Azure Sentinel and Azure Monitor Tables (bases Log Analytics)

Version 1.0 August 2020

Azure Plagnostics Storage of diagnostic logs for Azure resources Provides storage of metrics recorded by various Azure Provides Security Devices Protocol, Action Yes Common Event Format (CEF) Protocol, Action Protocol, Action Yes Common Event Format (CEF) Protocol, Action Protocol, Activity Protocol, Action Protocol	Table Name	Description	Log Sources	Relevant Data	Billable
AWS CloudTrail AWS CloudTrail og entries Azure activity of Azure activity such as creation/modification/deletion Azure Azure Azure activity Azure activity such as creation/modification/deletion Azure Azure Azure azure Azure Resources Provides storage of metrics recorded by various Azure Azure Resources Azure AD Azcount, Location, Activity No Source, Destination, yes Ves Sourchy Destination, yes Ves Azure AD Azcount, Location, Activity Ves Azure AD Azount, Location, Activity Azordos Resources Azure Sourch Destination, yes Ves Azure AD Azordos Resources Azure Sourch Destination, yes Ves Azure AD Azordos Resources Azure Sourch Destination, yes Ves Azure AD Azordos Resources Azure Sourch Destination, yes Ves Azure AD Azordos Resources Azure Sourch Destination, Azivity Azordos Resources Azure Sourch Destination, Azivity Azordos Resources Azure Sourch Center (ASC) Azure AD Azordos Resources Azure Sourch Center (ASC) Azure AD Azordos Resources Azure Sourch Center (ASC) Azure AD Azordos Resources Azure Sourch Center Azure Sourch Center (ASC) Azure AD Azordos Resources Azure Sou	AuditLogs		Azure AD		No
Azure Activity of Azure activity such as creation/modification/deletion of Azure Azure Account, Activity Yes AzureAzureAzure of diagnostic logs for Azure resources Azure resources Diagnostic data Yes Provides storage of metrics recorded by various Azure resources Metrics Source, Destination, Yes CommonSecurityLog Common Event Format (IEF) Security Devices Protocol, Action Yes Protocol, Action On Computer group membership Azure AD Account, Location, Activity No Microsoft DNS events (registrations, configuration Changes) Microsoft DNS events (registrations, configuration Changes) Microsoft DNS events (registrations, configuration Changes) Microsoft DNS DNS registrations, failures Yes Protocol, Action Yes Protocol, Action On No Microsoft DNS events (registrations, configuration Changes) Microsoft DNS DNS registrations, failures Yes Dnsimentory Log DNS records created on the DNS zone Microsoft DNS DNS registrations, failures Yes Protocol Microsoft Monitoring Agent heartbeat Microsoft Monitoring Agent Microsoft Monitoring Agent Microsoft Monitoring Agent Microsoft Monitori			AVAC Classed Tracil		V
AzureActivity of Azure resources, policy updates Azure Azure Account, Activity Yes AzureDiagnostics Storage of diagnostic logs for Azure resources Azure Resources Diagnostic data Yes resources Provides storage of metrics recorded by various Azure resources Azure Resources Diagnostic data Yes resources of metrics recorded by various Azure Resources Metrics Yes Sucre, Destination, Common Event Format (CEF) Security Devices Protocol, Action Yes ComputerGroup Information on computer group membership Azure AD Account, Location, Activity No ComputerGroup Information on computer group membership Azure AD Account, Location, Activity No Changes) Microsoft DNS events (registrations, configuration Changes) DNS registrations, failures Ves DNS registrations, failures Ves Windows event log entries (excluding Security event log) Windows event logs Errors, warnings Ves Heartbeat Microsoft Monitoring Agent heartbeat MMA agents MMA health No AMAS Shadow IT information: records of access to Application used, compliance yes applications typically used in "shadow IT" MCAS compliance Yes MacaShadowtReporting NetworkInformation: records of access to Application used, compliance Yes Azure AD Account, Location, Activity No Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of the Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Windows and Linux performance counters of Microsoft Monitoring Agent heartbeat Status of monitoring Agent logs Agents	AWSCIOUGITAII		AWS Cloud Frail	Account, Location, Activity	Yes
AzureMetrics resources Azure AD Account, Location, Activity No Azure AD Account, Coation, Activity No Azure AD Azcount, Coation, Activity No Azure AD Azero AD Azcount, Coation, Activity No Azure AD Azero A	AzureActivity		Azure	Account, Activity	Yes
Azure Mesources Metrics Yes CommonSecurityLog Common Event Format (CEF) Security Devices Se	AzureDiagnostics		Azure Resources	Diagnostic data	Yes
