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 = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "AccessControl"
   and AlertName == "UserInvitationAccepted"
| project UserId, TimeGenerated;
```

Block legacy authentication through Conditional Access:

```
let legacyAuthEvents = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "AccessControl"
   and AlertName == "LegacyAuthDetected"
| project UserId, AppDisplayName, TimeGenerated;
```

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

```
let userRiskEvents = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "IdentitySecurity"
   and AlertName == "UserRiskSignIn"
| project UserId, RiskScore, TimeGenerated;
```

Enable Sign-in Risk in Conditional Access policy:

```
let signInRiskEvents = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "IdentitySecurity"
   and AlertName == "SignInRiskDetected"
| project UserId, RiskScore, TimeGenerated;
```

Define and set Account Lockout policy on MFA:

```
let accountLockoutEvents = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "AccessControl"
   and AlertName == "AccountLockedOut"
| project UserId, TimeGenerated;
```

Disable Phone Call and SMS on MFA service settings:

```
let mfaServiceEvents = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "AccessControl"
   and AlertName == "MFAServiceSettingsChanged"
| project UserId, MFAMethod, TimeGenerated;
```

Enforce MFA on all accounts:

```
let allUsers = SecurityAlert
| where ProviderName == "AzureActiveDirectory" and Category == "AccessControl"
   and AlertName == "MFAEnforced"
| project UserId, TimeGenerated;
```