|  |  |  |
| --- | --- | --- |
|  | Table Name | Columns/Fields |
| Alerts & behaviors | AlertEvidence | Timestamp, AlertId, Title, Categories, AttackTechniques, ServiceSource, DetectionSource, EntityType, EvidenceRole, EvidenceDirection, FileName, FolderPath, SHA1, SHA256, FileSize, ThreatFamily, RemoteIP, RemoteUrl, AccountName, AccountDomain, AccountSid, AccountObjectId, AccountUpn, DeviceId, DeviceName, LocalIP, NetworkMessageId, EmailSubject, Application, ApplicationId, OAuthApplicationId, ProcessCommandLine, RegistryKey, RegistryValueName, RegistryValueData, AdditionalFields, Severity, CloudResource, CloudPlatform, ResourceType, ResourceID, SubscriptionId |
| Alerts & behaviors | AlertInfo | Timestamp, AlertId, Title, Category, Severity, ServiceSource, DetectionSource, AttackTechniques |
| Alerts & behaviors | BehaviorEntities | Timestamp, BehaviorId, ActionType, Categories, ServiceSource, DetectionSource, DataSources, EntityType, EntityRole, DetailedEntityRole, FileName, FolderPath, SHA1, SHA256, FileSize, ThreatFamily, RemoteIP, RemoteUrl, AccountName, AccountDomain, AccountSid, AccountObjectId, AccountUpn, DeviceId, DeviceName, LocalIP, NetworkMessageId, EmailSubject, EmailClusterId, Application, ApplicationId, OAuthApplicationId, ProcessCommandLine, RegistryKey, RegistryValueName, RegistryValueData, AdditionalFields |
| Alerts & behaviors | BehaviorInfo | Timestamp, BehaviorId, ActionType, Description, Categories, AttackTechniques, ServiceSource, DetectionSource, DataSources, DeviceId, AccountUpn, AccountObjectId, StartTime, EndTime, AdditionalFields |
| Apps & identities | AADSignInEventsBeta | Timestamp, Application, ApplicationId, LogonType, EndpointCall, ErrorCode, CorrelationId, SessionId, AccountDisplayName, AccountObjectId, AccountUpn, IsExternalUser, IsGuestUser, AlternateSignInName, LastPasswordChangeTimestamp, ResourceDisplayName, ResourceId, ResourceTenantId, DeviceName, AadDeviceId, OSPlatform, DeviceTrustType, IsManaged, IsCompliant, AuthenticationProcessingDetails, AuthenticationRequirement, TokenIssuerType, RiskLevelAggregated, RiskLevelDuringSignIn, RiskEventTypes, RiskState, UserAgent, ClientAppUsed, Browser, ConditionalAccessPolicies, ConditionalAccessStatus, IPAddress, Country, State, City, Latitude, Longitude, NetworkLocationDetails, RequestId, ReportId |
| Apps & identities | AADSpnSignInEventsBeta | Timestamp, Application, ApplicationId, IsManagedIdentity, ErrorCode, CorrelationId, ServicePrincipalName, ServicePrincipalId, ResourceDisplayName, ResourceId, ResourceTenantId, IPAddress, Country, State, City, Latitude, Longitude, RequestId, ReportId |
| Apps & identities | CloudAppEvents | Timestamp, ActionType, Application, ApplicationId, AppInstanceId, AccountObjectId, AccountId, AccountDisplayName, IsAdminOperation, DeviceType, OSPlatform, IPAddress, IsAnonymousProxy, CountryCode, City, ISP, UserAgent, ActivityType, ActivityObjects, ObjectName, ObjectType, ObjectId, ReportId, AccountType, IsExternalUser, IsImpersonated, IPTags, IPCategory, UserAgentTags, RawEventData, AdditionalFields, SessionData, AuditSource, OAuthAppId, UncommonForUser, LastSeenForUser |
| Apps & identities | IdentityDirectoryEvents | Timestamp, ActionType, Application, TargetAccountUpn, TargetAccountDisplayName, TargetDeviceName, DestinationDeviceName, DestinationIPAddress, DestinationPort, Protocol, AccountName, AccountDomain, AccountUpn, AccountSid, AccountObjectId, AccountDisplayName, DeviceName, IPAddress, Port, Location, ISP, ReportId, AdditionalFields |
