Detection Strategy for SSH Session Hijacking, Detection Strategy DET0256

Archived: 2026-04-05 12:52:19 UTC

AN0710

Suspicious reuse of SSH agent sockets across multiple users or processes, anomalous access to ~/.ssh/ or /tmp/ssh-* sockets, and abnormal patterns of lateral movement via SSH without new authentication events. Defender view: detect when one process accesses another user's SSH agent or when an existing SSH connection is used to pivot unexpectedly.

Log Sources

Mutable Elements

Field	Description
UserContext	Tune alerts for cross-user access to SSH agent sockets.
TimeWindow	Correlate lack of authentication with lateral SSH activity within a short timeframe.

AN0711

Unusual access to SSH agent sockets in /tmp/ or /private/tmp, process access to another user’s $SSH_AUTH_SOCK, and lateral SSH activity without corresponding login events. Defender view: correlation of socket access with anomalous network flows to internal systems.

Log Sources

Mutable Elements

Field	Description
SocketPathScope	Limit detection to monitored SSH agent socket directories.
BaselineUsers	Establish normal SSH agent ownership and expected usage for tuning.
