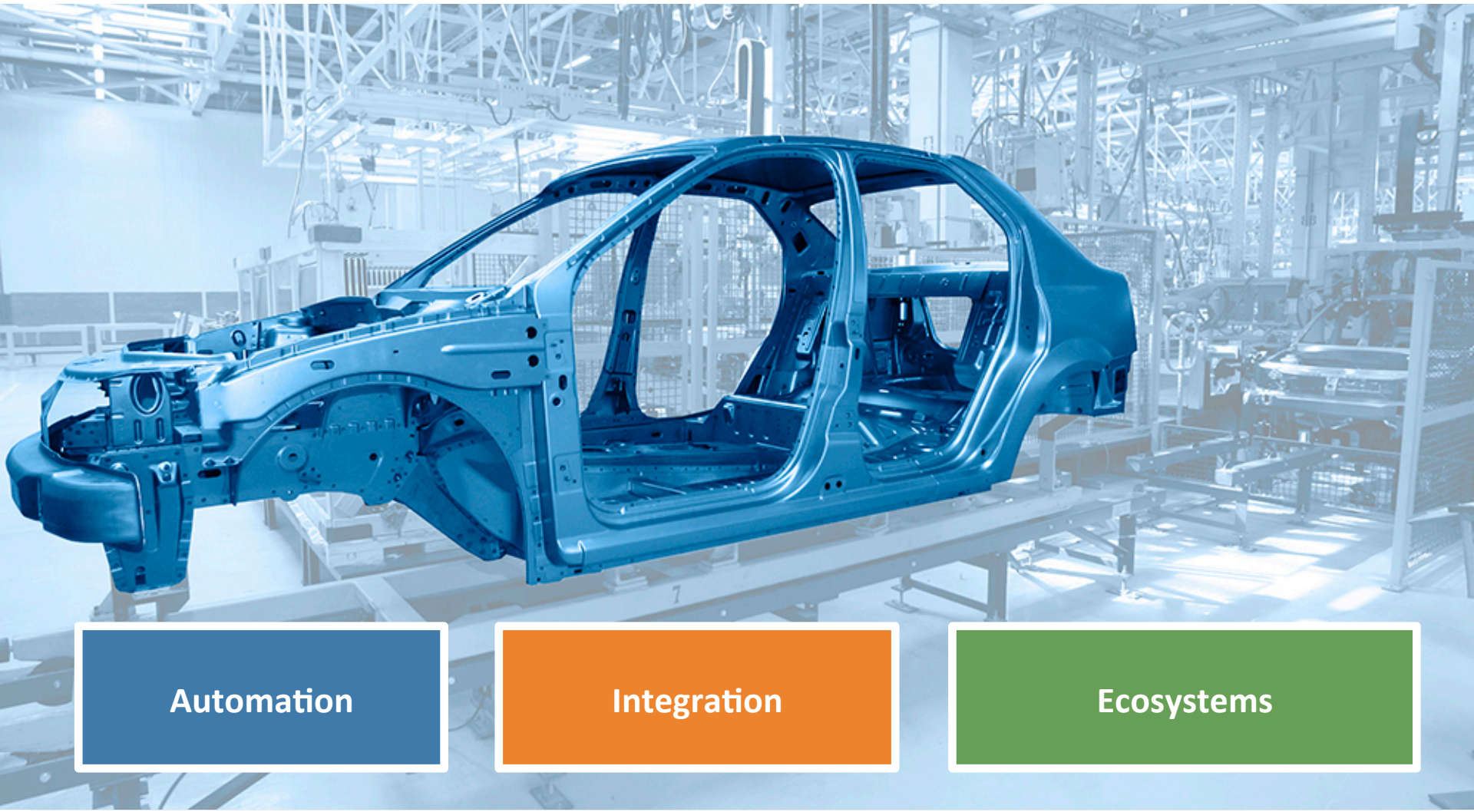
Sonatype

Continuous Acceleration
Accelerating Innovation with Software Supply Chain Management

