Detection of Valid Account Abuse Across Platforms, Detection Strategy DET0560

Archived: 2026-04-05 14:13:09 UTC

AN1543

Detection of compromised or misused valid accounts via anomalous logon patterns, abnormal logon types, and inconsistent geographic or time-based activity across Windows endpoints.

Log Sources

Mutable Elements

Field	Description
LogonType	Flag unexpected logon types (e.g., Type 10 for remote interactive logins) for sensitive accounts.
TimeWindow	Define acceptable hours for interactive logon activity (e.g., 9AM-6PM local).
GeoIPMismatch	Trigger on location anomalies based on prior user behavior or policy.

AN1544

Detection of valid account misuse through SSH logins, sudo/su abuse, and service account anomalies outside expected patterns.

Log Sources

Mutable Elements

Field	Description
UserContext	Identify logins to root or sudoers not aligned with normal usage profiles.
HostDensityThreshold	Number of unique systems a user authenticates to in a time window.
LoginMethod	Trigger on rarely used access methods such as password instead of SSH key.

AN1545

Detection of interactive and remote logins by service accounts or users at unusual times, with unexpected child process activity.

Log Sources

Mutable Elements

Field	Description
LoginOrigin	Login sourced from unexpected remote addresses.
ProcessTreeDepth	Track execution depth or anomalous chains post-login.

AN1546

Detection of valid account abuse in IdP logs via geographic anomalies, impossible travel, risky sign-ins, and multiple MFA attempts or failures.

Log Sources

Mutable Elements

Field	Description
MFAFailureCount	Threshold of failed MFA attempts before alerting.
RiskScoreThreshold	Custom threshold based on calculated identity risk.
IPGeoVelocity	Detect impossible travel (logins from two distant geolocations within short time).

AN1547

Detection of containerized service accounts or compromised kubeconfigs being used for cluster access from unexpected nodes or IPs.

Log Sources

Mutable Elements

Field	Description
ServiceAccountScope	Validate access from expected namespaces only.
ClusterIPWhitelist	Permit kubeconfig usage from a limited set of IPs.
