

WIZ

Version Control DFIR

Detection & forensic reference for Version Control Systems (VCS) - Log coverage and scope, incident readiness and relevant audit events across GitHub, GitLab, Bitbucket and Azure DevOps

Log Telemetry & Architecture

Log Scope and Availability method	Audit Logs Scope	Git Events (Read Only)	Git Events (Write)	Git tree	CI/CD Logs	Integration Logs	Application access logs (API requests)	Cloud vs Self Hosted
 GitHub	Enterprise - Available via UI, API and Streaming / Organization - Available via UI and API / Repository - included under organization / CI/CD - included under organization	Repository - Available via UI export, API and Streaming, retained for 7 days	Repository - Available via UI export, API and Streaming	Code - Available via CLI and API	Workflow Run and Job - Available via Actions UI, API and downloadable zip	Webhooks & GitHub Apps - Available via UI and API / Organization and Repository - Available via UI and API	Included with Enterprise License and log streaming	Self hosted additional System Logs include system-level events, application logs, and data about Git events.
 GitLab	Group and Project - Available via UI and API	Top-Level Group - Available via Streaming	Top-Level Group - Available via Streaming	Code - Available via Repositories API	Pipeline and Job - Available via CI/CD UI and API	Webhooks - Project and Group - Available in the UI	Not Supported	Self hosted additional local log files include application, API and integration logs.
 BitBucket	Enterprise - Requires Atlassian Guard and available via UI, API and streaming / Workspace and Repository - Available in the UI	Not Supported	Repository - Available if a webhook is preconfigured	Code - Available via Commits API	Pipeline run - Available if a webhook is preconfigured / Pipeline result logs - Pipelines UI and API	Webhooks - Available in the UI. For Atlassian Guard Premium Available via API and Streaming (Organization Audit Log).	Not Supported	Audit Log Events differ significantly between cloud and self hosted. / Self hosted additional local log files include application access logs, search logs and Git events information. / Self hosted does not have built in CI/CD capabilities.
 Azure DevOps	Organization - Available via UI, API and Streaming	Not Supported	Not Supported	Code - Available via Git Tree API	Pipelines - Available via Pipelines UI and API	Service Hooks - Availabe via History and Notifications API	Not Supported	Self hosted does not include native Audit Log features, server logs require preconfiguration.

Incident Readiness

GITHUB	GITLAB	BITBUCKET	AZURE DEVOPS
☐ Enable source IP disclosure ☐ Enable "Vigilant Mode" to flag unsigned commits as unverified ☐ Enterprise Enable API Request events ☐ Enterprise Stream audit logs	☐ Configure webhooks to log "Merge Requests" and "Push Events" directly to a SIEM ☐ Ultimate Set up audit event streaming for instances (which includes "repository_git_operation")	☐ Link the workspace to Atlassian Guard Premium and stream audit logs to a SIEM ☐ Configure webhooks to log "Push Events" directly to a SIEM	☐ Connect your organization to Microsoft Entra ID. ☐ Turn on "Log Audit Events" ☐ Configure a stream to Azure Monitor ☐ Configure a Service Hook to log "Push Events" directly to a SIEM

