Email Forwarding Rule Abuse Detection Across Platforms, Detection Strategy DET0576

Archived: 2026-04-05 18:04:57 UTC

AN1589

Creation of inbox rules via PowerShell (New-InboxRule) or transport rules using Exchange cmdlets. Correlates user behavior, cmdlet usage, and rule properties.

Log Sources

Mutable Elements

Field	Description
UserContext	Certain service accounts or admin contexts may be expected to run these rules.
TimeWindow	Correlate between rule creation and follow-on message forwarding within this timeframe.
TargetMailbox	Whitelisted or trusted destination addresses may be tuned per org policy.

AN1590

Creation or modification of Apple Mail rules by accessing plist files or GUI automation (AppleScript).

Log Sources

Mutable Elements

Field	Description
RuleFilePath	Different Mail versions store rules in slightly different locations.
ScriptTrigger	AppleScript usage for GUI automation may be common in automation workflows.

AN1591

Creation of email forwarding/redirect rules in Exchange Online via New-InboxRule or transport rule cmdlets, including auto-forwarding address field usage.

Log Sources

Mutable Elements

Field	Description
ForwardingSMTPAddress	Destination domain may vary; commonly tuned per org policies.
ActorId	Differentiate service/admin users vs standard user population.

AN1592

Modification of Thunderbird message filters file or execution of CLI tools (e.g., formail/procmail) that alter .forward behavior.

Log Sources

Mutable Elements

Field	Description
.forwardPath	User-based home directories; tune for specific user patterns.
ExecContext	Expected email client behavior may trigger similar file edits.
