GitHub Repository Best Practices

Guidelines and standard procedures for managing GitHub repositories securely and consistently, including access control, code hygiene, secret handling, branch management, pull request practices, and security alert remediation.

GitHub Secret Scanning Alert Remediation

Purpose

This SOP is to guide the team on how to review, remediate, and close GitHub secret scanning alerts raised for committed secrets such as passwords, tokens, keys, or connection strings.

Steps to Follow

1. **Go to the GitHub repository**
   - Open the impacted repository where the secret scanning alert has been raised.
2. **Open Security section**
   - Navigate to **Security** from the repository menu.
   - Go to **Security & Quality** if applicable.
3. **Open Secret Scanning**
   - Select **Secret Scanning**.
   - Filter or open the **Generic** view to see open generic secret findings.
4. **Review the exposed secrets**
   - Check all password/secret alerts listed.
   - Identify the impacted file, commit, secret type, and owner/team responsible.
5. **Rotate or validate the secret**
   - If the secret is active, rotate/revoke it from the actual source system.
   - Store the new value only in a secure location, such as **Azure Key Vault**, deployment environment variables, or secure pipeline variables.
   - Do not recommit the new secret in code.
   - Keep screenshot/evidence of rotation or revocation for audit proof.
   - If the secret is already expired or not valid, document the explanation clearly with supporting proof.
6. **Close the secret scanning alert**
   - Once remediation is complete, close the alert with the correct reason.
   - Add a clear comment mentioning the action taken, such as rotated, revoked, expired, or no longer valid.
   - Avoid unsupported closure reasons unless approved by the security team.
7. **Update the GitHub issue**

- Go to the **Issues** tab.
- Open the security issue created for the repository.
- Add a resolution comment with the remediation summary and evidence reference.
- Close the issue after all listed alerts are addressed.

8. **Submit EY security attestation form**
   - Fill the EY security form to register the finding as resolved: FORM

Important Notes

- Secrets must never be committed to code.
- Use **Key Vault**, environment variables, or secure CI/CD secret stores for all sensitive values.
- Rotation/revocation proof must be retained before closing the alert.
- If a secret is historic, inactive, or test-only, provide a proper explanation and evidence before closure.