CommonsecurityLog Common Event Format (CEF) Security Devices Protocol, Action Yes ComputerGroup Information on computer group membership Azure AD Account, Location, Activity No 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 Event Microsoft Monitoring Agent heartbeat Microsoft DNS DNS records Yes Event Microsoft Monitoring Agent heartbeat Microsoft DNS DNS records Yes Event Microsoft Monitoring Agent heartbeat Microsoft DNS DNS records Yes Event Microsoft Monitoring Agent heartbeat Microsoft DNS DNS records MMA health No MCAS Shadow IT information: records of access to applications typically used in "Shadow IT" MCAS NetworkMonitoring Network information on the monitored resources Azure AD Account, Location, Activity No Office Activity Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 Records related the functionality of monitoring agent logs Windows and Linux performance counters collected by Windows and Linux performance counters collected by Windows and Linux performance counters of Microsoft Monitoring Agent Sature of Event details (Sentier), Event Event Monitoring Agent Sature of Event details (Sentier), Event Event Monitoring Agent Sature of Event details (Sentier), Event Event Monitoring Agent Sature of Event details (Sentier), Event Event Monitoring Agent Sature of Event details (Sentier), Event Event Monitoring Agent Sature of Event details (Sentier), Event	AzureMetrics	resources	Azure Resources		Yes
Microsoft DNS events (registrations, configuration changes)	CommonSecurityLog		Security Devices		Yes
Dissivents changes) Microsoft DNS DNS registrations, failures Yes Dinsinventory Log DNS records created on the DNS zone Event Windows event log entries (excluding Security event log) Windows event logs Errors, warnings Yes Event Microsoft Monitoring Agent heartbeat McAS Shadow IT information: records of access to Application sypically used in 'shadow IT' McAS Shadow IT information: records of access to Application sypically used in 'shadow IT' McAS Shadow IT information: records of access to Application used, compliance Yes McAS Compliance Yes McAS Compliance Yes McAS Compliance Yes NetworkMonitoring Network information on the monitored resources Azure AD Account, Location, Activity No Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 Microsoft Monitoring Agents Microsoft Monitoring Agents Status of agents Agents Status of agents Yes Windows and Linux performance counters collected by Perf MAA Azure Security Center records related to the status of Azure Security Center Azure Security Center records related to the status of Azure Security Center Arp ADIP) Alert details (Sentinel, Security Center, MCAS, MSDATP, ATP Alert details Yes Security Resellinesummary Security Resellinesummary Microsoft Defender ATP logs for potential security issues Account, Source, Jocation, Azure Security Center Microsoft Defender ATP logs for potential security issues Microsoft Defender Azure Security Center records with statistics for the monitored endpoints with compliance and configured Security Petection Microsoft Defender ATP logs for potential security issues Microsoft Defender Azure Security Center records with statistics for the monitored endpoints with compliance and configured Microsoft Defender Azure AD Account, Source, Location, Azure AD Account, Source, Location, Activity Yes Security Center (Security Center missing/required upd	ComputerGroup		Azure AD	Account, Location, Activity	No
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 MCAS Shadow IT information: records of access to application super, application stepically used in "shadow IT" MCAS compliance Yes NetworkMonitoring Network information on the monitored resources Azure AD Account, Location, Activity No Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 activities No Microsoft Monitoring Agents Status of agents Yes Windows and Linux performance counters collected by MMA Part Security Center records related to the status of endpoint protection solution on monitored endpoints (ASC) ProtectionStatus endpoints yes configured policies for security Daseline Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies for security baseline Microsoft Defender ATP logs for potential security issues Security Detection detected on the monitored endpoints with compliance and configured policies for security security Center (ASC) Policy compliance stats Yes Windows Security Center records with statistics for the monitored endpoints with compliance and configured policies for security issues Microsoft Defender ATP logs for potential security issues Microsoft Defender ATP logs for potential security issues Microsoft Defender ATP logs for potential security issues Signinlogs Azure Activity Vest (Syslog Capable devices destination, action Yes Syslog Logs from syslog devices With statistics for security Center (ASC) Policy Cent	DnsEvents		Microsoft DNS	DNS registrations, failures	Yes
Heartbeat Microsoft Monitoring Agent heartbeat MMA agents MMA health No MCAS Shadow IT information: records of access to application used, application stypically used in "shadow IT" MCAS compliance Yes NetworkMonitoring Network information on the monitored resources Azure AD Account, Location, Activity No Office Activity: Exchange, Sharepoint, DLP, OneDrive Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 activities No Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 activities No No Office 365 activities No Office 365 activities No No No Office 365 activity No	DnsInventory	Log DNS records created on the DNS zone	Microsoft DNS	DNS records	Yes
