Detect disabled Windows event logging, Detection Strategy DET0187

Archived: 2026-04-05 14:27:29 UTC

AN0535

Detection of attempts to disable or tamper with Windows Event Logging. This includes stopping or disabling the EventLog service, modifying registry keys related to EventLog and Autologger, using `auditpol` or `wevtutil` to disable categories or clear audit policies, and detecting suspicious gaps or resets in event logs. Defenders observe registry changes, service state changes, process execution of disabling commands, and anomalies in event record sequences.

Log Sources

Mutable Elements

Field	Description
AuthorizedAdminAccounts	List of accounts authorized to legitimately modify audit policies or disable services.
TimeWindow	Correlation window between registry modification, service stop, and audit policy commands.
ServiceNames	Customizable set of monitored services such as EventLog, Sysmon, or custom loggers.
