Detect abuse of Trusted Relationships (third-party and delegated admin access), Detection Strategy DET0488

Archived: 2026-04-05 14:24:26 UTC

AN1344

Behavioral chain: (1) a login from a third-party account or untrusted source network establishes an interactive/remote session; (2) the session acquires elevated privileges or accesses sensitive resources atypical for that account; (3) subsequent lateral movement or data access occurs from the same session/device. Correlate Windows logon events, token elevation/privileged use, and resource access with third-party context.

Log Sources

Mutable Elements

Field	Description
ThirdPartyCIDRs	Ranges used by MSPs/contractors/VPN egress; used to enrich logons and network flows.
ExpectedAdminHosts	Servers where third-party admins are allowed; deviations raise risk.
TimeWindow	Correlation window linking logon → elevation → access (e.g., 30–120 minutes).
HighValueResources	File shares/AD objects/servers that should never be touched by third-party sessions.

AN1345

Behavioral chain: (1) sshd or federated SSO logins from third-party networks or identities; (2) rapid sudo/su privilege elevation; (3) access to sensitive paths or east-west SSH. Correlate auth logs, process execution, and network flows.

Log Sources

Mutable Elements

Field	Description
ThirdPartyUsers	POSIX accounts assigned to vendors/partners.
AllowedJumpHosts	Bastion hosts permitted for third-party access.
MFAExpected	Flag indicating whether PAM/MFA should be present; used to score risk.

AN1346

Behavioral chain: (1) third-party interactive login or mobileconfig-based device enrollment; (2) privilege use or admin group change; (3) lateral movement mounts/ssh. Correlate unified logs and network telemetry.

Log Sources

Mutable Elements

Field	Description
ManagedDeviceList	Known corp devices; treat unknown devices as higher risk.

AN1347

Behavioral chain: (1) delegated admin or external identity establishes session (e.g., partner/reseller DAP, B2B guest, SAML/OAuth trust); (2) role elevation or app consent/permission grant; (3) downstream privileged actions in the tenant. Correlate IdP sign-in, admin/role assignment, and consent/admin-on-behalf events.

Log Sources

Mutable Elements

Field	Description
TrustedPartnerTenantIDs	Tenant IDs of approved partners; any others are suspicious.
RequiredMFA	Require MFA for partner sessions; alert on bypass or step-up failure.
RoleScopeAllowList	Roles third-parties may hold (e.g., Helpdesk Admin); flag broader scopes.

AN1348

Behavioral chain: (1) cross-account or third-party principal assumes a role into the tenant/subscription/project; (2) privileged API calls are made in short succession; (3) access originates from unfamiliar networks or geos. Correlate assume-role/federation events with sensitive API usage.

Log Sources

Mutable Elements

Field	Description
ExternalAccountAllowList	Cross-account principals permitted to assume roles; used for allow-listing.
SensitiveAPIs	Provider-specific list of risky APIs for scoring.

Field	Description
GeoVelocityThreshold	Detect impossible travel between partner and tenant actions.

AN1349

Behavioral chain: (1) third-party app or admin connects via OAuth/marketplace install; (2) high-privilege scopes granted; (3) anomalous actions (mass read/exports, admin changes).

Log Sources

Mutable Elements

Field	Description
ApprovedApps	Catalog of sanctioned third-party apps and scopes.
ExportVolumeThreshold	Data export size/rate baselines to detect abnormal partner activity.

AN1350

Behavioral chain: (1) delegated administration offers/relationships created or modified by partner tenants; (2) mailbox delegation/impersonation enabled; (3) follow-on access from partner IPs.

Log Sources

Mutable Elements

Field	Description
MailboxDelegateAllowList	Specific mailboxes third-parties may manage.
