Rezilion

EBOOK

How Time Savings in DevSecOps is a Competitive Advantage

The expression "time is money" certainly applies to the software development process. Any time spent or squandered on avoidable tasks means a slower time-to-market for new releases or updates. That, in turn, can result in lost revenue or decreased customer satisfaction.

Time is a luxury many security and development teams simply do not have. One of the major reasons time is so tight is that organizations lack the technology talent they need, which puts more pressure on the professionals they do have to get lots of work done.

In its State of Software Engineers Report for 2022, technology staffing specialist Hired noted that the demand for software engineers continues to accelerate as competition for talent heats up. Software engineers on Hired received more than twice the average amount of interview requests in 2021 than in 2020, according to the report.

Demand for software engineers will not likely slow down any time soon.

"We've run out of ways to describe how much it's increasing," the report said. "Digital transformation may sound like a buzzword, but as more of the planet arrives online, as business owners become more creative and explore new distribution channels, as our lives evolve, we need software engineers."

Hired said it tracked 224,367 interview requests for software engineering roles in 2021, up from 106,101 in 2020. The most in-demand role on the Hired platform was for full-stack developers.

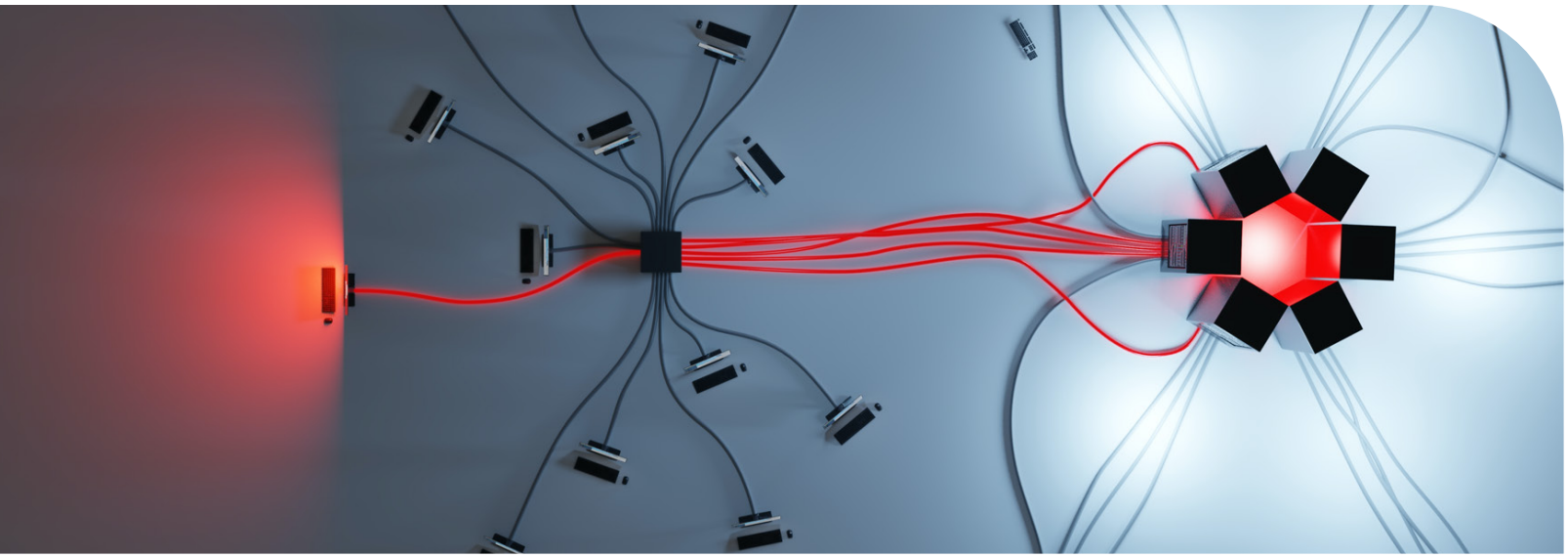
At the same time organizations are grappling with the developer talent gap, cybersecurity professionals are also in short supply. A 2021 report by the Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group noted that the cybersecurity skills shortage "continues on a downward, multi-year trend of bad to worse."

The report was based on a survey of 489 cybersecurity professionals worldwide and found that the security talent shortage had affected more than half the organizations in the study. Among the main impacts of the skills gap is a growing workload for cybersecurity teams, according to the report. A majority of the organizations surveyed said the security skills shortage and its associated impacts haven't improved over the past several years, and many said it got worse.