McasShadowltReporting applications typically used in "shadow IT" MCAS compliance yes applications typically used in "shadow IT" MCAS compliance yes applications typically used in "shadow IT" MCAS compliance yes applications typically used in "shadow IT" MCAS compliance yes applications typically used in "shadow IT" MCAS compliance yes applications typically used in "shadow IT" MCAS compliance yes applications typically used in "shadow IT" MCAS compliance yes application on the monitored resources application on the monitored resources of the provided in the provided i	Event	Windows event log entries (excluding Security event log)	Windows event logs	Errors, warnings	Yes
McasShadowitReporting applications typically used in "shadow IT" MCAS compliance Yes NetworkMonitoring Network information on the monitored resources Azure AD Account, Location, Activity No Office 365 Office 365 activities No Operation Records related the functionality of monitoring agent logs Microsoft Monitoring Status of agents Yes Perf MMA Windows and Linux performance counters collected by MMA Performance counters Performance counters Performance counters Yes ProtectionStatus Azure Security Center records related to the status of endpoints protection solution on monitored endpoints Azure Security Center (ASC) Ferformance counters Yes SecurityAlert ATP, ADIP) AZURE Security Center records related status of monitored endpoints ASC, MCAS, ATP, ALIP ALIP ALIP	Heartbeat		MMA agents		No
Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Office 365 microsoft Monitoring Records related the functionality of monitoring agent logs Windows and Linux performance counters collected by Perf MMA Azure Security Center records related to the status of endpoint protection solution on monitored endpoints Alert details (Sentine), Security Center, MCAS, MSDATP, ATP, ADIP) Azure Security Center, Ecords related status of endpoint protection solution on monitored endpoints SecurityBaseline Azure Security Center, MCAS, MSDATP, ATP, ADIP) Azure Security Center records related status of monitored endpoints vs. configured policies for security baseline endpoints vs. configured policies for security baseline Microsoft Defender ATP logs for potential security issues SecurityDetection detected on the monitored endpoints SecurityEvent Window Security event logs entries Windows Security SecurityEvent Window Security event logs entries SecurityEvent Window Security event logs entries Security Event (account, Source, Activity) SigninLogs Azure Azure Azure Account, Source, Activity Yes Syslog Logs from syslog devices Azure Security Center (account, source, Activity) Yes Syslog Logs from syslog devices Azure Azure Azure Security Center (account, source, Activity) Azure Security Center (account, source, Activity) Azure Security Center missing/required updates (Windows, Linux) Azure Security Center records with the status of current updates for the monitored endpoints Azure Security Center records with the status of current updates for the monitored endpoints Microsoft IIS Logs Microsoft IIS Logs Microsoft IIS Logs Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	McasShadowItReporting		MCAS	T 1	Yes
OfficeActivity Office 365 activity: Exchange, Sharepoint, DLP, OneDrive Records related the functionality of monitoring agent logs Windows and Linux performance counters collected by MMA Aure Security Center records related to the status of endpoint protection solution on monitored endpoints Alert details (Sentinel, Security Center, MCAS, MSDATP, ATP, ADIP) Azure Security Center records related status of endpoint vs. configured policies for security baseline Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies of edecated on the monitored endpoints SecurityBaselineSummary SecurityBaselineSummary Microsoft Defender ATP logs for potential security issues Azure Security center logs entries SecurityEvent Window Security event logs entries Microsoft Defender Azure Azure Azure Security Center logs entries SecurityEvent Window Security event logs entries SigninLogs Azure Security Center logs entries Azure Azure Security Center logs entries SecurityEvent Window Security event logs entries SigninLogs Azure Security Center logs entries Azure Azure Security Center logs entries SecurityEvent Window Security event logs entries Azure Azure Security Event log Azure Azure Security Event log Azure Azure Security Event log Azure Security Event log Azure Azure Security Event log Azure Security Center missing/required updates (Windows, Linux) Azure Security Center records with the status of current updates for the monitored endpoints Microsoft IIS Logs Microsoft IIS Logs Microsoft Eirewall Traffic allowed and traffic	NetworkMonitoring	Network information on the monitored resources	Azure AD		No
Perf Windows and Linux performance counters collected by Windows and Linux performance counters collected by MMA performance counters Performance co	OfficeActivity	Office 365 activity: Exchange, Sharepoint, DLP, OneDrive			No
