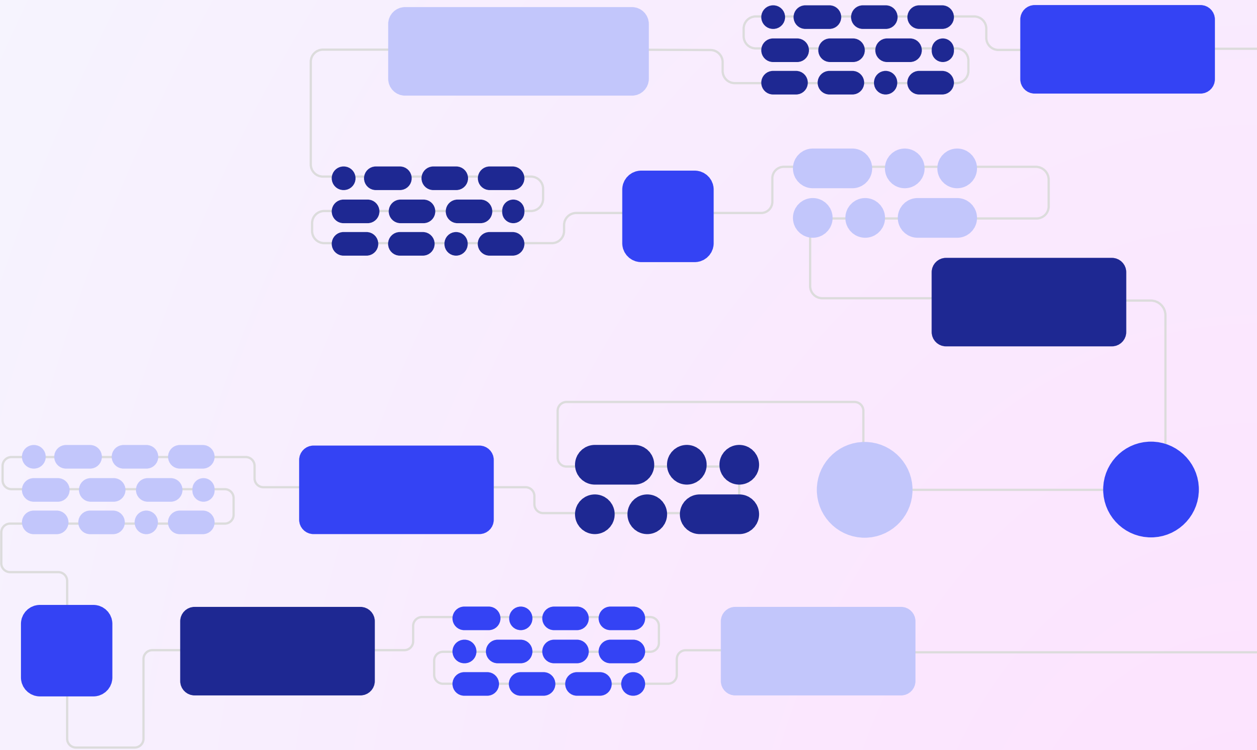
Chainguard

CISO & Developer Trends in Software Supply Chain Security

November 2023



Dan Lorenc
Co-Founder & CEO of Chainguard

I am happy to present the CISO & Developer Trends in Software Supply Chain Security Report that uncovers the level of importance, expectations, strategies, and outcomes of software supply chain security among an organization's developer and security teams.

The study further aimed to analyze key challenges and opportunities related to how organizations understand and prioritize software supply chain security.

To conduct this research, we set out to uncover these underlying themes:

- ✓ The importance of software supply chain security to developers and security leaders
- ✓ The pain points and successes in current approaches to software supply chain security among developers and security leaders
- ✓ The expectations around responsibility for software supply chain security across an organization's developers and security leaders

Software supply chain security is one of the fastest-moving, most interesting emerging areas in cybersecurity. It's a really fun area to work in because it tends to attract security professionals who are passionate about open source software and who see opportunity to correct some security challenges that are long overdue for fixes.

