Detection Strategy for Email Spoofing, Detection Strategy DET0431

Archived: 2026-04-05 17:56:59 UTC

AN1202

Monitor email message traces and headers for failed SPF, DKIM, or DMARC checks indicating spoofed sender identities. Correlate abnormal sender domains or mismatched return-paths with elevated spoofing likelihood.

Log Sources

Mutable Elements

Field	Description
SpoofScoreThreshold	Defines sensitivity to SPF/DKIM/DMARC failures; higher thresholds reduce false positives but may miss stealthier spoofing.
MonitoredDomains	Specifies which domains to enforce strict validation against; enterprise-specific tuning may be required.

AN1203

Detects spoofed emails by analyzing mail server logs (e.g., Postfix, Sendmail) for mismatched header fields, failed SPF/DKIM checks, and anomalies in SMTP proxy logs. Defender observes discrepancies between sending domain, return-path domain, and message metadata.

Log Sources

Mutable Elements

Field	Description
SenderDomainWhitelist	Defines approved sender domains to suppress alerts for expected mismatches, reducing false positives.
TimeWindow	Sets correlation period for repeated spoofing attempts to flag campaigns vs. isolated misconfigurations.

AN1204

Detects suspicious inbound mail traffic where SPF/DKIM/DMARC authentication fails or where sender and return-path domains mismatch, observable in Apple Mail unified logs or MDM-controlled logging pipelines.

Log Sources

Mutable Elements

Field	Description
RecipientSensitivity	Allows tuning based on which users (e.g., executives, finance staff) receive stricter spoofing detection policies.
HeaderMismatchTolerance	Defines tolerance for minor discrepancies in domain alignment, balancing detection with usability.

AN1205

Correlates Office 365 or Google Workspace audit logs for spoofed sender addresses, failed email authentication, and anomalies in message delivery metadata. Defender observes failed SPF/DKIM checks and domain mismatches tied to suspicious campaigns.

Log Sources

Mutable Elements

Field	Description
MessageVolumeThreshold	Defines thresholds for spoofed messages volume before alerts trigger, reducing noise for isolated misconfigs.
TargetedUserGroups	Restricts higher-sensitivity detection to high-value groups (executives, admins, finance) for efficiency.
