sonatype

The New Era of Software Liability

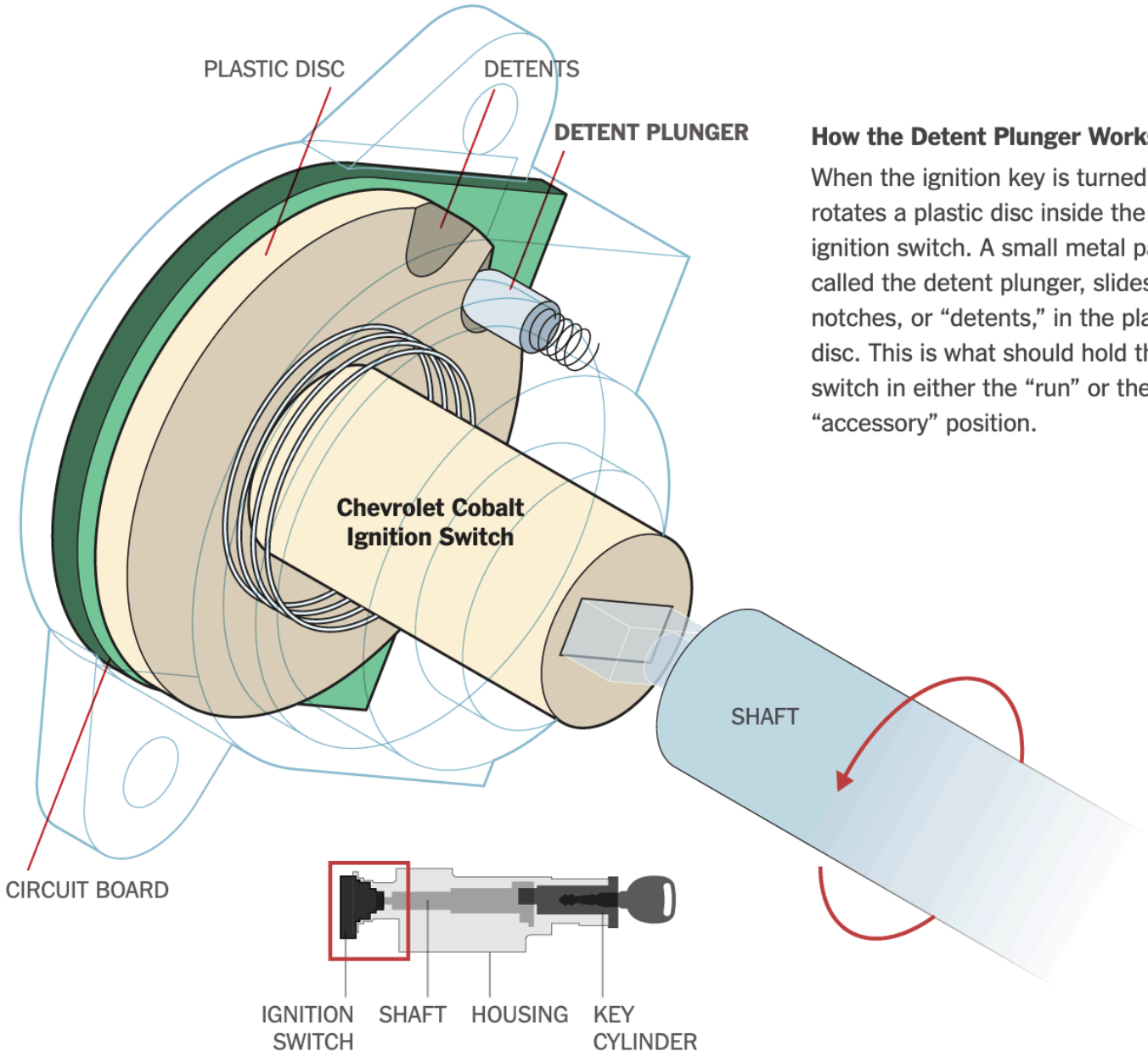
Stephen Magill
VP, Product Innovation, Sonatype

REGULATIONS

sonatype

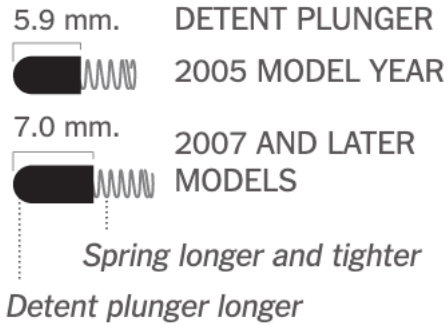
CARS!