Ilkka Turunen – SOLUTIONS ARCHITECT EMEA / APJ

Spoiler: We can learn from this



Automation

Integration

Ecosystems

Sonatype

A driving force:
Supporting millions of developers worldwide

MAVEN
easy to build

CENTRAL
easy to share

NEXUS REPOS
easy to manage

NEXUS LIFECYCLE
easy to automate

Sonatype

NEXUS at the ❤ of Continuous

Sonatype

Marc Andreessen 2011

SOGETI

Software is an innovation differentiator

Sonatype

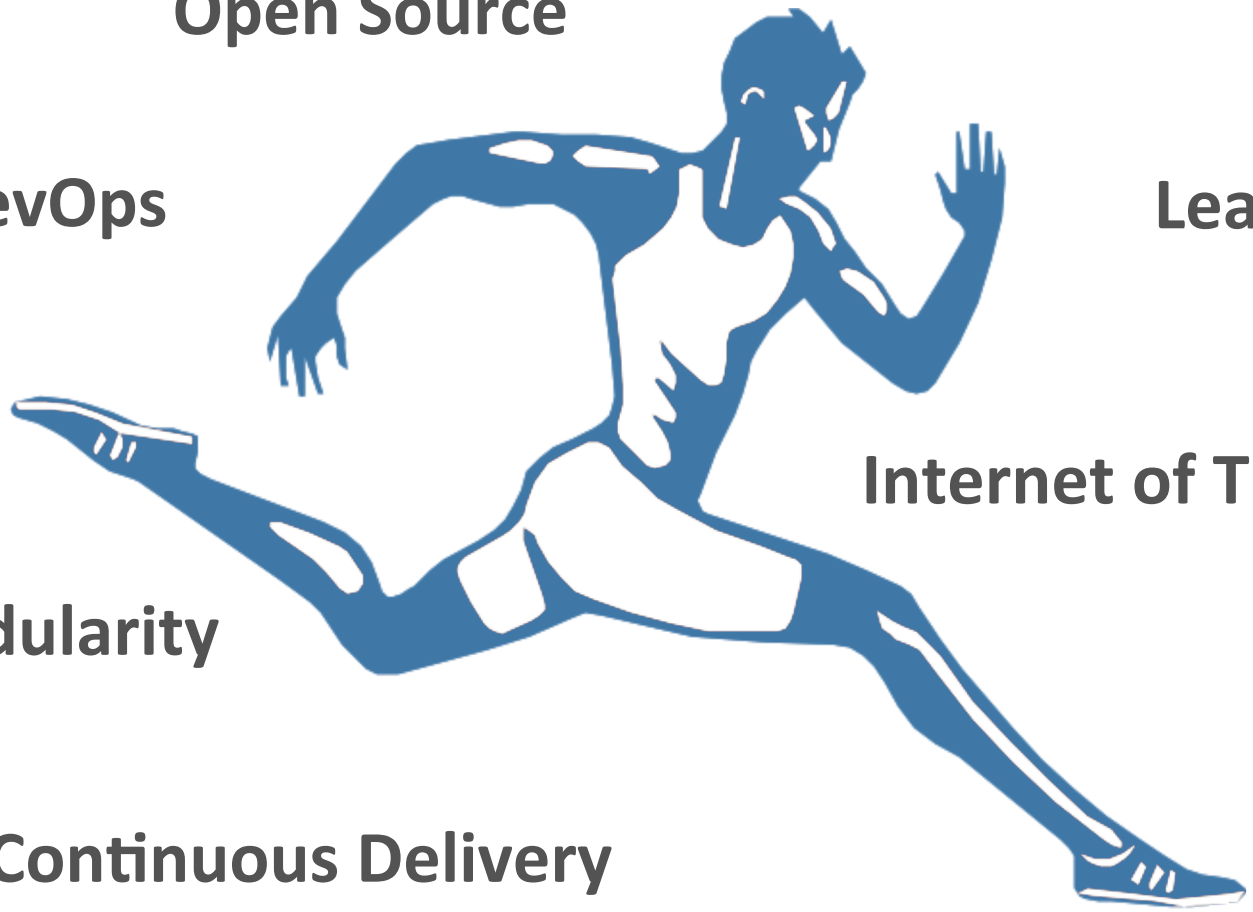
Agile

Continuous Integration

Open Source

DevOps

Lean



Internet of Things

Modularity

Continuous Delivery

Software Factories

https://www.flickr.com/photos/wwworks/2472232245/

Raw innovation
Innovation at any cost

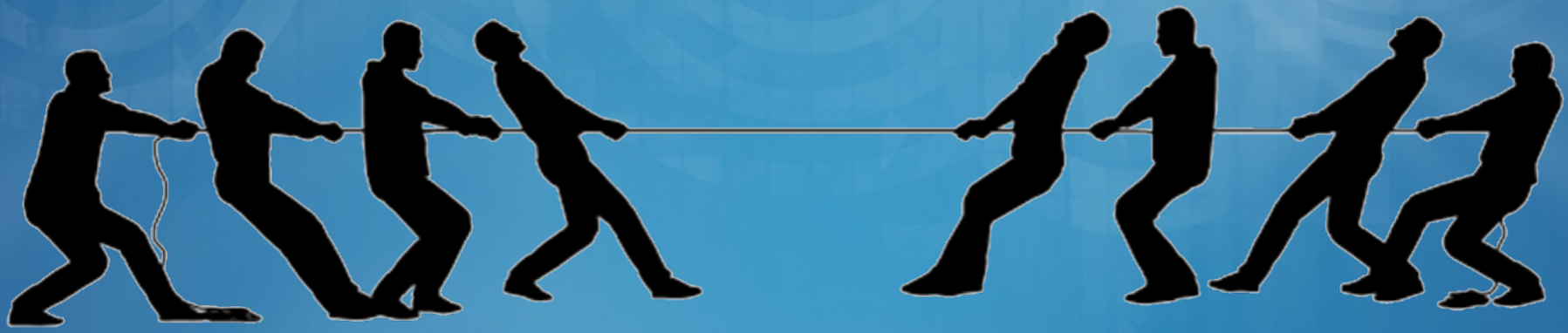
Quality?

Security?

Maintainability?

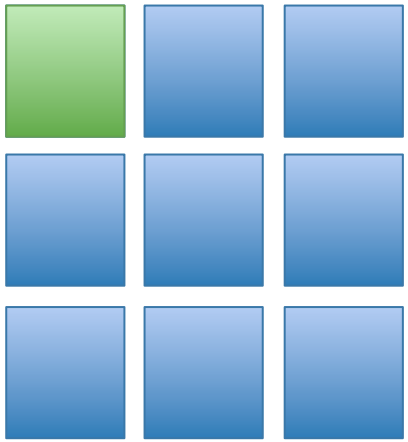
Repeatability?