| Apps & identities | IdentityInfo | Timestamp, ReportId, AccountObjectId, AccountUpn, OnPremSid, AccountDisplayName, AccountName, AccountDomain, CriticalityLevel, Type, DistinguishedName, CloudSid, GivenName, Surname, Department, JobTitle, EmailAddress, SipProxyAddress, Address, City, Country, IsAccountEnabled, Manager, Phone, CreatedDateTime, SourceProvider, ChangeSource, BlastRadius, CompanyName, DeletedDateTime, EmployeeId, OtherMailAddresses, RiskLevel, RiskLevelDetails, State, Tags, AssignedRoles, PrivilegedEntraPimRoles |
| Apps & identities | IdentityLogonEvents | Timestamp, ActionType, Application, LogonType, Protocol, FailureReason, AccountName, AccountDomain, AccountUpn, AccountSid, AccountObjectId, AccountDisplayName, DeviceName, DeviceType, OSPlatform, IPAddress, Port, DestinationDeviceName, DestinationIPAddress, DestinationPort, TargetDeviceName, TargetAccountDisplayName, Location, ISP, ReportId, AdditionalFields, UncommonForUser, LastSeenForUser |
| Apps & identities | IdentityQueryEvents | Timestamp, ActionType, Application, QueryType, QueryTarget, Query, Protocol, AccountName, AccountDomain, AccountUpn, AccountSid, AccountObjectId, AccountDisplayName, DeviceName, IPAddress, Port, DestinationDeviceName, DestinationIPAddress, DestinationPort, TargetDeviceName, TargetAccountUpn, TargetAccountDisplayName, Location, ReportId, AdditionalFields |
| Email & collaboration | EmailAttachmentInfo | Timestamp, NetworkMessageId, SenderFromAddress, SenderDisplayName, SenderObjectId, RecipientEmailAddress, RecipientObjectId, FileName, FileType, SHA256, FileSize, ThreatTypes, ThreatNames, DetectionMethods, ReportId |
| Email & collaboration | EmailEvents | Timestamp, NetworkMessageId, InternetMessageId, SenderMailFromAddress, SenderFromAddress, SenderDisplayName, SenderObjectId, SenderMailFromDomain, SenderFromDomain, SenderIPv4, SenderIPv6, RecipientEmailAddress, RecipientObjectId, Subject, EmailClusterId, EmailDirection, DeliveryAction, DeliveryLocation, ThreatTypes, ThreatNames, DetectionMethods, ConfidenceLevel, BulkComplaintLevel, EmailAction, EmailActionPolicy, EmailActionPolicyGuid, AuthenticationDetails, AttachmentCount, UrlCount, EmailLanguage, Connectors, OrgLevelAction, OrgLevelPolicy, UserLevelAction, UserLevelPolicy, ReportId, AdditionalFields, LatestDeliveryLocation, LatestDeliveryAction, ExchangeTransportRule, DistributionList, ForwardingInformation, ThreatClassification |
| Email & collaboration | EmailPostDeliveryEvents | Timestamp, NetworkMessageId, InternetMessageId, Action, ActionType, ActionTrigger, ActionResult, RecipientEmailAddress, DeliveryLocation, ThreatTypes, DetectionMethods, ReportId, SenderFromAddress, EmailDirection |
| Email & collaboration | EmailUrlInfo | Timestamp, NetworkMessageId, Url, UrlDomain, UrlLocation, ReportId |
| Email & collaboration | UrlClickEvents | Timestamp, Url, ActionType, AccountUpn, Workload, NetworkMessageId, ThreatTypes, DetectionMethods, IPAddress, IsClickedThrough, UrlChain, ReportId |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Devices | DeviceEvents | Timestamp, DeviceId, DeviceName, ActionType, FileName, FolderPath, SHA1, SHA256, MD5, FileSize, AccountDomain, AccountName, AccountSid, RemoteUrl, RemoteDeviceName, ProcessId, ProcessCommandLine, ProcessCreationTime, ProcessTokenElevation, LogonId, RegistryKey, RegistryValueName, RegistryValueData, RemoteIP, RemotePort, LocalIP, LocalPort, FileOriginUrl, FileOriginIP, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessFolderPath, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessParentId, InitiatingProcessParentFileName, InitiatingProcessParentCreationTime, InitiatingProcessLogonId, ReportId, AppGuardContainerId, AdditionalFields, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, CreatedProcessSessionId, IsProcessRemoteSession, ProcessRemoteSessionDeviceName, ProcessRemoteSessionIP, InitiatingProcessUniqueId |
