Programmatic and Excessive Access to Confluence Documentation, Detection Strategy DET0358

Archived: 2026-04-02 11:40:42 UTC

AN1019

Detection of excessive or programmatic access to Confluence spaces or pages, particularly by privileged users, through a combination of access logs, API usage, and identity context. Correlates logon sessions, user roles, and abnormal document viewing or export behavior. Identifies burst access patterns and tools/scripts abusing the Confluence API for mass enumeration or data scraping.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the time span (e.g., 5m, 1h) in which excessive access behavior becomes suspicious.
UserContext	Privileged user roles (e.g., domain admins) should be excluded or flagged if found accessing documentation repositories.
AccessThreshold	The number of pages viewed or exported by a single user before triggering detection logic.
AgentFilter	User agent strings that may indicate scripted, automated, or non-interactive access methods.