Net innovation
Net value to the organization



Sonatype

Modern Applications

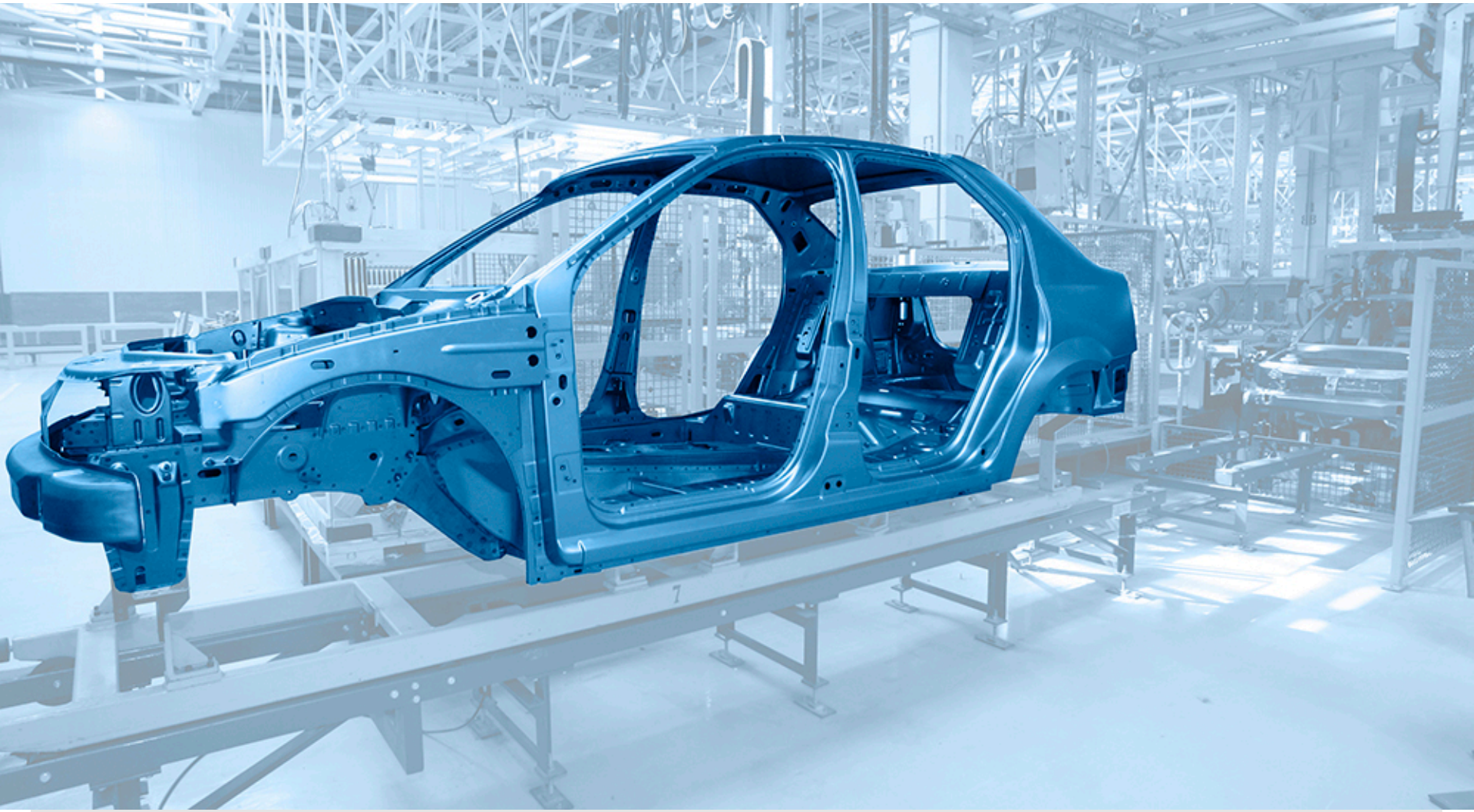


Are 90% open source code

According to the State of the Software Supply Chain report….

Components	Known Critical or Severe Security Vulnerabilities	Known restrictive licenses
106	24	9