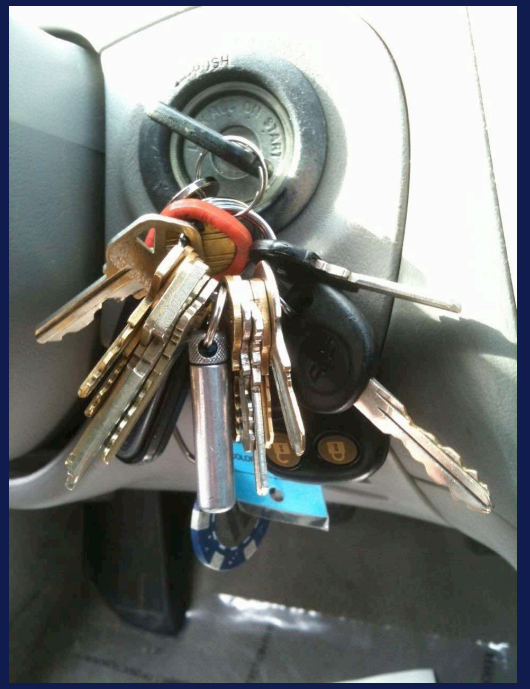
sonatype



How the Detent Plunger Works

When the ignition key is turned, it rotates a plastic disc inside the ignition switch. A small metal part, called the detent plunger, slides into notches, or "detents," in the plastic disc. This is what should hold the switch in either the "run" or the "accessory" position.





2014

sonatype

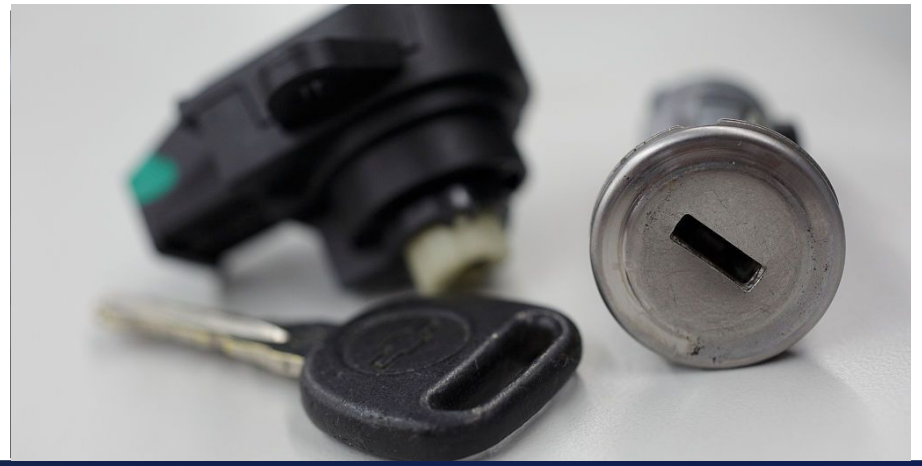
CAR AND DRIVER MAKES & MODELS SIGN IN

SUBSCRIBE REVIEWS NEWS FEATURES BUYER'S GUIDE

Massive GM Ignition Switch Issue: Manufacturers promise to pay suppliers more to improve quality next time. No need to track the parts or issue recalls they say.

Our frequently updated coverage of the ongoing safety issue.

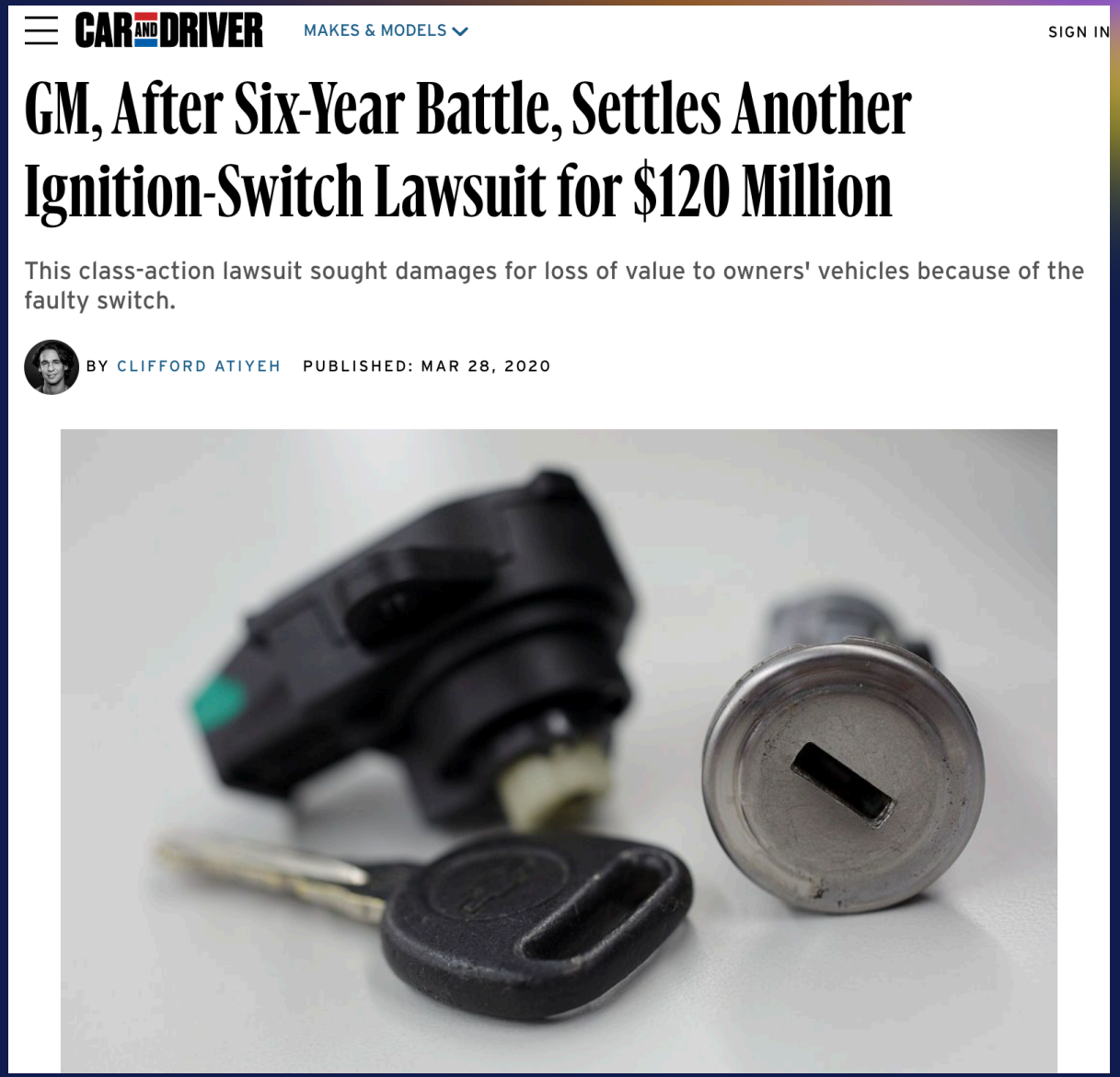
C/D BY CLIFFORD ATIYEH AND RUSTY BLACKWELL APR 21, 2021