In the aftermath of Log4j, you could feel a collective consciousness arriving from developers and security teams alike that we needed to call timeout and re-think this security domain. But there are no timeouts in our industry, and there has been a dizzying pace of innovation in the software supply chain security arena that is driving all kinds of change into developer workflows, as well as the security policies and "big picture" regulatory efforts that CISOs and security teams are wrestling to put into place.

It can be an intimidating arena for organizations who understand they are exposed in this massive way on critical software infrastructure that has not had the proper security investment. And you might feel that nagging sense that you are behind on the learning curve when it comes to critical concepts and patterns like software signing, provenance, container images, security and more.

To provide a starting point for the developers and security teams that are struggling with "not knowing what they don't know," Chainguard worked with The Harris Poll to survey more than 500 developers and security leaders to try to understand where we are today.

Most surveys just look at sheer numbers of vulnerabilities in open source code, unpatched software and more, but our goal with this survey was to go a level deeper and hear from the teams responsible for building a more secure supply chain on what they feel is working or lacking in their organization.

A good culture of software security comes from deep collaboration and comradery, which are often overlooked by the speeds and feeds of technology tools or the doom and gloom of the vulnerability landscape. We hope this data gives you inspiration for spotting opportunities where you need to improve your software supply chain security knowledge or processes, or for some of you, reassurance that you are actually doing much better than you thought you were.

As a developer and open source software maintainer turned CEO, I've experienced many of the findings and sentiments in this report first hand. I've felt stalled by security team controls in the past, impeding my progress to deliver engineering or product outcomes for customers. I've also broken common security sins for the sake of developer velocity and innovation. This is why I set out to start a company that builds synergies rather than obstacles for securing the entire software development lifecycle.

Solving the organizational and structural issues present in the software supply chain is not an easy feat for even the most resourced organizations, and I am proud Chainguard is playing a part in bridging the gaps to help both developers and security leaders tackle this pressing issue. There doesn't have to be a tradeoff for security among these teams. Tension can be solved with the right tools, trust pathways and a deeper commitment to collaborate. Chainguard is committed to building a future that allows developers and security leaders to work in harmony as they are building and maintaining software that keeps the world moving forward, one vulnerability patched at a time. Enjoy the report!

Dan Lorenc

Dan Lorenc
Co-Founder & CEO of Chainguard

Executive Summary

Software supply chain security has been a growing topic of focus for all organizations today. Software developers want to develop software that is secure and free of vulnerabilities so they can ship the best products and applications to users and customers. Security practitioners want to feel at ease knowing vulnerabilities aren't creeping in from the beginning of the software development process, which can create mounting technical and security debt. And CISOs want to trust the software their developers build, ship and run is secure, avoiding reputational damage or missing compliance requirements. Getting all of these groups on the same page when it comes to an organization's approach to software supply chain security is challenging.

To clearly identify the pain points developer and security decision-making teams see when working together to improve software supply chain security, Chainguard worked with The Harris Poll to conduct a survey asking developers and CISOs various questions about how they perceive the challenges their organizations face when it comes to software supply chain security, and the difficulties they face when working together as a collective unit. Respondents were asked to dig deep about what the biggest hurdles are for getting software supply chain security right in their organization, and explaining where "friction" can come from during the software development process from a security perspective.

The overall goal of this research is to help develop and present solutions that can bridge the gap between the issues of developers and CISOs in keeping the software supply chain secure, and to highlight where things are working so these efforts can continue in parallel with some needed changes. These changes offer an opportunity for developers and CISOs to better align software supply chain security priorities, including stronger collaboration to increase cohesion, lessen tension, and improve overall business performance.

