Voices of Practitioners: The State of Secrets in AppSec

GitGuardian Study Provides Insights From 507 IT Decision-Makers On Secrets Sprawl and Risk Mitigation

PARIS, FRANCE, May 9, 2023 /EINPresswire.com/ -- GitGuardian, the leading provider of automated secrets detection solutions, recently commissioned Sapio Research to conduct a study on the perceptions and practices of 507 IT and security decision-makers in the US and UK. The study, entitled "Voice of Practitioners: The State of Secrets in AppSec," aim to shed light on the risks posed by secrets sprawl and the measures taken to mitigate them in large enterprises.

The study reveals that senior management in large organizations is acutely aware of the risks associated with hard-coded secrets. A significant 75% of respondents reported having experienced a past leak, and 94% plan to improve their secrets management practices in the next 12-18 months. Interestingly, more than half of the respondents identified "source code and repositories" as key risk points within their software supply chains, with 47% specifically citing hard-coded secrets.

Despite this increased awareness, the study also highlights significant disparities in risk reduction strategies across the industry. For example, a concerning 27% of respondents revealed that they rely on manual code reviews, which are inefficient, to protect themselves from secret leaks.

"While press coverage of technology security matters tends to focus on penetrations of production systems, ransomware and other incidents involving external attackers, the truth is that one of the most pressing concerns for most organizations is the unintended publishing of internal secrets," said Stephen O'Grady, Principal Analyst with RedMonk. "As source code is increasingly fragmented and spread widely across organizations and the globe, it's become all too common to see secret certificates, keys and passwords ending up in publicly accessible repositories. Preventing this nightmare scenario is a major area of focus for organizations large and small."

In addition to the poll results, the study delves into the common pain-points experienced by large organizations as they grapple with an accumulating backlog of vulnerabilities. In 2022, GitGuardian partnered with a large-scale enterprise to help scale its leak prevention efforts using a multifaceted approach. With 7,500 developers and over 50,000 monitored sources, this

enterprise required a solution that was both robust and scalable.

The results of this successful deployment provide valuable insights into the best way to grow an application security strategy in large enterprises. According to the data, the most significant impact on reducing the risk of secrets sprawl comes from integrating GitGuardian's solution into the early stages of the development lifecycle and enabling developers to become autonomous on both the prevention and remediation fronts.

Overall, the study emphasizes the need for organizations to adopt a more proactive approach to security, leveraging automated tools and processes to identify and remediate vulnerabilities quickly and efficiently. By automating the triage and assignment processes, organizations can accelerate their security orchestration, improve their security posture, and free up valuable resources to focus on other critical tasks.

The risk companies face from the rapid sprawl of API keys, configuration variables, and secrets within engineering teams is immense. Secrets are the gateway to a company's most valuable asset, its data. We're at a critical time where it's necessary for engineering and security teams to have a holistic secrets strategy. While sprawl is a problem most companies experience, it's not a hard one to solve. There are tools available today that natively integrate into developer workflows for managing, orchestrating, and rotating secrets.- Brian Vallelunga, CEO of Doppler

Download the Voices of Practitioners study here: http://www.gitguardian.com/files/voice-of-practitioners-the-state-of-secrets-in-appsec
A [webinar](#) presenting the results of the study will be held on May 25, 2023 at 5PM CEST

Additional resources
GitGuardian - https://www.gitguardian.com/
State of Secrets Sprawl 2023 - https://www.gitguardian.com/state-of-secrets-sprawl-report-2023
Secrets Management Maturity Model - https://www.gitguardian.com/secrets-management-maturity-questionnaire

About GitGuardian
GitGuardian is a code security platform that provides solutions for DevOps generation. A leader in the market of secrets detection and remediation market, its solutions are already used by hundreds of thousands of developers, and it is the number one security application on the GitHub marketplace.
GitGuardian helps developers, cloud operation, security, and compliance professionals secure software development and define and enforce policies consistently and globally across all systems.

GitGuardian solutions monitor public and private repositories in real-time, detect secrets, sensitive files, IaC misconfigurations, and alert to allow investigation and quick remediation. Additionally, GitGuardian's Honeytoken module also exposes decoy resources like AWS

credentials, increasing the odds of catching intrusion in the software delivery pipeline.

GitGuardian is trusted by leading companies, including Instacart, Snowflake, Orange, Bouygues Telecom, Iress, Maven Wave, NOW: Pensions, DataDog, and PayFit.

About Sapio Research
Sapio Research is an award-winning, international full-service market research consultancy. Sapio can help in all areas of quantitative and qualitative research and welcome complex, challenging briefs. They work in the specific fields of audience understanding, brand research, and content research.

Holly Hagerman
Connect Marketing
+1 801-373-7888
hollyh@connectmarketing.com

This press release can be viewed online at: https://www.einpresswire.com/article/632540943