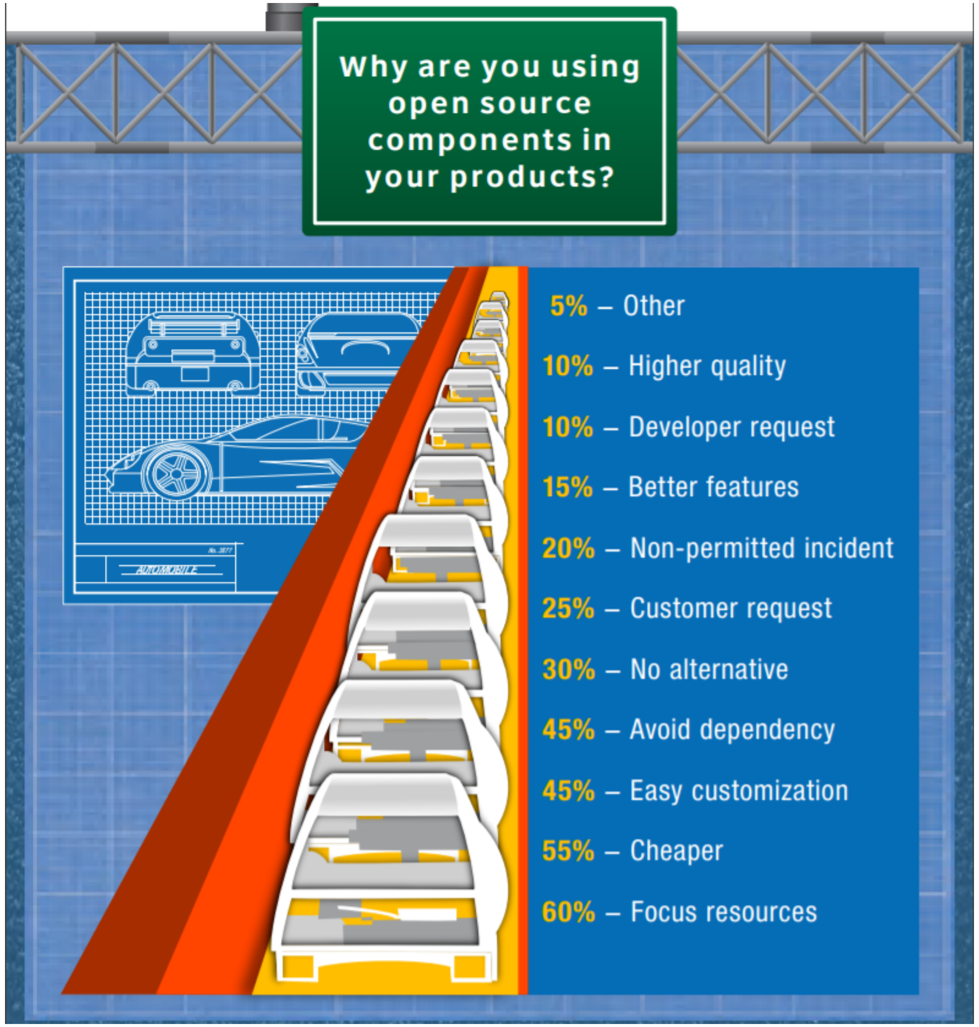
14x releases per year

- 3M npm components
- 2M Java components

- 900K NuGet components
- 870K PyPI components

Source: Sonatype

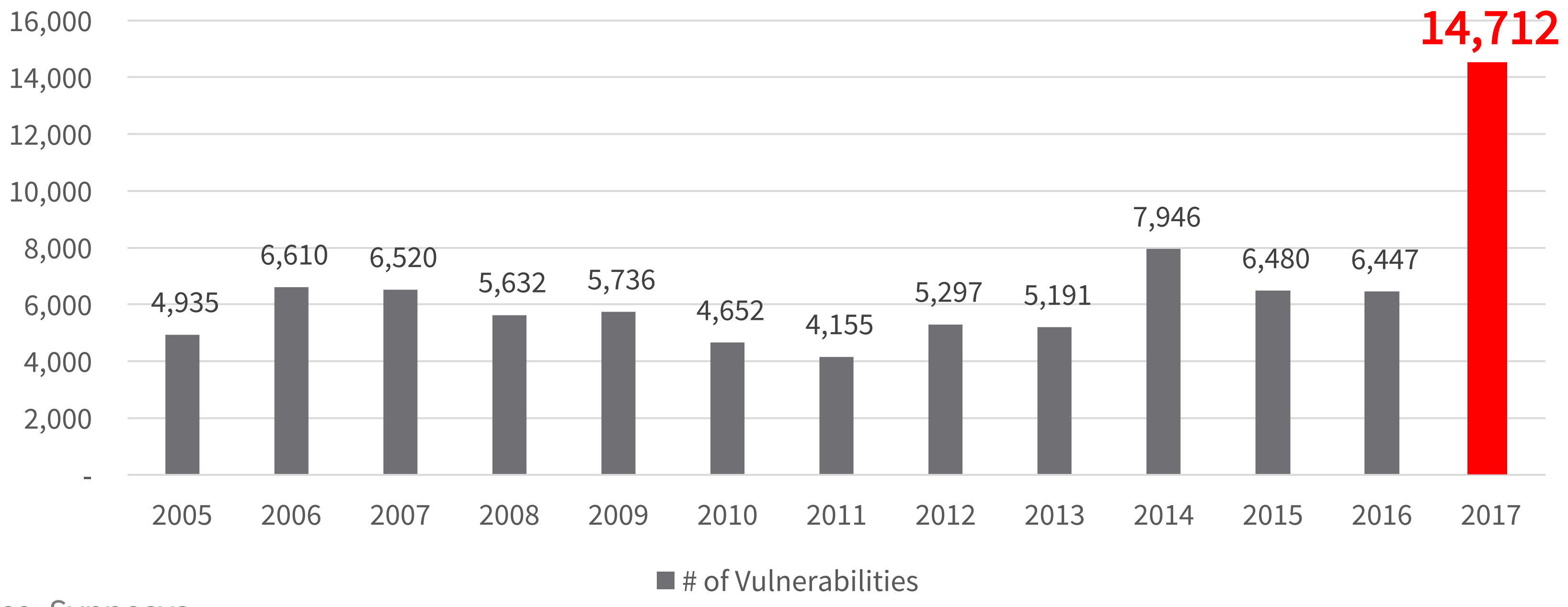
Open source software trends



Source: BearingPoint

Growth in OSS vulnerabilities