Key Findings

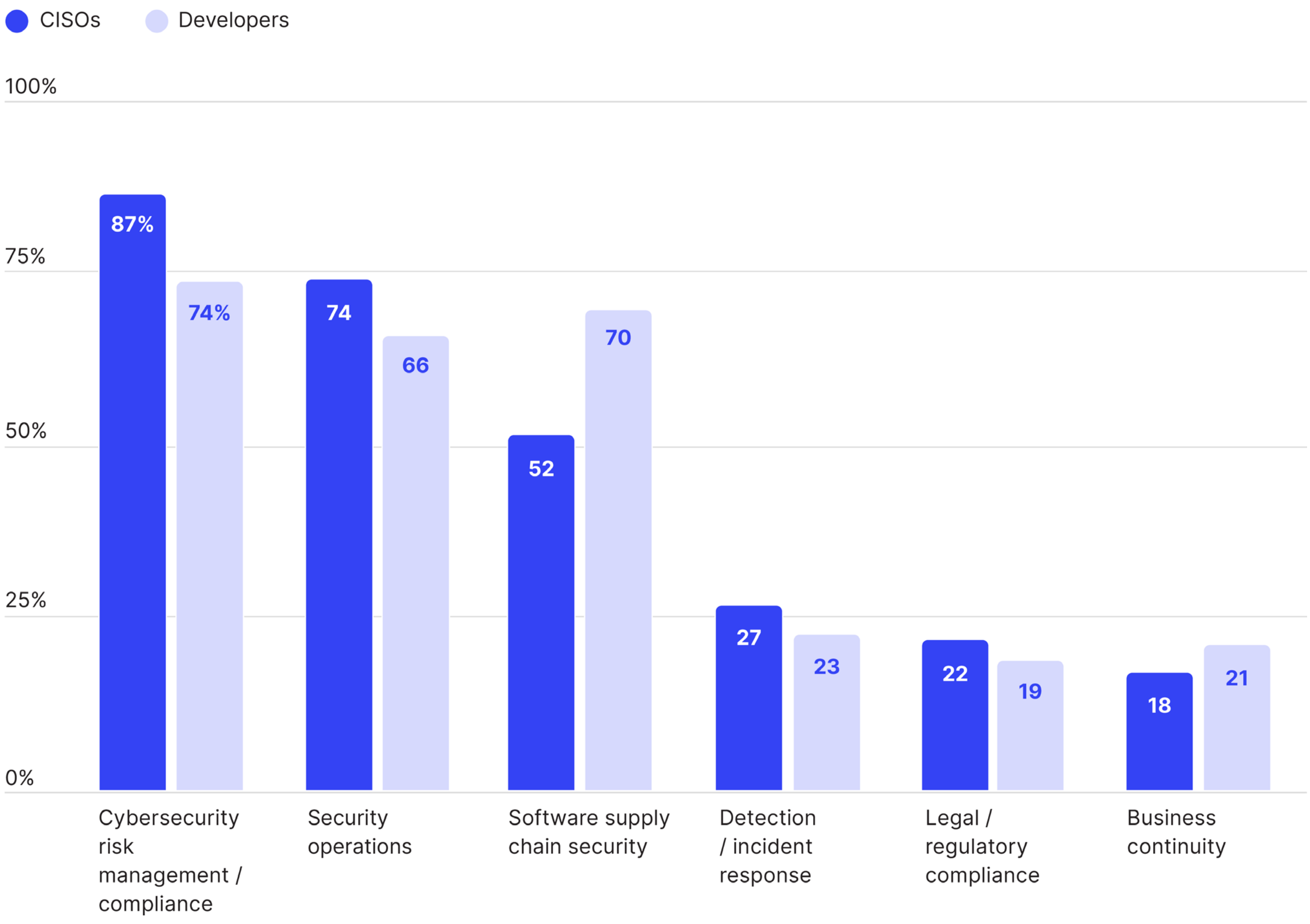
- ✓ **Fewer than half** of CISOs believe that developers are very familiar with the security risks of their development tools and workflows.
- ✓ **Only 2 in 5** developers say that CISOs are very familiar with container images, thus presenting an opportunity for better alignment on how to secure this critical technology in the supply chain.
- ✓ **Nearly 3 in 4** developers view current software supply chain security tools as being debilitating to their productivity.
- ✓ **Around 2 in 3** CISOs and developers agree that a lack of communication and collaboration between their teams is a problem when it comes to implementing better software supply chain security across their organization.

