Behavior-chain detection for T1133 External Remote Services across Windows, Linux, macOS, Containers, Detection Strategy DET0354

Archived: 2026-04-02 10:55:05 UTC

AN1004

Unusual or unauthorized external remote access attempts (e.g., RDP, VPN, Citrix) → repeated failed logins followed by a successful session from uncommon geolocations or outside business hours → subsequent internal lateral movement or data exfiltration activities.

Log Sources

Mutable Elements

Field	Description
BusinessHours	Normal business hours for logon activity.
KnownRemoteIPs	List of approved external IPs or VPN endpoints.
FailedLogonThreshold	Number of failed logons before raising suspicion (e.g., >5).
GeoIPWhitelist	Geographic regions allowed for remote access.
TimeWindow	Time window to correlate failed attempts and success (e.g., 15m).

AN1005

Repeated SSH, VPN, or RDP gateway authentication attempts from external IPs → subsequent successful logon → remote shell or lateral movement activity (e.g., scp/sftp).

Log Sources

Mutable Elements

Field	Description
KnownSSHClients	Legitimate IPs or client fingerprints for SSH/VPN.
FailedLogonThreshold	Number of failed SSH logins to trigger alert.
TimeWindow	Correlation window for failed attempts and success.

AN1006

Unexpected inbound or outbound VNC/SSH/Screen Sharing connections from external sources → repeated failed logins followed by success → remote interactive sessions or abnormal file transfers.

Log Sources

Mutable Elements

Field	Description
KnownVNCServers	List of approved VNC/SSH sources.
TimeWindow	Time correlation between failed attempts and success.

AN1007

Connections to exposed container services (e.g., Docker API, Kubernetes API server) from unauthorized external IPs → abnormal container creation/start → lateral activity within cluster nodes.

Log Sources

Mutable Elements

Field	Description
AllowedCIDRs	Approved external IP ranges for container APIs.
TimeWindow	Correlation window for API calls and container starts.