Embrace proven supply chain principles

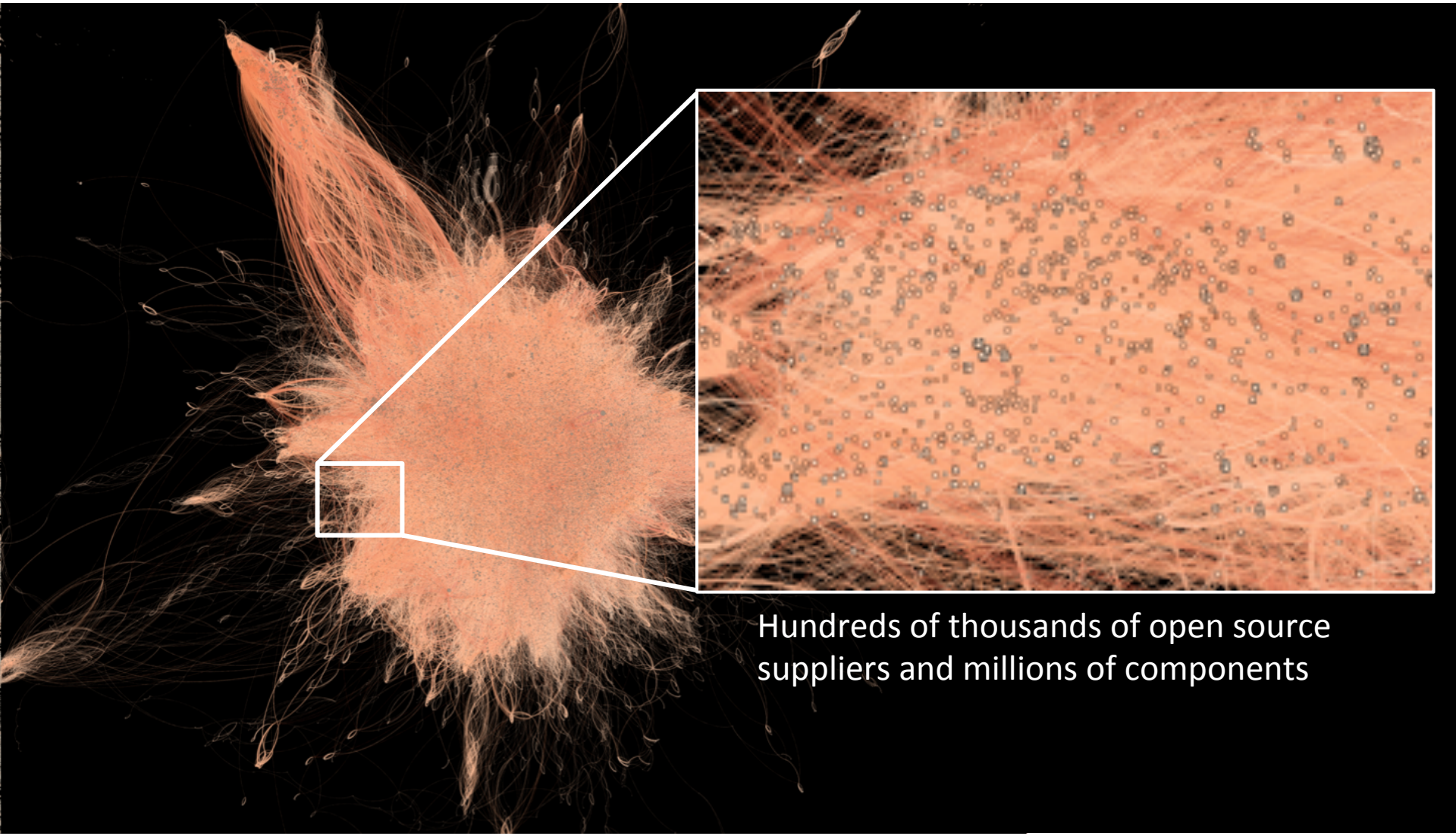


Sonatype

The Missing Link

Sonatype

Your software supply chain is complicated



Hundreds of thousands of open source suppliers and millions of components

Houston, we have a problem

In 2014, organizations downloaded
a version of Bouncy Castle
with a level 10 vulnerability

42,124

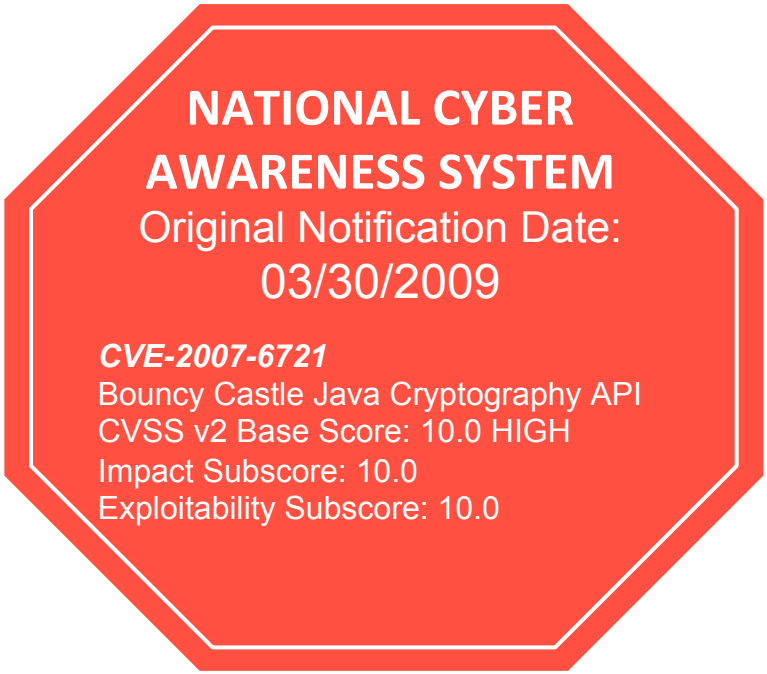
times into

XXXX

applications…

7

years after the
vulnerability was fixed.



BOUNCY CASTLE

Large Enteprise Customer in Financial Sector

Central Downloads

900k

CVE Downloads

60k

Industry Average……6.22%

Asus – Possible $206M future fine

Security

Feds spank Asus with 20-year audit probe for router security blunder

One crappy vendor down, who's next?

23 Feb 2016 at 20:10, Iain Thomson 72 73

- 12,937 vulnerable routers found
- Login credentials for 3,131 stolen
- Future fine $16,000 per instance

ASUS must get in contact with existing customers to tell them about the need for firmware upgrades and to tell them about bug fixes within 30 days of them becoming available. If it violates this, the firm will have to pay $16,000 for every instance where it fails in the future.

Source: http://www.theregister.co.uk/2016/02/23/asus_router_flaws_settlement/

What if manufacturers built cars the way we build software: without supply chain visibility, process and automation …

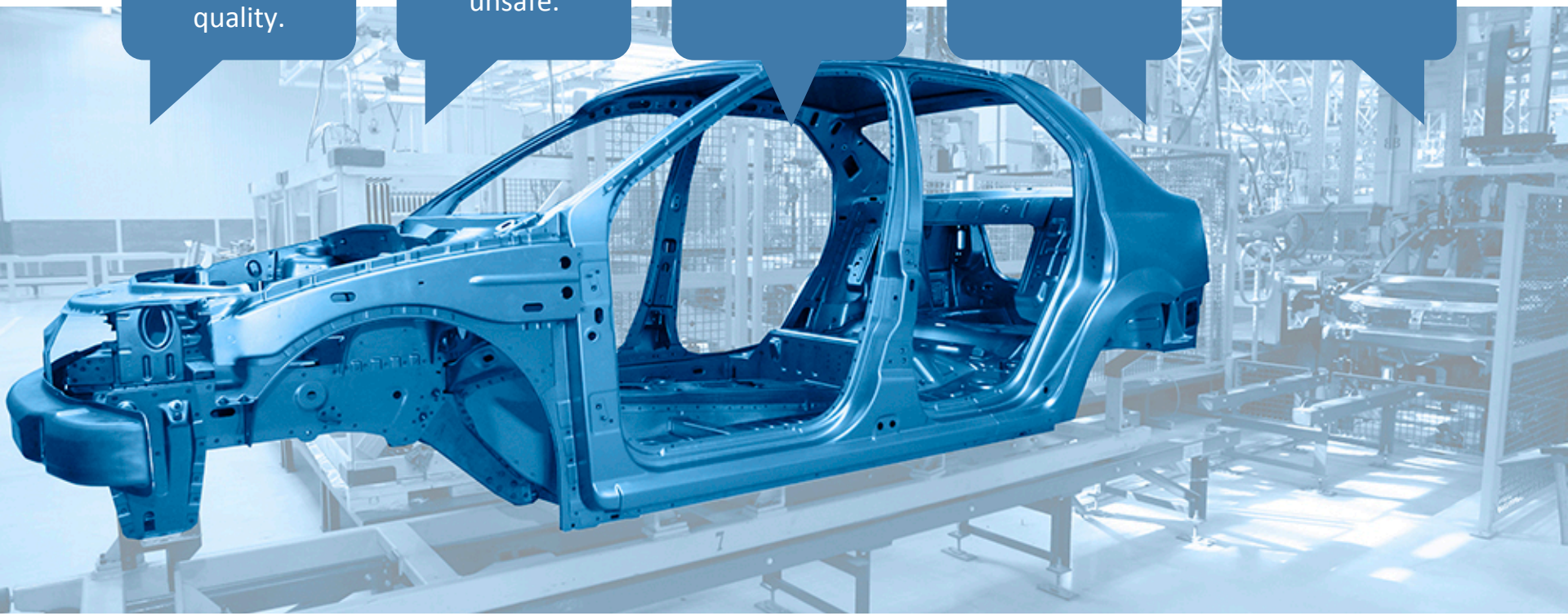
Manufacturers could choose **any supplier** they want for any given part, regardless of quality.