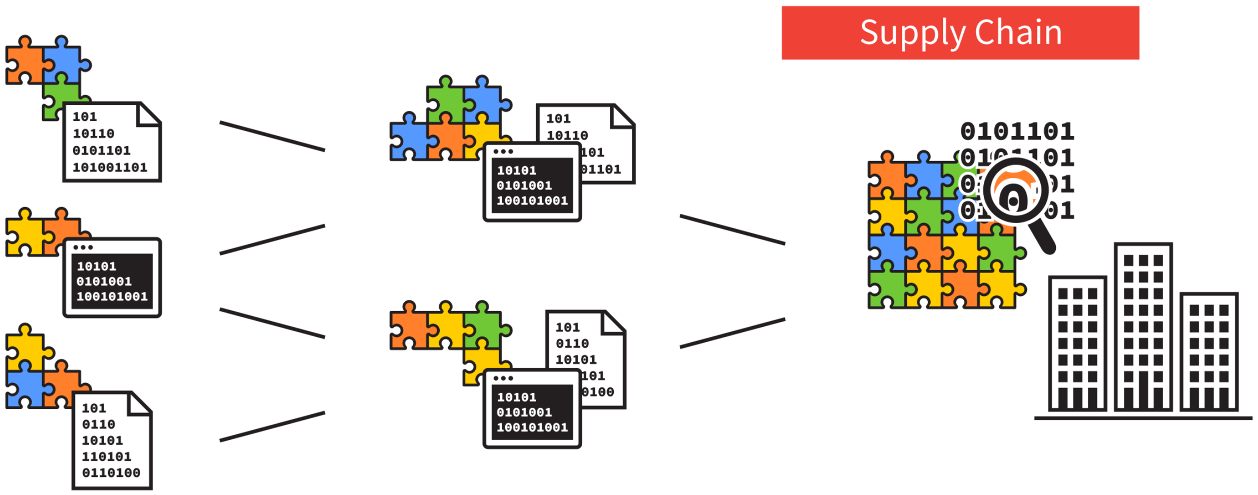
- 2017 – 14,712 new vulnerabilities reported to CVE list
  - 4,800 OSS-related security vulnerabilities
  - Number of OSS vulnerabilities per codebase increased by 134%
- 2018 – on pace to reach 16,500 vulnerabilities, breaking last year's record



