Sophos osquery Extension: Table Schema

sophos_directory_journal

Description

Directory events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the directory event occured If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: created(0), renamed(1), deleted(2), permissionsModified(3), ownershipModified(4)
PID	unsigned_bigint	The ID of the process that modified the directory
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that modified the directory
sophosPID	text	The ID of the process that modified the directory and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread that opened the handle to the directory
sophosTID	text	Hidden The ID of the thread that opened the handle to the directory and its start time creating a unique identifier
pathname	text	The pathname of the directory
size	unsigned_bigint	The size in bytes of the directory
targetPathname	text	The new directory path after a rename event Only populated for events with eventType(s): renamed (1)
fileId	text	The fileId of the directory
creationTime	unsigned_bigint	The time (unix epoch) the directory was created
lastAccessTime	unsigned_bigint	The time (unix epoch) the directory was last accessed
lastWriteTime	unsigned_bigint	The time (unix epoch) the directory was last written to
changeTime	unsigned_bigint	The time (unix epoch) the directory was last changed
numberOfHardLinks	integer	The number of hardlinks for the directory

Column	Type	Description
fileAttributes	integer	The file attributes as a bit mask: READONLY(0x00000001), HIDDEN(0x00000002), SYSTEM(0x00000004), DIRECTORY(0x00000010), ARCHIVE(0x00000020), DEVICE(0x00000040), NORMAL(0x00000080), TEMPORARY(0x00000100), SPARSE_FILE(0x00000200), REPARSE_POINT(0x00000400), COMPRESSED(0x00000800), OFFLINE(0x00001000), NOT_CONTENT_INDEXED(0x00002000), ENCRYPTED(0x00004000), VIRTUAL(0x00010000)
fileType	integer	The file type as an integer: unknown(0), portable executable (WINPE)(1), executable and linkable format (ELF binary)(2)
fileTypeClass	integer	The file type class as an integer: unknown(0), directory(1), binary(2), data(3), other(4)
dacl	text	The file discretionary access control list as a string Only populated for events with eventType(s): permissionsModified(3)
owner	text	The owner of a directory as a SID Populated for events with eventType(s): ownershipModified(4) Can be populated for eventType(s): permissionsModified(3)
newCreationTime	unsigned_bigint	The time (unix epoch) the new directory was created
newLastAccessTime	unsigned_bigint	The time (unix epoch) the new directory was last accessed
newLastWriteTime	unsigned_bigint	The time (unix epoch) the new directory was last written to
newChangeTime	unsigned_bigint	The time (unix epoch) the new directory was changed

Example

```
SELECT
    *
FROM
    sophos_directory_journal
WHERE
    time > 1559641265
```

sophos_dns_journal

Description

Dns events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: request(0)
PID	unsigned_bigint	The ID of the process that produced the dns event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the dns event
sophosPID	text	The ID of the process that produced the dns event and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread that produced the dns event
sophosTID	text	Hidden The ID of the thread that produced the dns event and its start time creating a unique identifier
name	text	The name of the domain name system that made the request

Example

```
SELECT
    *
FROM
    sophos_dns_journal
WHERE
    time > 1559641265
```

sophos_endpoint_info

Description

Gets Sophos endpoint information. (For internal use only)

Columns

Column	Type	Description

Column	Type	Description
endpoint_id	text	The endpoint id of the machine

Example

```
SELECT
    endpoint_id
FROM
    sophos_endpoint_info
```

sophos_events_details

Description

List of events details from Sophos Event Store.

Multiple Sophos event details are grouped together in families.
This event details table requires you provide a familyId constraint.

To find the event summary familyIds for this machine use the 'sophos_events_summary' table.

Columns

Column	Type	Description
id	text	The ID of the event details
familyId	text	The familyId of the event summary found in the 'sophos_events_summary' table
time	unsigned_bigint	The time (unix epoch) the event took place
timeStamp	text	The time the event took place as an ISO8601 format date string
raw	text	The raw JSON string containing all the event details data

Example

```
SELECT
   JSON_EXTRACT(raw, '$.resourceId') as resourceId
FROM
   sophos_events_details
WHERE
   familyId = "{192B7B6D - 1091 - 493F - AED7 - D0AA0565A3BB}"
```

sophos_events_summary

Description

List of events summaries from Sophos Event Store.

Multiple Sophos events are grouped together in families. This event summary table will contain a single entry for each familyId. The entry typically shows the latest event details and contains a current severity for the whole family group.

To retrieve all the details relating to the event summary you must query the 'sophos_events_details' table.

Columns

Column	Type	Description
id	text	The ID of the event summary
familyId	text	The familyId of the event summary that should be used when querying the 'sophos_events_details' table
time	unsigned_bigint	The time (unix epoch) the event took place
timeStamp	text	The time the event took place as an ISO8601 format date string
severity	integer	The severity of the event: green(1), amber(2), red(3)
reboot	integer	If the event requires a reboot: none(0), recommended(1), mandatory(2)
type	text	The type of the event. Valid types are: malware_protection, web_security, malicious_behavior, control, malicious_traffic, exploit_protection
raw	text	The raw JSON string containing all the event summary data

Example

```
SELECT
   json_extract(raw, '$.resourceId') AS resourceid
FROM
   sophos_events_summary
WHERE
   severity = 2
```

sophos_file_hash_journal

Description

FileHash events from Sophos journals.

