2024

ANNUAL STATE OF **CONTINUOUS SECURITY**

The integration of security into the Software Development Lifecycle (SDLC) stands as a critical imperative for organizations navigating today's complex cybersecurity landscape. This report encapsulates the key findings of the survey, shedding light on the importance attributed to security integration, the perceived benefits, prevalent challenges, and landscape of continuous security strategies.

Although there has been a shift in organizations adopting a Continuous Security strategy, up to **41% in 2023 up from 12% in 2022**, still a staggering **59% don't have one in place**.

Organizations recognize that the top benefits of a Continuous Security strategy are:

- Enabling real-time collaboration between development, operations, and security teams (54%)
- Reducing Security Risk (53%)
- Empowering development teams with the flexibility to manage security within existing workflows (52%)

However, despite recognizing the benefits, **94% of organizations recognize that their current application security processes are causing bottlenecks in development and delaying time to market**, to at least some extent, with **30% "to a great extent."**

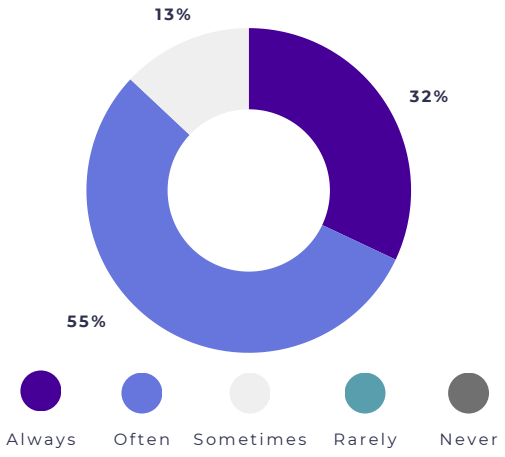
Top reasons for these bottlenecks are:

- Application security is static/not updated when requirements change, requiring rework (49%)
- Difficulty in identifying the correct project and feature level security requirements (46%)
- Poor collaboration/lack of a feedback loop between Development and security teams (43%)

CONTINUOUS SECURITY REQUIRES MORE THAN 'SOMETIMES' OR 'OFTEN'

While 100% of organizations find it at least important to integrate security into the SDLC, the vast majority still fail to do so throughout the development process.

HOW FREQUENTLY ARE SECURITY PROCESSES INTEGRATED INTO THE SOFTWARE DEVELOPMENT LIFECYCLE FROM THE BEGINNING OF THE DEVELOPMENT PROCESS?



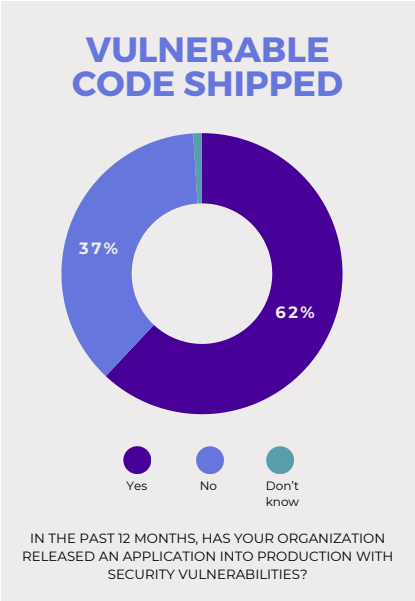
WABBI

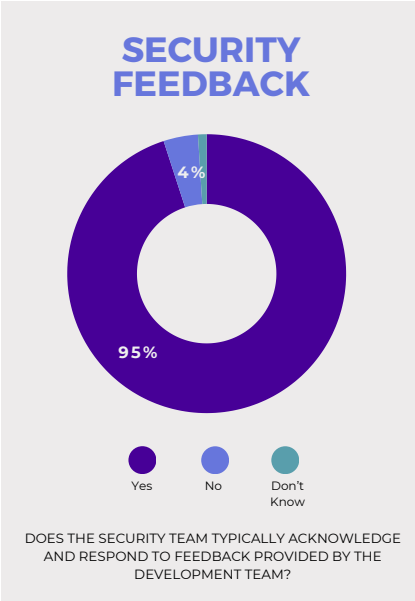
Key Findings

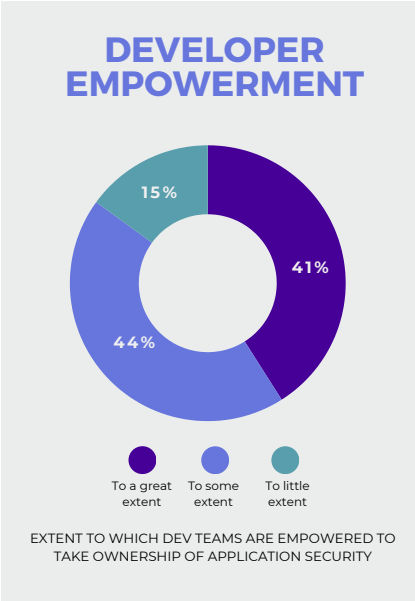
- Organizations continue to understand the **business impact of integrating security into the SDLC** goes **beyond security breach (58%)** with delays in project delivery ranking second (48%) in impacts in not integrating security into the SDLC
- **86% find it challenging** to access **accurate, application specific security**, requirements with **22% of them finding it to be *Very Challenging***
- Enterprises are more likely to find integrating security into the SDLC to be *Critical* but 86% of mid-size organizations (500-999 employees) only find it *Very Important*

Notable Changes

- **242% increase** in adoption of a a Continuous Security strategy
- **113% increase** in *always* integrating security into the SDLC
- Increased collaboration between security and development teams with **20% increase** reported in security team acknowledging and responding to feedback provided by the development team
- **Inability to meet compliance requirements moves into the Top 3** concerns of not integrating security into the SDLC, having previously been in the bottom 3







con·tin·u·ous se·cu·ri·ty
/kən'tinyəwəs sə'kyŏorədē/

In software development, the practice of automating and orchestrating the deployment of application security processes to enable dynamic management of security requirements in the SDLC in response to internal and external changes, so code is always ready to ship in compliance with the security program without creating delivery delays.