sonatype

What Happened

- 30M Cars Recalled
- $900M in fines
- $600M in settlements
- -$3B in shareholder value



CAR AND DRIVER MAKES & MODELS SIGN IN

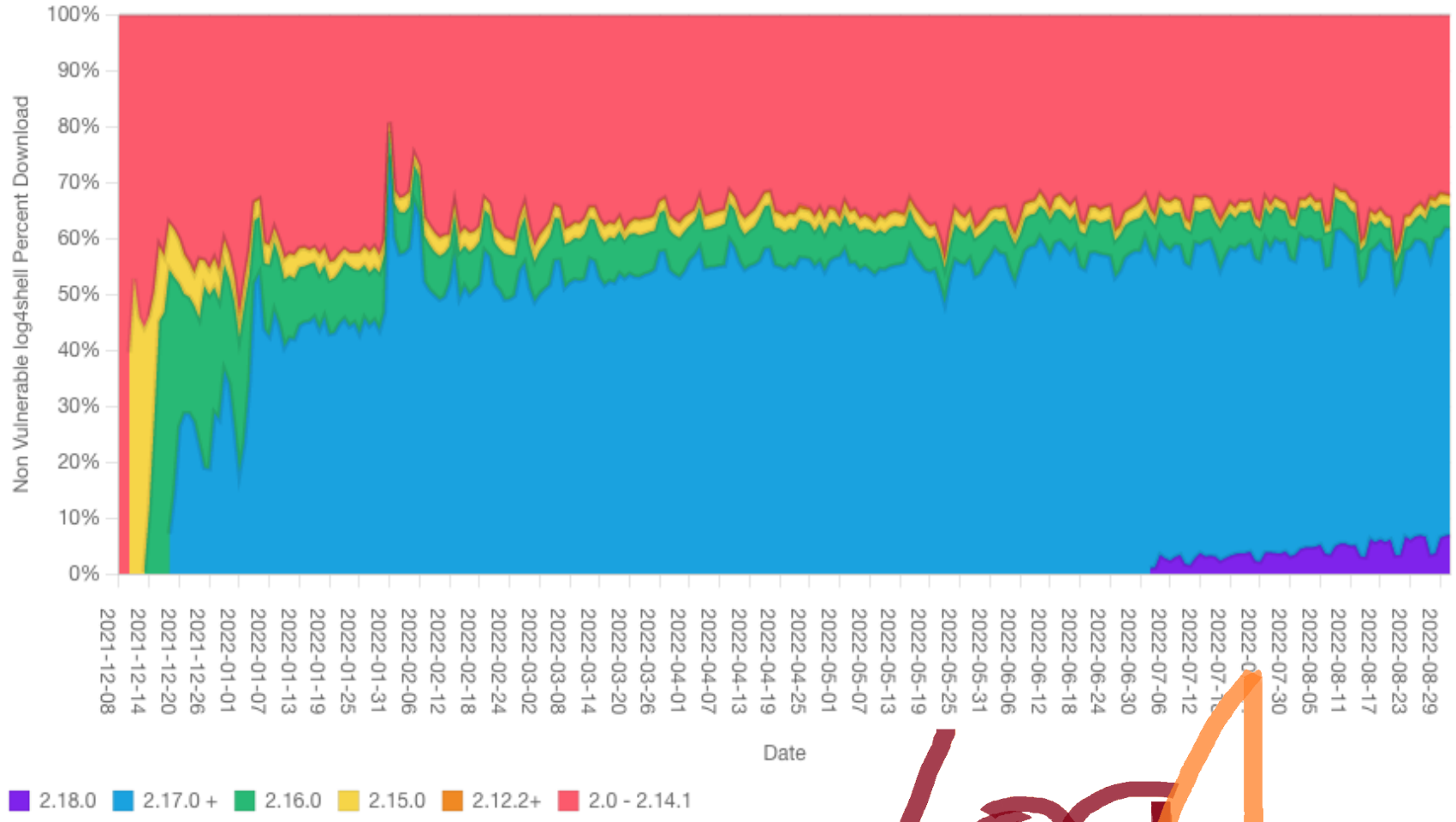
GM, After Six-Year Battle, Settles Another Ignition-Switch Lawsuit for $120 Million

This class-action lawsuit sought damages for loss of value to owners' vehicles because of the faulty switch.