Attack Detection & Forensics Matrix

Platform & Tactic		Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
Goal		Breach the organization tenant	Run malicious code in CI/CD	Establish permanent backdoors	Gain administrative control	Blind security/incident response	Harvest secrets or cloud keys	Map out internal landscape	Pivot to cloud or other systems	Steal intellectual property/logs/secret access	Disrupt or sabotage software
Forensic Indicator		Anomalous geographic logins, shadow third-party integrations, invitations to untrusted domains	Workflows triggered from unverified forks or untrusted IPs	New deploy keys on sensitive repps, unexpected integration installations, webhooks pointing to external domains, tokens granted to unfamiliar accounts	Unexpected elevation to organization owner, overriding branch protection requirements	Lowering authentication barriers, marking active leaks as resolved, dropping branch protections, deleting logs	Secret scanning alerts on active credentials, users bypassing push protection, overwriting production pipeline secrets, secrets provided to unexpected workflow job	Script-driven API enumeration	Forking private repositories, allow private repository forks, tokens assuming broad roles	Bulk git read events (clone/download), audit log exports by unexpected users	Uploading malicious code, publishing malicious packages, Purging resources, removing integrations, deleting security rules
 GitHub	Enterprise Cloud	<code>oauth_application.create</code> <code>integration_installation.create</code> <code>org_invite_member</code>	<code>workflows.*</code>	<code>public_key.create</code> <code>personal_access_token.access_granted</code> <code>integration_installation.create</code> <code>oauth_application.create</code> <code>org_invite_member</code> <code>ip_allow_list.entry.*</code>	<code>org.update_member</code> <code>team.add_repository</code> <code>team.update_repository_permission</code> <code>repo.update_member</code> <code>protected_branch.policy_override</code> <code>personal_access_token.auto_approve.*</code>	<code>org.disable_saml</code> <code>org.disable_two_factor_requirement</code> <code>secret_scanning.alert.resolve</code> <code>protected_branch.destroy</code> <code>workflows.delete_workflow_run</code> <code>ip_allow_list.disable</code> <code>audit_log_streaming.destroy</code> <code>dependabot.alerts.disable</code> <code>environment.remove_protection_rule</code>	<code>secret_scanning.alert.create</code> <code>secret_scanning.push_protection.bypass</code> <code>recovery_codes.viewed</code>	<code>api.request</code> <code>business.security_center.export.risk</code>	<code>private_repository.forking.enable?</code> <code>integration_installation.repositories_added</code> <code>org.add_outside_collaborator</code>	<code>git.clone</code> <code>repo.download.zip</code> <code>*.audit_log.export</code>	<code>packages.package_published</code> <code>packages.package_version_published</code> <code>repo.access</code> <code>repo.destroy</code> <code>org.delete</code> <code>team.destroy</code> <code>integration_installation.destroy</code> <code>protected_branch.destroy</code> <code>git.push</code>
	Enterprise Server										
 GitLab	GitLab.com	<code>personal_access_token.used_from_unseen_ip</code> <code>user_signed_in_from_unseen_ip</code> <code>login_failed_with.*</code>	<code>ci_runner.created</code> <code>ci_runner.registered</code>	<code>add_gpg_key</code> <code>add_ssh_key</code> <code>member.created</code> <code>ip_restrictions_changed</code> <code>project_access_token.created</code> <code>user_email_changed_and_user_signed_in</code> <code>user_access_unlocked</code> <code>unlock_user</code> <code>user.created</code> <code>deploy_token.created</code> <code>ci_variable.created</code>	<code>member.role.created</code> <code>member.role.updated</code> <code>member.updated</code> <code>user.enable_admin_mode</code> <code>user impersonation</code> <code>user_external_status.updated</code>	<code>webhook.destroyed</code> <code>member.destroyed</code> <code>user.destroyed</code> <code>user.disable.*</code> <code>audit_events_streaming.*</code> <code>amazon_s3_configuration.*</code> <code>destroy.event_streaming.destination</code> <code>delete_status_check</code> <code>protected_branch.allow_force_push.updated</code> <code>group.require_two_factor_authentication.updated</code> <code>disable_personal_access_tokens.updated</code> <code>disable_ssh_keys.updated</code>	<code>variable.viewed_api</code> <code>secrets_manager.read.*</code> <code>user.authorized_oauth_application</code> <code>password.reset.requested</code>	<code>repository.file.accessed_api</code> <code>group.ci_cd_settings.accessed</code>	<code>project.fork.operation</code> <code>user.authenticated_using_job_token</code> <code>set_runner_associated_projects</code>	<code>repository.git.operation</code> <code>repository.download.operation</code> <code>job.artifact.download</code> <code>project.export.file.download.started</code> <code>group.visibility.level.updated</code> <code>project.visibility.level.updated</code> <code>direct_transfer_relation.export.downloaded</code>	<code>deployment.started</code> <code>deployment.approved</code> <code>package_registry.package_deleted</code> <code>project.destroyed</code> <code>organization.hard_deleted</code> <code>organization.soft_deleted</code>