Given the significant talent shortages facing many development teams—combined with the rising need to ensure that software products are secure—it is not difficult to see why teams are so crunched for time.

DevSecOps, which is designed to build security into the development process throughout the software development lifecycle, can help organizations save time in a number of ways. This can help them turn out secure software products in a more timely manner and thus enhance their overall competitive posture.

Specifically, DevSecOps can save time in the areas of workflow integration, vulnerability remediation and product time-to-market. By working to enhance these areas through technology deployment and improved processes, organizations can save their teams a lot of time—and enable them to focus instead on designing, building, testing, and releasing innovative new products.



AUTOMATED WORKFLOW IS A MAJOR PART OF THE SOFTWARE DEVELOPMENT PROCESS. It is what enables teams to complete their tasks more quickly and increase efficiency and accuracy.

DevSecOps helps enable workflow integration. That's because vulnerability detection and security controls are built into the workflow, so that security remains a priority throughout the software development lifecycle. Within a DevOps development environment, the success of cybersecurity ultimately relies on how effectively security controls are part of the workflow.

The workflow integration enabled by the DevSecOps model inherently leads to time savings for team members. Consider the example of a developer who is working on code for a new software application. If the developer has to conduct a test related to a security issue, he or she would typically need to stop the work on one user interface, move to another user interface to do the testing, and then go back to the initial work environment to continue the coding work.

This is what happens if there is no workflow integration in place, and it results in additional work for the developer as well as increased complexity and friction in the process. It also means more overall time spent on the development project.

If, on the other hand, there is a security tool deployed that integrates security right into the development workflow, then there is no need to move things around to perform security testing on code.

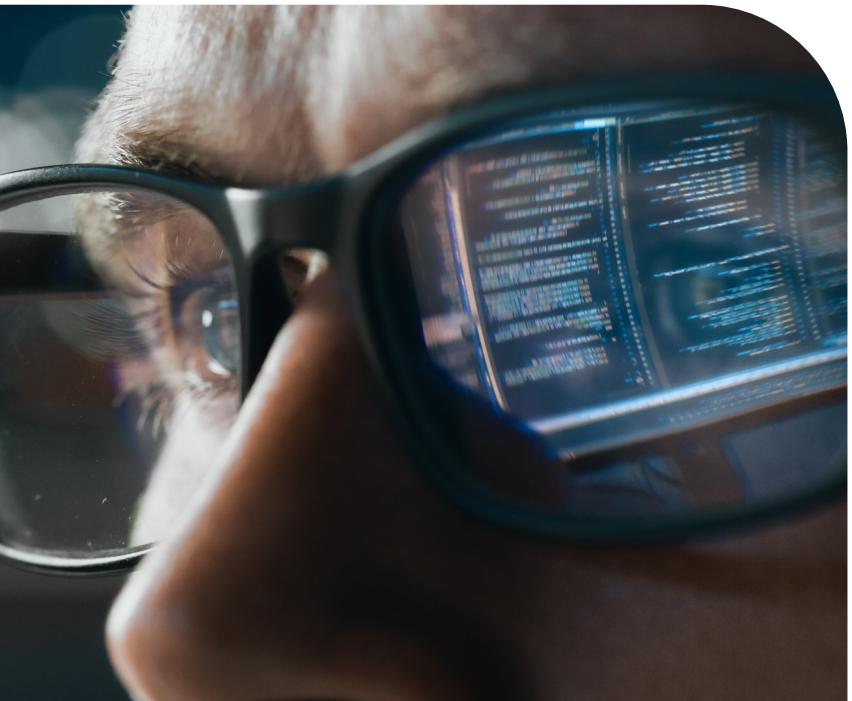
This greatly eases the process, eliminates the complexity, and saves time. The developer is happy, the security team is happy, and presumably the end users of the software will be happy as well because they received a secure, reliable application delivered on time.

It's also worth noting that the more organizations can reduce friction among team members, the greater the likelihood they can keep these professionals happy and employed with the organization. So a side benefit in terms of time savings is reducing the need to hire and train new team members.

DEVSECOPS AND THE AUTOMATED WORKFLOW INTEGRATION IT SUPPORTS also contribute to faster remediation of software vulnerabilities, another time saver for organizations. Teams are able to complete tasks more quickly and increase efficiency and accuracy.

