Detection of Data from Information Repositories, Detection Strategy DET0754

Archived: 2026-04-05 15:49:54 UTC

AN1886

Monitor for newly constructed logon behavior within Microsoft's SharePoint can be configured to report access to certain pages and documents.[1] Sharepoint audit logging can also be configured to report when a user shares a resource.[2] The user access logging within Atlassian's Confluence can also be configured to report access to certain pages and documents through AccessLogFilter.[3] Additional log storage and analysis infrastructure will likely be required for more robust detection capabilities.
In the case of detecting collection from shared network drives monitor for unexpected and abnormal accesses to network shares.
Monitor for third-party application logging, messaging, and/or other artifacts that may leverage information repositories to mine valuable information. Information repositories generally have a considerably large user base, detection of malicious use can be non-trivial. At minimum, access to information repositories performed by privileged users (for example, Active Directory Domain, Enterprise, or Schema Administrators) should be closely monitored and alerted upon, as these types of accounts should generally not be used to access information repositories. If the capability exists, it may be of value to monitor and alert on users that are retrieving and viewing a large number of documents and pages; this behavior may be indicative of programmatic means being used to retrieve all data within the repository. In environments with high-maturity, it may be possible to leverage User-Behavioral Analytics (UBA) platforms to detect and alert on user-based anomalies.

Log Sources