Source: Synposys

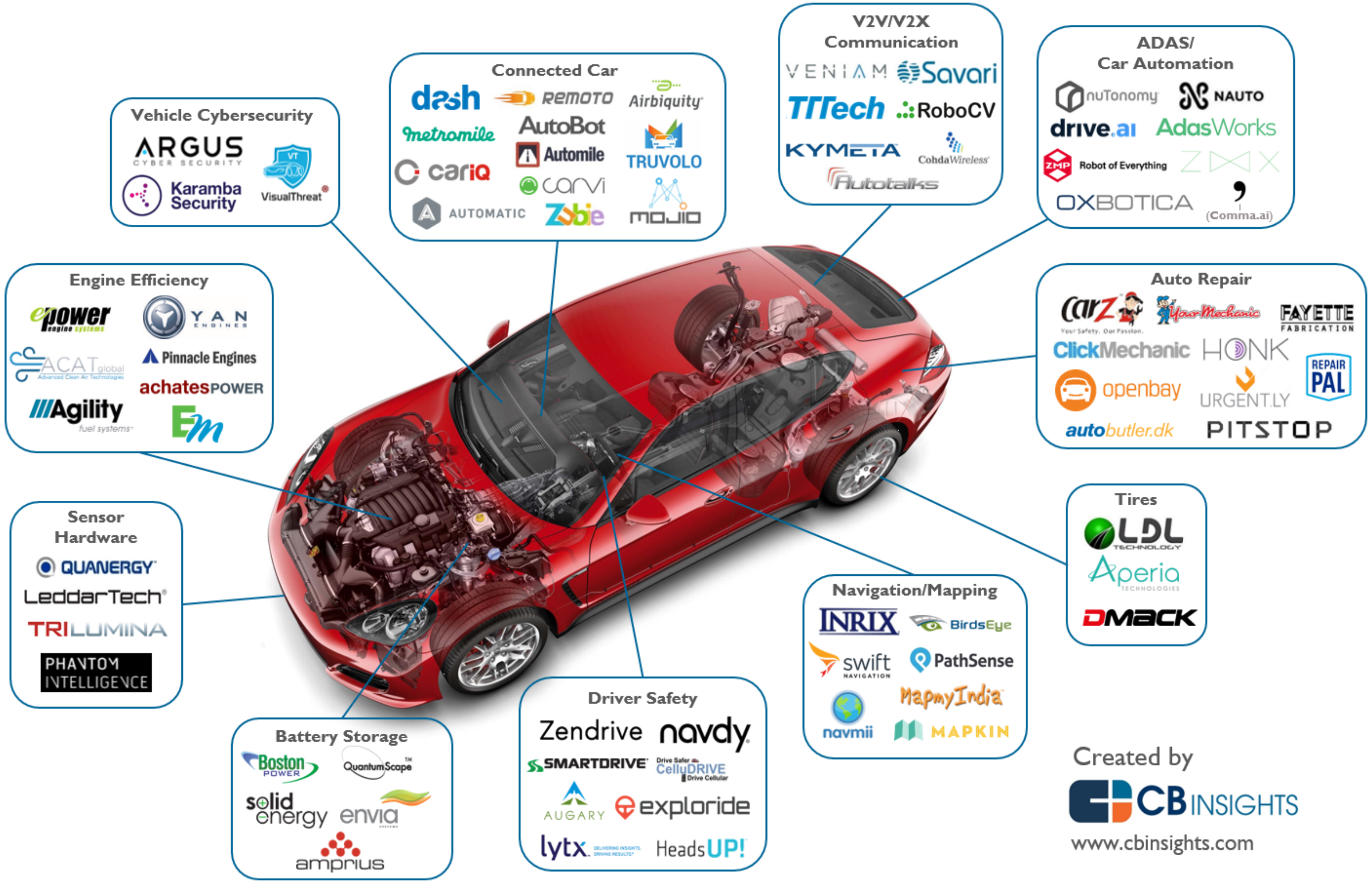
Software procurement model

- Organizations leverage third-party code to lower costs and increase efficiency
- Third-party software is distributed in binary format without the source code
  - Challenging for auto manufacturers and their suppliers to keep track of the OSS components they use and identify any associated vulnerabilities



It is hard to identify binaries from third parties

Unbundling the automobile



Vehicle Cybersecurity
- ARGUS Cyber Security
- VisualThreat
- Karamba Security

Connected Car
- dash
- Remoto
- Airbiquity
- metromile
- AutoBot
- TRUVOLO
- Automile
- cariQ
- carvi
- AUTOMATIC
- Zubie
- mojio

V2V/V2X Communication
- VENIAM
- Savari
- TTTech
- RoboCV
- KYMETA
- Cohda Wireless
- Autotalks

ADAS/ Car Automation
- nuTonomy
- NAUTO
- drive.ai
- AdasWorks
- ZMP Robot of Everything
- ZOOX
- OXBOTICA
- (Comma.ai)

Engine Efficiency
- epower engine systems
- YAN Engines
- ACAT global Advanced Clean Air Technologies
- Pinnacle Engines
- achatesPOWER
- Agility fuel systems
- EM

Auto Repair
- CarZ Your Safety. Our Passion.
- YourMechanic
- FAYETTE FABRICATION
- ClickMechanic
- HONK
- REPAIR PAL
- openbay
- URGENT.LY
- autobutler.dk
- PITSTOP

Sensor Hardware
- QUANERGY
- LeddarTech
- TRILUMINA
- PHANTOM INTELLIGENCE

Tires
- LDL Technology
- Aperia Technologies
- DMACK

Navigation/Mapping
- INRIX
- BirdsEye
- swift navigation
- PathSense
- MapmyIndia
- navmii
- MAPKIN

Driver Safety
- Zendrive
- navdy
- SMARTDRIVE
- CellyDRIVE Drive Safer Drive Cellular
- AUGARY
- exploride
- lytx
- HeadsUP!

Battery Storage
- Boston Power
- QuantumScape
- solid energy
- envia
- amprius

Created by

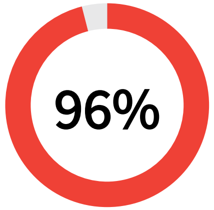
CB INSIGHTS

www.cbinsights.com

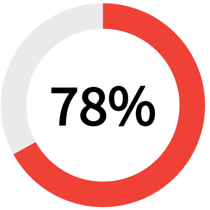
Source: CB Insights

insignary

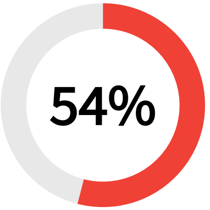
Organizations are unprepared



of scanned applications included open source software components, with an average of **257** components per application.



of the codebase examined contained at least one vulnerability, with an average of **64** vulnerabilities per application.



of vulnerabilities found in analyzed applications ranked “**HIGH SEVERITY**.”

