Failed Logins Exceeding Threshold

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Detects multiple failed login attempts within a short period, which could indicate a brute-force attack.

MITRE ATT&CK

Credential Access

Kural sorgusu

```
SecurityEvent
| where EventID == 4625  // Failed login event
| summarize Count = count() by Account, bin(Time
| where Count > 5
```

Lateral Movement via SMB

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Detects possible lateral movement attempts via SMB (Server Message Block) by identifying connections to multiple machines in a short period.

MITRE ATT&CK

Lateral Movement

Kural sorgusu

```
SecurityEvent
| where EventID == 5140 // Network share object
| summarize ConnectionCount = count() by Account
| where ConnectionCount > 10
```

Successful Local Sign

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

--

MITRE ATT&CK

Initial Access

Kural sorgusu

```
SecurityEvent
| where Activity contains "success" and Account
```

Multiple Logins from Different Geolocations

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Detects if a user logs in from two different geographic locations within a short period, indicating a potential compromise.

MITRE ATT&CK

- Initial Access
- Credential Access

Kural sorgusu

```
SigninLogs
| extend GeoLocation = strcat(LocationDetails.co
| summarize make_set(GeoLocation), make_set(IPAd
| where array_length(set_GeoLocation) > 1  // Mo
```

High Number of VPN Logins in Short Time

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Tracks when an account logs into the VPN multiple times in a short period, possibly indicating compromised credentials.

MITRE ATT&CK

- Initial Access
- Credential Access

Kural sorgusu

```
SigninLogs
| where AppDisplayName == "VPN"
| summarize Count = count() by UserPrincipalName
| where Count > 5
```

Suspicious File Changes in Sensitive Directories

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Detects file creation, deletion, or modification in sensitive directories (e.g., C:\Windows\System32).

MITRE ATT&CK

Persistence

Defense Evasion

Kural sorgusu

```
SecurityEvent
| where EventID in (4663, 5145) // File access o
| where FilePath contains "C:\\Windows\\System32
```

Unusual Process Execution (Living off the Land)

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Detects the use of system-native tools, like regsvr32, mshta, or rundll32, often used by attackers to bypass defenses.

MITRE ATT&CK

Execution

Defense Evasion

Kural sorgusu

```
SecurityEvent
| where EventID == 4688 // Process creation even
| where ProcessName in ("regsvr32.exe", "mshta.e
```

Suspicious PowerShell Commands

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Identifies potentially malicious PowerShell command execution by searching for unusual or sensitive cmdlet usage.

MITRE ATT&CK

Execution

Kural sorgusu

```
SecurityEvent
| where EventID == 4104 // PowerShell event
| where CommandLine contains "Invoke-WebRequest"
```

Successful Login After Multiple Failures

Orta	Özel	Etkin
Önem Derecesi	İçerik Kaynağı	Durum

Açıklama

Monitors if an account has a successful login after multiple failed attempts, a potential sign of compromised credentials.

MITRE ATT&CK

- Initial Access
- Credential Access

Kural sorgusu

```
let failed_logins = SecurityEvent
    | where EventID == 4625 // Failed login ev
    | summarize FailedCount = count() by Accou
let successful_login = SecurityEvent
    | where EventID == 4624 // Successful logi
    | project Account, TimeGenerated;
```