Rezilion

EBOOK

Save Time in Development and Security with The Four Pillars of DevSecOps

Software development and security professionals—who might find themselves at odds with one another on occasion—can likely agree on at least one thing: they don't have sufficient time to achieve all they need to accomplish in order to complete tasks and to get them done securely.

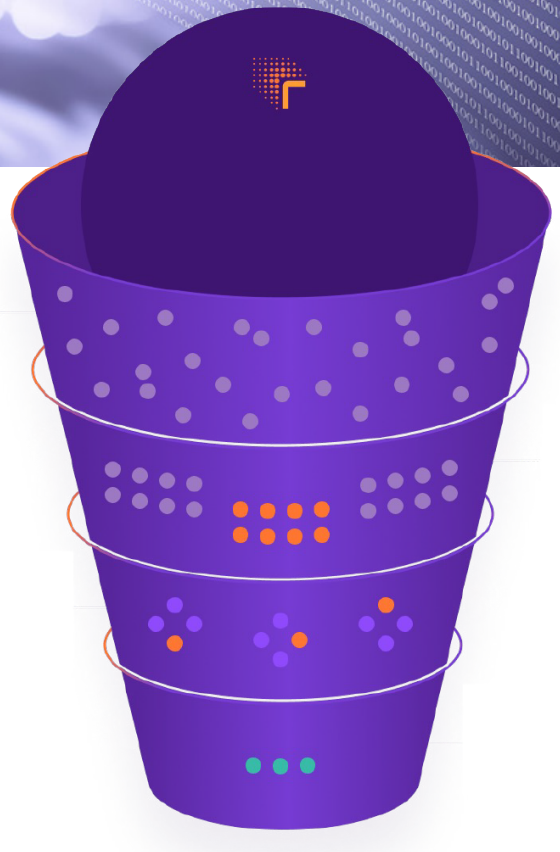
PART OF THE SENSE OF URGENCY COMES FROM THE ONGOING SHIFT TO DIGITAL BUSINESS. It's a software-driven world, and organizations and individual users want new applications and features delivered quickly. They rely on software to perform all kinds of tasks at work and at home.

Senior-level executives understand the need for their organizations to produce software rapidly to remain competitive, so it should come as no surprise that there is significant pressure on development teams to deliver software on time.

These executives also understand that software needs to be secure, and, as a result developers are not the only ones experiencing time crunches. Security teams need to find and address software flaws quickly, in keeping with the rush to get products out the door and into users' hands. And with the number of discovered vulnerabilities continuing to rise, the backlog to patch vulnerabilities grows longer.

Given that many teams are facing resource constraints because of the long-term cybersecurity skills gap, current team members have to work all the harder.

It's clear that organizations need to find ways to save development and security professionals time and also build security into the development process from the earliest stages of software creation. Software vulnerabilities have been responsible for a number of security attacks, and these are becoming more damaging, in some cases affecting not only the initial targets but their supply chain partners as well.



ONE SOLUTION TO SAVING TIME AND ALSO MAKING SECURITY AN INHERENT PART of the development process is to deploy the DevSecOps model, which is designed to include security in the development process throughout the software development life cycle.

With DevSecOps, organizations can turn out secure software products in a timelier manner and enhance their overall competitive posture. The model consists of four pillars—discovery, validation, prioritization, and remediation— each of which aligns with the vulnerability management process that enterprises need in order to mitigate the risk of software flaws.

This ebook examines each of these DevSecOps pillars and how they tie into a vulnerability management program. Learn why you need to include each pillar in order to see DevSecOps succeed in your organization.

DISCOVERY IS A VITAL COMPONENT OF DEVSECOPS AND VULNERABILITY MANAGEMENT because without it, organizations are not able to identify the software flaws that could eventually be exploited by bad actors and used to launch attacks.

Discovery is oftentimes made possible by solutions such as vulnerability scanners, tools that analyze software code and search for known vulnerabilities. Some organizations need to use vulnerability scanning and management so that they can be compliant with regulations and industry standards such as the International Organization for Standardization's ISO 27001 Information Security Management System (ISMS).

Security teams deploy scanning tools to collect information from the endpoint devices on enterprise networks, such as which version of a software program is installed on devices. They can then compare this information with known vulnerabilities as reported by the software vendors who produced the software, or others tracking vulnerabilities.

It has never been more important to find software vulnerabilities as early as possible, given the state of the threat landscape and the role vulnerabilities play in making attacks possible.