On average, these vulnerabilities were disclosed almost 6 years ago.

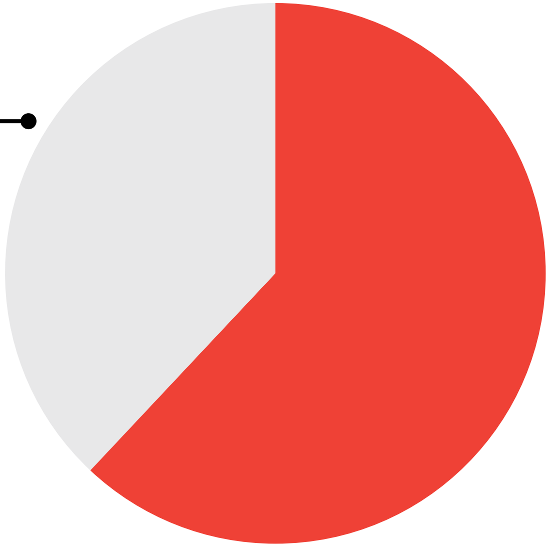
2011

Source: Synposys

insignary

Organizations are unprepared

“How well does your organization control which open source and third-party components are used in development?”



38%

have a complete software bill of materials for each application.

62%

of organizations do not have meaningful controls over what components are in their applications.

Source: Sonatype

insignary

Equifax breach was preventable

EQUIFAX

	Heartbleed	Shellshock	Freak	Ghost	DROWN	SambaCry	Jakarta
Discovery	2014	2014	2015	2015	2016	2016	2017
Release	2011	1989	1990s	2000	1990s	1990s	2007
Component	OpenSSL	Bash	OpenSSL	GNU C Library	OpenSSL	SAMBA	Apache Struts

Exploited Known Security Vulnerability in Apache Struts

March 2017

April 2017

May ~ July 2017

First discovered
patch update in March

60 days to fix

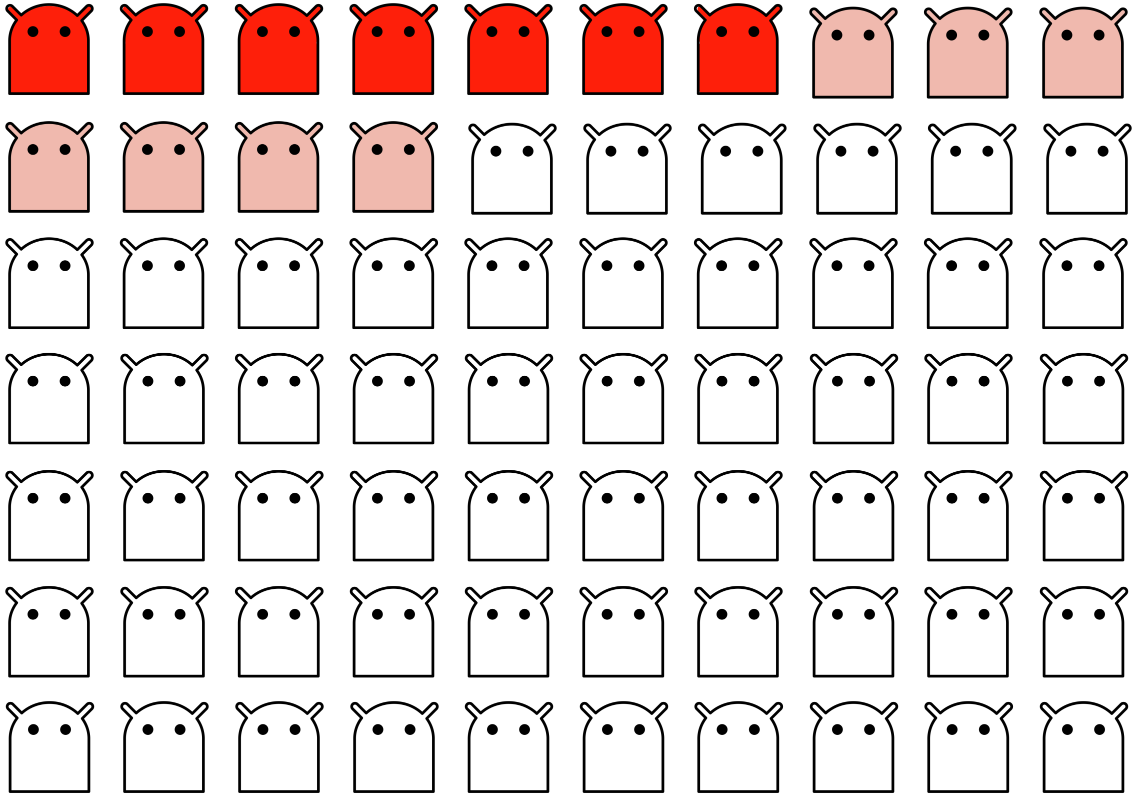
Breach occurred
in mid-May to July

Personal data of 148 million individuals exposed

insignary

1 in 5 Android apps are vulnerable

- Comprehensive binary scan of 700 Android apps on the Google Play Store, consisting of the 20 most popular apps in each of the 35 Android app categories
- 136 apps contained known security vulnerabilities, meaning approximately 1 in 5 apps do not use the correct, most up-to-date OSS component versions available
- 57% of the detected vulnerable apps contained vulnerabilities that ranked "High Severity"