BY CLIFFORD ATIYEH PUBLISHED: MAR 28, 2020

(c) **Limitations of Liability**. NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA OR OTHER LOSSES, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY UNDER THESE TERMS SHALL NOT EXCEED THE GREATER OF THE AMOUNT YOU PAID FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE OR ONE HUNDRED DOLLARS ($100). THE LIMITATIONS IN THIS SECTION APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

FIGURE 1.5. ADOPTION OF LOG4SHELL RELEASES FROM AUGUST 2021–AUGUST 2022



38% consumption of vulnerable versions

sonatype

https://www.sonatype.com/log4j

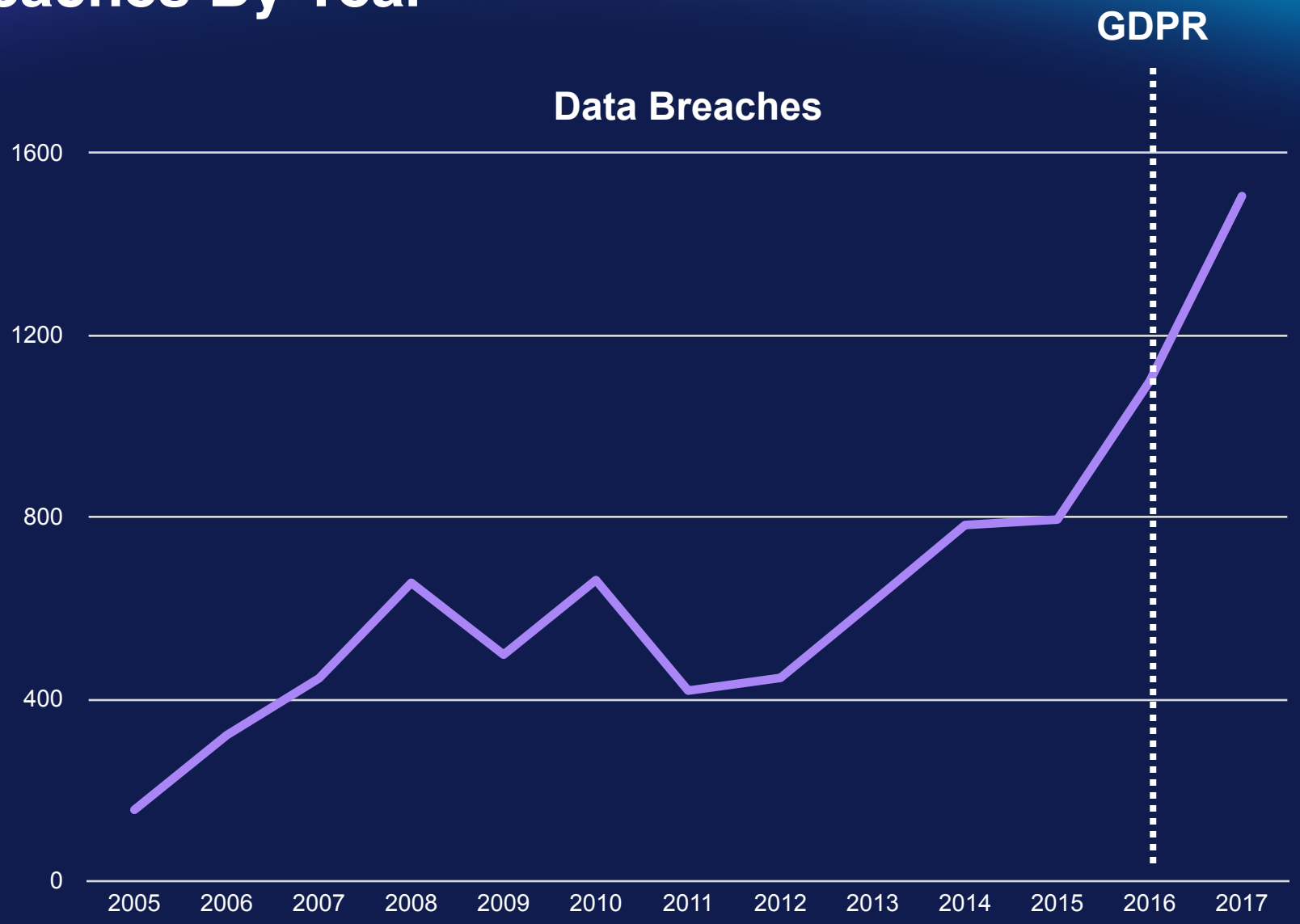
Regulations Are Coming

sonatype

First Came Data Governance

sonatype

Data Breaches By Year



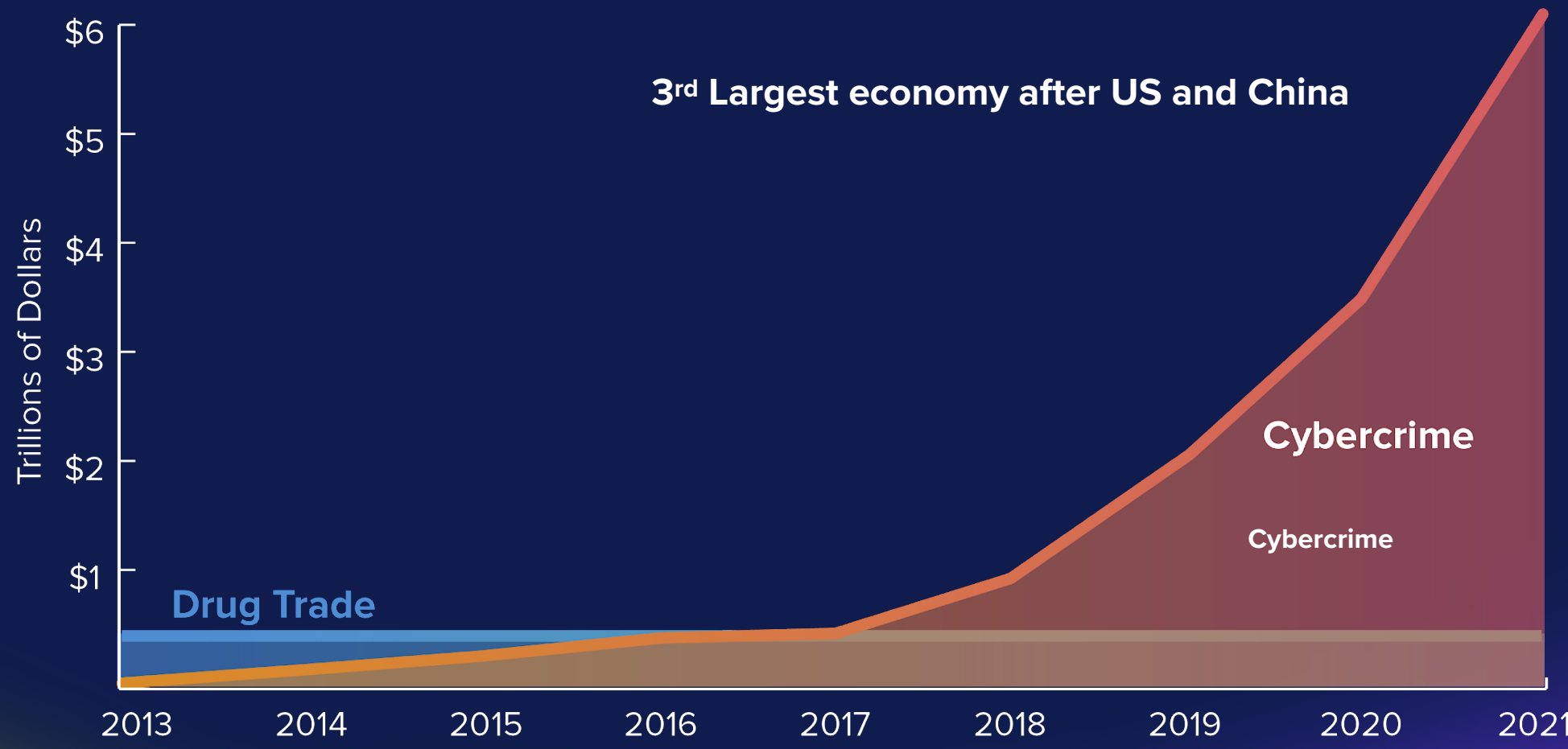
Source:
https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

