gitleaks

- **Konfiguration (gitleaks.toml)**
  - Regeln (rules)
    - id, description
    - regex, path, tags
    - secretGroup, entropy
  - Keywords
    - Vorfilter für Regex
  - Allowlist (rules.allowlist)
    - Commits, Pfade, Regexe
  - Globale Allowlist
    - Commit-Hashes ignorieren
    - generierte Dateien ausschließen
- **Integration in Workflows**
  - Developer-Workflow
    - Pre-Commit-Hooks lokal
    - Manuelle Scans vor Push
  - CI/CD-Pipelines
    - Scan bei jedem Build
    - Merge-/Pull-Requests blockieren
  - Git-Server-Hooks
    - Pre-Receive-Hooks
    - Zentrale Policy-Erzwingung
- **Einsatzszenarien**
  - Schutz von Cloud-Credentials
    - AWS/Azure/GCP Keys
    - GitHub/GitLab Tokens
  - Audits & Pentests
    - Fremde Repos prüfen
    - Legacy-Code bewerten
  - Open-Source-Freigabe
    - Letzter Check vor Veröffentlichung
  - Regelmäßiges Monitoring
    - Periodische Organisation-Scans
- **Best Practices**
  - Secrets sofort revoken/rotieren
  - Git-Historie bereinigen (BFG o.ä.)
  - Nutzung von Secret-Stores
    - Vault, KMS, Password Manager
  - Entwickler sensibilisieren
    - Schulungen & Coding-Guidelines
- **Grundlagen**
  - SAST-Tool für Secrets
  - Open Source, CLI-basiert
  - Scannt Git-Repos & Verzeichnisse
- **Installation**
  - Paketmanager
    - Debian/Ubuntu
      - apt install gitleaks
    - Fedora/RHEL
      - dnf install gitleaks
  - Manuelles Binary
    - GitHub-Release herunterladen
      - https://github.com/gitleaks/gitleaks/releases
      - nach /usr/local/bin auspacken und verschieben
- **Basis-Nutzung**
  - Aktuelles Repo scannen
    - gitleaks detect .
  - Detailausgabe
    - gitleaks detect -v
  - Ohne Git-Metadaten
    - gitleaks detect ~~no-git~~ source .
  - Verzeichnis Scann
    - in Json Datei
      - gitleaks dir . -f json -r gitleaks-report.json

© 2026 by Kleinhirn.eu