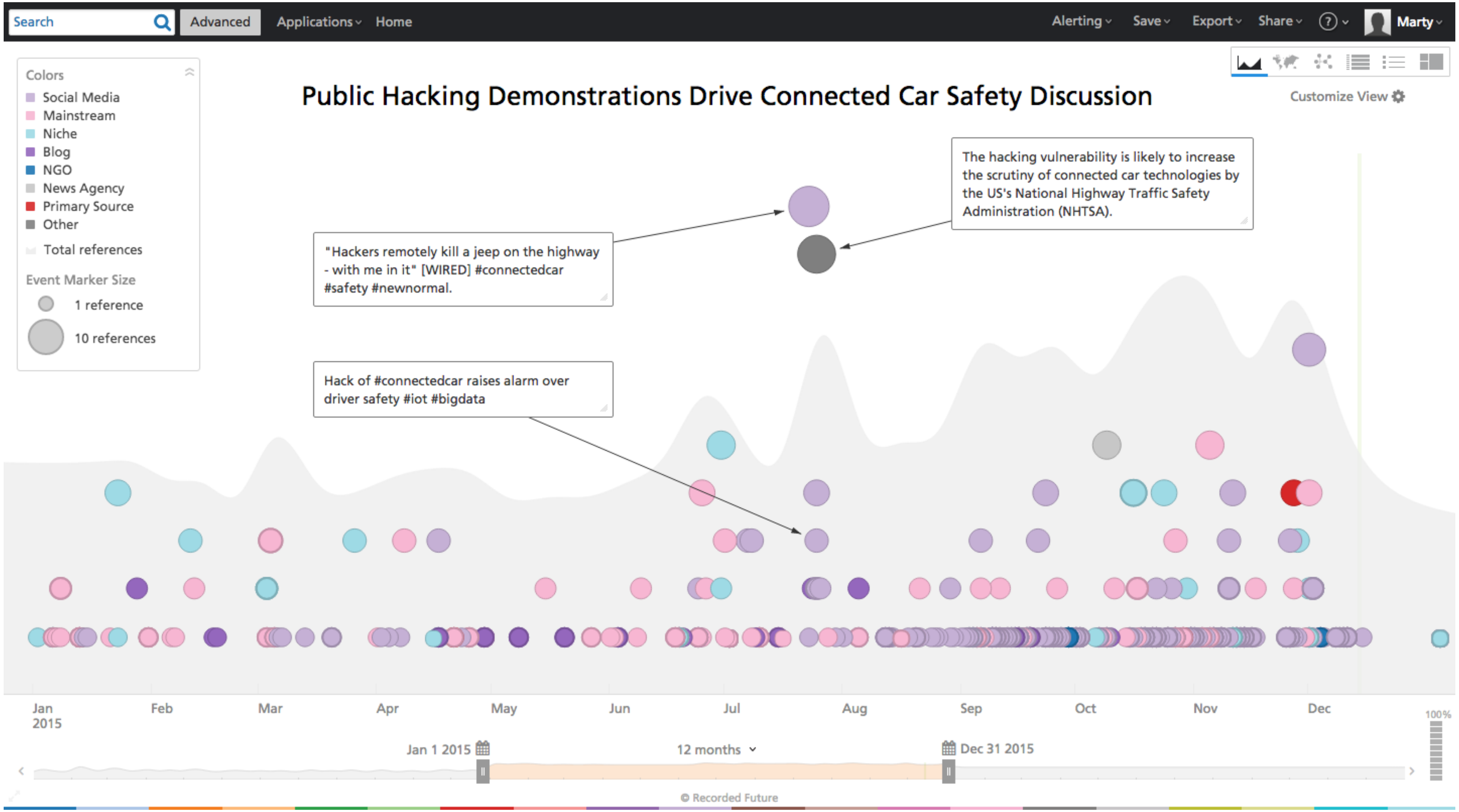


insignary

Innovation is outpacing security

- Miller/Valasek: Viral hijacking of the brakes and transmission of a Jeep Cherokee. As a result, Chrysler recalled 1.4 million vehicles to fix the exploited bug.
- GM: For five years, millions of their vehicles were vulnerable to a remote exploit, ranging from tracking vehicles to disabling the brakes.
- Tesla: A four-year-old vulnerability in Model S's infotainment system could have enabled a fully remote hack to start the car or cut the motor.
- Evenchick's CANtact: Open source toolkit designed to interact with the Controller Area Network (CAN) bus. A user disclosed a security vulnerability that could have enabled a hacker to control the vehicle.