Perf MMA Azure Security Center records related to the status of endpoint protection solution on monitored endpoints endpoint protection solution on monitored endpoints endpoint protection solution on monitored endpoints Alert details (Sentinel, Security Center, MCAS, MSDATP, ATP, ADIP) Azure Security Center records related status of monitored endpoints vs. configured policies for security baseline Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies Acure Security Center records with statistics for the monitored endpoints with compliance and configured policies Acure Security Center records with statistics for the monitored endpoints with compliance and configured Acure Security Center records with statistics for the monitored endpoints with compliance and configured Acure Security Center records with statistics for the monitored endpoints with compliance and configured Acure Security Center records with statistics for the monitored endpoints with compliance and configured Acure Security Center records with statistics for the monitored endpoints with compliance and configured Acure Security Center records with statistics for the monitored endpoints Acure Security Center records with statistics for the monitored endpoints Acure Active Directory Sign In logs Acure Active Directory S	Operation	Records related the functionality of monitoring agent logs		Status of agents	Yes
ProtectionStatus endpoint protection solution on monitored endpoints Alert details (Sentinel, Security Center, MCAS, MSDATP, ATP, ADIP) ATP, ADIP) ATP, ADIP) ATP, ADIP) ATP, ADIP) AZure Security Center records related status of monitored endpoints vs. configured policies for security baseline Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies SecurityBaselineSummary SecurityBaselineSummary Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints SecurityEvent Window Security SecurityEvent Window Security event logs entries Azure Azure Azure Active Directory Sign In logs Azure Azure Azure Azure Azure Azure Azure Security Center Azure Azu	Perf	·		Performance counter	Yes
Alert details (Sentinel, Security Center, MCAS, MSDATP, ATP, ADIP) Azure Security Center records related status of monitored endpoints vs. configured policies for security baseline (ASC) security baseline (ASC) security baseline (ASC) SecurityBaselineSummary SecurityBaselineSummary SecurityBaselineSummary SecurityBaselineSummary SecurityBaselineSummary SecurityBaselineSummary Microsoft Defender ATP logs for potential security issues Microsoft Defender ATP ACCOUNT, Source, Activity Yes Microsoft Defender ATP ACCOUNT, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP ACCOUNT, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP Account, Source, Defender ATP Account, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP Account, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP Account, Source, Activity Yes Account, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP Account, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP Account, Source, Activity Yes Account, Source, Activity Yes Account, Source, Activity Yes Microsoft Defender ATP Account, Source, Account, Source, Activity Yes Account, Sour	ProtectionStatus	1	· ·		,,
SecurityAlert ATP, ADIP) ATP Alert details Yes Azure Security Center records related status of monitored endpoints vs. configured policies for security baseline (ASC) security baseline Security Center records with statistics for the monitored endpoints with compliance and configured policies for security issues of the monitored endpoints with compliance and configured policies (ASC) Policy compliance stats Yes SecurityBaselineSummary policies Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Microsoft Defender ATP Potential security issues Windows Security SecurityEvent Window Security event logs entries Event log Account, Source, Activity Yes SigninLogs Azure Active Directory Sign In logs Azure AD Activity Yes Syslog-capable Event, account, source, devices destination, action Yes Used for ingestion of threat intel data from supported providers Various TI sources Hash Yes Update (Windows, Linux) Azure Security Center Computer, Update Yes Wicrosoft IIS Logs Microsoft IIS Logs Microsoft IIS Logs Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic			_ ' _ '	protection	Yes
SecurityBaseline endpoints vs. configured policies for security baseline (ASC) security baseline No Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies (ASC) Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints SecurityDetection detected on the monitored endpoints Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Microsoft Defender ATP Potential security issues Yes Windows Security Event log Account, Source, Activity Yes Account, Source, Location, Activity Yes Syslog Azure Active Directory Sign In logs Azure Azur	SecurityAlert	, , , , , , , , , , , , , , , , , , , ,		Alert details	Yes
Azure Security Center records with statistics for the monitored endpoints with compliance and configured policies Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Mindows Security Maccount, Source, Destination Mindows Security Maccount, Source, Destination Mindows Security Mindows Security Mindo		Azure Security Center records related status of monitored	Azure Security Center	Status of updates vs.	
