Detection Strategy for Impersonation, Detection Strategy DET0286

Archived: 2026-04-02 10:37:25 UTC

AN0792

Monitor for anomalous email activity originating from Windows-hosted applications (e.g., Outlook) where the sending account name or display name does not match the underlying SMTP address. Detect abnormal volume of outbound messages containing sensitive keywords (e.g., 'payment', 'wire transfer') or anomalous login locations for accounts associated with email sending activity.

Log Sources

Mutable Elements

Field	Description
KeywordList	Adjust impersonation detection keywords based on local business risk terms (e.g., 'ACH', 'Invoice').
GeoLocationBaseline	Define trusted geographic regions for normal user email activity.

AN0793

Monitor mail server logs (Postfix, Sendmail, Exim) for anomalous From headers mismatching authenticated SMTP identities. Detect abnormal relay attempts, spoofed envelope-from values, or large-scale outbound campaigns targeting internal users.

Log Sources

Mutable Elements

Field	Description
KnownRelayHosts	Filter trusted relays or automated notification systems from impersonation alerts.

AN0794

Monitor Mail.app activity or unified logs for anomalous SMTP usage, including mismatches between display name and authenticated AppleID or Exchange credentials. Detect use of third-party mail utilities that attempt to send on behalf of corporate identities.

Log Sources

Mutable Elements

Field	Description
TrustedMailClients	Allowlist known third-party clients used for legitimate email activity.

AN0795

Monitor SaaS mail platforms (Google Workspace, M365, Okta-integrated apps) for SendAs/SendOnBehalfOf operations where the delegated permissions are unusual or newly granted. Detect impersonation attempts where adversaries configure rules to auto-forward or auto-reply with impersonated content.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	gcp:workspaceaudit	SendAs: Outbound messages with alias identities that differ from primary account

Mutable Elements

Field	Description
DelegationBaseline	Maintain baseline of normal SendAs/SendOnBehalf relationships to reduce false positives.

AN0796

Monitor Office Suite applications (Outlook, Word mail merge, Excel macros) for abnormal automated message sending, especially when macros or scripts trigger email delivery. Detect patterns of impersonation language (urgent, payment, executive request) combined with anomalous execution of Office macros.

Log Sources

Mutable Elements

Field	Description
MacroExecutionThreshold	Threshold for correlating macro execution with email sending activity.