insignary



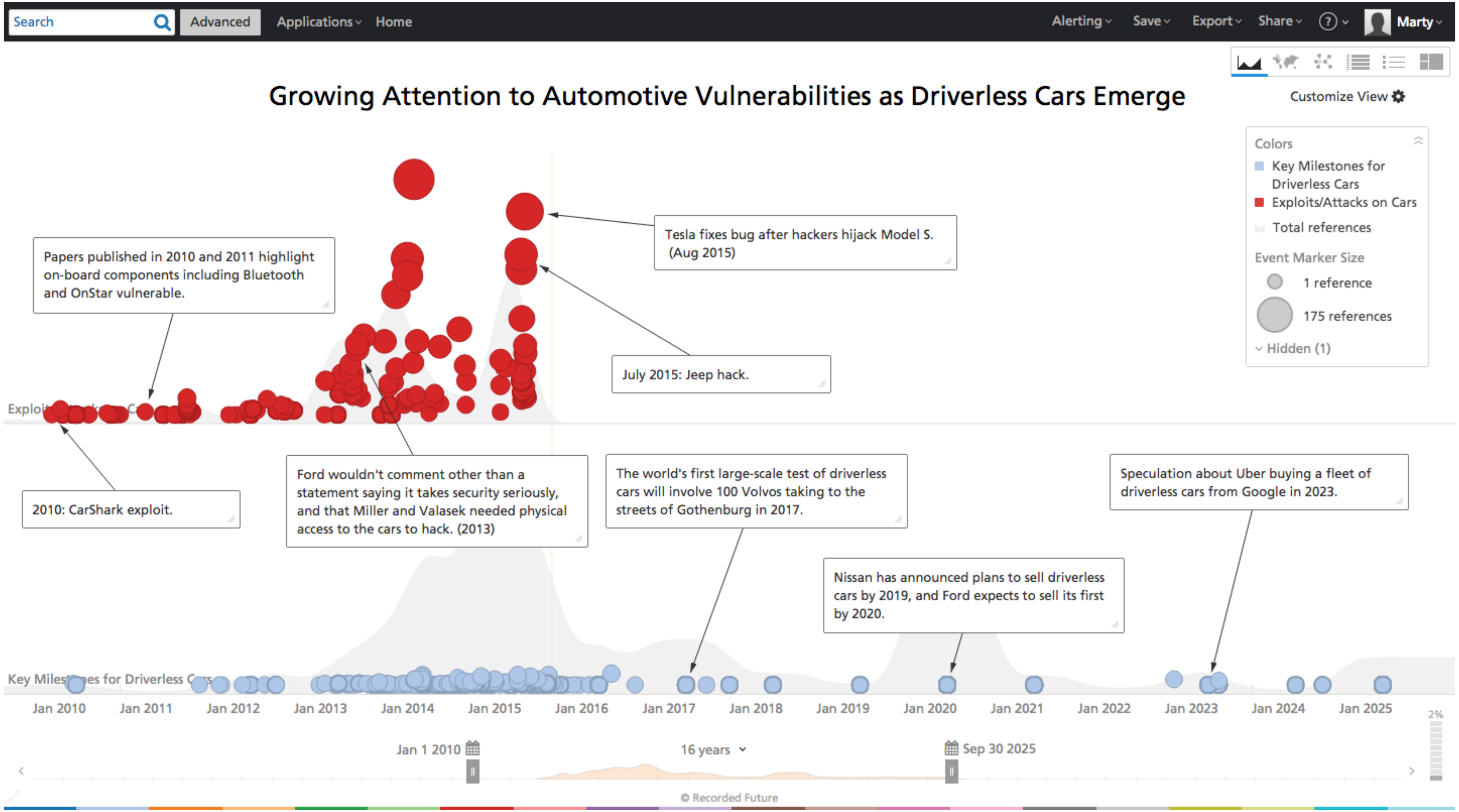
Public Hacking Demonstrations Drive Connected Car Safety Discussion

"Hackers remotely kill a jeep on the highway - with me in it" [WIRED] #connectedcar #safety #newnormal.

The hacking vulnerability is likely to increase the scrutiny of connected car technologies by the US's National Highway Traffic Safety Administration (NHTSA).

Hack of #connectedcar raises alarm over driver safety #iot #bigdata

Source: Recorded Future



Growing Attention to Automotive Vulnerabilities as Driverless Cars Emerge

Papers published in 2010 and 2011 highlight on-board components including Bluetooth and OnStar vulnerable.

Tesla fixes bug after hackers hijack Model S. (Aug 2015)

July 2015: Jeep hack.

2010: CarShark exploit.

Ford wouldn't comment other than a statement saying it takes security seriously, and that Miller and Valasek needed physical access to the cars to hack. (2013)

The world's first large-scale test of driverless cars will involve 100 Volvos taking to the streets of Gothenburg in 2017.

Speculation about Uber buying a fleet of driverless cars from Google in 2023.

Nissan has announced plans to sell driverless cars by 2019, and Ford expects to sell its first by 2020.

