DevOps Secrets Discovery

Name	Link	Description	Free/$	Scans
Amazon CodeGuru Reviewer	https://aws.amazon.com/codeguru/	Ensures that your code follows best practices for AWS Key Management Service (AWS KMS), Amazon Elastic Cloud Compute (Amazon EC2), application programming interfaces (APIs), common Java or Python crypto, and TLS (Transport Layer Security)/SSL (Secure Socket Layer) libraries.	$ 90-day trial	Code
Rep-supervisor	https://github.com/auth0/repo-supervisor	detect secrets and passwords in your code	Free	Code
SonarLint	https://www.sonarsource.com/products/sonarlint/	IDE plugin that helps you find & fix bugs and security issues from the moment you start writing code.	Free	Code
SonarQube Secrets plugin	https://github.com/Skyscanner/sonar-secrets	Designed to identify hardcoded secrets in source code, such as passwords, API keys, AWS credentials, tokens, etc	Free	Code
GitGuardian	https://www.gitguardian.com/	Enterprise-grade secrets detection	$	Code/Respositories
yataf (Yet Another Tool for Analysis of Files)	https://github.com/Damian89/yataf	Simple tool to analyze a files/urls content - it was primarily created to analyze the content of a javascript file against a given set of regular expressions. The main goal is to give you an idea if a files content might be of interest. This means that yataf tries to find secrets in the content as well as potential endpoints.	Free	Files
Spectral	https://spectralops.io/	continuously scan and monitor known and unknown assets to stop data breaches before they happen.	$	Multiple
Truffle Hog	https://github.com/trufflesecurity/trufflehog	Find secrets everywhere, including branches, commit history.	Free	Multiple
Horizon3.ai NodeZero	https://www.horizon3.ai/nodezero/	Provides continuous autonomous penetration testing as a true SaaS offering.	$	Pen Testing
Pentera Automated Security Validation	https://pentera.io/use-cases/#password-risk-assessment	Automatically discovers password transmissions and preventing potential attacks.	$	Pen Testing
Git Hound	https://github.com/ezekg/git-hound	helps prevent sensitive data from being committed into a repository by sniffing potential commits against PCRE regular expressions.	Free	Repo Commits
Git-Secrets	https://github.com/awslabs/git-secrets	Scans commits, commit messages, and --no-ff merges to prevent adding secrets into your git repositories.	Free	Repo Commits
GitHub Secrets Scanning	https://docs.github.com/en/code-security/secret-scanning/about-secret-scanning	Scans repositories for known types of secrets, to prevent fraudulent use of secrets that were committed accidentally.	Free	Repositories
Gitrob	https://github.com/michenriksen/gitrob	help find potentially sensitive files pushed to public repositories on Github.	Free	Repositories
GittyLeaks	https://github.com/kootenpv/gittyleaks	Works by trying to find words like 'username', 'password', and 'email' and shortenings in quoted strings, config style or JSON format. It captures the value assigned to it	Free	Repositories
Nightfall	https://try.nightfall.ai/radar	Automatically detect 150+ types of PII, credentials & secrets, including API keys and certificates	$	Repositories
Repo Security Scanner	https://github.com/techjacker/repo-security-scanner	Finds secrets accidentally committed to a git repo, eg passwords, private keys	Free	Repositories
CyberArk CPM Scanner	https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.0/en/Content/PASIMP/Accounts-Feed.htm	The Privileged Access Security solution scans your machines according to the source that was defined, such as Active Directory or a CSV file, to discover privileged accounts in your organization (such as Windows and Unix accounts) and their dependencies (such as Windows Services), giving you a clear and comprehensive picture of existing accounts in your organization.	Included w/ CyberArk License	Servers/Workstations
CyberArk DnA	https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/PrivCloud-Assess-network.htm	Automatically discovers and analyzes any privileged and nonprivileged account within servers and desktops.	Free	Servers/Workstations

Excessive Privilege Detection

Name	Link	Description	Free/$	Scans
CyberArk Kubiscan	https://github.com/cyberark/KubiScan	A tool for scanning Kubernetes cluster for risky permissions in Kubernetes's Role-based access control (RBAC) authorization model.	Free	Kubernetes clusters
CyberArk Cloud Entitlements Manager (CEM)	https://www.cyberark.com/products/cloud-entitlements-manager/	Remove excessive permissions across your cloud footprint.	$	AWS, Azure, GCP IAM & K8s clusters
BoodHound	https://github.com/BloodHoundAD/BloodHound	easily gain a deeper understanding of privilege relationships in an Active Directory or Azure environment.	Free	LDAP/AD
CyberArk zBang	https://github.com/cyberark/zBang	risk assessment tool that detects potential privileged account threats in the scanned network.	Free	LDAP/AD
SkyArk	https://github.com/cyberark/SkyArk	Discover the most privileged entities in the target AWS and Azure.	Free	AWS/Azure