sonatype

Next is Security

sonatype

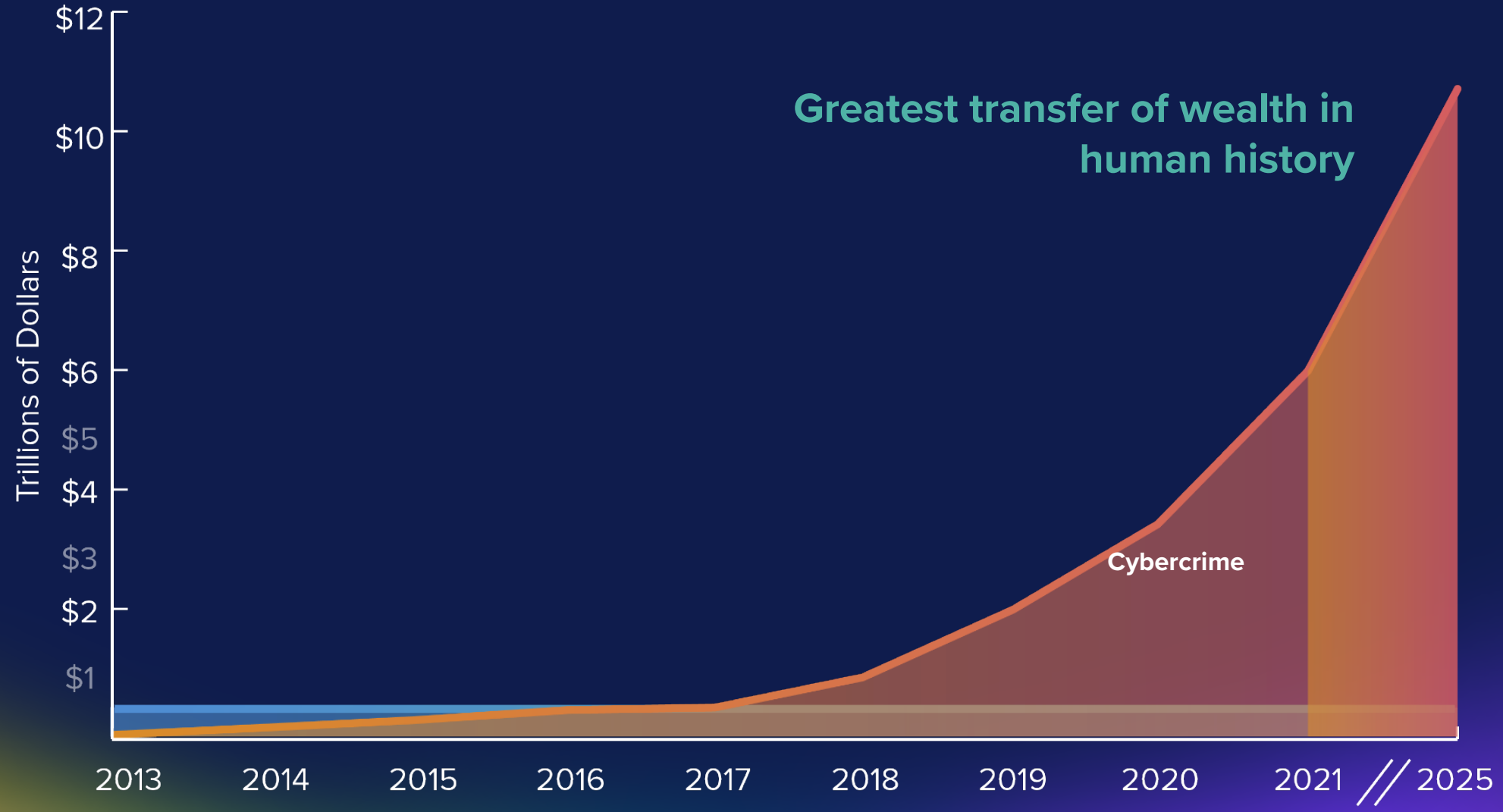
Cybercrime – a $6 Trillion industry in 2021



https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

sonatype

Cybercrime – $10.5 Trillion by 2025



https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

sonatype

Hospitals Are At Risk From Cyber Attacks

Over

500

healthcare breaches in 2021 -

US Department of Health and Human Services (HHS)

Ransomware attacks on hospitals increased

123%

in the past year -

2021 SonicWall Cyber Threat Report

Ransomware cost hospitals nearly

$21B

last year -

24%

of attacked hospitals noted a subsequent rise in their mortality rates.

Cynerio

Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act

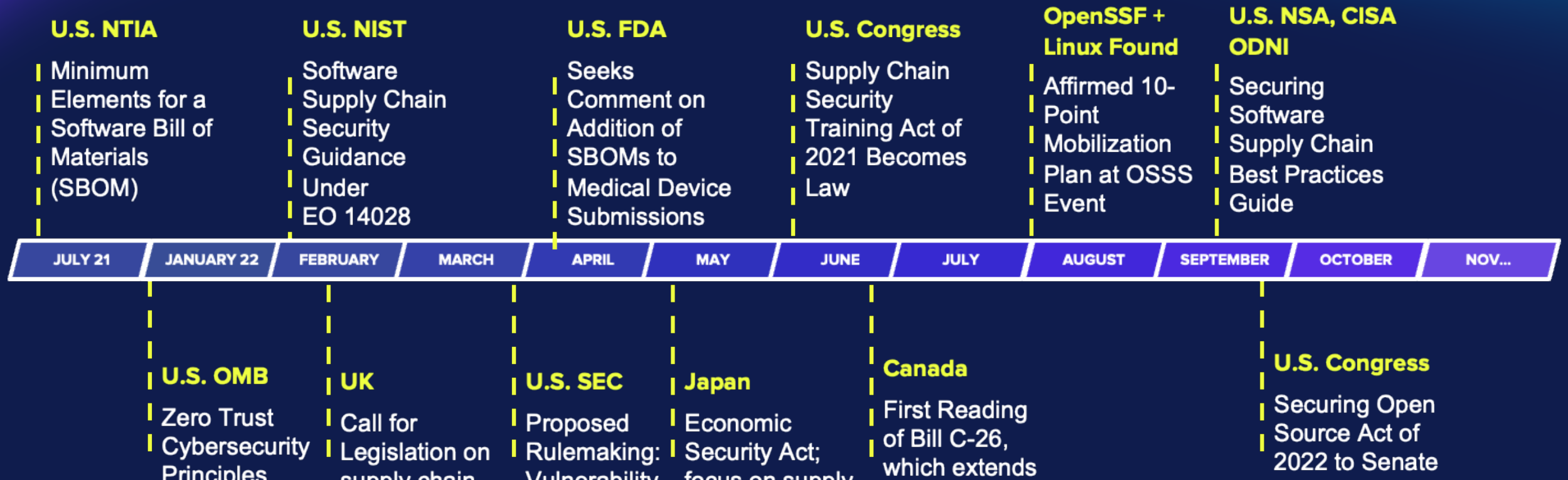
---

Guidance for Industry and Food and Drug Administration Staff

Document issued on March 30, 2023.

