ProCheckUp

SpiralGuard

Advanced Credential Discovery & Secret Exposure Detection

Discover. Validate. Remediate.

Multi-repo Scanning
Designed for large, mixed codebases

Context-aware Validation
Reduces scanner noise and false positives

Prioritised Remediation
Actionable rotation and clean-up steps

Credential exposure remains one of the fastest routes from a source code repository to a real-world breach. As development teams grow, repositories multiply, and cloud adoption accelerates, secrets are unintentionally committed to code — and frequently remain there for months or years before discovery. **SpiralGuard** is ProCheckUp's proprietary credential discovery platform engineered to identify exposed secrets across enterprise environments quickly, accurately, and at scale. By combining intelligent pattern recognition, entropy analysis, Hyperdimensional Computing (HD), contextual validation, and LLM-assisted scoring, SpiralGuard helps organisations reduce exposure risk while eliminating the false-positive noise that overwhelms traditional scanners.

WHY CREDENTIAL EXPOSURE MATTERS

- **Unauthorised Cloud Compromise**

Exposed cloud API keys grant attackers direct access to infrastructure, storage, databases, and compute resources — often without triggering standard security alerts.

- **Supply Chain & Lateral Movement**

CI/CD pipeline secrets, service account tokens, and OAuth credentials enable attackers to pivot across systems and compromise build pipelines at scale.

- **Data Breaches & Regulatory Exposure**

Database credentials and connection strings expose customer records, financial data, and personal information — triggering GDPR and wider regulatory obligations.

- **Secrets Persist Longer Than Expected**

In large environments, exposed credentials often remain undetected for months or years — particularly within historical commit histories and legacy repositories.

- **Traditional Tools Miss Modern Secrets**

Low-entropy secrets, custom token formats, and organisation-specific credentials routinely evade standard pattern-matching scanners.

- **Developer Workflows Create Systemic Risk**

Without pre-commit controls or CI/CD scanning, a single developer mistake — hardcoding a secret in a config file — can expose an entire cloud environment.

SPIRALGUARD CAPABILITIES

SpiralGuard employs a three-phase detection architecture designed to identify credential exposure at enterprise scale while minimising unnecessary scan overhead and analyst noise. The platform is built around a recall-first philosophy — no genuine secret is sacrificed for throughput.

Phase 1 Noise Filter & Triage	Phase 2 Structural Peek	Phase 3 Full Credential Scan
Known noise paths (minified assets, binary files, vendor trees) are filtered before scanning. Hyperdimensional Computing-based triage scores remaining files to prioritise high-risk content.	Lightweight structural and token-based inspection analyses file headers, key-name patterns, and token shapes to identify credential candidates before committing to full deep scan.	Regex pattern matching, Shannon entropy analysis, HD n-gram scoring, and LLM-assisted contextual reasoning are applied in combination to confirm genuine credentials with very low false-negative rates.

KEY FEATURES

- **Enterprise Multi-repo Scanning**

Scans across GitHub, GitLab, Azure DevOps, Bitbucket, and internal repositories — including active branches, commit history, and Infrastructure-as-Code templates.

- **AI-assisted Contextual Analysis**

LLM-assisted scoring distinguishes genuine secrets from benign strings by evaluating surrounding code context, variable names, and file type — dramatically reducing false positives.

- **Entropy + Pattern-based Detection**

Combines Shannon entropy analysis with signature-based and behavioural detection to identify both known credential formats and previously unseen secret types.

- **Adaptive Online Learning**

Learns organisation-specific credential patterns and evolving token formats over time, improving accuracy on successive scans without manual rule updates.

- **Risk-based Prioritisation**

Findings are scored by credential type, validation outcome, repository sensitivity, and exposure window — directing analyst effort to the highest-impact issues first.

- **Low False Positive Rate**

Context-aware refinement suppresses benign public material, test fixtures, and sample values, reducing analyst review burden by up to 80% vs. regex-only tools.

- **Drift Detection**

Detects newly emerging credential formats as they appear in the wild, ensuring SpiralGuard remains effective as cloud and SaaS platforms introduce new secret structures.

- **Structured Reporting**

Outputs executive summary, technical finding tables, credential classification analysis, and per-repository audit reports in both human-readable and machine-readable formats.

WHAT WE DETECT

SpiralGuard identifies a comprehensive range of exposed credentials and sensitive authentication material across enterprise codebases:

Cloud Credentials
- AWS Access Keys
- Azure Storage Account Keys
- Azure Client Secrets
- Azure Cosmos DB Keys
- GCP Service Account Keys
- Azure Function Keys

Application Secrets
- Database Passwords
- Connection Strings
- JWT Secrets
- OAuth Tokens
- Refresh Tokens
- Session Secrets

Third-party & API Keys
- GitHub PATs
- Mapbox Tokens
- SendGrid API Keys
- OpenAI API Keys
- Slack Tokens
- Stripe Keys

Cryptographic Material
- SSH Private Keys
- TLS Certificates
- Signing Keys
- Encryption Secrets
- PGP Keys

CI/CD & DevOps
- Azure DevOps PATs
- GitHub Actions Secrets
- Jenkins Credentials
- Terraform State Keys
- Docker Registry Creds

Infrastructure
- SAS Tokens
- SQL Credentials
- MongoDB URIs
- Redis Auth Strings
- Kubernetes Secrets

Identity & Auth
- SAML Certificates
- LDAP Bind Passwords
- Kerberos Keytabs
- API Bearer Tokens
- Basic Auth Headers

Custom Enterprise Tokens
- Internal SSO Secrets
- CRM API Keys
- HR System Credentials
- Financial Platform Keys
- Organisation-specific Formats

OUR ASSESSMENT APPROACH

Every SpiralGuard engagement follows a structured four-stage workflow, tailored to the client's repository estate, development workflow, and risk appetite.

