Techstrong Research

PulseMeter

Sponsored by

PRISMA® CLOUD
BY PALO ALTO NETWORKS

Inspired by the desire to operate and contribute value with less friction, authors of the DevSecOps Manifesto sought ways to "…create awesome products and services, provide insights directly to developers, and generally favor iteration over trying to always come up with the best answer before a deployment."* DevSecOps focuses on shifting security left by bringing attention and resources to security earlier in the software development lifecycle and by embedding security into the entire development process through automation and iterative software delivery.

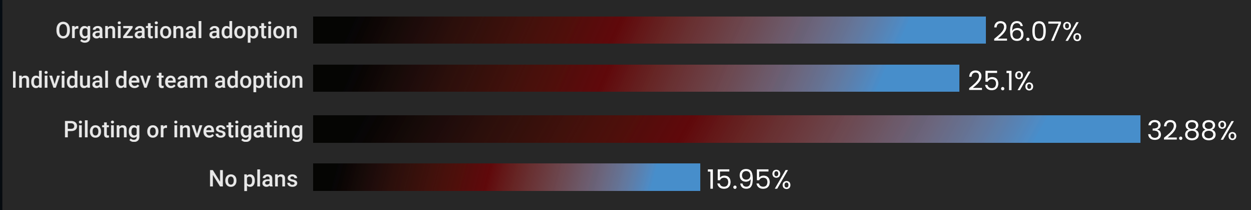
While organizations are adopting DevSecOps and the principles of shift left, security covers a dynamic software landscape that is much more complex than the traditional application, system and OS stack of the past. Contemporary cloud applications and infrastructure encompass a constantly shifting mix of commercial and open source software, including cloud-native (containers, microservices, serverless and Kubernetes orchestration), infrastructure-as-code (IaC), a plethora of cloud provider services, and observability, tracing and telemetry software. To keep pace, DevSecOps and SecOps must be as dynamic as the cloud stack it seeks to secure.

In 2022, Techstrong Research polled our community of DevOps, cloud-native, cybersecurity and digital transformation readers and viewers to take their pulse on DevSecOps. The Techstrong Research PulseMeter results show significant adoption of DevSecOps. Over 50% of respondents have already adopted DevSecOps principles, and another 32% of respondents are considering adopting it soon. The benefits gained from shifting security left are numerous, but the most-cited benefits include fewer vulnerabilities and an enhanced security posture. The biggest hindrance to DevSecOps adoption is resource constraints within teams, mainly caused by a shortage of time to shift left and the skilled resources required to undertake the initiative.

DevSecOps Adoption

Software organizations and teams are focusing on creating secure software.

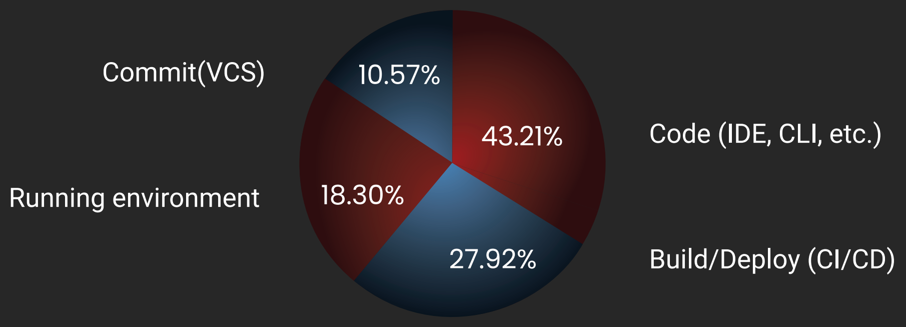
Where are you on your DevSecOps journey?



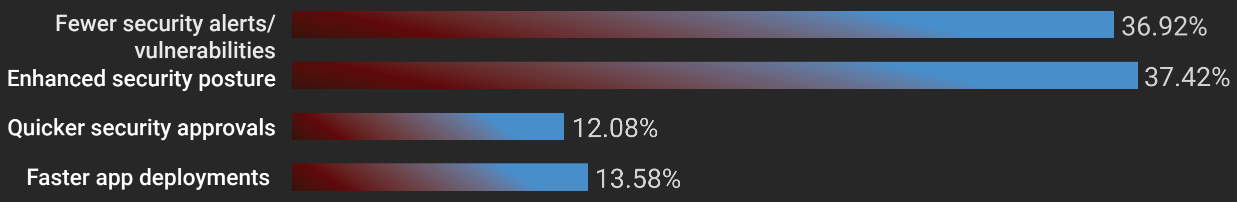
Shift Left Successes

Most organizations find security issues early in development but a significant number still emerge in production.

What is the earliest stage you identify and remediate security issues?