An April 2022 alert posted by multiple cybersecurity authorities in the United States, Australia, Canada, New Zealand, and United Kingdom noted that malicious cybercriminals had targeted global Internet-facing systems such as email servers and Virtual Private Network (VPN) servers with exploits of newly disclosed vulnerabilities in 2021.

In the advisory, the agencies, including the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) and Federal Bureau of Investigation (FBI), provided details about the top 15 Common Vulnerabilities and Exposures (CVEs) that cyber bad actors were routinely exploiting in 2021, as well as on other CVEs that were frequently exploited.

Attackers aggressively targeted newly disclosed critical software vulnerabilities against a broad set of targets, including public and private sector organizations around the world, the alert said.

Among the top exploited vulnerabilities noted by the agencies was the highly publicized Log4Shell, which affects Apache's Log4j library, an open-source logging framework. A bad actor can exploit the vulnerability by submitting a specially crafted request to a vulnerable system that causes it to execute arbitrary code. The request allows attackers to take complete control of the system, steal data, launch ransomware, or conduct other malicious activities.

The widespread exploitation of the vulnerability, first disclosed in December 2021, shows the ability of malicious actors to quickly weaponize known software vulnerabilities and go after organizations before they have had a chance to apply a fix, the alert said.

To a lesser extent, bad actors continued to exploit publicly known, older software vulnerabilities across a range of targets, the alert said. The exploitation of older vulnerabilities illustrates the ongoing risk organizations face when they fail to patch software in a timely manner, or when they are using software that's no longer supported by the vendor.

The cybersecurity authorities urged organizations to apply mitigations such as security patches to systems and to implement a centralized patch management system, in order to decrease the risk of compromise by malicious cyber actors.

It's clear that organizations need to prioritize the discovery phase of DevSecOps if they hope to successfully mitigate vulnerabilities and defend themselves effectively.

DevSecOps Pillar 2: Validation

THE VALIDATION PILLAR OF DEVSECOPS IS IMPORTANT because it's where the software bugs that represent genuine risks are separated from the vulnerabilities that don't pose any serious security risks.

Validation is essentially a technical analysis that determines if a particular vulnerability in a piece of software code is exploitable within the specific context in which the code is deployed. For example, when code or packages of code are deployed within a container, most of it is not going to be used. A portion might simply be code bloat, or perhaps it is a component of the operating system.

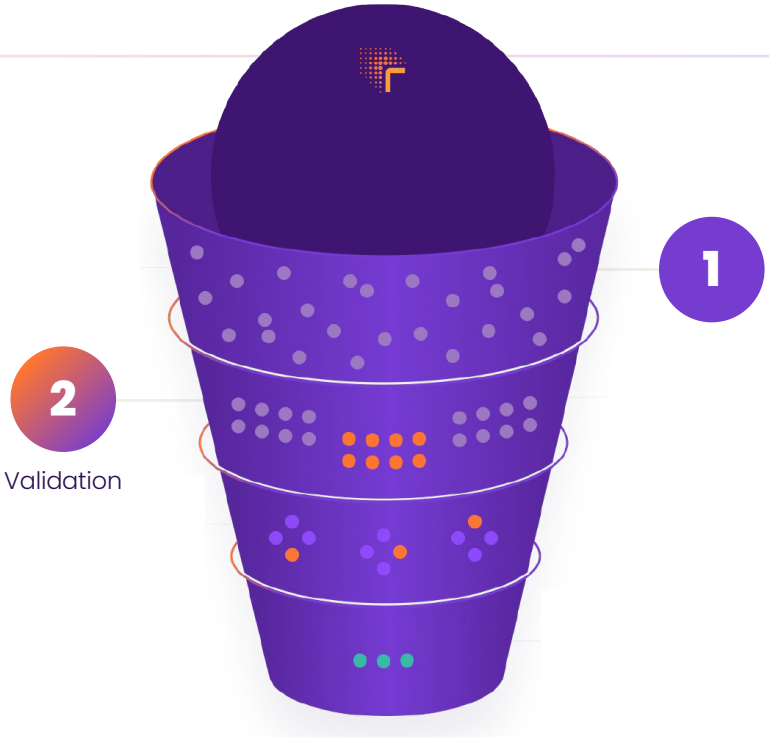
When a piece of vulnerable code can be deployed in a container but cannot be loaded into memory, then it is technically not exploitable and therefore not a cyber threat.

The vulnerability validation process is by nature always deterministic, providing a definitive yes or no answer to the query of whether a particular vulnerability can be exploited.