Any part can be chosen even if it is outdated or known to be unsafe.

There is **no inventory** of the parts that were used, or where.

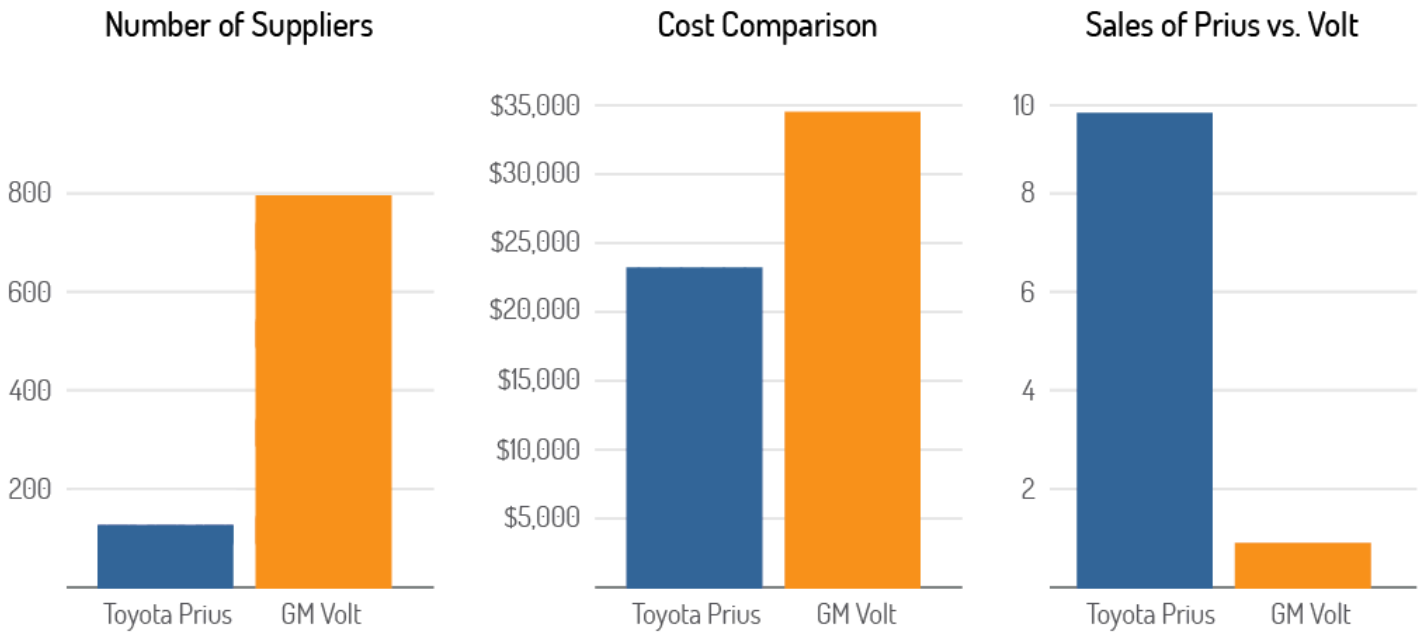
Since parts aren't tracked, it's **challenging to issue a recall**.

There is **no quality control** or consistency from car to car.

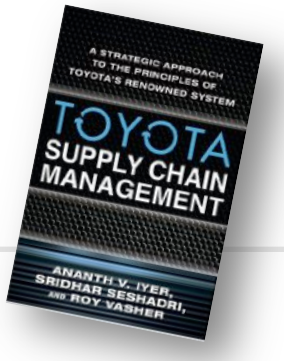


Sonatype

Supply chain advantage



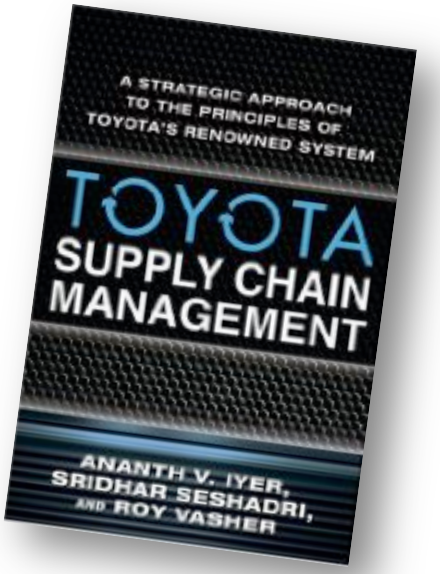
Source: Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System, by Ananth Iyer and Sridhar Seshadri



Sonatype

Supply chain advantage

	Toyota Advantage	Toyota Prius	Chevy Volt
Unit Retail Price	**61%**	$24,200	$39,900
Units Sold/Month	**13x**	23,294	1,788
In-House Production	**50%**	27%	54%
Plant Suppliers	**16%**	125	800
Firm-Wide Suppliers	***4%***	*224*	*5,500*