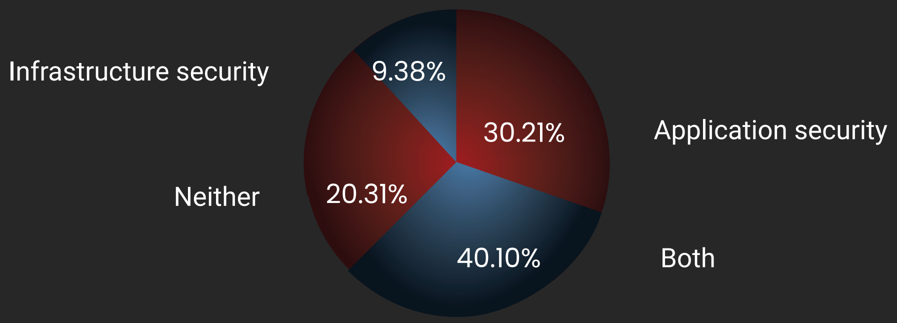
Top benefit of embedding security earlier in the dev life cycle?



Infrastructure and Applications

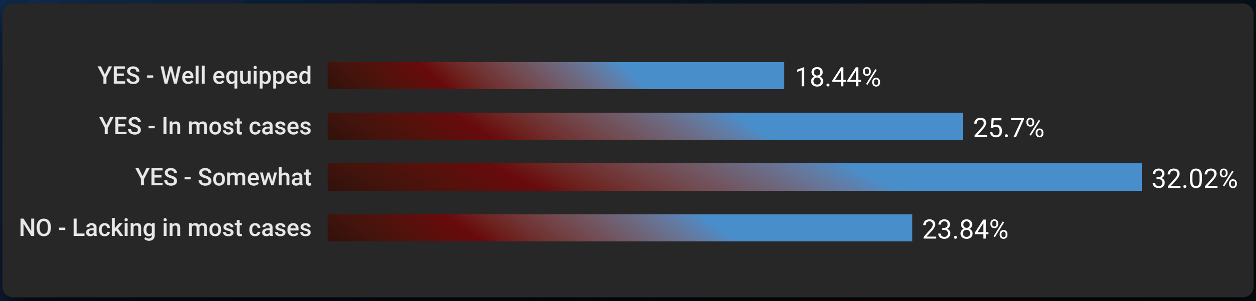
Developers play key roles in securing both application and infrastructure software.

Developers in your organization currently play an active role in:

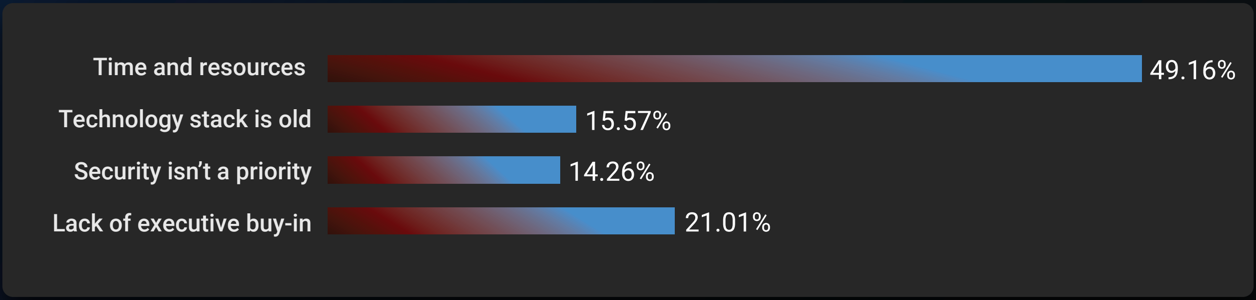


Increased security resources and time are in high demand as organizations are under pressure to deliver more software capabilities faster.

Does your dev team have the needed app security resources?



What is the biggest roadblock to implementing DevSecOps practices?



Techstrong Research Analyst View

As DevOps and Agile software development continue to take root in organizations of all sizes, the benefits of integrating security into the pipelines is well understood. Yet, DevSecOps encompasses much more than shifting left in the development process. Dynamic infrastructure software (infrastructure-as-code), serverless and Kubernetes also must be secured as part of any DevSecOps initiative.

DevSecOps principles must be implemented across parallel workflow pipelines in development, platform engineering, operations and site reliability engineering (SRE). Security automation throughout these pipelines promises to speed the remediation of vulnerabilities, decrease misconfigurations and manage cloud drift to help reduce breaches and data loss. To see the benefits of DevSecOps, DevOps and Agile organizations must infuse security expertise and technologies from design to runtime as a continuous process.

References: *DevSecOps Manifesto, https://www.devsecops.org