| Devices | DeviceFileCertificateInfo | Timestamp, DeviceId, DeviceName, SHA1, IsSigned, SignatureType, Signer, SignerHash, Issuer, IssuerHash, CertificateSerialNumber, CrlDistributionPointUrls, CertificateCreationTime, CertificateExpirationTime, CertificateCountersignatureTime, IsTrusted, IsRootSignerMicrosoft, ReportId |
| Devices | DeviceFileEvents | Timestamp, DeviceId, DeviceName, ActionType, FileName, FolderPath, SHA1, SHA256, MD5, FileOriginUrl, FileOriginReferrerUrl, FileOriginIP, PreviousFolderPath, PreviousFileName, FileSize, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessMD5, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessFolderPath, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessIntegrityLevel, InitiatingProcessTokenElevation, InitiatingProcessParentId, InitiatingProcessParentFileName, InitiatingProcessParentCreationTime, RequestProtocol, RequestSourceIP, RequestSourcePort, RequestAccountName, RequestAccountDomain, RequestAccountSid, ShareName, SensitivityLabel, SensitivitySubLabel, IsAzureInfoProtectionApplied, ReportId, AppGuardContainerId, AdditionalFields, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, InitiatingProcessUniqueId |
| Devices | DeviceImageLoadEvents | Timestamp, DeviceId, DeviceName, ActionType, FileName, FolderPath, SHA1, SHA256, MD5, FileSize, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessIntegrityLevel, InitiatingProcessTokenElevation, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessFolderPath, InitiatingProcessParentId, InitiatingProcessParentFileName, InitiatingProcessParentCreationTime, ReportId, AppGuardContainerId, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, InitiatingProcessUniqueId |
| Devices | DeviceInfo | Timestamp, DeviceId, DeviceName, ClientVersion, PublicIP, OSArchitecture, OSPlatform, OSBuild, IsAzureADJoined, JoinType, AadDeviceId, LoggedOnUsers, RegistryDeviceTag, OSVersion, MachineGroup, ReportId, OnboardingStatus, AdditionalFields, DeviceCategory, DeviceType, DeviceSubtype, Model, Vendor, OSDistribution, OSVersionInfo, MergedDeviceIds, MergedToDeviceId, IsInternetFacing, SensorHealthState, IsExcluded, ExclusionReason, ExposureLevel, AssetValue, DeviceManualTags, DeviceDynamicTags, HardwareUuid, CloudPlatforms, AzureVmId, AzureResourceId, AzureVmSubscriptionId, GcpFullResourceName, AwsResourceName, MitigationStatus, ConnectivityType, HostDeviceId, DiscoverySources, IsTransient, OsBuildRevision |
| Devices | DeviceLogonEvents | Timestamp, DeviceId, DeviceName, ActionType, LogonType, AccountDomain, AccountName, AccountSid, Protocol, FailureReason, IsLocalAdmin, LogonId, RemoteDeviceName, RemoteIP, RemoteIPType, RemotePort, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessIntegrityLevel, InitiatingProcessTokenElevation, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessFolderPath, InitiatingProcessParentId, InitiatingProcessParentFileName, InitiatingProcessParentCreationTime, ReportId, AppGuardContainerId, AdditionalFields, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, InitiatingProcessUniqueId |
| Devices | DeviceNetworkEvents | Timestamp, DeviceId, DeviceName, ActionType, RemoteIP, RemotePort, RemoteUrl, LocalIP, LocalPort, Protocol, LocalIPType, RemoteIPType, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessFolderPath, InitiatingProcessParentFileName, InitiatingProcessParentId, InitiatingProcessParentCreationTime, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessIntegrityLevel, InitiatingProcessTokenElevation, ReportId, AppGuardContainerId, AdditionalFields, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, InitiatingProcessUniqueId |