	Self Managed										
	Dedicated										
 BitBucket	Cloud	<code>User accepted invite to workspace</code> <code>User account access granted to an application</code>		<code>User added to workspace</code> <code>Project Access key added</code> <code>Repository Access key added</code> <code>SSH key added</code> <code>Security key added</code> <code>App password added</code> <code>Webhook added</code>	<code>Branch restrictions removed</code> <code>Branch restrictions updated</code> <code>User added to group</code> <code>User access to project changed</code> <code>User access to repository changed</code> <code>Branch write access changed</code> <code>Group * access permissions changed</code>	<code>Workspace 2SV requirement disabled</code> <code>Slack notification rule removed</code> <code>2SV disabled</code> <code>Security key removed</code> <code>Workspace IP allowlisting disabled</code> <code>Workspace IP allowlisted addresses changed</code> <code>App password removed</code>	<code>Recovery codes viewed</code>			<code>Workspace privacy changed</code> <code>Repository transferred from workspace</code> <code>Project privacy changed</code> <code>Repository privacy changed</code>	
	Data Center	<code>AuthenticationSuccessfulEvent</code> <code>SshAuthenticationSuccessfulEvent</code> <code>ApplicationSetupEvent</code> <code>UserExportSucceededEvent</code>	<code>HookScript*</code> <code>RepositoryHookEnabledEvent</code> <code>RepositoryHookEvent</code> <code>AnalyticalActionRunEvent</code>	<code>GpgkeyCreatedEvent</code> <code>SshkeyCreatedEvent</code> <code>AccessTokenCreatedEvent</code> <code>SshAccessKeyGrantedEvent</code> <code>UserCreatedEvent</code> <code>UserCredentialUpdatedEvent</code> <code>InternalProjectWebhookCreatedEvent</code> <code>InternalRepositoryWebhookCreatedEvent</code>	<code>GroupMembershipsCreatedEvent</code> <code>*PermissionModifiedEvent</code> <code>*PermissionGrantedEvent</code>	<code>ServerEmailAddressChangeEvent</code> <code>MailHostConfigurationChangedEvent</code> <code>HookScriptDeletedEvent</code> <code>UserCreatedEvent</code> <code>UserDeletedEvent</code> <code>LoggingSettingsDisabledEvent</code>	<code>CodeSearchSuccessfulEvent</code> <code>RepositoriesSearchSuccessfulEvent</code> <code>RepositoryAccessedEvent</code> <code>UserExportStartedEvent</code>			<code>RepositoryCloneEvent</code> <code>RepositoryPullEvent</code> <code>MirrorInstalledEvent</code> <code>Full data export triggered</code> <code>RepositoryForkedEvent</code>	<code>RepositoryPushEvent</code> <code>RepositoryOtherWriteEvent</code> <code>RepositoryDeletedEvent</code> <code>ProjectDeletedEvent</code>
 Azure DevOps	Services	<code>Token.PatPublicDiscoveryEvent</code> <code>Extension.Installed</code> <code>Extension.VersionUpdated</code> <code>Library.ServiceConnectionCreated</code> <code>ServiceHooks.SubscriptionCreated</code>	<code>Pipelines.PipelineCreated</code> <code>Pipelines.VariablesSetAtRuntime</code> <code>Pipelines.PipelineModified</code>	<code>Token.PatCreateEvent</code> <code>Token.SshCreateEvent</code> <code>Group.UpdateGroupMembership.Add</code> <code>Extension.Installed</code>	<code>Artifacts.Feed.Project.Modify.Permissions</code> <code>Git.RefUpdatePoliciesBypassed</code> <code>Group.UpdateGroupMembership.Add</code> <code>Organization.Update.Owner</code> <code>OrganizationPolicy.EnforcePolicyRemoved</code> <code>Policy.PolicyConfigRemoved</code> <code>Security.ModifyAccessControlLists</code>	<code>AuditLog.StreamDeleted</code> <code>AuditLog.StreamDisabledByUser</code> <code>CheckConfiguration.Disabled</code> <code>CheckConfiguration.Deleted</code>	<code>AuditLog.StreamRead</code> <code>AuditLog.AccessLog</code>	<code>Library.ServiceConnectionExecuted</code> <code>Library.ServiceConnectionShared*</code>	<code>Git.RepositoryForked</code>	<code>Pipelines.DeploymentJobCompleted</code> <code>Release.DeploymentsCompleted</code> <code>Release.DeploymentCompleted</code> <code>Release.ReleaseCreated</code> <code>Project.UpdateVisibilityCompleted</code> <code>Git.RepositoryDeleted</code> <code>Git.RepositoryDestroyed</code> <code>Project.DeleteCompleted</code>	

¹ Not including GitHub Enterprise Managed Users security logs ² Not available in GitHub Enterprise Server audit logs