tables

CommonSecurityLog

This table is for collecting events in the Common Event Format, that are most often sent from different security appliances such as Check Point, Palo Alto and more.

- **SigninLogs** — This table contains al the signin logs of the Azure Active Directory. You will find here which user have tried to login using the Azure Active Directory, from which IP and with what device. Also the result of the login attempt is logged over here.

```
// show all successful logins in the Azure portal
SigninLogs
| where AppDisplayName == "Azure Portal"
    and ResultType == 0



    SigninLogs
```

```
| where RiskLevelDuringSignIn == 'none'
| take 5
```

- **AuditLogs** — This table contains the audit log of the Azure Active Directory. You will find here all changes that happened to the Azure Active Directory (e.g users created, users added to groups etc.). Azure AD Privileged Identity Management is also sending its logs to this table.

```
// show all newly created users
AuditLogs
| where OperationName == "Add user"// show all PIM requests
AuditLogs
| where OperationName == "Add member to role requested (PIM a
ctivation)"
     or OperationName == "Remove member from role completed
(PIM deactivate)"
| extend Account = tostring(InitiatedBy.["user"].["userPrinci
palName"])
| distinct TimeGenerated, Account, ResultDescription
```

- **AzureActivity** — This table contains the audit log of the Azure Resource Manager. All activities executed trough the Azure Resource Manager send to this table (e.g. VM deployed, App Service updated, ARM template deployed etc.). Note that Azure Policy is sending log data to this table and permission/RBAC changes in Azure are also logged into this table.

```
// show all password resets on linux VMs
AzureActivity
| where Resource contains "VMAccessLinuxPasswordReset"
    and ActivityStatus == "Succeeded"// Show all new Azure Ro
le assignments
AzureActivity
| where ResourceProvider == "Microsoft.Authorization'
    and OperationNameValue == "Microsoft.Authorization/roleAs
```

```
signments/write"
    and ActivityStatus == "Succeeded"
```

- **OfficeActivity** — This is the table that contains al Office 365 related events. At the moment of writing the following applications will write logs to this table: Microsoft Exchange 365, Microsoft SharePoint 365 and OneDrive. In this table you wil find both the operational events as the audit events as well.

```
// Get all Exchange related events
OfficeActivity
| where OfficeWorkload == "Exchange"// Get all SharePoint and
OneDrive related events
OfficeActivity
| where OfficeWorkload == "SharePoint"// Get all OneDrive rel
ated Events
OfficeActivity
| where OfficeWorkload == "SharePoint" or OfficeWorkload ==
"OneDrive"
| sort by TimeGenerated


OfficeActivity
| where Operation contains "upload" and SourceFileExtension h
as_any (".exe",".msi")

File Extension modified into an Executable.txt:
OfficeActivity
| where  Operation =~ "FileRenamed" and DestinationFile Exten
sion has_any (Common Executables) and DestinationFileExtensio
n != SourceFileExtension and (SourceFileExtension != "Ink" an
d DestinationFileExtension != "url")
```

- **SecurityEvents** — As you have connected Windows machines to the Log Analytics workspace that is being used by Azure Sentinel, security events out of the Windows Eventlog are forwarded to this table.

```
// Get all login events that are not produced by NT Authority
\System
SecurityEvent
| where EventID == "4624"
    and Account <> "NT AUTHORITY\\SYSTEM"
```

- **Syslog** — If you have any Linux machines connected to Log Analytics, this table contains all events that are forwarded by Syslog. Note that Syslog is not limited to Linux machines. Some network devices will also use syslog. You probably need a syslog forwarder service in order to hook these devices up to Log Analytics.

```
// Get all logs from the cron deamon in linux
Syslog
| where ProcessName == "CRON"
```

- **SecurityAlerts** — As you have connected Microsoft security products such as Defender ATP, Azure AD Identity Protection, Cloud App Security etc. this table will contain the alerts that have been generated by these products. Sentinel self will also log its incidents to this table.

```
// Get all alerts reported by Microsoft Cloud App Security
SecurityAlert
| where ProviderName == "MCAS"// Get all alerts reported by S
entinel
SecurityAlert
| where ProviderName == "Azure Sentinel"
```