Top Organizational Security Priorities for Developers and CISOs

The majority of both developers and CISOs rate cybersecurity risk management / compliance, security operations, and software supply chain security as top priorities for their roles.

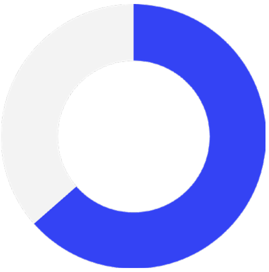
While a majority of both CISOs and developers view supply chain security as a top priority, there appears to be some discrepancy around how much of a priority it is and where it falls in the prioritization stack.

Top Security Priorities By Role



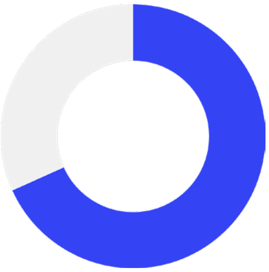
Developer Perceptions of Software Supply Chain Security Responsibilities

Developers have a sense of pride and ownership when it comes to software supply chain security in their organization. When compared to CISOs, developers feel more responsible for implementing safe software practices and reducing risks on the software supply chain. Additionally, the majority of developers say they are very security-conscious in their role.



68%

of developers view themselves as primarily responsible for prevention, mitigation, and/or remediation of supply chain security attacks or compromises



72%

of developers say they are very security-conscious in their role

CISOs Disagree on Developers' Security Prowess

Despite developers having a sense of pride about their role securing the software supply chain and believing they take a security-centric approach to their work, less than half of CISOs are fully confident that developers understand the security risks of their development and workflow tools. While most agree that developers have some level of familiarity with the security risks of their roles, less than half feel that developers are very familiar with these risks. This slightly tempered positivity about their organization's approach to software security could be in part due to their perception that developers are not fully aware of the security risks related to aspects of their work.

Fewer than half of CISOs say developers are "very familiar" with the security risks of:

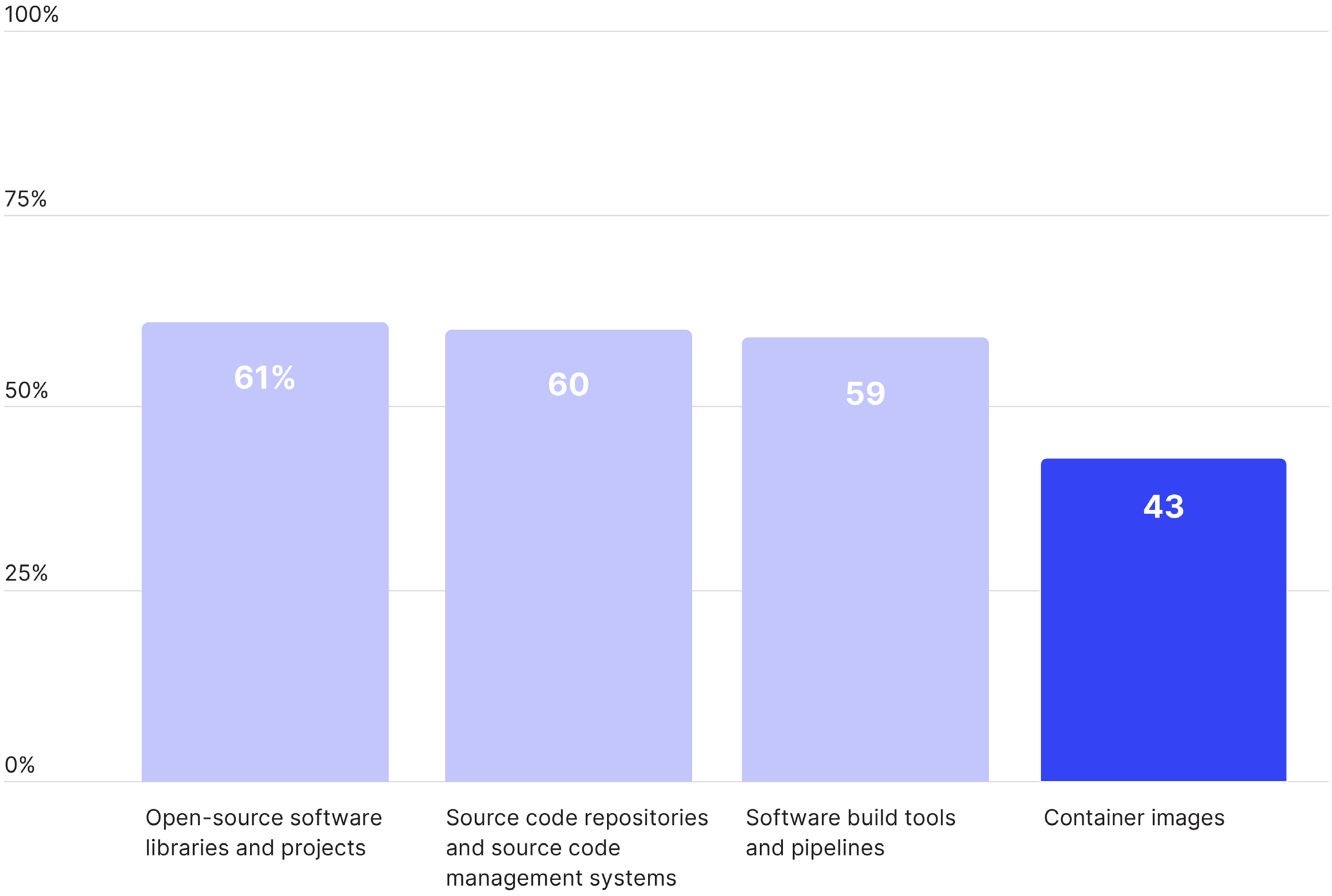
49%	49%	43%	43%
Open-source software libraries and projects	Source code repositories and source code management systems	Software build tools and pipelines	Container images

Do CISOs Understand Developer Tools and Workflows?

For the most part, developers believe CISOs have a good understanding of most developer tooling and workflows such as open source software and software build tools and pipelines.

However, developers appear less confident in their security team's familiarity with how **container images** fit into their work, presenting an opportunity for better alignment when it comes to securing containers.

Percentage of Developers Who Think CISOs Are "Very Familiar" with the Security Risks of:



Importance of Software Supply Chain Security Among CISOs and Developers

CISOs and developers agree that software supply chain security is essential to both teams' day-to-day work and their organization's holistic business health.

92% of developers say software supply chain security is important to their day-to-day work

39% of developers say it's *absolutely essential*

93% of CISOs say effective software supply chain security practices demonstrate organizational maturity and protect their organization from existing threats and risks

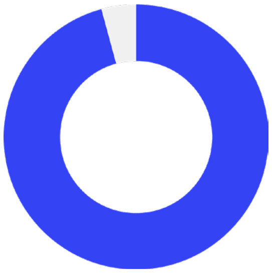
96% of CISOs say it is important for meeting government or regulatory requirements

Obstacles Impacting Software Supply Chain Security

The factors increasing tension between developers and CISOs are obstacles both teams encounter throughout the process. These can be both technical and communication-related. Both teams agree:

94%

of developers identify obstacles in maintaining software supply chain security

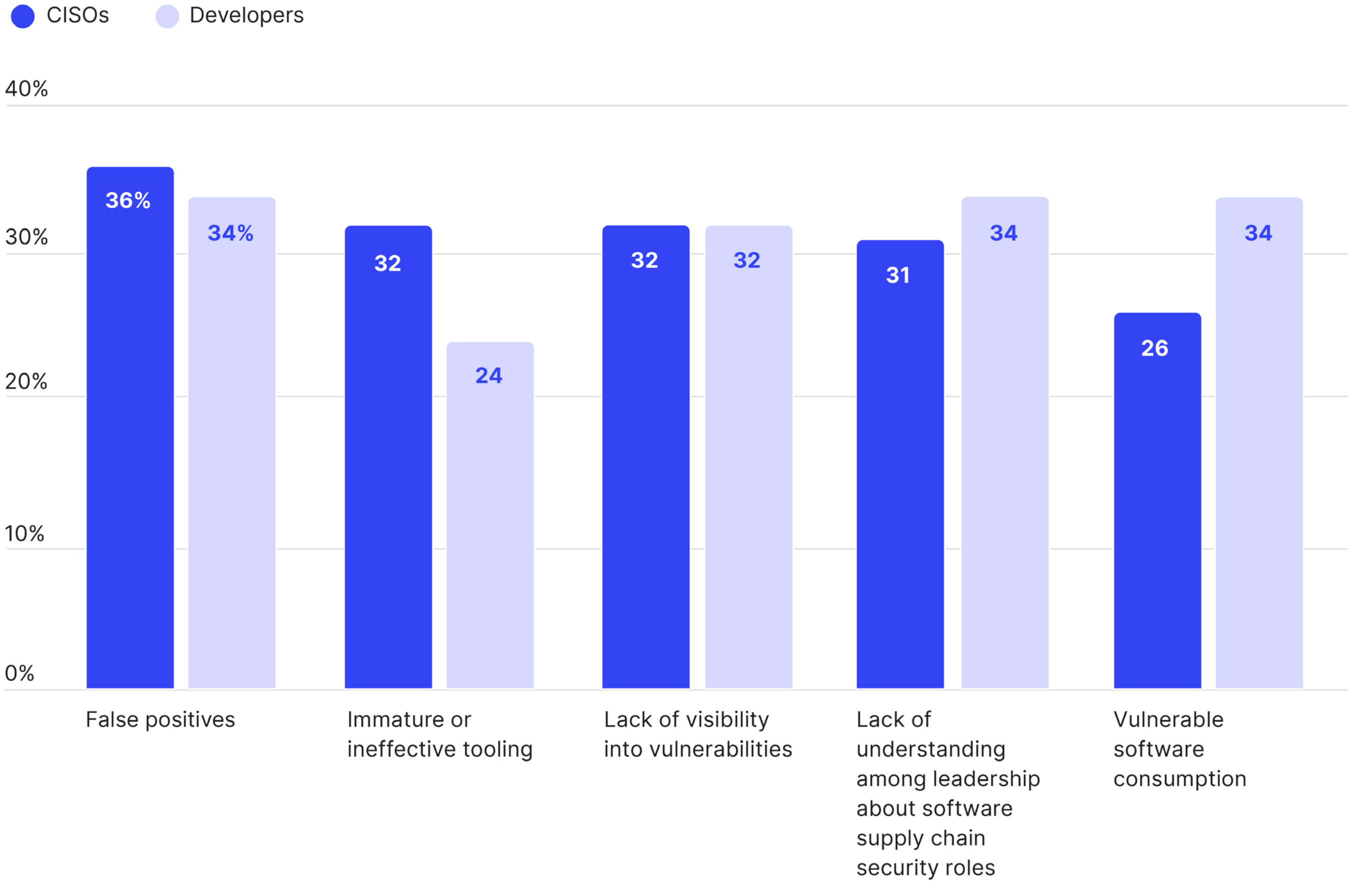


98%

of CISOs identify obstacles in maintaining software supply chain security

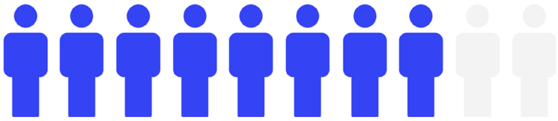
Both groups also cite **software vulnerabilities, scanner false positives and lack of cohesion between CISOs and developers** as main obstacles to software supply chain security.