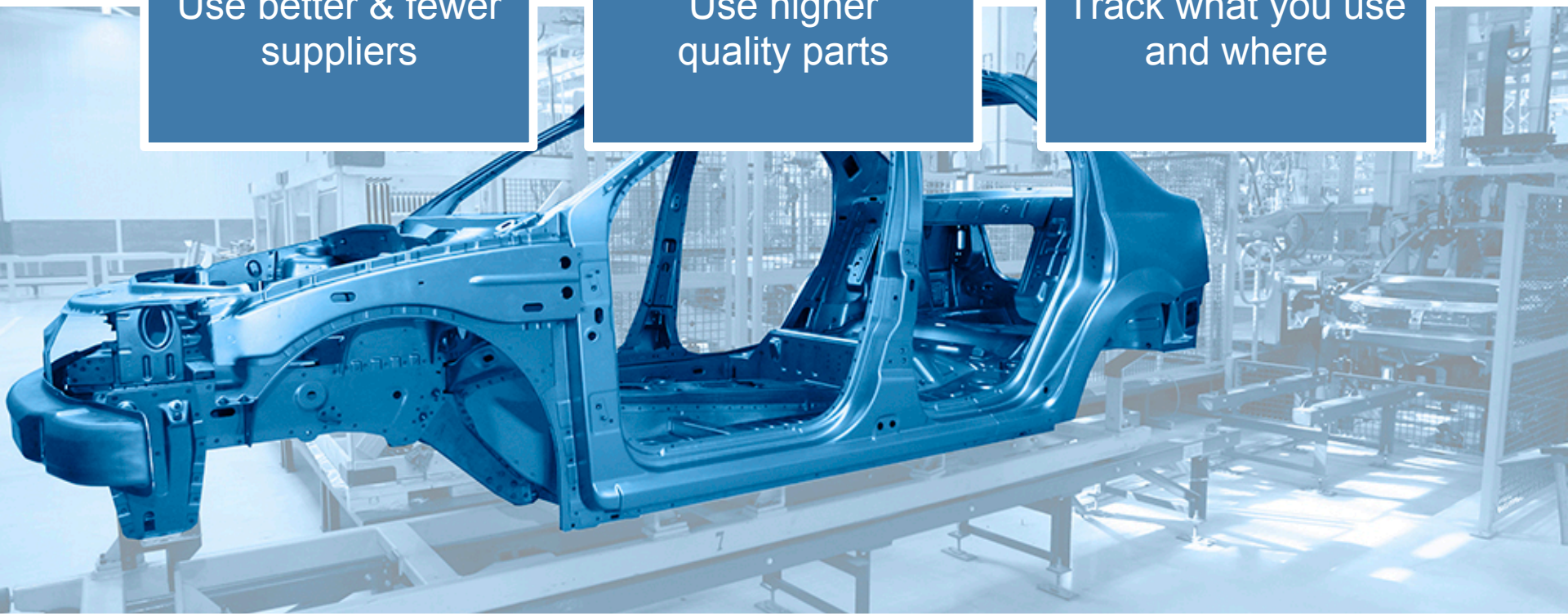


Source: Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System, by Ananth Iyer and Sridhar Seshadri

Speed, efficiency & quality for agile, continuous, and DevOps

Automate your software supply chain with three proven principles:

- Use better & fewer suppliers
- Use higher quality parts
- Track what you use and where



Sonatype

Speed, efficiency & quality for agile, continuous, and DevOps

Optimize the movement of parts, assemblies, and finished goods from development to delivery.

Enterprise Requirements

Hundreds to thousands of applications.
Hundreds to tens of thousands of developers. Diverse ecosystem support.

Automation

THE KEY TO OPERATING AT SCALE

In order to automate:

- Precise identification is essential
- Metadata must be machine actionable
- Policies must conform to the business

Antipattern: humans in the flow of analysis and (re)action

Integration

MAKE DEVELOPERS MORE PRODUCTIVE—NOT LESS

In order to empower:

- Real-time information delivery
- Information must be intuitive and actionable
- Corrective action must be in context

Antipattern: asynchronous audits driving unplanned, unscheduled rework

Ecosystems

MUST SUPPORT DIVERSE TECHNOLOGY ENVIRONMENTS

In order to support:

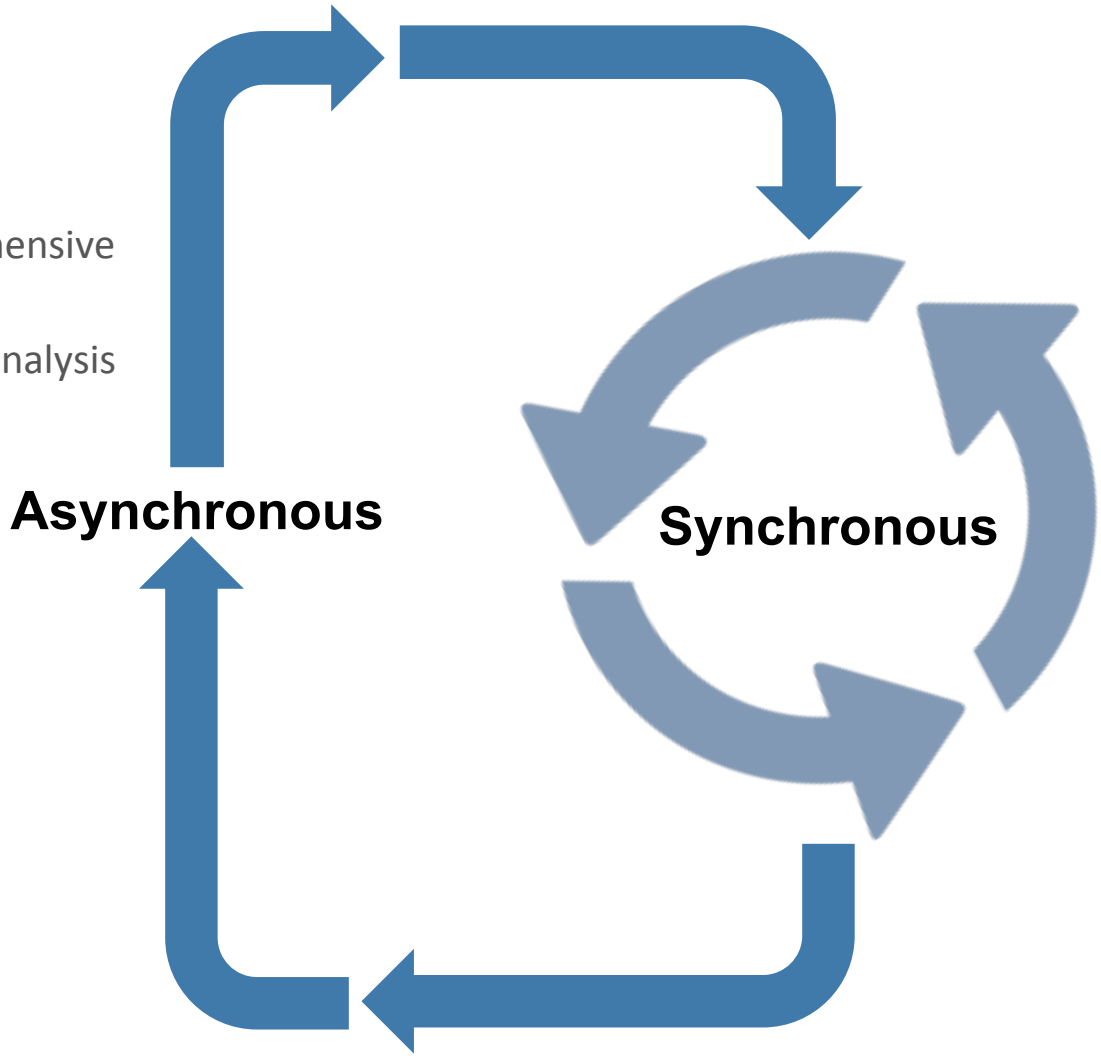
- Coordinate system must be abstracted
- Crowd must drive data research
- Must support other requirements for scale

Antipattern: Infrastructure bound to a single ecosystem

Tools for Software Integrity

Two very distinctly different classes of technology

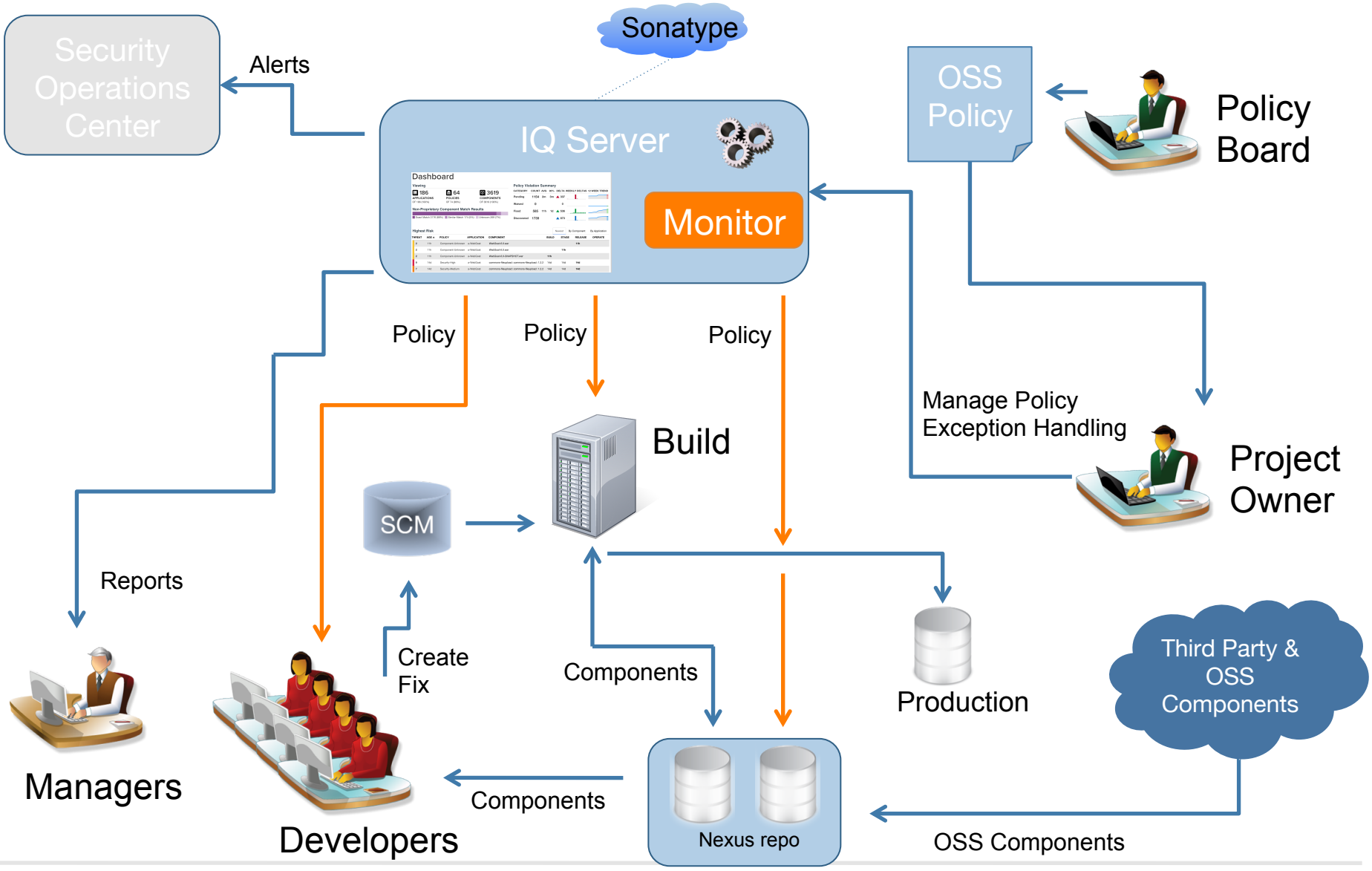
- Very comprehensive
- Requires human analysis



