Contents

Top 300 Azure Sentinel Used Cases KQL (Kusto Query Language) queries.

1. Failed login attempts:

```
SecurityEvent
| where EventID == 4625
```

2. Successful login attempts:

```
SecurityEvent
| where EventID == 4624
```

3. Brute-force attacks:

```
SecurityEvent
| where EventID == 4625
| summarize count() by TargetUserName
| where count_ > <threshold>
```

4. Account lockouts:

```
SecurityEvent
| where EventID == 4740
```

5. User account changes:

```
SecurityEvent
| where EventID == 4738 or EventID == 4720
```

6. Privileged account usage:

```
SecurityEvent
| where EventID in (4672, 4673, 4688) and AccountType == 'User'
```

7. Suspicious process execution:

```
SecurityEvent
| where EventID == 4688 and InitiatingProcessCommandLine has_any ('powershell.exe', 'cmd.exe')
```

8. Data exfiltration:

```
SecurityEvent
| where EventID == 5145 and AccessMask == '0x2'
```

9. Network traffic anomalies:

```
SecurityAlert
| where ProviderName == 'MicrosoftNetworkProtection' and AlertType == 'AnomalousNetworkTraffic'
```

10. Malware detection:

```
SecurityAlert
| where ProviderName == 'MicrosoftDefenderATP' and AlertType == 'MalwareDetection'
```

11. DDoS attacks:

```
SecurityAlert
| where ProviderName == 'DDoSProtection' and AlertType == 'DDoSGeneric'
```

12. Suspicious PowerShell activity:

```
SecurityEvent
| where EventID == 4104 and (CommandLine has_any ('Invoke-Expression', 'Invoke-Script', 'iex'))
```

13. Unusual account behavior:

```
SecurityEvent
| where EventID == 4724 or EventID == 4725
```

14. Privilege escalation attempts:

```
SecurityEvent
| where EventID == 4672 and NewProcessName contains 'cmd.exe'
```

15. Failed service principal logins:

```
AuditLogs
| where OperationName == 'Sign-in by service principal' and ResultType == 'failure'
```

16. Suspicious Azure AD sign-ins:

```
AuditLogs
| where ActivityDisplayName == 'Sign-in' and ResultType == 'failure'
```

17. Unusual lateral movement:

```
SecurityEvent
| where EventID == 4624 and LogonType == 3
```

18. Azure resource modifications:

```
AzureActivity
| where OperationName == 'Microsoft.Resources/subscriptions/resourcegroups/write'
```

19. Unusual DNS queries:

```
DnsEvents
| where QueryType == 'A' and isnotempty(QueryName) and notstartswith(QueryName, 'Microsoft')
```

20. Data access by unusual IP addresses:

```
SecurityEvent
| where EventID == 4663 and (SourceAddress notlike 'x.x.x.x' and SourceAddress notlike 'y.y.y.y')
```

21. Large data exports:

```
AuditLogs
| where OperationName == 'Export' and ResultType == 'success'
```

22. Unusual process creation:

```
SecurityEvent
| where EventID == 4688 and (NewProcessParentName != 'C:\Windows\System32\svchost.exe')
```

23. Suspicious Azure VM operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Compute/virtualMachines' and OperationName in
('Microsoft.Compute/virtualMachines/write', 'Microsoft.Compute/virtualMachines/delete')
```

24. Failed SQL Database access attempts:

```
SecurityEvent
| where EventID == 18456 and LogonType == 8
```

25. Azure AD user password changes:

```
AuditLogs
| where ActivityDisplayName == 'Password reset' and ResultType == 'success'
```

26. Account enumeration attempts:

```
SecurityEvent
| where EventID == 4625 and FailureReason == 3221225578
```

27. Suspicious Azure Storage operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Storage/storageAccounts' and OperationName in
('Microsoft.Storage/storageAccounts/write', 'Microsoft.Storage/storageAccounts/delete')
```

28. Suspicious PowerShell modules loaded:

```
SecurityEvent
| where EventID == 4104 and (ParentImage contains 'powershell.exe' or Image contains 'powershell.exe')
```

29. Failed Exchange mailbox login attempts:

```
SecurityEvent
| where EventID == 4625 and LogonType == 10
```

30. Suspicious Azure Key Vault access:

```
AuditLogs
| where ActivityDisplayName == 'Access granted to Key Vault' and ResultType == 'success'
```

31. Unusual VPN logins:

```
SecurityEvent
| where EventID == 4647 and LogonType == 21
```

32. Failed RDP login attempts:

```
SecurityEvent
| where EventID == 4625 and LogonType == 10
```

33. Suspicious Azure Function operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Web/sites/functions' and OperationName in
('Microsoft.Web/sites/functions/write', 'Microsoft.Web/sites/functions/delete')
```

34. Unusual Azure AD application registrations:

```
AuditLogs
| where ActivityDisplayName == 'Add an application' and ResultType == 'success'
```

35. Suspicious network port scans:

```
SecurityEvent
| where EventID == 5156 and Port >= 1 and Port <= 1024
```

36. Failed Azure VM login attempts:

```
AzureActivity
| where ResourceType == 'Microsoft.Compute/virtualMachines' and OperationName ==
'Microsoft.Compute/virtualMachines/login/action'
```

37. Unusual Azure NSG rule modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Network/networkSecurityGroups/securityRules' and
OperationName in ('Microsoft.Network/networkSecurityGroups/securityRules/write',
'Microsoft.Network/networkSecurityGroups/securityRules/delete')
```

38. Unusual Azure AD group modifications:

```
AuditLogs
| where ActivityDisplayName == 'Add member to group' and ResultType == 'success'
```

39. Suspicious Azure Data Factory operations:

```
AzureActivity
| where ResourceType == 'Microsoft.DataFactory/factories' and OperationName in
('Microsoft.DataFactory/factories/write', 'Microsoft.DataFactory/factories/delete')
```

40. Unusual Azure Key Vault secret accesses:

```
AuditLogs
| where ActivityDisplayName == 'Get secret' and ResultType == 'success'
```

41. Suspicious Azure Logic Apps operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Logic/workflows' and OperationName in
('Microsoft.Logic/workflows/write', 'Microsoft.Logic/workflows/delete')
```

42. Unusual Azure AD role assignments:

```
AuditLogs
| where ActivityDisplayName == 'Add role assignment' and ResultType == 'success'
```

43. Suspicious Azure Event Grid operations:

```
AzureActivity
| where ResourceType == 'Microsoft.EventGrid/topics' and OperationName in
('Microsoft.EventGrid/topics/write', 'Microsoft.EventGrid/topics/delete')
```

44. Unusual Azure AD application role assignments:

```
AuditLogs
| where ActivityDisplayName == 'Add app role assignment' and ResultType == 'success'
```

45. Suspicious Azure Service Bus operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ServiceBus/namespaces' and OperationName in
('Microsoft.ServiceBus/namespaces/write', 'Microsoft.ServiceBus/namespaces/delete')
```

46. Failed Azure Function execution attempts:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Error'
```

47. Unusual Azure AD guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite user' and ResultType == 'success'
```

48. Suspicious Azure Event Hub operations:

```
AzureActivity
| where ResourceType == 'Microsoft.EventHub/namespaces' and OperationName in
('Microsoft.EventHub/namespaces/write', 'Microsoft.EventHub/namespaces/delete')
```

49. Unusual Azure AD risky sign-ins:

```
AuditLogs
| where ActivityDisplayName == 'Risky sign-in detected' and ResultType == 'success'
```

50. Suspicious Azure IoT Hub operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Devices/IotHubs' and OperationName in
('Microsoft.Devices/IotHubs/write', 'Microsoft.Devices/IotHubs/delete')
```

51. Unusual Azure AD administrator role assignments:

```
AuditLogs
| where ActivityDisplayName == 'Add member to role' and ResultType == 'success'
```

52. Suspicious Azure Container Registry operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ContainerRegistry/registries' and OperationName in
('Microsoft.ContainerRegistry/registries/write', 'Microsoft.ContainerRegistry/registries/delete')
```

53. Failed Azure Logic App execution attempts:

```
AzureDiagnostics
| where Category == 'LogicAppRuntime' and Level == 'Error'
```

54. Unusual Azure AD password reset attempts:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'failure'
```

55. Suspicious Azure Kubernetes Service operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ContainerService/managedClusters' and OperationName in
('Microsoft.ContainerService/managedClusters/write',
'Microsoft.ContainerService/managedClusters/delete')
```

56. Failed Azure API Management operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

57. Unusual Azure AD consent grants:

```
AuditLogs
| where ActivityDisplayName == 'Grant OAuth2 permissions' and ResultType == 'success'
```

58. Suspicious Azure Batch operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Batch/batchAccounts' and OperationName in
('Microsoft.Batch/batchAccounts/write', 'Microsoft.Batch/batchAccounts/delete')
```

59. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Error'
```

60. Unusual Azure AD OAuth application consents:

```
AuditLogs
| where ActivityDisplayName == 'Consent to application' and ResultType == 'success'
```

61. Suspicious Azure HDInsight operations:

```
AzureActivity
| where ResourceType == 'Microsoft.HDInsight/clusters' and OperationName in
('Microsoft.HDInsight/clusters/write', 'Microsoft.HDInsight/clusters/delete')
```

62. Failed Azure Key Vault access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Error'
```

63. Unusual Azure AD domain role assignments:

```
AuditLogs
| where ActivityDisplayName == 'Add member to directory role' and ResultType == 'success'
```

64. Suspicious Azure Media Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Media/mediaservices' and OperationName in
('Microsoft.Media/mediaservices/write', 'Microsoft.Media/mediaservices/delete')
```

65. Failed Azure Front Door operations:

```
AzureDiagnostics
| where Category == 'Frontdoor' and Level == 'Error'
```

66. Unusual Azure AD B2B guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite guest user' and ResultType == 'success'
```

67. Suspicious Azure Machine Learning operations:

```
AzureActivity
| where ResourceType == 'Microsoft.MachineLearningServices/workspaces' and OperationName in
('Microsoft.MachineLearningServices/workspaces/write',
'Microsoft.MachineLearningServices/workspaces/delete')
```

68. Failed Azure API Gateway operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

69. Unusual Azure AD B2C user sign-ups:

```
AuditLogs
| where ActivityDisplayName == 'Sign up user' and ResultType == 'success'
```

70. Suspicious Azure Managed Identity operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ManagedIdentity/userAssignedIdentities' and OperationName in
('Microsoft.ManagedIdentity/userAssignedIdentities/write',
'Microsoft.ManagedIdentity/userAssignedIdentities/delete')
```

71. Failed Azure Data Factory operations:

```
AzureDiagnostics
| where Category == 'DataFactoryPipelineRuns' and Level == 'Error'
```

72. Unusual Azure AD B2C user password resets:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'success'
```

73. Suspicious Azure CDN operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cdn/profiles' and OperationName in ('Microsoft.Cdn/profiles/write',
'Microsoft.Cdn/profiles/delete')
```

74. Failed Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Error'
```

75. Unusual Azure AD B2C user profile updates:

```
AuditLogs
| where ActivityDisplayName == 'Update user' and ResultType == 'success'
```

76. Suspicious Azure Logic App runs:

```
AzureDiagnostics
| where Category == 'LogicAppRuns' and Level == 'Error'
```

77. Failed Azure Key Vault secret access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Error'
```

78. Unusual Azure DevOps pipeline modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.DevOps/pipelines' and OperationName in
('Microsoft.DevOps/pipelines/write', 'Microsoft.DevOps/pipelines/delete')
```

79. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

80. Failed Azure Container Registry operations:

```
AzureDiagnostics
| where Category == 'ContainerRegistry' and Level == 'Error'
```

81. Unusual Azure API Management service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service' and OperationName in
('Microsoft.ApiManagement/service/write', 'Microsoft.ApiManagement/service/delete')
```

82. Suspicious Azure Cognitive Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.CognitiveServices/accounts' and OperationName in
('Microsoft.CognitiveServices/accounts/write', 'Microsoft.CognitiveServices/accounts/delete')
```

83. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Error'
```

84. Unusual Azure Data Lake operations:

```
AzureActivity
| where ResourceType == 'Microsoft.DataLakeStore/accounts' and OperationName in
('Microsoft.DataLakeStore/accounts/write', 'Microsoft.DataLakeStore/accounts/delete')
```

85. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

86. Failed Azure IoT Hub operations:

```
AzureDiagnostics
| where Category == 'IotHubD2CLogs' and Level == 'Error'
```

87. Unusual Azure Data Explorer (ADX) cluster operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Kusto/clusters' and OperationName in
('Microsoft.Kusto/clusters/write', 'Microsoft.Kusto/clusters/delete')
```

88. Suspicious Azure Cache for Redis operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

89. Failed Azure Kubernetes Service operations:

```
AzureDiagnostics
| where Category == 'KubeApiServerAuditLogs' and Level == 'Error'
```

90. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Warning'
```

91. Suspicious Azure Databricks operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Databricks/workspaces' and OperationName in
('Microsoft.Databricks/workspaces/write', 'Microsoft.Databricks/workspaces/delete')
```

92. Failed Azure API Management service operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Warning'
```

93. Unusual Azure Bot Service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.BotService/botServices' and OperationName in
('Microsoft.BotService/botServices/write', 'Microsoft.BotService/botServices/delete')
```

94. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

95. Failed Azure Container Instance operations:

```
AzureDiagnostics
| where Category == 'ContainerInstanceLogs' and Level == 'Warning'
```

96. Unusual Azure API Management API modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service/apis' and OperationName in
('Microsoft.ApiManagement/service/apis/write', 'Microsoft.ApiManagement/service/apis/delete')
```

97. Suspicious Azure Cognitive Search operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

98. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Warning'
```

99. Unusual Azure Data Factory pipeline executions:

```
AzureDiagnostics
| where Category == 'DataFactoryPipelineRuns' and Level == 'Warning'
```

100. Suspicious Azure Notification Hubs operations:

```
AzureActivity
| where ResourceType == 'Microsoft.NotificationHubs/namespaces' and OperationName in
('Microsoft.NotificationHubs/namespaces/write', 'Microsoft.NotificationHubs/namespaces/delete')
```

101. Failed Azure Event Hubs operations:

```
AzureDiagnostics
| where Category == 'EventHub' and Level == 'Warning'
```

102. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Information'
```

103. Suspicious Azure HDInsight operations:

```
AzureActivity
| where ResourceType == 'Microsoft.HDInsight/clusters' and OperationName in
('Microsoft.HDInsight/clusters/write', 'Microsoft.HDInsight/clusters/delete')
```

104. Failed Azure Key Vault access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Warning'
```

105. Unusual Azure Kubernetes Service operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ContainerService/managedClusters' and OperationName in
('Microsoft.ContainerService/managedClusters/write',
Microsoft.ContainerService/managedClusters/delete')
```

106. Suspicious Azure Logic Apps operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Logic/workflows' and OperationName in
('Microsoft.Logic/workflows/write', 'Microsoft.Logic/workflows/delete')
```

107. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Warning'
```