Supply Chain Security Obstacles

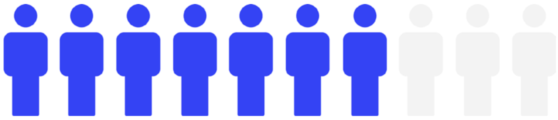


Prioritizing Software Supply Chain Security Causes Tension

Despite agreement around importance, implementing proper software supply chain security practices causes tension between developer and security teams.



77% of CISOs are in agreement that the need to prioritize software supply chain security causes tension between their team and developers



68% of developers are in agreement that the need to prioritize software supply chain security causes tension between their team and the security team

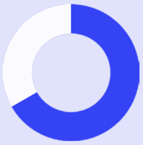
One area of tension for developers is that they do not want their productivity and day-to-day to be impacted by changes in software supply chain security approaches. They also cited current security tools, or lack thereof, do not enable them to do their best work.

56%
of developers say it is impossible to do their best work with their current software supply chain security tools, or lack thereof, in place

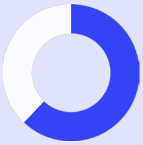
82%
of developers agree that software security practices shouldn't make it more difficult to get their work done

73%
of developers agree that the work/tools their security team requires them to use interferes with their productivity and innovation

Ultimately, there is clearly room for collaborative improvement, with both the majority of CISOs and developers agreeing that lack of communication and collaboration between their teams is a problem.



69% of CISOs agree that lack of communcation and collaboration between security and developer teams is a problem