monitored endpoints with compliance and configured policies Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Microsoft Defender ATP Potential security issues Yes Windows Security Event log Account, Source, Activity Yes Account, Source, Location, Activity Yes Syslog Logs from syslog devices Used for ingestion of threat intel data from supported providers Update Update Update Microsoft IIS Logs Microsoft IIS Logs Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Microsoft Firewall Microsoft Firewall Azure Security Center (ASC) Policy compliance stats Yes Account, Source, Stats Yes Account, Source, Activity Yes Account, Source, Activity Yes Account, Source, Deatination, URL, Vestination, action Yes Activity Yes Activity Yes Activity Yes Account, source, destination, action Yes Acure Security Center Computer, Update Yes Source, Destination, URL, Yes Microsoft IIS Logs Microsoft Firewall Traffic allowed and traffic	SecurityBaseline		(ASC)	security baseline	No
SecurityBaselineSummary policies (ASC) Policy compliance stats Yes Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints ATP Potential security issues Yes Windows Security Event log Account, Source, Activity Yes SigninLogs Azure Active Directory Sign In logs Azure AD Accivity Yes Syslog Logs from syslog devices Syslog-capable devices destination, action Yes ThreatIntelligenceIndicator Directory Sign In logs Azure Security Center missing/required updates (Windows, Linux) Azure Security Center records with the status of current updates for the monitored endpoints Azure Security Center Source, Destination, URL, Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic		1			
Microsoft Defender ATP logs for potential security issues detected on the monitored endpoints Microsoft Defender ATP Potential security issues Yes Windows Security Event log Account, Source, Activity Yes Account, Source, Activity Yes Account, Source, Location, Activity Yes Syslog Logs from syslog devices Used for ingestion of threat intel data from supported providers Acure Security Center missing/required updates Update (Windows, Linux) Account, Source, Activity Yes Account, Source, Activity Yes Account, Source, Location, Activity Yes Syslog-capable devices Event, account, source, destination, action Malicious IP, Host, URL, Hash Yes Acure Security Center Update (Windows, Linux) Acure Security Center Updates or the monitored endpoints Acure Security Center Acure Security Center Computer, Update Yes Source, Destination, URL, Status Code Yes Microsoft IIS Logs Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic			-		.,
SecurityDetection detected on the monitored endpoints ATP Potential security issues Yes Windows Security Event log Account, Source, Activity Yes Account, Source, Activity Yes Account, Source, Location, Activity Yes Account, Source, Location, Activity Yes Account, Source, Location, Activity Yes Syslog-capable Event, account, source, devices destination, action Yes Used for ingestion of threat intel data from supported providers Update (Windows, Linux) Azure Security Center missing/required updates (Windows Security Event log Account, Source, Activity Yes Syslog-capable Event, account, source, devices destination, action Yes Malicious IP, Host, URL, Yes Azure Security Center missing/required updates (Windows, Linux) Azure Security Center Computer, Update Yes Azure Security Center Computer, Update Yes Source, Destination, URL, Source, Destination, URL, Source, Destination, URL, Source, Destination, URL, Status Code Yes Microsoft IIS Logs Microsoft IIS Logs Microsoft Firewall Traffic allowed and traffic	SecurityBaselineSummary		, ,	Policy compliance stats	Yes
