# Detection Strategy for T1136 - Create Account across platforms, Detection Strategy DET0583

Archived: 2026-04-05 15:12:17 UTC

### AN1604

Adversary uses built-in OS tools or API calls to create local or domain accounts for persistence or lateral movement. Tools such as 'net user', PowerShell, or MMC snap-ins may be used. Detection focuses on Event ID 4720 paired with process lineage and user context.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| TimeWindow | Correlation between Event ID 4720 and creating process may vary by environment and automation delays |
| ParentProcessName | Tools like net.exe or powershell.exe can be normal or malicious depending on user context |
| UserContext | System vs. administrator vs. low-privilege user context changes alert criticality |

### AN1605

Adversary invokes 'useradd', 'adduser', or equivalent system commands or scripts to create local users. Detection focuses on command execution and audit trail of passwd/shadow file modifications.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| BinaryPath | Custom scripts or renamed binaries may evade simple path-based detection |
| ExecutionTime | Account creation outside maintenance windows may indicate compromise |

### AN1606

Adversary creates new users using 'dscl' commands, GUI tools, or by modifying user plist files. Detection includes monitoring dscl invocation and user-related plist changes.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| UsernamePattern | Attackers may use service-like names to hide malicious accounts |
| ExecutionSource | Accounts created via Terminal vs GUI vs remote session can affect confidence |

### AN1607

Adversary creates users via IAM/IdP API or portal (e.g., Azure AD, Okta). Detection involves monitoring API calls, admin action logs, and correlation with role assignments.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| AdminThreshold | Trigger alert only when account is assigned privileged roles |
| AutomationExemptions | Exclude accounts from known automation processes or provisioning pipelines |

### AN1608

Account creation via cloud service APIs or CLI, often associated with key generation. Monitored via CloudTrail or equivalent audit logs.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| Region | Alert on account creation outside expected geographies |
| ServiceScope | Filter on creation of users scoped to sensitive services |

---