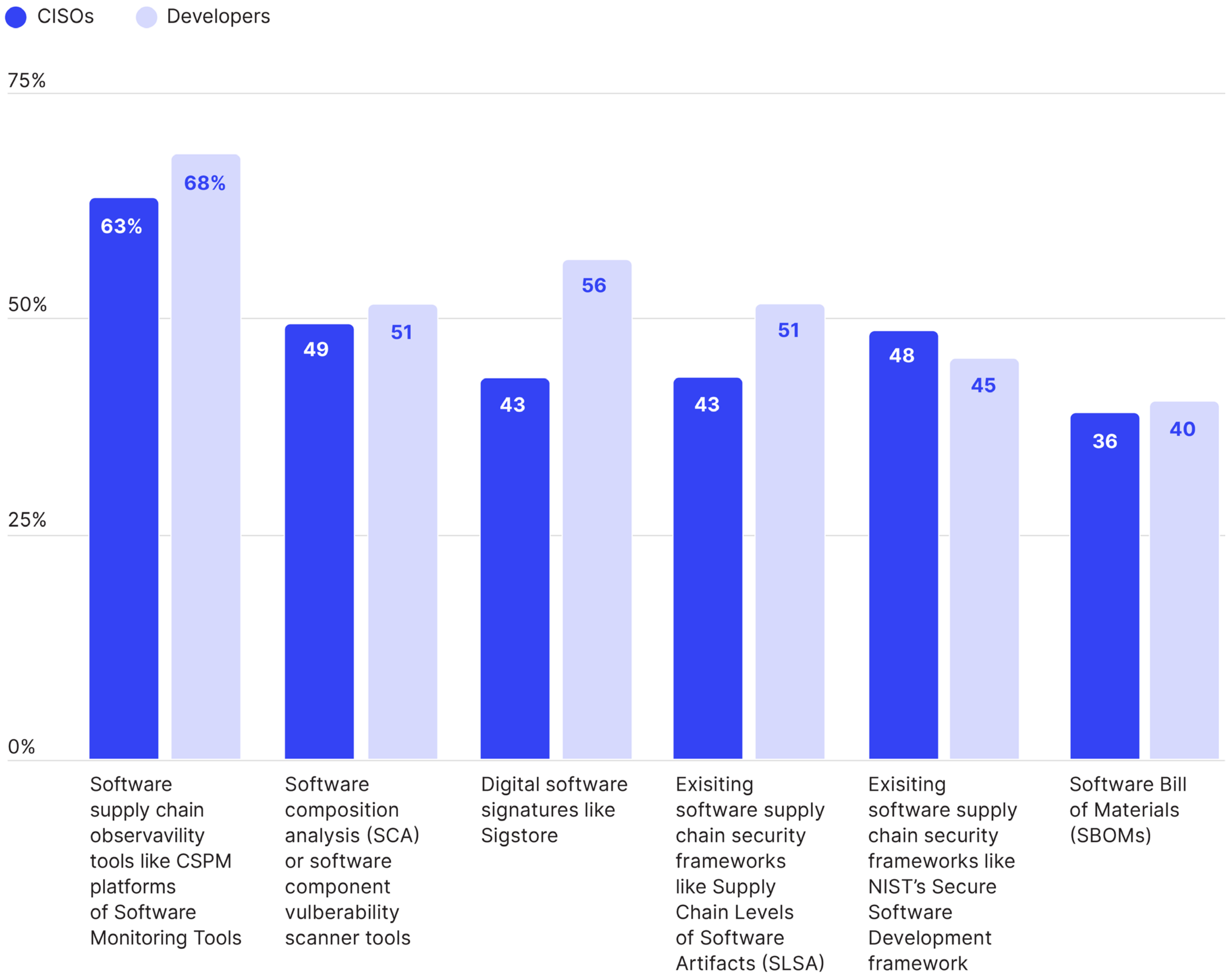


64% of developers agree that lack of communication and collaboration between security and developer teams is a problem

Organizations Are Adopting Software Supply Chain Security Tooling and Practices

In alignment with the importance already placed on software supply chain security by developers and CISOs, most organizations already have some tools in place to address software supply chain security within their organization:

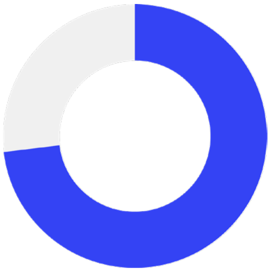
Software Supply Chain Security Tools In Place



The Five Year Forecast on Software Supply Chain Security

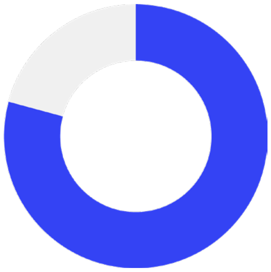
Both CISOs and developers expect changes to come in the next five years for software supply chain security at their organizations.

The good news: in addition to many software supply chain security tools and practices being implemented within organizations today, the majority of CISOs and developers believe that prioritization of software supply chain security will increase over the next five years at their organizations.



74%

of developers believe prioritization of software security will increase



85%

of CISOs believe prioritization of software security will increase

Methodology

The research was conducted online in the U.S. by The Harris Poll on behalf of Chainguard among 520 Security Decision-Makers (n=268) and Developers (n=252) aged 21+ and employed full-time or part-time. Developers are currently employed as a developer and Security Decision-Makers have a title of director or higher with a job function in security, compliance, and/or risk with significant decision-making responsibilities for security/risk/compliance at their organization. The survey was conducted February 9-24, 2023. Data are weighted where necessary for each audience by employee size to bring them in line with their actual proportions in the population.

Respondents for this survey were selected from among those who have agreed to participate in our surveys. The sampling precision of Harris online polls is measured by using a Bayesian credible interval. For this study, the sample data is accurate to within + 8.1 percentage points for Security Decision-Makers and + 7.4 percentage points for Developers using a 95% confidence level. This credible interval will be wider among subsets of the surveyed population of interest.