Because vulnerability detection and remediation are built into the workflow, fixes are handled throughout the software development lifecycle. Tools such as Rezilion's platform help reduce the vulnerability backlog by up to 85%, which means there are fewer bugs to patch. That means teams save time because they are able to prioritize and focus on remediating exploitable vulnerabilities in their environment instead of wasting time to fix vulnerabilities that do not pose any risk.

In addition, if teams are able to remediate vulnerabilities more quickly, they are in effect shortening the attack window. If they do not address vulnerabilities early, the opportunity is there for attackers to exploit any weaknesses in the software. And if vulnerabilities are indeed exploited, that is going to slow down processes all the more.



As research firm Gartner has noted, "the sheer volume of reported vulnerabilities means that organizations are challenged to remediate them in appropriate time frames. Based on how fast vulnerabilities can be exploited, organizations must be prepared to perform emergency remediation on key systems within hours of a vendor releasing a patch to address a vulnerability, as well as heavily invest in mitigation measures."

They also need to continue refining their remediation process maturity to achieve non-emergency remediation across all system types within weeks, rather than months or years, the firm said.

Gartner said it recommends four best practices to operationalize effective remediation time frames:

1. **Align vulnerability management to risk appetite.** Security leaders can align vulnerability management practices to their organization's requirements by assessing specific use cases and the organization's operational risk appetite for particular risks.
2. **Prioritize vulnerabilities based on risk.** Organizations need to implement multifaceted, risk-based vulnerability prioritization, based on factors such as the severity of the vulnerability, current exploitation activity, business criticality, and exposure of affected systems.
3. **Combine compensating controls and remediation solutions.**
   By combining compensating controls that can do virtual patching with remediation solutions such as patch management tools, organizations can reduce their attack surface more effectively.
4. **Use technologies to automate vulnerability analysis.** Organizations can improve remediation windows and efficiency by deploying technologies that automate vulnerability analysis.

DEVSECOPS HELPS BRING THE SECURITY AND DEVELOPMENT FUNCTIONS INTO HARMONY, and that can result in faster time-to-market for products.

Developers are looking to build software products and get them out the door and into the hands of users as quickly as possible. The security team, on the other hand, is aiming to ensure that the code is as free from vulnerabilities as possible before software even gets to users. This not only leads to possible clashes and friction among the teams, but it can ultimately slow down progress in completing products.

DevSecOps, by emphasizing and addressing security from the beginning of the lifecycle, helps support a "secure it—ship it" approach that enables development organizations to avoid costly delays such as reverting back to earlier stages of development because of a vulnerability discovered late in the process.

Delays in development, at a time when a company's customers or internal users are expecting and demanding new software capabilities and upgrades quickly, can mean a competitive disadvantage for companies. Slow, methodical development processes are not acceptable in today's highly competitive environment.

When teams can take care of security controls as they progress through every step of development, they can code more and not have to keep turning back to make fixes. That means their release frequency goes up. And when release frequency goes up, teams are able to deliver products to production more quickly, which can lead to increased revenue, greater productivity, and more innovation.

Faster delivery, in some cases, enables companies to beat the competition to market on an innovative, new application, which can have big repercussions. As online career site Indeed noted in a January 2022 report, "being the first company to enter the marketplace has such a strong correlation with success that this practice has its own term—the first-mover advantage.

The benefits can include increased brand recognition, customer loyalty, and increased sales that often accompany a business that is the first to enter the marketplace with a new product, Indeed said. Other potential advantages include creating extensive supplier options, defining industry standards, developing retailer relationships, increased brand recognition, and establishing economies of scale.

SUMMARY: The Need for Speed—and Security—In DevSecOps

WHEN IT COMES TO SOFTWARE DEVELOPMENT, today's business environment is all about speed and agility. Without the ability to turn out applications quickly and securely, a company will probably not be able to compete effectively in its markets.

At the same time, software security needs to be imperative for development teams. A given piece of software that has significant vulnerabilities when it goes into production can end up being the source of a major breach that affects hundreds or thousands of organizations within a supply chain.

These might seem like conflicting forces—speed vs security controls. But it does not need to be that way, thanks to the DevSecOps model. DevSecOps actually promotes time savings in a number of ways, adding efficiencies to the entire process of development. Recent developments in the market are helping to make speedier, more secure development environments possible. They are enabling time savings throughout the process of software creation.

Development teams that adopt the model can balance security with speed, quickly producing software that's free of vulnerabilities making time a true competitive advantage.

About Rezilion

Rezilion's platform automatically secures the software you deliver to customers. Rezilion's continuous runtime analysis detects vulnerable software components on any layer of the software stack and determines their exploitability, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30-day free trial.