LEGIT SECURITY

Use Case

Detecting and preventing secrets in code

Legit Security automatically scans the SDLC for secrets, delivering code to cloud traceability that lets organizations quickly identify their origin, propagation, criticality, and the exact code where they are being used. This helps prioritize response actions, lowers mean time to resolution, and enables automated guardrails to prevent future violations.

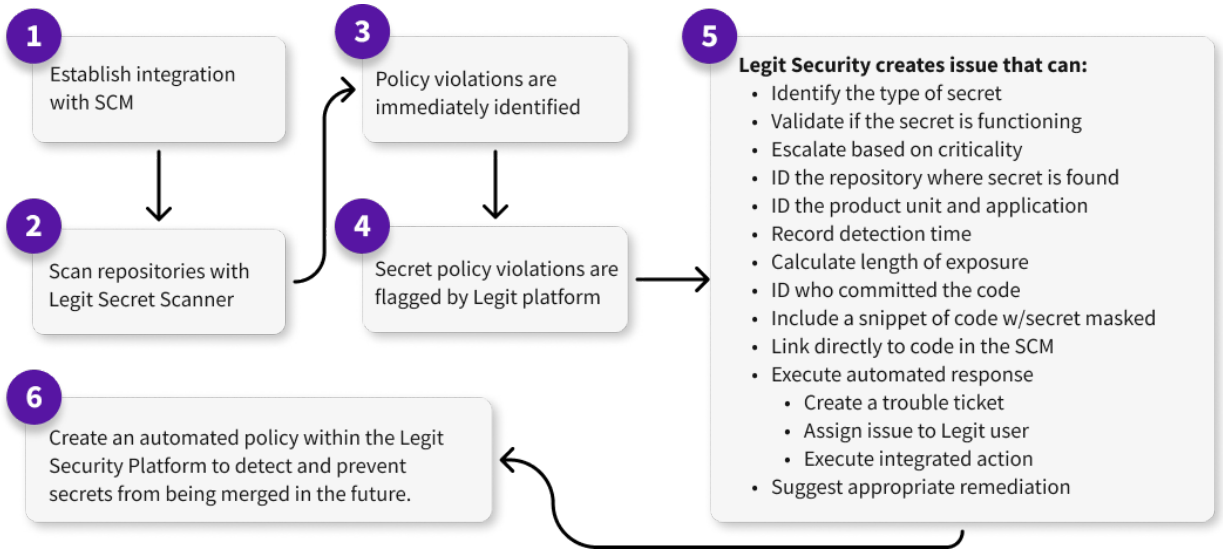
Key Challenges

Secrets in code are common, hard to track down, and exist forever

Secrets in exposed repositories provide access to breaches and lateral movement

Secrets in runtime can be difficult to remove without impacting production applications

Legit Security in Action



Problems Solved

- Automatically scans the SDLC for any secrets in code
- Prioritizes secrets based on criticality to production apps
- Identifies and securely shows specific code where secrets are used
- Track secret propagation to all runtime or pre-prod code
- Identifies which developers are putting secrets into code
- Maps the complete code to cloud journey of individual secrets

<1hr Begin detecting and remediating secrets within minutes of deployment

Automated guardrails for developing secure code to meet compliance requirements

Understand how to remediate secrets without costly interruptions to production

www.legitsecurity.com

www.linkedin.com/company/legitsecurity