

Advanced Threat Hunting Schema

Unable to do certain threat hunts as we only have a Defender Plan 1 license as part of Business Prem. Required E5.




Business Prem limits our hunts to specific schemas (tables) which don't include Device Events, Networking Events, Email Events, Email Attachment info and several others.

<https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-schema-tables>

What we currently have access to under Plan 1:

Schema reference

 Search table name

- AlertEvidence
- AlertInfo
- BehaviorEntities
- BehaviorInfo
- CloudAppEvents
- DeviceTvmInfoGathering
- DeviceTvmInfoGatheringKB
- DeviceTvmSecureConfigurationAssessment
- DeviceTvmSecureConfigurationAssessmentKB
- DeviceTvmSoftwareEvidenceBeta
- DeviceTvmSoftwareInventory
- DeviceTvmSoftwareVulnerabilities
- DeviceTvmSoftwareVulnerabilitiesKB
- ExposureGraphEdges
- ExposureGraphNodes
- IdentityInfo
- IdentityLogonEvents