Azure Sentinel and Azure Monitor Tables (bases Log Analytics)

Version 1.0 August 2020

Table Name	Description	Log Sources	Relevant Data	Billable
AuditLogs	Azure AD activities audit such as creation and modification of users, groups, applications	Azure AD	Account, Location, Activity	No
AWSCloudTrail	AWS CloudTrail log entries	AWS CloudTrail	Account, Location, Activity	Yes
AzureActivity	Azure activity such as creation/modification/deletion of Azure resources, policy updates	Azure	Account, Activity	Yes
AzureDiagnostics	Storage of diagnostic logs for Azure resources	Azure Resources	Diagnostic data	Yes
AzureMetrics	Provides storage of metrics recorded by various Azure resources	Azure Resources	Metrics	Yes
CommonSecurityLog	Logs from security devices logging via syslog using Common Event Format (CEF)	Security Devices	Source, Destination, Protocol, Action	Yes
ComputerGroup	Information on computer group membership	Azure AD	Account, Location, Activity	No
DnsEvents	Microsoft DNS events (registrations, configuration changes)	Microsoft DNS	DNS registrations, failures	Yes
DnsInventory	Log DNS records created on the DNS zone	Microsoft DNS	DNS records	Yes
Event	Windows event log entries (excluding Security event log)	Windows event logs	Errors, warnings	Yes
Heartbeat	Microsoft Monitoring Agent heartbeat	MMA agents	MMA health	No
McasShadowItReporting	MCAS Shadow IT information: records of access to applications typically used in “shadow IT”	MCAS	Application used, compliance	Yes
NetworkMonitoring	Network information on the monitored resources	Azure AD	Account, Location, Activity	No
OfficeActivity	Office 365 activity: Exchange, Sharepoint, DLP, OneDrive	Office 365	O365 user and admin activities	No
Operation	Records related the functionality of monitoring agent logs	Microsoft Monitoring Agents	Status of agents	Yes
Perf	Windows and Linux performance counters collected by MMA	Windows and Linux performance counters	Performance counter	Yes
ProtectionStatus	Azure Security Center records related to the status of endpoint protection solution on monitored endpoints	Azure Security Center (ASC)	Status of endpoint protection	Yes
SecurityAlert	Alert details (Sentinel, Security Center, MCAS, MSDATP, ATP, ADIP)	AS, ASC, MCAS, ATP, ATP	Alert details	Yes
SecurityBaseline	Azure Security Center records related status of monitored endpoints vs. configured policies for security baseline	Azure Security Center (ASC)	Status of updates vs. security baseline	No
SecurityBaselineSummary	Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies	Azure Security Center (ASC)	Policy compliance stats	Yes
SecurityDetection	Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints	Microsoft Defender ATP	Potential security issues	Yes
SecurityEvent	Window Security event logs entries	Windows Security Event log	Account, Source, Activity	Yes
SigninLogs	Azure Active Directory Sign In logs	Azure AD	Account, Source, Location, Activity	Yes
Syslog	Logs from syslog devices	Syslog-capable devices	Event, account, source, destination, action	Yes
ThreatIntelligenceIndicator	Used for ingestion of threat intel data from supported providers	Various TI sources	Malicious IP, Host, URL, Hash	Yes
Update	Azure Security Center missing/required updates (Windows, Linux)	Azure Security Center	Computer, Update	Yes
UpdateSummary	Azure Security Center records with the status of current updates for the monitored endpoints	Azure Security Center	Computer, Update	Yes
W3CIISLog	Microsoft IIS Logs	Microsoft IIS Logs	Source, Destination, URL, Status Code	Yes
WindowsFirewall	Microsoft Windows Firewall log entries (firewall running on endpoints)	Microsoft Firewall Logs	Traffic allowed and traffic dropped on endpoints	Yes