sonatype

Standards and Regulations Activity



sonatype

Standards and Regulations Activity - Europe Union

- June 2021 - European Union has joined with the United States government to launch the U.S.-European Union Trade and Technology Council.
- July 2021 - European Agency for Cyber Security (ENISA) issued the "Understanding the increase in Supply Chain Security Attacks,"
- May 2022 - European Parliament and European Union Member States reached an agreement on New Rules on Cybersecurity of Network and Information Systems
- July 2022 - European Agency for Cyber Security (ENISA) shared its "Cybersecurity Threat Landscape Methodology"

ENISA Threat Landscape for Supply Chain Attacks

sonatype

Current Mandates: Provide SBOMs

sonatype

Future is Recall and Liability

sonatype

EU Cyber Resilience Act

From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I **shall immediately take the corrective measures necessary** to bring that product with digital elements or the manufacturer's processes into conformity, **to withdraw or to recall the product, as appropriate**.

–Page 40, paragraph 12 of the Cyber Resilience Act

sonatype

National Cybersecurity Strategy

"We must begin to **shift liability** onto those entities that fail to take **reasonable precautions** to secure their software while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be **held liable when they fail to live up to the duty of care** they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product."

Donoghue v Stevenson “Paisley Snail Case”

Macpherson v Buick Motor Company

Every other industry has gone through an evolution of due care challenges

sonatype

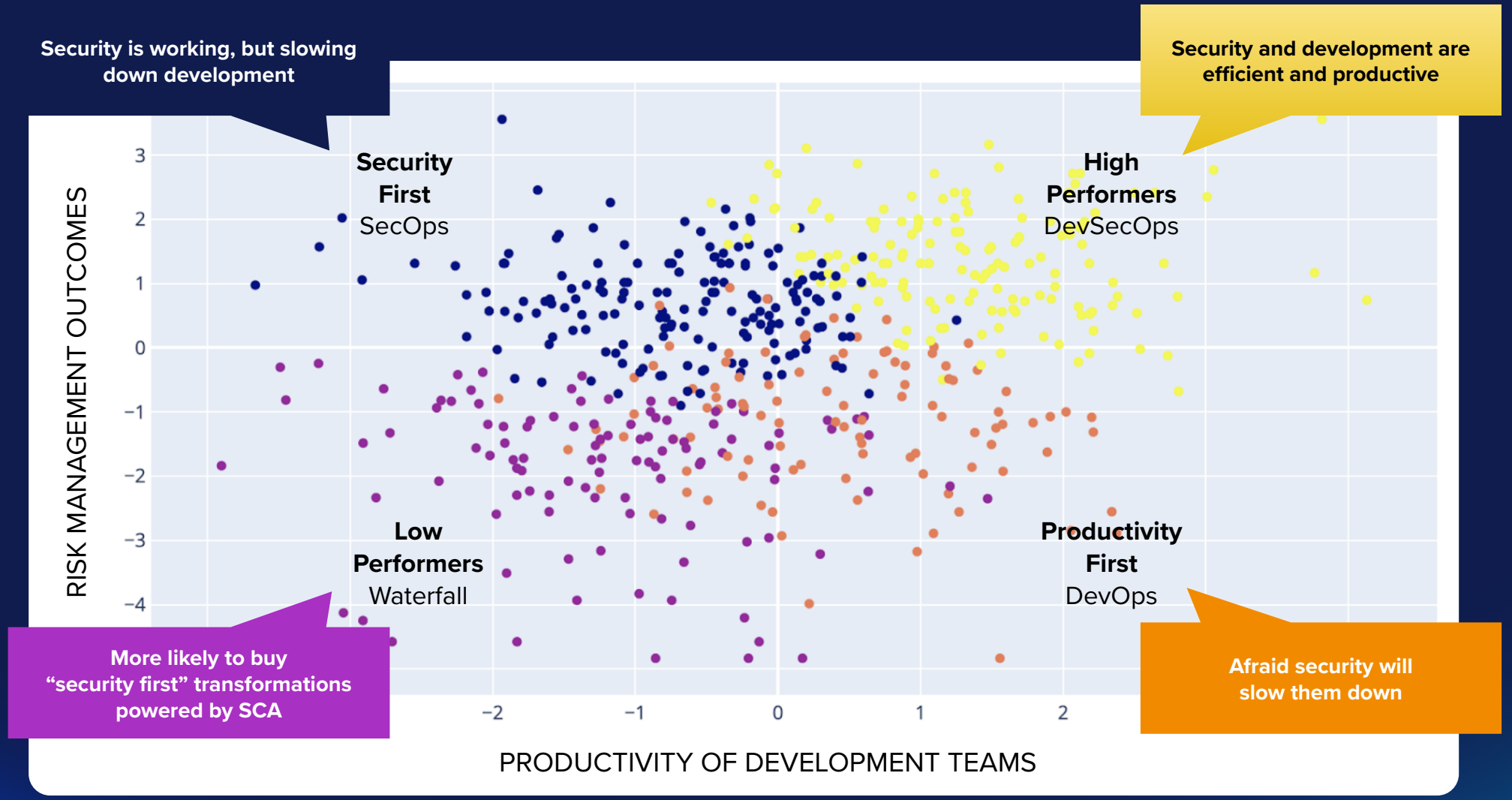
https://www.sonatype.com/launchpad/key-changes-in-software-liability