- **AzureDiagnostics** — This table contains diagnostic data from all resources that have been configured to send diagnostic logs to your log analytics workspace. E.g. logs of your Azure SQL database resource is logged to this table. This is the legacy table where a lot of resources write their logs to. Most of the new resources will write their logs to their own dedicated tables.

```
// Get all SQL successfull authentications
AzureDiagnostics
| where clientIP_s != ""
| where ResourceProvider == "MICROSOFT.SQL"
and action_name_s == "DATABASE AUTHENTICATION SUCCEEDED"
```

ThreatIntelligenceIndicator — This is a table that is being used by Azure Sentinel to store custom threat intelligence. Threat intelligence of various services such as MISP and Minemeld can be forwarded to Azure Sentinel. As data is forwarded, it is stored in this table. You can use this table to match ip-addresses, file hashes etc. that are threat indicators with ip addresses that are being used in your environment.

```
// Show a limited set of data that is in the threat intellige
nce table
ThreatIntelligenceIndicator
| limit 50
```

DeviceNetworkEvents
| where RemoteIP == "insert destination IPv4 address here"

| where RemotePort == "insert destination port number here”

DeviceNetworkEvents
| where RemoteUrl has "insert URL here"

EmailEvents
// Choose one or more of the following options to detect malicious email deliveries
| where SenderFromAddress has "insert sender email here"
| where SenderIPv4 == "insert sending server IP here"
| where SenderMailFromAddress has "insert envelope sender email here"

Email attachment

If you already know the SHA256 hash of a malicious email attachment, the following query will detect relevant email deliveries.

EmailAttachmentInfo
| where SHA256 == "insert SHA256 hash here"

DeviceLogonEvents
// Choose to see local sign ins by host, or by username
// If you know the exact device name, you may use "has" instead of "contains"
| where DeviceName contains "insert part of device name here"
| where AccountName == "insert the username here"

Cloud user sign in

There are cases where you might need to look into suspicious sign ins, an IP address or a source country accessing your Microsoft Cloud environment could be an incident precursor.

```
AADSignInEventsBeta
| where IPAddress == "insert suspicious IP address here"
// To choose the Country, insert the ISO 3166 country code [h
ttps://en.wikipedia.org/wiki/List_of_ISO_3166_country_codes]
| where Country == "insert ISO country code"
```

File hash

If you need to search for a specific file hash, whether you have SHA256, SHA1 or MD5, you can use the following query to hunt.

```
DeviceFileEvents
// Replace SHA256 with SHA1 or MD5, depending on what you hav
e available
| where SHA256 == "insert hash here"
```

Process injection

If you have a clue of a malicious activity involving process injection, or if you would like to hunt following a report you might have gone through, the following query could help you in your quest.

```
DeviceProcessEvents
| where InitiatingProcessParentFileName contains "insert file name here"
| where InitiatingProcessFileName contains "insert filename here"
```

DnsEvents
| where EventId !in ('list', 'expected', 'eventIDs', 'generated', 'in', 'your', 'dataset')

HTTP PUT POST Threat Hunt.txt

DNSLogs
| where Request_Method in ('PUT', 'POST')

Brute Force on Password Protected Office Apps.txt

Event
| where Source matches regex @"office" or EventLog matches regex @"office" and EventID == 300 and (RenderedDescription contains "password" or EventData contains "password" or ParameterXml contains "password")

Sentinel Table	Description	Log Sources	Relevant Data	Billable
AuditLogs	Azure AD activities audit such as creation/modification of users, groups, applications	Azure AD	Account, Location, Activity	Yes
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	No
AzureDiagnostics	Storage of diagnostic logs for Azure resources (resources have to be configured to send the diagnostics logs to the specific Log Analytics workspace)	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 (as configured in the Log Analytics workspace data collection)	Azure AD	Account, Location, Activity	No
DnsEvents	Microsoft DNS events (registrations, configuration changes). Note: DNS queries outside the authoritative zone are not recorded.	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" (filesharing, meetings, etc.)	MCAS	Application used, compliance	Yes
NetworkMonitoring	Network information on the monitored resources	Azure AD	Account, Location, Activity	Yes
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 (data collection, availability, issues)	Microsoft Monitoring Agents	Status of Sentinel agents	No
Perf	Windows and Linux performance counters collected by MMA	Windows and Linux performance counters	Performance counters	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	No
SecurityBaseline	Azure Security Center records related status of monitored endpoints vs. configured policies for security baseline (levels of patching, etc.)	Azure Security Center (ASC)	Status of updates vs. security baseline	No
SecurityBaselineSummary	Azure Security Center records with statistics for the monitored endpoints related to compliance with 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 (MISP, MineMeld, etc.)	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