Solutions on the market such as Rezilion's software attack surface management platform platform provide the analytics capabilities security teams need so they can identify which vulnerabilities can actually be exploited by bad actors. Among the benefits of validation is that they allow security and development teams to do less patching. That means they can spend more time creating new software products and features, free of the burden of patch backlogs.

Rezilion's platform is capable of reducing patching needs by 85% or more by aggregating vulnerability scanning results and automatically filtering the results to focus only on what is actually loaded and exploitable—the actual risk.

In a particular use case involving a Rezilion customer, a Fortune 500 software company experienced $4.3 million in savings per year using the platform. The firm has about 1,300 servers in production, and discovered more than 5 million total vulnerabilities.



By deploying Rezilion, the company determined that nearly half of the vulnerabilities were not loaded into code and therefore were not a risk. The savings came in not having to devote time and resources to patching these vulnerabilities.

The platform enables users to visualize a Dynamic Software Bill of Materials (SBOM) by mapping and dynamically tracking the function, status and interactions of each piece of code in the organization's environment. They can manage the full vulnerability backlog from a single place, by aggregating scan data from any type or number of tools, and accurately report on the effectiveness of the organization's vulnerability management program.

Considering the large number of software vulnerabilities and limited security resources at many companies, the ability to drive greater efficiencies with vulnerability management is vital for organizations. This is why validation is one of the pillars of DevSecOps.

PRIORITIZATION LETS TEAMS QUICKLY DETERMINE WHICH OF THE TRULY SERIOUS VULNERABILITIES they should remediate first because of the potential risks they might pose to their organization and others.

The fact is, not all vulnerabilities are equal in terms of the damage they can potentially do and the impact they can have on organizations and their customers and business partners. For example, some code might be so widely used that an exploitable security vulnerability could threaten hundreds or thousands of organizations.

Prioritization, like the other three pillars of DevSecOps, is vital to the successful use of the model and to effective vulnerability management.

One of the common ways to prioritize vulnerabilities is through the Common Vulnerability Scoring System (CVSS). This is a free and open industry standard for assessing the severity of vulnerabilities. It attempts to assign severity scores to vulnerabilities, which enables teams to prioritize responses and resources according to the potential threat.

It's common for the teams that handle patching to try to resolve issues within an acceptable time, but oftentimes they are not aware of the bug until another team responsible for security testing has validated the existence of the vulnerability. This could happen days after the vulnerability has remained open, giving bad actors plenty of opportunity to exploit it.

Organizations need a more effective way to prioritize software fixes before bad actors can exploit them to launch attacks. Solutions such as the Rezilion platform helps teams prioritize which vulnerabilities need to be addressed first and which do not need to be remediated right away because they do not pose an immediate risk to the environment.

The idea of prioritizing vulnerabilities has become a focus at many organizations, including the U.S. federal government. For example, the Cybersecurity and Infrastructure Security Agency (CISA) in late 2021 issued a directive to federal civilian agencies to prioritize the remediation of those vulnerabilities that are being actively exploited by adversaries.

The directive establishes a catalog of known exploited vulnerabilities and requires agencies to fix such vulnerabilities within specific timeframes. The effort is aimed at sending a clear message to all organizations nationwide to focus patching on the subset of vulnerabilities that are causing harm now, and enable CISA to drive continuous prioritization of vulnerabilities based on its understanding of adversary activity.

Although the directive applies directly to federal civilian agencies, CISA strongly recommended that private businesses and other government entities prioritize mitigation of the vulnerabilities listed in CISA's public catalog and sign up to receive notifications when new vulnerabilities are added.

REMEDIATION, THE FOURTH AND FINAL PILLAR OF DEVSECOPS, is the step in the vulnerability management process that all others lead to. Without remediation, there's really no point to the other phases.

Not all methods of remediation are as effective as others, however. The key to fixing software bugs efficiently is to automate the task. This can speed up the process of eliminating the security risks by fixing the software, and it can also hasten the delivery of products.

So to excel at remediation, security, and development teams should focus on "smart remediation" that leverages automation wherever possible. This approach actually fits in well with the previous stages of vulnerability management—and the other pillars of DevSecOps—each of which aim for the most efficient method of addressing software bugs.

Research firm Gartner has noted that the threat landscape is different for every organization, and a reasonable timeframe for fixing vulnerabilities will also vary. Perceived "industry standard" vulnerability remediation timeframes don't account for organization—specific constraints, technology cohabitation considerations, internal policies, or external compliance requirements, the firm says.