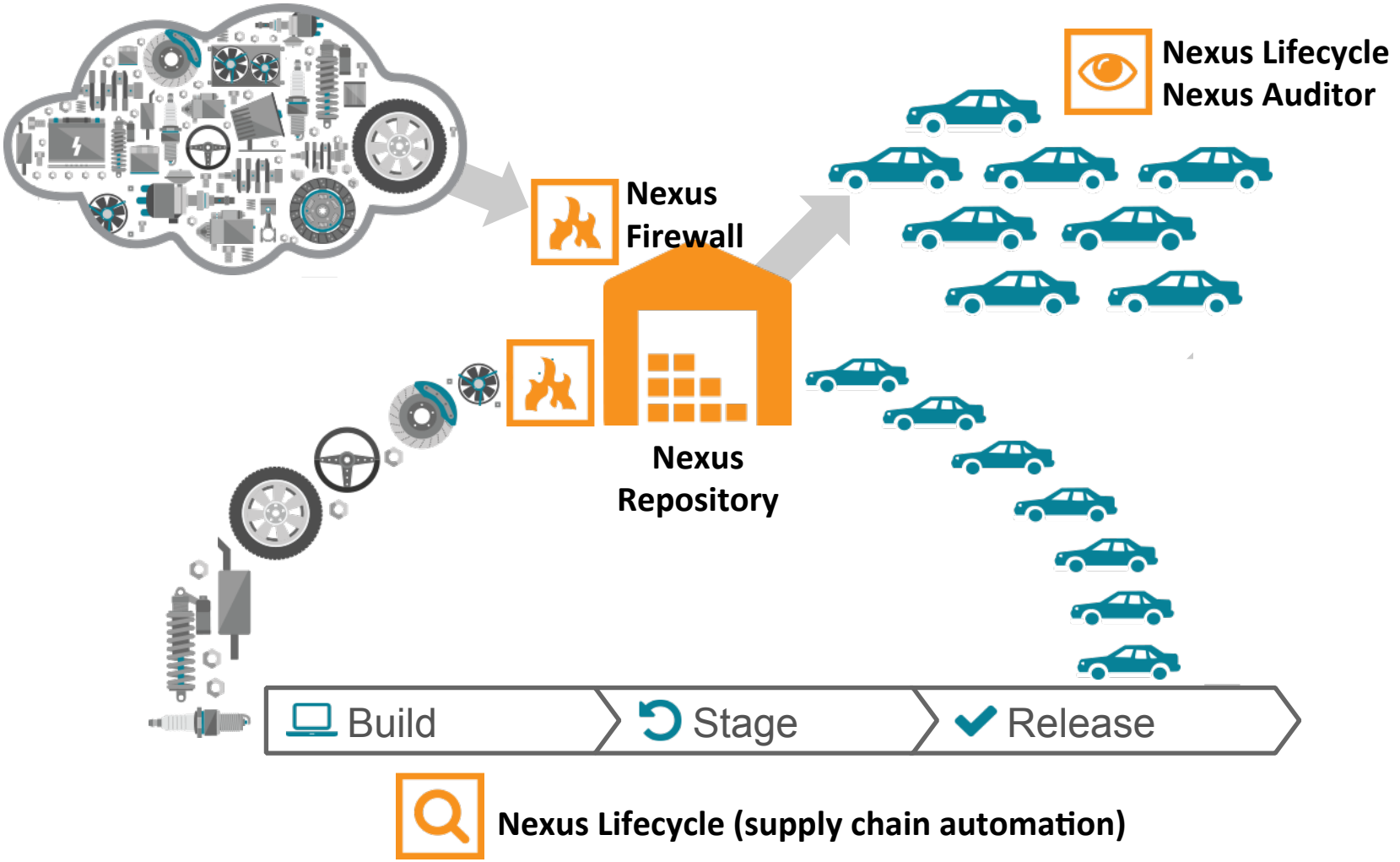
- Comprehensive at wire speed
- Machines automate action

Sonatype

Nexus Lifecycle – Where do you fit in?

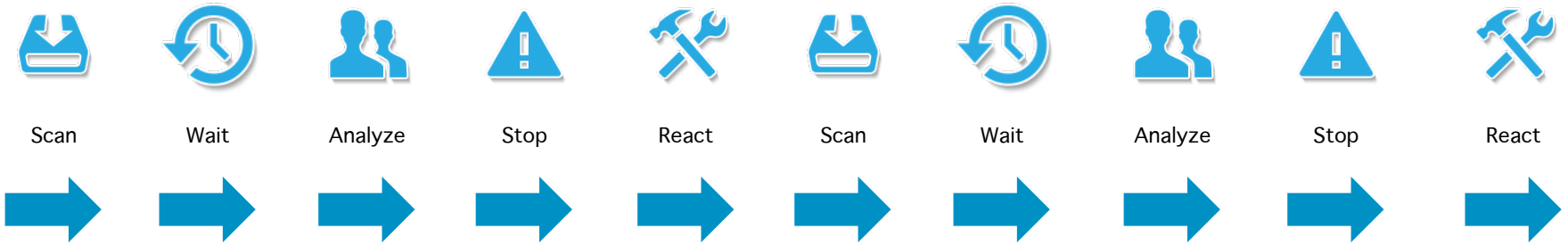


Nexus platform of Software Supply Chain solutions



Tools for Software Integrity

Asynchronous Software Composition Analysis



Synchronous Software Supply Chain Automation

Sonatype

THANK YOU!

Come say hi to us at Booth #3 in the Benjamin Britten Lounge

State of the software Supply Chain 2015:
http://www.sonatype.com/speedbumps

Sonatype