Behavioral Detection Strategy for Remote Service Logins and Post-Access Activity, Detection Strategy DET0269

Archived: 2026-04-02 10:38:43 UTC

AN0750

Logon via RDP or WMI by a user account followed by uncommon command execution, file manipulation, or lateral network connections.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between remote login and post-access activity
LogonUser	Limit to service accounts or privileged users for higher fidelity
RemoteHostList	Allowlisting known admin jumpboxes or deployment tools

AN0751

SSH session from new source IP followed by interactive shell or privilege escalation (e.g., sudo, su) and outbound lateral connection.

Log Sources

Mutable Elements

Field	Description
SourceIP	Limit to new/unexpected SSH source IPs
CommandList	Flag suspicious post-SSH command patterns

AN0752

Remote login via ARD or SSH followed by screensharingd process activity or modification of TCC-protected files.

Log Sources

Mutable Elements

Field	Description
RemoteService	Differentiate ARD vs SSH access patterns
TargetedPath	Tunable list of sensitive directories or TCC targets

AN0753

Use of cloud-based bastion or VM console session followed by commands that initiate outbound SSH or RDP sessions from the cloud instance to other environments.

Log Sources

Mutable Elements

Field	Description
SourceAssetTag	Limit detection to cloud admin/bastion hosts
TargetPortList	Define critical remote service ports to flag

AN0754

vSphere API logins (vimService) or SSH to ESXi host followed by unauthorized shell commands or lateral remote logins from the ESXi host.

Log Sources

Mutable Elements

Field	Description
SessionType	Filter by DCUI, SSH, vSphere API
CommandPattern	Watch for remote access tool invocations (e.g., netcat, ssh)
