HCP Vault Radar

あらゆるプラットフォーム、クラウド、データセンターなどにわたり、未管理のシークレットを検出して修正

検証

公開されているシークレットをコード、リポジトリ、インフラをまたいで自動で検出および分類することで、シークレットが無秩序に拡散するのを防ぎます。これにより、チームは迅速に修正策を講じ、データ侵害のリスクを軽減することが可能です。

保護

コードベースおよび共同作業ツール全体で検出された、未管理のシークレットに優先順位を付けることで、技術的資産を保護します。この的を絞ったアプローチでは、最も重大な脅威から優先的に対応し、影響の大きい漏洩に集中して取り組めるため、修正作業を合理化して、全体的なセキュリティ態勢を強化できます。

管理

データ漏洩を回避してガバナンスを強化します。Radar は開発ワークフローに直接組み込むことができるため、セキュリティポリシーを適用して、シークレットが本番環境に到達するのを阻止します。これにより、ソフトウェア開発のライフサイクル全体で規制コンプライアンスに対応し、リスクを軽減することができます。

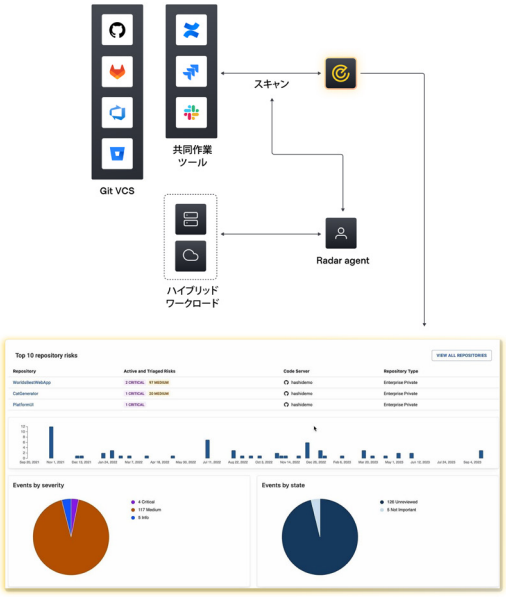
未管理のシークレットの検出

環境全体にわたり、未管理のシークレットを検出して優先順位を付けます。

SaaS 環境を継続的にスキャンして、セキュリティ上の問題に発展する前に、露呈した状態のシークレットを**検出します**。

セキュリティチームは開発サイクルの早い段階でリスクを特定することで、**迅速な対応を取ることができます**。

脆弱性が悪用される前に修正策を講じることができるため、漏洩の可能性が**軽減されます**。

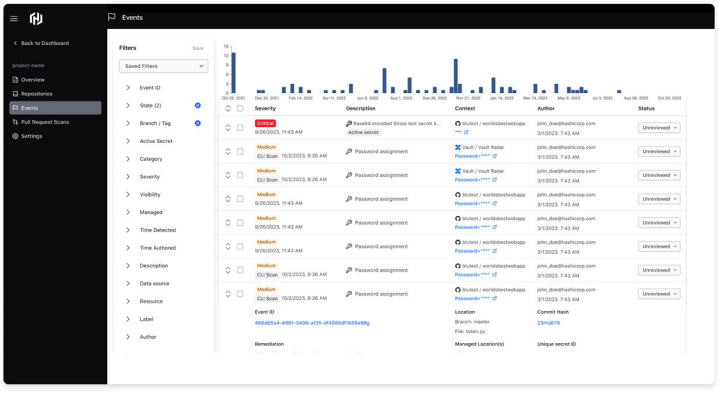


リスクの優先順位付け

シークレットの使用状況チェックに基づいて、重大度を**割り当てます**。

AWS のキーや GitHub のトークンといった特定のクレデンシャルに対して、使用状況チェックを**実行します**。

検出されたシークレットと Vault のデータの**相関付けを行い**、本番環境における関連性やリスクを評価します。



シークレットの漏洩を回避

pull リクエストのチェックを組み込み、コードがマージまたはプッシュされる前に Vault Radar でシークレットを検出可能にすることで、シークレットの漏洩を回避できます。このプロアクティブなアプローチにより、クレデンシャルが露呈した状態でコードベースに登録されるのを未然に防げます。

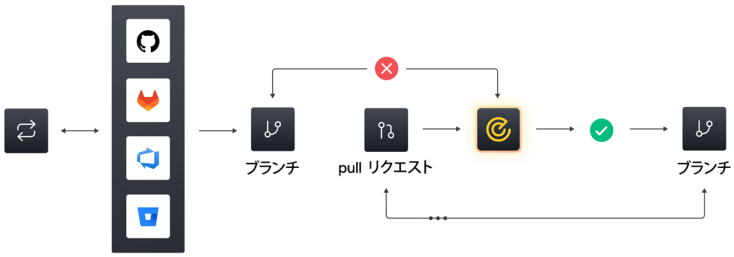
pre-commit Webhook:

- コードの変更点をコミット前に**傍受して**、ハードコードされたシークレットや未管理のクレデンシャルを検出
- リスクの高いコミットをリアルタイムで**阻止して**、機密データがコードベースに登録されるのを回避

pre-receive Webhook:

- 露呈した状態にあるクレデンシャルを伴うリスクの高いコミットが、共有ブランチに対して実行されるのを**阻止**
- 露呈した状態のシークレットを開発ワークフローの最後の砦で食い止めることで、インシデント対策を**強化**

CI/CD パイプライン前



CI/CD パイプライン内

対応すべきアクションを提示

シークレットのタイプに応じた修正ガイダンスが見つかることで、漏洩を速やかに解決しやすくなります。

- シークレットのタイプに応じた具体的で実践的な**修正ガイダンスを提供**
- チームは漏洩の状況ごとに一貫して適切な**対策が可能**
- 修正プロセスでの推測をなくすことで、対応にかかる**時間を短縮**

Vault との相関付けにより、漏洩している利用可能なシークレットを特定

相関付け機能を使用して、検出されたシークレットと Vault に保管されているシークレットを照合することで、露呈した状態にあるシークレットのうち、有効であり、利用されているものの特定につながります。Radar は、利用可能でありながら未管理のこうしたシークレットを明確にして、機密データに対する最も重大な脅威を浮き彫りにします。

- 露呈した状態にあるクレデンシャルが積極的に利用されているかを**判定し**、該当する場合にリスクレベルを高める
- 安全に管理するために、Vault に移行するべき未管理のシークレットを**明示**
- 本番システムや機密データと紐付いている有効なシークレットを明ら**か**にして、修正作業に**優先順位を付ける**