# Detection Strategy for T1550.002 - Pass the Hash (Windows), Detection Strategy DET0409

Archived: 2026-04-05 14:01:44 UTC

## Analytics

- Windows

### AN1144

Detects anomalous NTLM LogonType 3 authentications that occur without accompanying domain logon events, especially from lateral systems or involving built-in administrative tools. Monitors for mismatches between source user context and system being accessed. Correlates LogonSession creation, NTLM authentications, and process/service initiation to identify suspicious use of stolen password hashes for remote access or service logon without password entry. Detects overpass-the-hash by combining Kerberos ticket issuance with NTLM-based lateral movement.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| TimeWindow | Allows tuning the correlation timeframe between authentication, session creation, and process/network activity. |
| SourceAccountAnomalyThreshold | Supports tuning detection sensitivity based on deviations from normal user login patterns or usage context. |
| LogonTypeFilter | Allows focusing detection on specific logon types (e.g., LogonType 3 for network logon, Type 10 for RDP). |

---