| Devices | DeviceNetworkInfo | Timestamp, DeviceId, DeviceName, NetworkAdapterName, MacAddress, NetworkAdapterType, NetworkAdapterStatus, TunnelType, ConnectedNetworks, DnsAddresses, IPv4Dhcp, IPv6Dhcp, DefaultGateways, IPAddresses, ReportId, NetworkAdapterVendor |
| Devices | DeviceProcessEvents | Timestamp, DeviceId, DeviceName, ActionType, FileName, FolderPath, SHA1, SHA256, MD5, FileSize, ProcessVersionInfoCompanyName, ProcessVersionInfoProductName, ProcessVersionInfoProductVersion, ProcessVersionInfoInternalFileName, ProcessVersionInfoOriginalFileName, ProcessVersionInfoFileDescription, ProcessId, ProcessCommandLine, ProcessIntegrityLevel, ProcessTokenElevation, ProcessCreationTime, AccountDomain, AccountName, AccountSid, AccountUpn, AccountObjectId, LogonId, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessLogonId, InitiatingProcessIntegrityLevel, InitiatingProcessTokenElevation, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessFolderPath, InitiatingProcessParentId, InitiatingProcessParentFileName, InitiatingProcessParentCreationTime, InitiatingProcessSignerType, InitiatingProcessSignatureStatus, ReportId, AppGuardContainerId, AdditionalFields, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, CreatedProcessSessionId, IsProcessRemoteSession, ProcessRemoteSessionDeviceName, ProcessRemoteSessionIP, ProcessUniqueId, InitiatingProcessUniqueId |
| Devices | DeviceRegistryEvents | Timestamp, DeviceId, DeviceName, ActionType, RegistryKey, RegistryValueType, RegistryValueName, RegistryValueData, PreviousRegistryKey, PreviousRegistryValueName, PreviousRegistryValueData, InitiatingProcessAccountDomain, InitiatingProcessAccountName, InitiatingProcessAccountSid, InitiatingProcessAccountUpn, InitiatingProcessAccountObjectId, InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5, InitiatingProcessFileName, InitiatingProcessFileSize, InitiatingProcessVersionInfoCompanyName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, InitiatingProcessVersionInfoInternalFileName, InitiatingProcessVersionInfoOriginalFileName, InitiatingProcessVersionInfoFileDescription, InitiatingProcessId, InitiatingProcessCommandLine, InitiatingProcessCreationTime, InitiatingProcessFolderPath, InitiatingProcessParentId, InitiatingProcessParentFileName, InitiatingProcessParentCreationTime, InitiatingProcessIntegrityLevel, InitiatingProcessTokenElevation, ReportId, AppGuardContainerId, AdditionalFields, InitiatingProcessSessionId, IsInitiatingProcessRemoteSession, InitiatingProcessRemoteSessionDeviceName, InitiatingProcessRemoteSessionIP, InitiatingProcessUniqueId |
| Cloud Infrastructure | CloudAuditEvents | Timestamp, AuditSource, DataSource, ActionType, OperationName, AzureResourceId, AwsResourceName, GcpFullResourceName, Account, IPAddress, IsAnonymousProxy, CountryCode, City, ISP, UserAgent, RawEventData, AdditionalFields, ReportId |
| Cloud Infrastructure | CloudProcessEvents | Timestamp, AzureResourceId, AwsResourceName, GcpFullResourceName, ContainerImageName, KubernetesNamespace, KubernetesPodName, KubernetesResource, ContainerName, ContainerId, ActionType, FileName, FolderPath, ProcessId, ProcessName, ParentProcessName, ParentProcessId, ProcessCommandLine, ProcessCreationTime, ProcessCurrentWorkingDirectory, AccountName, LogonId, InitiatingProcessId, AdditionalFields, ReportId |