Start preparing now

sonatype

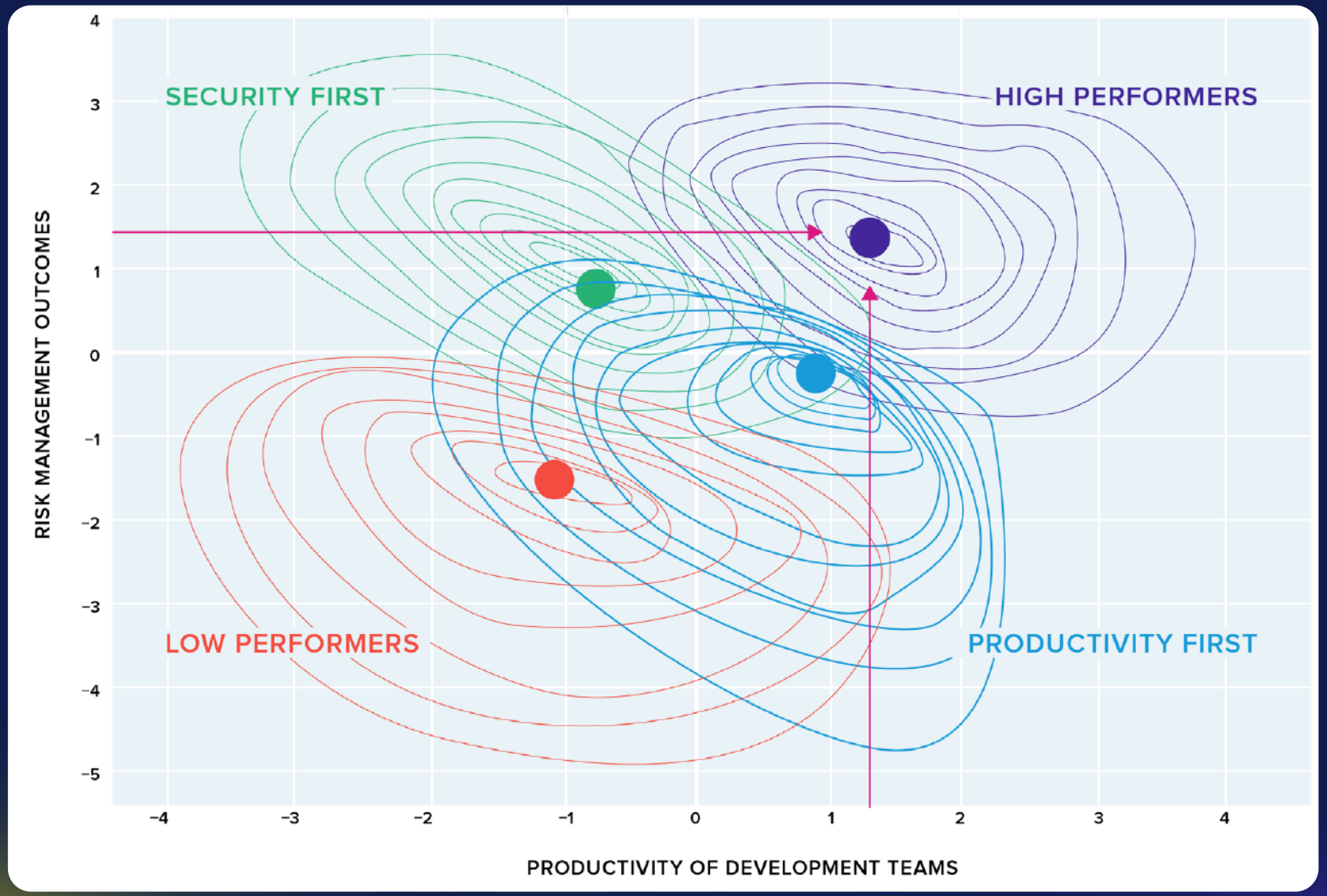
"Never let a good crisis go to waste."

- Winston Churchill



https://www.sonatype.com/ssc

sonatype



HIGH PERFORMERS:

Better risk management outcomes

Higher developer productivity

Improved job satisfaction

sonatype

https://www.sonatype.com/ssc

Self Evaluation:

If I told you about a new vulnerability right now. Can you tell me:

- ❑ Are you even using this exact component?
- ❑ In which applications?
- ❑ Can you track the remediation across the portfolio?
- ❑ How long until you could ship/deploy an update?