1. Discover

Analyse repositories, commit histories, branches, configuration files, IaC deployments, and CI/CD pipeline artefacts to identify potential credential exposure.

2. Validate

Exposed credentials are validated against live services — where authorised — to determine which secrets remain active and exploitable versus rotated or expired.

3. Prioritise

Findings are reviewed, deduplicated, and risk-ranked by credential type, validation outcome, and repository context, so teams focus on genuine business risk.

4. Remediate

Actionable guidance is provided for credential rotation, revocation, Git history rewriting, Key Vault migration, and long-term pre-commit scanning controls.

DELIVERABLES

- **Executive Summary**
  Business-focused overview of credential exposure risks, confirmed active secrets, and prioritised recommendations — designed for CISOs, CIOs, and senior stakeholders.
- **Credential Inventory**
  Complete listing of identified credentials with type, severity, source file, repository attribution, and validation outcome for every finding.
- **Technical Assessment Report**
  Detailed per-finding analysis including evidence, CVSS severity rating, business impact assessment, and step-by-step remediation guidance.
- **Remediation Action Plan**
  Prioritised rotation schedule, Git history rewrite instructions, Key Vault migration guidance, and pre-commit scanning deployment steps.

BENEFITS

Reduce Breach Risk

Identify credentials that could provide attackers with direct access to cloud platforms, databases, and production infrastructure before they are exploited.

Protect Cloud Environments

Discover exposed AWS, Azure, and GCP credentials — and validate whether they remain active — before threat actors find and abuse them.

Focus on What Matters

SpiralGuard doesn't just find secrets: it determines which are active, so remediation effort is directed at genuine, exploitable risk.

Improve Security Visibility

Gain insight into credential exposure across current repositories, historical commits, branches, and CI/CD pipelines — including accumulated legacy debt.

Support Compliance & Governance

Demonstrate proactive security controls, improve credential management practices, and support GDPR, ISO 27001, and SOC 2 obligations.

Reduce Remediation Cost

The earlier credential exposure is identified, the lower the operational impact of remediation. Proactive scanning is significantly cheaper than incident response.

TYPICAL REMEDIATION GUIDANCE

Finding Type	Immediate Action	Longer-term Control
Cloud / API Key	Revoke or rotate the exposed key immediately and review recent usage logs for unauthorised access.	Migrate secrets to a managed vault (Key Vault, Secrets Manager). Enforce pre-commit scanning.
Azure Client Secret	Delete all existing secrets for the app registration and generate new values. Audit sign-in logs.	Replace hardcoded secrets with Managed Identity + Key Vault references. Train developers on Secret ID vs Value.
Database Credential	Rotate the database password and validate whether external access was possible during the exposure window.	Use least-privilege service accounts, centralised secret storage, and connection string injection at runtime.
Private Key / Hash	Replace all key material immediately and investigate access logs for signs of misuse.	Harden key lifecycle controls, restrict repository access, and add key-file patterns to .gitignore.

ProCheckUp | Service Description

GitHub Secret Exposure Assessment

Identify exposed credentials across your repositories — determine whether they remain active — and reduce the risk of cloud compromise, unauthorised access, and data breach.

THE CHALLENGE ORGANISATIONS FACE

Many organisations manage hundreds or thousands of repositories, millions of lines of source code, multiple development teams, complex cloud environments, and extensive third-party integrations — with limited visibility of historical code exposure.

"How do you know whether sensitive credentials have been exposed, where they are located, and whether they remain active today?"

WHY ORGANISATIONS CHOOSE THIS SERVICE

- **Reduce Unauthorised Access Risk**
  Identify credentials that could provide attackers with direct access to cloud, applications, databases, and infrastructure.
- **Protect Cloud Environments**
  Discover exposed AWS, Azure, and GCP credentials before they are abused by threat actors or automated credential-stuffing tools.
- **Prioritise What Matters**
  We determine which credentials remain active so teams focus remediation on genuine, exploitable risk — not theoretical exposure.
- **Improve Security Visibility**
  Gain insight into credential exposure across current repositories, historical commits, branches, and development pipelines.
- **Support Compliance & Governance**
  Demonstrate proactive security controls and improve credential management practices across the software development lifecycle.
- **Reduce Remediation Costs**
  The earlier credential exposure is identified, the lower the cost and operational impact of remediation.

WHY PROCHECKUP

- **Security Specialists**
  Experienced consultants with expertise in application security, cloud security, offensive security, and credential exposure assessments.
- **Proprietary Technology**
  Powered by SpiralGuard — ProCheckUp's advanced secret discovery and validation platform — not commodity open-source tools.
- **Risk-Focused Reporting**
  Findings are presented in terms of business impact and remediation priorities, not just raw technical data — designed for both technical and executive audiences.
- **Scalable Assessments**
  Suitable for organisations ranging from small development teams to enterprises managing thousands of repositories and complex cloud environments.

Protect Your Credentials Before Attackers Find Them

Discover. Validate. Remediate.

+44 (0)20 7612 7777 | info@procheckup.com | www.procheckup.com