108. Unusual Azure Media Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Media/mediaservices' and OperationName in
('Microsoft.Media/mediaservices/write', 'Microsoft.Media/mediaservices/delete')
```

109. Suspicious Azure API Gateway operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiGateway/service' and OperationName in
('Microsoft.ApiGateway/service/write', 'Microsoft.ApiGateway/service/delete')
```

110. Failed Azure Logic App execution attempts:

```
AzureDiagnostics
| where Category == 'LogicAppRuntime' and Level == 'Warning'
```

111. Unusual Azure AD password reset attempts:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'failure'
```

112. Suspicious Azure Stream Analytics operations:

```
AzureActivity
| where ResourceType == 'Microsoft.StreamAnalytics/streamingjobs' and OperationName in
('Microsoft.StreamAnalytics/streamingjobs/write', 'Microsoft.StreamAnalytics/streamingjobs/delete')
```

113. Failed Azure SQL Database operations:

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents' and Level == 'Warning'
```

114. Unusual Azure AD guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite user' and ResultType == 'success
```

115. Suspicious Azure CDN operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cdn/profiles' and OperationName in ('Microsoft.Cdn/profiles/write',
'Microsoft.Cdn/profiles/delete')
```

116. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Warning'
```

117. Unusual Azure AD B2B guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite guest user' and ResultType == 'success'
```

118. Suspicious Azure Redis Cache operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

119. Failed Azure Front Door operations:

```
AzureDiagnostics
```

```
| where Category == 'Frontdoor' and Level == 'Warning'
```

120. Unusual Azure AD B2B user sign-ins:

```
AuditLogs
| where ActivityDisplayName == 'B2B user sign-in' and ResultType == 'success'
```

121. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

122. Failed Azure Data Lake operations:

```
AzureDiagnostics
| where Category == 'DataLakeStoreLogs' and Level == 'Warning'
```

123. Unusual Azure AD B2B user password resets:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'success'
```

124. Suspicious Azure Machine Learning operations:

```
AzureActivity
| where ResourceType == 'Microsoft.MachineLearningServices/workspaces' and OperationName in
('Microsoft.MachineLearningServices/workspaces/write',
'Microsoft.MachineLearningServices/workspaces/delete')
```

125. Failed Azure API Gateway operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Warning'
```

126. Unusual Azure AD B2B user profile updates:

```
AuditLogs
| where ActivityDisplayName == 'Update user' and ResultType == 'success'
```

127. Suspicious Azure Logic App runs:

```
AzureDiagnostics
| where Category == 'LogicAppRuns' and Level == 'Warning'
```

128. Failed Azure Key Vault secret access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Warning'
```

129. Unusual Azure DevOps pipeline modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.DevOps/pipelines' and OperationName in
('Microsoft.DevOps/pipelines/write', 'Microsoft.DevOps/pipelines/delete')
```

130. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

131. Failed Azure Container Registry operations:

```
AzureDiagnostics
| where Category == 'ContainerRegistry' and Level == 'Warning'
```

132. Unusual Azure API Management service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service' and OperationName in
('Microsoft.ApiManagement/service/write', 'Microsoft.ApiManagement/service/delete')
```

133. Suspicious Azure Cognitive Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.CognitiveServices/accounts' and OperationName in
 ('Microsoft.CognitiveServices/accounts/write', 'Microsoft.CognitiveServices/accounts/delete')
```

134. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Warning'
```

135. Unusual Azure Data Lake operations:

```
AzureActivity
| where ResourceType == 'Microsoft.DataLakeStore/accounts' and OperationName in
('Microsoft.DataLakeStore/accounts/write', 'Microsoft.DataLakeStore/accounts/delete')
```

136. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

137. Failed Azure IoT Hub operations:

```
AzureDiagnostics
| where Category == 'IotHubD2CLogs' and Level == 'Warning'
```

138. Unusual Azure Data Explorer (ADX) cluster operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Kusto/clusters' and OperationName in
('Microsoft.Kusto/clusters/write', 'Microsoft.Kusto/clusters/delete')
```

139. Suspicious Azure Cache for Redis operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

140. Failed Azure Kubernetes Service operations:

```
AzureDiagnostics
| where Category == 'KubeApiServerAuditLogs' and Level == 'Warning'
```

141. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Error'
```

142. Suspicious Azure Databricks operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Databricks/workspaces' and OperationName in
('Microsoft.Databricks/workspaces/write', 'Microsoft.Databricks/workspaces/delete')
```

143. Failed Azure API Management service operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

144. Unusual Azure Bot Service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.BotService/botServices' and OperationName in
('Microsoft.BotService/botServices/write', 'Microsoft.BotService/botServices/delete')
```

145. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

146. Failed Azure Container Instance operations:

```
AzureDiagnostics
| where Category == 'ContainerInstanceLogs' and Level == 'Error'
```

147. Unusual Azure API Management API modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service/apis' and OperationName in
('Microsoft.ApiManagement/service/apis/write', 'Microsoft.ApiManagement/service/apis/delete')
```

148. Suspicious Azure Cognitive Search operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

149. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Error'
```

150. Unusual Azure Data Factory pipeline executions:

```
AzureDiagnostics
| where Category == 'DataFactoryPipelineRuns' and Level == 'Error'
```

151. Suspicious Azure Notification Hubs operations:

```
AzureActivity
| where ResourceType == 'Microsoft.NotificationHubs/namespaces' and OperationName in
('Microsoft.NotificationHubs/namespaces/write', 'Microsoft.NotificationHubs/namespaces/delete')
```

152. Failed Azure Event Hubs operations:

```
AzureDiagnostics
| where Category == 'EventHub' and Level == 'Error'
```

153. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Information'
```

154. Suspicious Azure HDInsight operations:

```
AzureActivity
| where ResourceType == 'Microsoft.HDInsight/clusters' and OperationName in
('Microsoft.HDInsight/clusters/write', 'Microsoft.HDInsight/clusters/delete')
```

155. Failed Azure Key Vault access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Error'
```

156. Unusual Azure Kubernetes Service operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ContainerService/managedClusters' and OperationName in
('Microsoft.ContainerService/managedClusters/write',
'Microsoft.ContainerService/managedClusters/delete')
```

157. Suspicious Azure Logic Apps operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Logic/workflows' and OperationName in
('Microsoft.Logic/workflows/write', 'Microsoft.Logic/workflows/delete')
```

158. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Error'
```

159. Unusual Azure Media Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Media/mediaservices' and OperationName in
('Microsoft.Media/mediaservices/write', 'Microsoft.Media/mediaservices/delete')
```

160. Suspicious Azure API Gateway operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiGateway/service' and OperationName in
('Microsoft.ApiGateway/service/write', 'Microsoft.ApiGateway/service/delete')
```

161. Failed Azure Logic App execution attempts:

```
AzureDiagnostics
| where Category == 'LogicAppRuntime' and Level == 'Error'
```

162. Unusual Azure AD password reset attempts:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'failure'
```

163. Suspicious Azure Stream Analytics operations:

```
AzureActivity
| where ResourceType == 'Microsoft.StreamAnalytics/streamingjobs' and OperationName in
('Microsoft.StreamAnalytics/streamingjobs/write', 'Microsoft.StreamAnalytics/streamingjobs/delete')
```

164. Failed Azure SQL Database operations:

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents' and Level == 'Error'
```

165. Unusual Azure AD guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite user' and ResultType == 'success'
```

166. Suspicious Azure CDN operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cdn/profiles' and OperationName in ('Microsoft.Cdn/profiles/write',
'Microsoft.Cdn/profiles/delete')
```

167. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Error'
```

168. Unusual Azure AD B2B guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite guest user' and ResultType == 'success'
```

169. Suspicious Azure Redis Cache operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

170. Failed Azure Front Door operations:

```
AzureDiagnostics
| where Category == 'Frontdoor' and Level == 'Error'
```

171. Unusual Azure AD B2B user sign-ins:

```
AuditLogs
| where ActivityDisplayName == 'B2B user sign-in' and ResultType == 'success'
```

172. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

173. Failed Azure Data Lake operations:

```
AzureDiagnostics
| where Category == 'DataLakeStoreLogs' and Level == 'Error'
```

174. Unusual Azure AD B2B user password resets:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'success'
```

175. Suspicious Azure Machine Learning operations:

```
AzureActivity
| where ResourceType == 'Microsoft.MachineLearningServices/workspaces' and OperationName in
('Microsoft.MachineLearningServices/workspaces/write',
'Microsoft.MachineLearningServices/workspaces/delete')
```

176. Failed Azure API Gateway operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

177. Unusual Azure AD B2B user profile updates:

```
AuditLogs
| where ActivityDisplayName == 'Update user' and ResultType == 'success'
```

178. Suspicious Azure Logic App runs:

```
AzureDiagnostics
| where Category == 'LogicAppRuns' and Level == 'Error'
```

179. Failed Azure Key Vault secret access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Error'
```

180. Unusual Azure DevOps pipeline modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.DevOps/pipelines' and OperationName in
('Microsoft.DevOps/pipelines/write', 'Microsoft.DevOps/pipelines/delete')
```

181. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

182. Failed Azure Container Registry operations:

```
AzureDiagnostics
| where Category == 'ContainerRegistry' and Level == 'Error'
```

183. Unusual Azure API Management service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service' and OperationName in
('Microsoft.ApiManagement/service/write', 'Microsoft.ApiManagement/service/delete')
```

184. Suspicious Azure Cognitive Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.CognitiveServices/accounts' and OperationName in
('Microsoft.CognitiveServices/accounts/write', 'Microsoft.CognitiveServices/accounts/delete')
```

185. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Error'
```

186. Unusual Azure Data Lake operations:

```
AzureActivity
| where ResourceType == 'Microsoft.DataLakeStore/accounts' and OperationName in
('Microsoft.DataLakeStore/accounts/write', 'Microsoft.DataLakeStore/accounts/delete')
```

187. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

188. Failed Azure IoT Hub operations:

```
AzureDiagnostics
| where Category == 'IotHubD2CLogs' and Level == 'Error'
```

189. Unusual Azure Data Explorer (ADX) cluster operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Kusto/clusters' and OperationName in
('Microsoft.Kusto/clusters/write', 'Microsoft.Kusto/clusters/delete')
```

190. Suspicious Azure Cache for Redis operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

191. Failed Azure Kubernetes Service operations:

