GitGuardian Cuts False Positives by 50% with Machine Learning

The company's latest breakthrough in secrets detection will relieve Security and Engineering teams from noisy scanning results.

BOSTON, MASS., UNITED STATES, June 26, 2024 /EINPresswire.com/ -- GitGuardian, the world leader in automated secrets detection and remediation, announced today groundbreaking progress in eliminating false positives thanks to in-house Machine Learning. With the upcoming introduction of FP Remover, GitGuardian is pushing its state-of-the-art secrets detection engine precision to new heights, removing as much as 50% of False Positives. As a result, security and engineering teams will spend significantly less time reviewing and dismissing false alerts.

False Positives occur when a detection system incorrectly identifies harmless events as risks. This is a common problem with most security vulnerabilities, including secrets. It's a waste of time and resources, creating unnecessary stress and tiring out teams. Ultimately, too many false positives risk making teams ignore real threats when they appear.

However, no detector is foolproof; some false positives will always fall through the cracks. Otherwise, it would mean that the detection is too narrow and that many true positives were missed, which could lead to security breaches of all sizes. The challenge here is to find the right balance: not missing true positives while showing users as few false positives as possible.

"For years, GitGuardian's secrets detection team has adopted a data-driven approach to make its detectors as precise as possible. This is a daunting task, and we still have a few false positives that make it through our algorithms," said Eric Fourrier, CEO of GitGuardian. "In a groundbreaking achievement that will set a new industry standard, GitGuardian's Machine Learning experts and Secret Detection team have joined forces to create FP Remover, a new ML model that achieves unseen signal-to-noise ratio for secret detection: it cuts down the number of incidents users have to remediate, so they can focus where it matters, real exposed secrets."

For practitioners, it means that GitGuardian will continue to present the same number of true positives as before, and significantly fewer false positives.

FP Remover can understand code and identify false positives like a developer: it recognizes potential secrets that aren't actually secrets based on code-specific syntax or context understanding. Powered by in-house Machine Learning, it's built on a transformer architecture

trained on a large amount of code data and fine-tuned on GitGuardian's secrets detection datasets. FP Remover was designed to ensure users' security and privacy: their data never leaves GitGuardian's infrastructure.

More precisely, for generic secrets, FP remover will eliminate half of the 10% of false positives that were incorrectly identified as secrets, but will also discard 0.3% of true positives. This tradeoff is considered acceptable because GitGuardian's secrets detection is comprehensive enough to have a very low rate of missed true positives.

FP Remover will drastically improve the efficiency of Security and Engineering teams without affecting the detection of real incidents. Reducing the number of false positives will help them:

- Save time and resources: Security and engineering teams will spend significantly less time reviewing and dismissing false alerts.
- Increase their precision: Avoid overlooking genuine threats due to the volume of false positives.
- Reduce alert fatigue: Continuous false alarms can lead to desensitization, causing real threats to be ignored.

"FP Remover is a major improvement to GitGuardian's user experience and for code security overall. Users will spend more time remediating actual incidents, and less time investigating false alarms," Eric added. "While it represents an important milestone in our continuous efforts to improve our secrets detection engine, it is just the beginning of what can be achieved through Machine Learning. Over time, our teams will improve the performance of our ML models with our community of 500K developers and customers. But detection without remediation is just noise. This is why our ML teams are already focused on supplying additional information and context about secrets identified through our generic detectors. This will assist our users in prioritizing and addressing the most critical vulnerabilities."

Research showed that upon discovering an exposed valid secret, 90% remain active for at least five days. GitGuardian is fighting against Secrets Sprawl by letting Security and Engineering teams collaborate more efficiently on remediating actual vulnerabilities.

Additional resources
GitGuardian Website: https://www.gitguardian.com/

About GitGuardian
GitGuardian is the code security platform for the DevOps generation. Founded in 2017, it has become the leader in automated secrets detection and is now focused on providing a comprehensive software supply chain security platform.

GitGuardian helps security teams define and enforce secure coding practices consistently and globally at every step of the software development process. Centered on collaboration between

security and development teams, GitGuardian also helps organizations enhance their security posture by decentralizing and accelerating the remediation of hardcoded secrets incidents and vulnerabilities in open-source dependencies, misconfigurations in infrastructure-as-code, and detecting intrusion in the software supply chain.

Widely adopted by developer communities, GitGuardian is the #1 security application on GitHub Marketplace and is used by over 500 thousand developers and leading companies, including Snowflake, Orange, Acquia, ING, Mirantis, Maven Wave, Payfit, Webflow and Bouygues Telecom. To learn more about GitGuardian, visit https://www.gitguardian.com.

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