Source: Recorded Future

Addressing security threats before they become a problem

insignary

Static code analyzers

- Designed to analyze source code to find common programming errors, such as buffer overflows and SQL Injection Flaws
- Offers limited binary code analysis by disassembling binary code to obtain source code
  - Potential violation of intellectual property laws

Limitations of SAST and DAST

<table>
<tr><th>Static Application Security Testing</th><th>Dynamic Application Security Testing</th></tr>
<tr><td colspan="2">Can help automakers and their software suppliers identify coding errors – effective in detecting bugs in internally developed code.</td></tr>
<tr><td colspan="2">Ineffective in spotting OSS-related security vulnerabilities in third-party code. Since 2004, National Vulnerability Database (NVD) disclosed 74,000+ vulnerabilities. SAST and DAST were able to find 13.</td></tr>
<tr><td>National Security Agency (NSA) – the average SAST tool can only find 14% of security issues in an application.</td><td>Helpful for verifying compliance and finding misconfiguration issues.</td></tr>
<tr><td>Best practice – when examining custom source code for vulnerabilities during development.</td><td>Best practice – when testing compiled applications for common runtime vulnerabilities.</td></tr>
<tr><td colspan="2">Ineffective at finding security vulnerabilities that enter via open source</td></tr>
</table>

Source: Synopsys

insignary

When auto OEMs and their suppliers have limited visibility into and control over OSS components in their in-house and third-party code base, they are ill-equipped to defend against security breaches targeting OSS vulnerabilities.

With the emergence of connected cars and eventually, autonomous vehicles, software security equates to passenger privacy and safety.

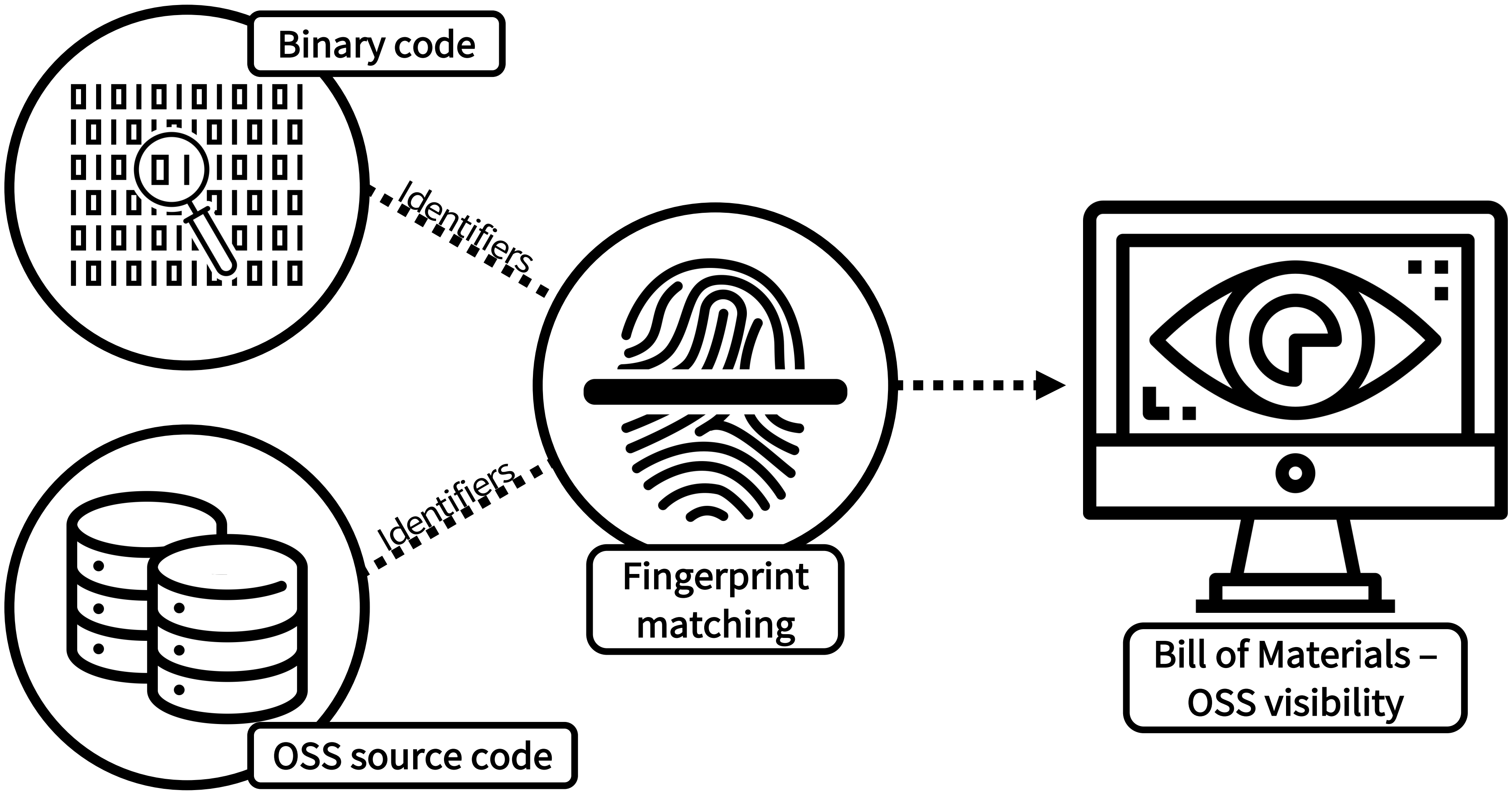
Vehicle manufacturers and their suppliers must take proper steps to address the challenge of managing their use of OSS throughout the complex and entangled automotive software supply chain.