```
AzureDiagnostics
| where Category == 'KubeApiServerAuditLogs' and Level == 'Error'
```

192. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Warning'
```

193. Suspicious Azure Databricks operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Databricks/workspaces' and OperationName in
('Microsoft.Databricks/workspaces/write', 'Microsoft.Databricks/workspaces/delete')
```

194. Failed Azure API Management service operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Warning'
```

195. Unusual Azure Bot Service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.BotService/botServices' and OperationName in
('Microsoft.BotService/botServices/write', 'Microsoft.BotService/botServices/delete')
```

196. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

197. Failed Azure Container Instance operations:

```
AzureDiagnostics
| where Category == 'ContainerInstanceLogs' and Level == 'Warning'
```

198. Unusual Azure API Management API modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service/apis' and OperationName in
('Microsoft.ApiManagement/service/apis/write', 'Microsoft.ApiManagement/service/apis/delete')
```

199. Suspicious Azure Cognitive Search operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

200. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Warning'
```

201. Unusual Azure Data Factory pipeline executions:

```
AzureDiagnostics
| where Category == 'DataFactoryPipelineRuns' and Level == 'Warning'
```

202. Suspicious Azure Notification Hubs operations:

```
AzureActivity
| where ResourceType == 'Microsoft.NotificationHubs/namespaces' and OperationName in
('Microsoft.NotificationHubs/namespaces/write', 'Microsoft.NotificationHubs/namespaces/delete')
```

203. Failed Azure Event Hubs operations:

```
AzureDiagnostics
| where Category == 'EventHub' and Level == 'Warning'
```

204. Unusual Azure Functions executions:

```
AzureDiagnostics

| where Category == 'FunctionAppLogs' and Level == 'Information'
```

205. Suspicious Azure HDInsight operations:

```
AzureActivity
| where ResourceType == 'Microsoft.HDInsight/clusters' and OperationName in
('Microsoft.HDInsight/clusters/write', 'Microsoft.HDInsight/clusters/delete')
```

206. Failed Azure Key Vault access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Warning'
```

207. Unusual Azure Kubernetes Service operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ContainerService/managedClusters' and OperationName in
('Microsoft.ContainerService/managedClusters/write',
'Microsoft.ContainerService/managedClusters/delete')
```

208. Suspicious Azure Logic Apps operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Logic/workflows' and OperationName in
('Microsoft.Logic/workflows/write', 'Microsoft.Logic/workflows/delete')
```

209. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Warning'
```

210. Unusual Azure Media Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Media/mediaservices' and OperationName in
('Microsoft.Media/mediaservices/write', 'Microsoft.Media/mediaservices/delete')
```

211. Suspicious Azure API Gateway operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiGateway/service' and OperationName in
('Microsoft.ApiGateway/service/write', 'Microsoft.ApiGateway/service/delete')
```

212. Failed Azure Logic App execution attempts:

```
AzureDiagnostics
| where Category == 'LogicAppRuntime' and Level == 'Warning'
```

213. Unusual Azure AD password reset attempts:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'failure'
```

214. Suspicious Azure Stream Analytics operations:

```
AzureActivity
| where ResourceType == 'Microsoft.StreamAnalytics/streamingjobs' and OperationName in
('Microsoft.StreamAnalytics/streamingjobs/write', 'Microsoft.StreamAnalytics/streamingjobs/delete')
```

215. Failed Azure SQL Database operations:

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents' and Level == 'Warning'
```

216. Unusual Azure AD guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite user' and ResultType == 'success'
```

217. Suspicious Azure CDN operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cdn/profiles' and OperationName in ('Microsoft.Cdn/profiles/write',
'Microsoft.Cdn/profiles/delete')
```

218. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Warning'
```

219. Unusual Azure AD B2B guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite guest user' and ResultType == 'success'
```

220. Suspicious Azure Redis Cache operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

221. Failed Azure Front Door operations:

```
AzureDiagnostics
| where Category == 'Frontdoor' and Level == 'Warning'
```

222. Unusual Azure AD B2B user sign-ins:

```
AuditLogs
| where ActivityDisplayName == 'B2B user sign-in' and ResultType == 'success'
```

223. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

224. Failed Azure Data Lake operations:

```
AzureDiagnostics
| where Category == 'DataLakeStoreLogs' and Level == 'Warning'
```

225. Unusual Azure AD B2B user password resets:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'success'
```

226. Suspicious Azure Machine Learning operations:

```
AzureActivity
| where ResourceType == 'Microsoft.MachineLearningServices/workspaces' and OperationName in
('Microsoft.MachineLearningServices/workspaces/write',
'Microsoft.MachineLearningServices/workspaces/delete')
```

227. Failed Azure API Gateway operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Warning'
```

228. Unusual Azure AD B2B user profile updates:

```
AuditLogs
| where ActivityDisplayName == 'Update user' and ResultType == 'success'
```

229. Suspicious Azure Logic App runs:

```
AzureDiagnostics
| where Category == 'LogicAppRuns' and Level == 'Warning'
```

230. Failed Azure Key Vault secret access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Warning'
```

