Datadog's State of DevSecOps 2024 Report Finds Organizations Aren't Fully Embracing Automation for Securing Cloud Deployments

April 17, 2024 at 4:05 PM EDT

The report also found that adoption of DevOps practices leads to improved security outcomes

NEW YORK, April 17, 2024 /PRNewswire/ -- Datadog, Inc. (NASDAQ: DDOG), the monitoring and security platform for cloud applications, today announced its new report, the *State of DevSecOps 2024*. The report found that a surprising amount of organizations aren't embracing automation when it comes to securing cloud deployments.

At least 38% of organizations leveraging AWS had deployed workloads or completed sensitive actions manually through the AWS console in a production environment within a 14-day period, meaning they are relying on manual click operations instead of automation.

Adoption of infrastructure as code (IaC) also varied across cloud providers. IaC is considered a critical practice when securing cloud production environments, as it helps ensure that human operations have limited permissions on production environments, all changes are peer reviewed and issues are identified earlier in the process. The report found that in AWS, over 71% of organizations use IaC through at least one popular IaC technology such as Terraform, CloudFormation or Pulumi. This number is lower in Google Cloud, at 55%.

"These findings from the *State of DevSecOps* show that there is still room for improvement when it comes to embracing automation for the sake of improving security," said Andrew Krug, Head of Security Advocacy at Datadog. "Modern DevOps practices go hand-in-hand with strong security measures—and in fact, security helps drive operational excellence across the organization. While security starts with visibility, securing applications is only realistic when practitioners are given enough context and prioritization to understand which security signals matter and which are irrelevant."

Other key findings from the report include:

- While attacks from automated security scanners represent the largest number of exploitation attempts, the vast majority of these attacks are harmless and only generate noise for defenders. Out of the tens of millions of malicious requests that were identified coming from such scanners, only 0.0065% successfully triggered a vulnerability.
- A substantial number of organizations continue to rely on long-lived credentials—one of themost common causes of data breaches—in their CI/CD pipelines, even in cases where short-lived ones would be both more practical and more secure. 63% used a form of long-lived credential at least once to authenticate GitHub Actions pipelines.
- Java applications are the most impacted by third-party vulnerabilities; 90% of Java services are susceptible to one or more critical or high-severity vulnerabilities introduced by a third-party library, versus an average of 47% for other programming languages.

For the report, Datadog analyzed tens of thousands of applications and container images, along with thousands of cloud environments to assess the security posture of applications today and evaluate the adoption of best practices that are at the core of DevSecOps.

Datadog's *State of DevSecOps 2024* is available now. For the full results, please visit: https://dtdg.co/pr-devsecops2024. To learn how Datadog helps companies secure their cloud environments, visit: https://www.datadoghq.com/product/cloud-security-management/.

About Datadog

Datadog is the observability and security platform for cloud applications. Our SaaS platform integrates and automates infrastructure monitoring, application performance monitoring, log management, user experience monitoring, cloud security and many other capabilities to provide unified, real-time observability and security for our customers' entire technology stack. Datadog is used by organizations of all sizes and across a wide range of industries to enable digital transformation and cloud migration, drive collaboration among development, operations, security and business teams, accelerate time to market for applications, reduce time to problem resolution, secure applications and infrastructure, understand user behavior and track key business metrics.

Forward-Looking Statements

This press release may include certain "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, or the Securities Act, and Section 21E of the Securities Exchange Act of 1934, as amended including statements on the benefits of new products and features. These forward-looking statements reflect our current views about our plans, intentions, expectations, strategies and prospects, which are based on the information currently available to us and on assumptions we have made. Actual results may differ materially from those described in the forward-looking statements and are subject to a variety of assumptions, uncertainties, risks and factors that are beyond our control, including those risks detailed under the caption "Risk Factors" and elsewhere in our Securities and Exchange Commission filings and reports, including the Quarterly Report on Form 10-Q filed with the Securities and Exchange Commission on November 7, 2023, as well as future filings and reports by us. Except as required by law, we undertake no duty or obligation to update any forward-looking statements contained in this release as a result of new information, future events, changes in expectations or otherwise.

Contact
Dan Haggerty
press@datadoghq.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/datadogs-state-of-devsecops-2024-report-finds-organizations-arent-fully-embracing-automation-for-securing-cloud-deployments-302119865.html

SOURCE Datadog, Inc.