Software composition analysis tools

<table>
<tr><th>Hash comparison</th><th>Fingerprint matching</th></tr>
<tr><td colspan="2">Can scan binaries without source code or reverse engineering.</td></tr>
<tr><td colspan="2">Able to operate on shared libraries and comment code.</td></tr>
<tr><td>Requires database of hash values derived from compiled binaries of OSS components – a hugely expensive feature, since binaries change depending on compile time options.</td><td>Independent of CPU architecture and compile time options – no need to maintain separate databases of hash or checksum values.</td></tr>
<tr><td>Scans binaries at faster speed than alternative methodologies.</td><td>Great coverage of OSS components.</td></tr>
<tr><td colspan="2">Enables effective OSS risk management in organization’s security program.</td></tr>
</table>

insignary

Fingerprinting technology

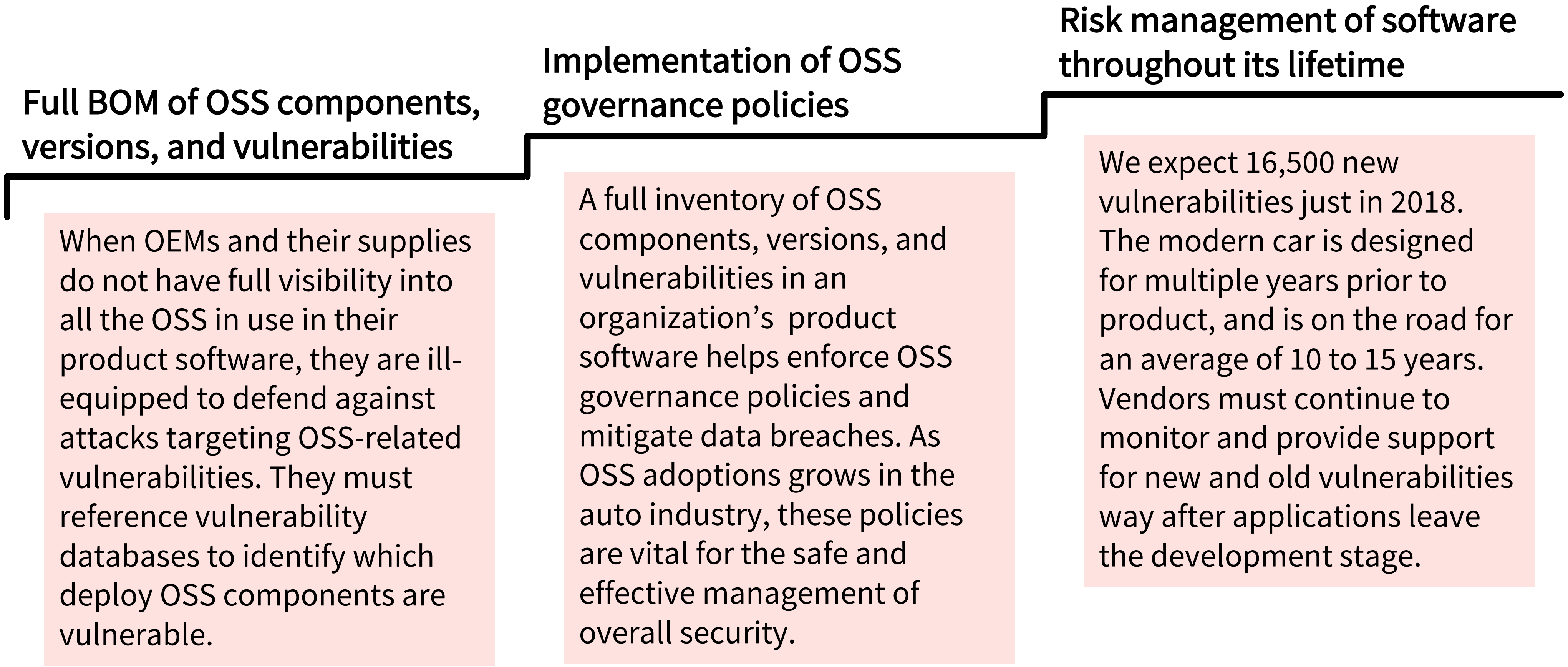


Source: Synopsys

Binary scanning – taking proper, preventative action

insignary

Managing OSS in auto supply chain



Full BOM of OSS components, versions, and vulnerabilities

When OEMs and their supplies do not have full visibility into all the OSS in use in their product software, they are ill-equipped to defend against attacks targeting OSS-related vulnerabilities. They must reference vulnerability databases to identify which deploy OSS components are vulnerable.

Implementation of OSS governance policies

A full inventory of OSS components, versions, and vulnerabilities in an organization's product software helps enforce OSS governance policies and mitigate data breaches. As OSS adoptions grows in the auto industry, these policies are vital for the safe and effective management of overall security.

Risk management of software throughout its lifetime

We expect 16,500 new vulnerabilities just in 2018. The modern car is designed for multiple years prior to product, and is on the road for an average of 10 to 15 years. Vendors must continue to monitor and provide support for new and old vulnerabilities way after applications leave the development stage.

Source: Synopsys

insignary

Q&A

insignary