231. Unusual Azure DevOps pipeline modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.DevOps/pipelines' and OperationName in
('Microsoft.DevOps/pipelines/write', 'Microsoft.DevOps/pipelines/delete')
```

232. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

233. Failed Azure Container Registry operations:

```
AzureDiagnostics
| where Category == 'ContainerRegistry' and Level == 'Warning'
```

234. Unusual Azure API Management service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service' and OperationName in
('Microsoft.ApiManagement/service/write', 'Microsoft.ApiManagement/service/delete')
```

235. Suspicious Azure Cognitive Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.CognitiveServices/accounts' and OperationName in
('Microsoft.CognitiveServices/accounts/write', 'Microsoft.CognitiveServices/accounts/delete')
```

236. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Warning'
```

237. Unusual Azure Data Lake operations:

```
AzureActivity
| where ResourceType == 'Microsoft.DataLakeStore/accounts' and OperationName in
('Microsoft.DataLakeStore/accounts/write', 'Microsoft.DataLakeStore/accounts/delete')
```

238. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

239. Failed Azure IoT Hub operations:

```
AzureDiagnostics
| where Category == 'IotHubD2CLogs' and Level == 'Warning'
```

240. Unusual Azure Data Explorer (ADX) cluster operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Kusto/clusters' and OperationName in
('Microsoft.Kusto/clusters/write', 'Microsoft.Kusto/clusters/delete')
```

241. Suspicious Azure Cache for Redis operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

242. Failed Azure Kubernetes Service operations:

```
AzureDiagnostics
| where Category == 'KubeApiServerAuditLogs' and Level == 'Warning'
```

243. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Error'
```

244. Suspicious Azure Databricks operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Databricks/workspaces' and OperationName in
('Microsoft.Databricks/workspaces/write', 'Microsoft.Databricks/workspaces/delete')
```

245. Failed Azure API Management service operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

246. Unusual Azure Bot Service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.BotService/botServices' and OperationName in
('Microsoft.BotService/botServices/write', 'Microsoft.BotService/botServices/delete')
```

247. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

248. Failed Azure Container Instance operations:

```
AzureDiagnostics
| where Category == 'ContainerInstanceLogs' and Level == 'Error'
```

249. Unusual Azure API Management API modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service/apis' and OperationName in
('Microsoft.ApiManagement/service/apis/write', 'Microsoft.ApiManagement/service/apis/delete')
```

250. Suspicious Azure Cognitive Search operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

251. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Error'
```

252. Unusual Azure Data Factory pipeline executions:

```
AzureDiagnostics
| where Category == 'DataFactoryPipelineRuns' and Level == 'Error'
```

253. Suspicious Azure Notification Hubs operations:

```
AzureActivity
| where ResourceType == 'Microsoft.NotificationHubs/namespaces' and OperationName in
('Microsoft.NotificationHubs/namespaces/write', 'Microsoft.NotificationHubs/namespaces/delete')
```

254. Failed Azure Event Hubs operations:

```
AzureDiagnostics
| where Category == 'EventHub' and Level == 'Error'
```

255. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Warning'
```

256. Suspicious Azure HDInsight operations:

```
AzureActivity
| where ResourceType == 'Microsoft.HDInsight/clusters' and OperationName in
('Microsoft.HDInsight/clusters/write', 'Microsoft.HDInsight/clusters/delete')
```

257. Failed Azure Key Vault access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Error'
```

258. Unusual Azure Kubernetes Service operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ContainerService/managedClusters' and OperationName in
('Microsoft.ContainerService/managedClusters/write',
'Microsoft.ContainerService/managedClusters/delete')
```

259. Suspicious Azure Logic Apps operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Logic/workflows' and OperationName in
('Microsoft.Logic/workflows/write', 'Microsoft.Logic/workflows/delete')
```

260. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Error'
```

261. Unusual Azure Media Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Media/mediaservices' and OperationName in
('Microsoft.Media/mediaservices/write', 'Microsoft.Media/mediaservices/delete')
```

262. Suspicious Azure API Gateway operations:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiGateway/service' and OperationName in
('Microsoft.ApiGateway/service/write', 'Microsoft.ApiGateway/service/delete')
```

263. Failed Azure Logic App execution attempts:

```
AzureDiagnostics
| where Category == 'LogicAppRuntime' and Level == 'Error'
```

264. Unusual Azure AD password reset attempts:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'failure'
```

265. Suspicious Azure Stream Analytics operations:

```
AzureActivity
| where ResourceType == 'Microsoft.StreamAnalytics/streamingjobs' and OperationName in
('Microsoft.StreamAnalytics/streamingjobs/write', 'Microsoft.StreamAnalytics/streamingjobs/delete')
```

266. Failed Azure SQL Database operations:

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents' and Level == 'Error'
```

267. Unusual Azure AD guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite user' and ResultType == 'success'
```

268. Suspicious Azure CDN operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cdn/profiles' and OperationName in ('Microsoft.Cdn/profiles/write',
'Microsoft.Cdn/profiles/delete')
```

269. Failed Azure Monitor Alert actions:

```
AzureDiagnostics
| where Category == 'Platform' and Level == 'Error'
```

270. Unusual Azure AD B2B guest user additions:

```
AuditLogs
| where ActivityDisplayName == 'Invite guest user' and ResultType == 'success'
```

271. Suspicious Azure Redis Cache operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

272. Failed Azure Front Door operations:

```
zureDiagnostics
| where Category == 'Frontdoor' and Level == 'Error'
```

273. Unusual Azure AD B2B user sign-ins:

```
AuditLogs
| where ActivityDisplayName == 'B2B user sign-in' and ResultType == 'success'
```

274. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

275. Failed Azure Data Lake operations:

```
AzureDiagnostics
| where Category == 'DataLakeStoreLogs' and Level == 'Error'
```

276. Unusual Azure AD B2B user password resets:

```
AuditLogs
| where ActivityDisplayName == 'Self-service password reset' and ResultType == 'success'
```

277. Suspicious Azure Machine Learning operations:

```
AzureActivity
| where ResourceType == 'Microsoft.MachineLearningServices/workspaces' and OperationName in
('Microsoft.MachineLearningServices/workspaces/write',
'Microsoft.MachineLearningServices/workspaces/delete')
```

278. Failed Azure API Gateway operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

279. Unusual Azure AD B2B user profile updates:

```
AuditLogs
| where ActivityDisplayName == 'Update user' and ResultType == 'success'
```

280. Suspicious Azure Logic App runs:

```
AzureDiagnostics
| where Category == 'LogicAppRuns' and Level == 'Error'
```

281. Failed Azure Key Vault secret access attempts:

```
AzureDiagnostics
| where Category == 'KeyVault' and Level == 'Error'
```

282. Unusual Azure DevOps pipeline modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.DevOps/pipelines' and OperationName in
('Microsoft.DevOps/pipelines/write', 'Microsoft.DevOps/pipelines/delete')
```

283. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

284. Failed Azure Container Registry operations:

```
AzureDiagnostics
| where Category == 'ContainerRegistry' and Level == 'Error'
```

285. Unusual Azure API Management service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service' and OperationName in
('Microsoft.ApiManagement/service/write', 'Microsoft.ApiManagement/service/delete')
```

286. Suspicious Azure Cognitive Services operations:

```
AzureActivity
| where ResourceType == 'Microsoft.CognitiveServices/accounts' and OperationName in
('Microsoft.CognitiveServices/accounts/write', 'Microsoft.CognitiveServices/accounts/delete')
```

287. Failed Azure Batch operations:

```
AzureDiagnostics
| where Category == 'BatchAccountLogs' and Level == 'Error'
```

288. Unusual Azure Data Lake operations:

```
AzureActivity
| where ResourceType == 'Microsoft.DataLakeStore/accounts' and OperationName in
('Microsoft.DataLakeStore/accounts/write', 'Microsoft.DataLakeStore/accounts/delete')
```

289. Suspicious Azure Search service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.Search/searchServices' and OperationName in
('Microsoft.Search/searchServices/write', 'Microsoft.Search/searchServices/delete')
```

290. Failed Azure IoT Hub operations:

```
AzureDiagnostics
| where Category == 'IotHubD2CLogs' and Level == 'Error'
```

291. Unusual Azure Data Explorer (ADX) cluster operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Kusto/clusters' and OperationName in
('Microsoft.Kusto/clusters/write', 'Microsoft.Kusto/clusters/delete')
```

292. Suspicious Azure Cache for Redis operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Cache/redis' and OperationName in ('Microsoft.Cache/redis/write',
'Microsoft.Cache/redis/delete')
```

293. Failed Azure Kubernetes Service operations:

```
AzureDiagnostics
| where Category == 'KubeApiServerAuditLogs' and Level == 'Error'
```

294. Unusual Azure Functions executions:

```
AzureDiagnostics
| where Category == 'FunctionAppLogs' and Level == 'Error'
```

295. Suspicious Azure Databricks operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Databricks/workspaces' and OperationName in
('Microsoft.Databricks/workspaces/write', 'Microsoft.Databricks/workspaces/delete')
```

296. Failed Azure API Management service operations:

```
AzureDiagnostics
| where Category == 'ApiManagementGatewayLogs' and Level == 'Error'
```

297. Unusual Azure Bot Service modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.BotService/botServices' and OperationName in
('Microsoft.BotService/botServices/write', 'Microsoft.BotService/botServices/delete')
```

298. Suspicious Azure SQL Database operations:

```
AzureActivity
| where ResourceType == 'Microsoft.Sql/servers/databases' and OperationName in
('Microsoft.Sql/servers/databases/write', 'Microsoft.Sql/servers/databases/delete')
```

299. Failed Azure Container Instance operations:

```
AzureDiagnostics
| where Category == 'ContainerInstanceLogs' and Level == 'Error'
```

300. Unusual Azure API Management API modifications:

```
AzureActivity
| where ResourceType == 'Microsoft.ApiManagement/service/apis' and OperationName in
('Microsoft.ApiManagement/service/apis/write', 'Microsoft.ApiManagement/service/apis/delete')
```

Important Note: Monitor and analyze various activities in Azure Sentinel. Also adjust the KQL queries based on your specific configuration and naming conventions.