Gartner suggests that organizations take a structured risk—and fact-based approach to vulnerability management as part of their overall security programs.

"The sheer volume of reported vulnerabilities means that organizations are challenged to remediate them in appropriate time frames," the firm says. "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."

Organizations also must continue refining their remediation process maturity to achieve non-emergency remediation across all types of systems within weeks, rather than months or years, Gartner says. The firm suggests four best practices to achieve effective remediation timeframes:

- **Align vulnerability management** to the organization's operational risk appetite, IT operational capacity/capabilities and its ability to absorb disruption when trying to remediate vulnerabilities.
- **Implement multifaceted, risk-based vulnerability prioritization** based on factors such as the severity of a vulnerability, current exploitation activity, business criticality and exposure of the affected system.
- **Integrate tools** that perform virtual patching, such as intrusion detection and prevention systems and web application firewalls, with remediation solutions such as patch management tools to reduce the attack surface more effectively.
- **Use solutions to automate vulnerability analysis,** which can improve remediation efficiency.

For Rezilion, automating vulnerability remediation has been a priority in its product strategy. The company's platform distills thousands of vulnerabilities to a handful of packages that need to be updated to remediate vulnerabilities and meet security and compliance requirements. The solution executes an organization's remediation plan with automated tickets and issues to notify developers about which components they need to upgrade.

The platform tracks a team's remediation efforts and service level agreements (SLAs), to ensure that it is not out of compliance.

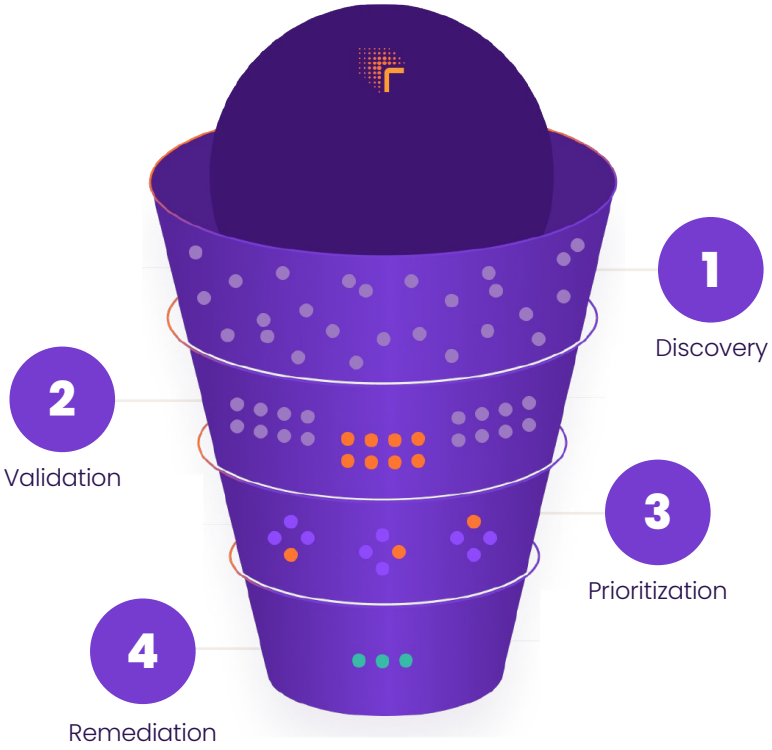
Tying It All Together: Embrace the Pillars of DevSecOps To Supercharge Your Program

THE WAY MANY ORGANIZATIONS HAVE BEEN HANDLING VULNERABILITY MANAGEMENT is clearly not working—based on the number of security incidents that can be traced back to software bugs.

DevSecOps offers a way for security and development teams to not only save themselves time, but more effectively produce software that is secure and reliable.

Rezilion research reveals that a large majority of software vulnerabilities pose no risk to organizations. A vulnerability is only as dangerous as the threat exploiting it, and the vast majority of vulnerabilities with "high severity" CVSS scores have never been seen in the wild nor linked to data breaches.

By putting the right tools in place that allow them to prioritize vulnerabilities and focus on only the real threats, and by leveraging the four pillars of DevSecOps, security teams can help their organizations run a much more efficient and secure development processes.



Find out how Rezilion can help you fully embrace all four pillars of DevSecOps and bring your vulnerability management program to the next level. Book a demo and see our platform in action at https://www.rezilion.com/request-a-demo.

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.