SecurityEventWindow Security event logs entriesEvent logAccount, Source, ActivityYesSigninLogsAzure Active Directory Sign In logsAzure ADActivityYesSyslog-capableEvent, account, source, devicesEvent, account, source, devicesEvent, account, source, devicesUsed for ingestion of threat intel data from supported providersMalicious IP, Host, URL, HashYesThreatIntelligenceIndicatorAzure Security Center missing/required updates (Windows, Linux)Azure Security CenterComputer, UpdateYesUpdateAzure Security Center records with the status of current updates for the monitored endpointsAzure Security CenterComputer, UpdateYesW3CIISLogMicrosoft IIS LogsMicrosoft IIS LogsStatus CodeYesMicrosoft Windows Firewall log entries (firewall runningMicrosoft FirewallTraffic allowed and traffic	SecurityDetection	· · · · · · · · · · · · · · · · · · ·	ATP	Potential security issues	Yes
Azure Active Directory Sign In logs Azure AD Activity Yes Syslog-capable devices Used for ingestion of threat intel data from supported providers Azure Security Center missing/required updates (Windows, Linux) Azure Security Center records with the status of current updates for the monitored endpoints Walcious IP, Host, URL, Hash Yes Azure Security Center Computer, Update Yes Source, Destination, action Yes Azure Security Center Computer, Update Yes Microsoft IIS Logs Microsoft IIS Logs Microsoft Firewall Microsoft Firewall Traffic allowed and traffic	SecurityEvent	Window Security event logs entries	,	Account, Source, Activity	Yes
Syslog-capable devices destination, action Yes Used for ingestion of threat intel data from supported providers Various TI sources Hash Yes Azure Security Center missing/required updates (Windows, Linux) 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 Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic				Account, Source, Location,	
Syslog Logs from syslog devices devices destination, action Yes Used for ingestion of threat intel data from supported providers Various TI sources Hash Yes Azure Security Center missing/required updates (Windows, Linux) 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 Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	SigninLogs	Azure Active Directory Sign In logs		•	Yes
ThreatIntelligenceIndicator providers Various TI sources Hash Yes Azure Security Center missing/required updates (Windows, Linux) Azure Security Center Computer, Update Yes 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 Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	Syslog				Yes
Azure Security Center missing/required updates (Windows, Linux) Azure Security Center Azure Security Center Azure Security Center Azure Security Center Computer, Update Yes Azure Security Center UpdateSummary Updates for the monitored endpoints Azure Security Center Computer, Update Yes Source, Destination, URL, Source, Destination, URL, Microsoft IIS Logs Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	ThroatIntolligoncolndicator		Various Tl savrage		Voc
Update (Windows, Linux) Azure Security Center Computer, Update Yes Azure Security Center records with the status of current updates for the monitored endpoints Azure Security Center Computer, Update Yes Source, Destination, URL, W3CIISLog Microsoft IIS Logs Microsoft IIS Logs Microsoft Firewall Microsoft Firewall Traffic allowed and traffic	inreatintelligenceindicator	'	various 11 sources	паSП	res
UpdateSummary updates for the monitored endpoints Azure Security Center Computer, Update Yes W3CIISLog Microsoft IIS Logs Microsoft IIS Logs Microsoft IIS Logs Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	Update	(Windows, Linux)	Azure Security Center	Computer, Update	Yes
W3CIISLog Microsoft IIS Logs Microsoft IIS Logs Microsoft IIS Logs Status Code Yes Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	UpdateSummary		Azure Security Center	Computer, Update	Yes
Microsoft Windows Firewall log entries (firewall running Microsoft Firewall Traffic allowed and traffic	· ·		,	Source, Destination, URL,	
				I .	Yes
windows newall on endpoints logs dropped on endpoints res	WindowsFirewall	Microsoft Windows Firewall log entries (firewall running on endpoints)	Microsoft Firewall Logs	Traffic allowed and traffic dropped on endpoints	Yes