Detection of Default Account Abuse Across Platforms, Detection Strategy DET0465

Archived: 2026-04-05 16:23:15 UTC

AN1283

Detection of default account usage such as Guest or Administrator performing interactive or remote logons on systems outside of installation or maintenance windows.

Log Sources

Mutable Elements

Field	Description
UserContext	Default usernames like 'Administrator' or 'Guest' may be renamed or disabled by the organization. Detection logic should account for name changes.
TimeWindow	Restrict detection to unusual hours or outside of expected maintenance windows.

AN1284

Monitoring for SSH logins from default accounts such as 'root', especially when login is via password and not key-based authentication.

Log Sources

Mutable Elements

Field	Description
SSHMethod	Environments using passwordless SSH should not have password logins enabled for root or other default accounts.
RemoteIPWhitelist	Logins from jump boxes may be whitelisted depending on environment policies.

AN1285

Use of known default service accounts or root-level cloud accounts performing authentication or changes to IAM policy.

Log Sources

Mutable Elements

Field	Description
AccountList	Organizations may rename or rotate default IAM accounts; detection logic should be updated with any renamed or aliased default identities.
GeoLocation	Authentication attempts from unusual geographic regions should trigger anomaly detection.

AN1286

Abuse of system-generated or default privileged accounts such as 'root' or 'vpxuser' logging into ESXi hosts.

Log Sources

Mutable Elements

Field	Description
AccountName	If 'vpxuser' is replaced or configured differently, detection logic must reflect the change.
IPRange	Legitimate vCenter IP ranges may be whitelisted to avoid false positives.

AN1287

Login activity from default admin credentials (e.g., 'admin', 'cisco') on routers, firewalls, and switches.

Log Sources

Mutable Elements

Field	Description
Username	Default usernames vary by vendor; defenders should adapt logic to their specific appliance list.
InterfaceType	Telnet and HTTP-based access to network devices should be blocked and monitored if enabled.
