Detection Strategy for Addition of Email Delegate Permissions, Detection Strategy DET0373

Archived: 2026-04-05 17:00:23 UTC

AN1051

Detection of anomalous or unauthorized mailbox delegation activity (e.g., Add-MailboxPermission, Default/Anonymous mailbox permissions, Gmail delegation setup).

Log Sources

Mutable Elements

Field	Description
DelegatePermissionLevel	Threshold for unexpected delegate roles such as FullAccess or SendAs.
FolderTargetScope	Mailbox folder targeted by delegation (Inbox, Root, Calendar, etc.).
DelegatorToDelegatePairing	Pairings of delegate and delegator users that are expected.
MailflowAnomalyThreshold	Spike in outbound mail after delegate addition, used to catch phishing or mass exfil.

AN1052

Execution of PowerShell commands that modify mailbox permissions using Exchange cmdlets (e.g., Add-MailboxPermission), often tied to BEC or post-compromise persistence.

Log Sources

Mutable Elements

Field	Description
PowerShellCmdletFilter	Exchange cmdlets to include or exclude based on scope (e.g., Add-MailboxPermission, Set-MailboxFolderPermission).
ExecutionParent	Flag suspicious script or interactive shell launch by non-admins.
TimeWindow	Window in which Add-MailboxPermission is followed by anomalous usage (e.g., SendAs events).

Source: https://attack.mitre.org/detectionstrategies/DET0373#AN1052