Requirement

Rule in Kusto Query Language	Description
Inactive users in SharePoint Online	Required
Only invited users should be automatically admitted	Required
Block legacy authentication through Conditional Access	Required
Secure Score for Identity: 5. Enable User Risk in Conditional Access policy	Required
Enable Sign-in Risk in Conditional Access policy	Required
Define and set Account Lockout policy on MFA	Required
Disable Phone Call and SMS on MFA service settings	Required
Enforce MFA on all accounts	Required

Inactive users in SharePoint Online

```
let inactive_threshold_days = 90;
let current_time = now();

SharePointAudit
| where Activity == "Sign Out"
| where TimeGenerated >= ago(inactive_threshold_daysd)
| project UserDisplayName, TimeGenerated, SiteURL
```

Only invited users should be automatically admitted:

```
let invitedUsers = ...; // Invited users data source
InvitedUsers
| where isnotnull(invitationAcceptedTime)
| project userPrincipalName, invitationAcceptedTime;
```

Block legacy authentication through Conditional Access:

```
let legacyAuthEvents = ...; // Legacy authentication events data source
legacyAuthEvents
| where riskLevel == "high"
| project userPrincipalName, appDisplayName, riskLevel;
```

Secure Score for Identity: 5. Enable User Risk in Conditional Access policy:

```
let userRiskEvents = ...; // User risk events data source
userRiskEvents
| where riskScore >= 5
| project userPrincipalName, riskScore;
```

Enable Sign-in Risk in Conditional Access policy:

```
let signInRiskEvents = ...; // Sign-in risk events data source
signInRiskEvents
| where riskScore >= 5
| project userPrincipalName, riskScore;
```

Define and set Account Lockout policy on MFA:

```
let accountLockoutEvents = ...; // Account lockout events data source
accountLockoutEvents
| where isnotnull(lockoutTime)
| project userPrincipalName, lockoutTime;
```

Disable Phone Call and SMS on MFA service settings:

```
let mfaServiceEvents = ...; // MFA service events data source
mfaServiceEvents
| where mfaMethod !in ("Phone Call", "SMS")
| project userPrincipalName, mfaMethod;
```

Enforce MFA on all accounts:

```
let allUsers = ...; // All users data source
allUsers
| where isnotnull(mfaActivationTime)
| project userPrincipalName, mfaActivationTime;
```