Columns

Column	Type	Description

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: set(0), unset(1)
fileId	text	The fileId of the file directory in a json structure: Volume GUID, fileId
sha256	text	The SHA-256 hash of the file
fileSize	unsigned_bigint	The file size in bytes

Example

```
SELECT
    *
FROM
    sophos_file_hash_journal
WHERE
    time > 1559641265
```

sophos_file_journal

Description

File events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL

Column	Type	Description
subject	text	The subject of the file event can be: FileBinaryChanges, FileBinaryReads, FileDataChanges, FileDataReads, FileOtherChanges, FileOtherRead Where binary is defined as a PE file on the machine, data is of specific extension type set: doc, docx, xls, xlsx, ppt, pptx, pdf, rtf, wpd and other is any other type of extension. Supported with multiple equals operators for known subjects.
eventType	integer	The event type: created(0), renamed(1), deleted(2), modified(3), hardLinkCreated(4), timestampsModified(5), permissionsModified(6), ownershipModified(7), accessed(8), binaryFileMapped(9)
PID	unsigned_bigint	The ID of the process that produced the file event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the file event
sophosPID	text	The ID of the process that produced the file event and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread that produced the file event
sophosTID	text	Hidden The ID of the thread that produced the file event and its start time creating a unique identifier
fileSize	unsigned_bigint	The file size in bytes
pathname	text	The path name of the file
targetPathname	text	The target pathname of the file. Only populated for events with eventType: renamed(1) and hardLinkCreated(4)
fileId	text	The fileId of the directory
creationTime	unsigned_bigint	The time (unix epoch) the file was created
lastAccessTime	unsigned_bigint	The time (unix epoch) the file was last accessed
lastWriteTime	unsigned_bigint	The time (unix epoch) the file was last written to
changeTime	unsigned_bigint	The time (unix epoch) the file was last changed
numberOfHardLinks	integer	The number of hardlinks for the directory

Column	Type	Description
fileAttributes	integer	The file attributes as a bit mask: READONLY(0x00000001), HIDDEN(0x00000002), SYSTEM(0x00000004), DIRECTORY(0x00000010), ARCHIVE(0x00000020), DEVICE(0x00000040), NORMAL(0x00000080), TEMPORARY(0x00000100), SPARSE_FILE(0x00000200), REPARSE_POINT(0x00000400), COMPRESSED(0x00000800), OFFLINE(0x00001000), NOT_CONTENT_INDEXED(0x00002000), ENCRYPTED(0x00004000), VIRTUAL(0x00010000)
fileType	integer	The file type as an integer: unknown(0), portable executable(1), executable and linkable format (ELF binary)(2)
fileTypeClass	integer	The file type class as an integer: unknown(0), directory(1), binary(2), data(3), other(4)
sha256	text	The SHA-256 hash of the file Can be populated for eventType(s): renamed(1), deleted(2), hardLinkCreated(4), permissionsModified(6), accessed(8)
pesha256	text	The PESHA-256 hash of the file Can be populated for eventType(s): renamed(1), deleted(2), hardLinkCreated(4), permissionsModified(6), accessed(8)
dacl	text	The file discretionary access control list as a string Only populated for events with eventType(s): permissionsModified (6)
owner	text	The owner of a directory as a SID Populated for events with eventType(s): ownershipModified (7) Can be populated for eventType(s) permissionsModified (6)
newCreationTime	unsigned_bigint	The time (unix epoch) the new file was created
newLastAccessTime	unsigned_bigint	The time (unix epoch) the new file was last accessed

Column	Type	Description
newLastWriteTime	unsigned_bigint	The time (unix epoch) the new file was written to
newChangeTime	unsigned_bigint	The time (unix epoch) the new file was changed

Example

```
SELECT
    *
FROM
    sophos_file_journal
WHERE
    subject = "FileBinaryChanges"
```

sophos_file_properties

Description

Gets Sophos properties for a file using either the pathname or sha256.
Either the pathname or sha256 can be used as a constraint for querying this table.
Most fields in this table will only be populated when querying for a binary file.

Columns

Column	Type	Description
sha256	text	The SHA-256 of a file
pathname	text	The file path
appId	text	Hidden The app ID as a json structure containing: status - enum: unknown(0), invalid(1), undetermined(2) ruleId - string category - int - a unique identifier that classifies the type of application name - string - appId name
fileSize	unsigned_bigint	The size of the file (in bytes)
sha1	text	The SHA-1 hash of the file
mlScoreData	text	Hidden The ml scores as a json structure containing: version - int - the version of the structure peMalwareScore - int - -1 is unknown, 0-100 is the score from a successful ML PE Malware scan pePuaScore - int - -1 is unknown, 0-100 is the score from a successful ML PE PUA scan vdlFlags - int - VDL flags providing additional data about the ML scores expireTime - int64 - the time the ML score expires (zero is never) configVersion - string - SHA256 hash of the configuration items used to produce the ML scores

Column	Type	Description
mlScore	integer	The machine learning malware score. -1 is unknown, 0-100 is the score from a successful ML PE Malware scan
puaScore	integer	The machine learning PUA score. -1 is unknown, 0-100 is the score from a successful ML PE PUA scan
globalRepData	text	Hidden The global reputation as a json structure containing: version - int - the version of the structure reputation - int - -1 is unknown, 0-100 is the local reputation lookupType - enum - Lookup type used for the Local Reputation score unknown(0), sha256(1), sha1(2) expireTime - int64 - Time ML scores expire (zero is never) sampleRate - int - Telemetry Sample Rate. 0 means no samples, all values indicate sample 1 every N occurrences (average randomized occurrence) reputationData - JSON string - the intermediate results of a Local Reputation Analysis
localRepData	text	Hidden The local reputation as a json structure containing: version - int - the version of the structure reputation - int - -1 is unknown, 0-100 is the local reputation lookupType - enum - Lookup Type used for the Local Reputation score: unknown(0), customerHash(1), customerCertThumbprint(2), customerSigner(3), customerPath(4), sophosHash(5), sophosCertThumbprint(6), sophosSigner(7) cryptoStrength - int - Cryptographic security strength of Lookup Type used for the Local Reputation score sampleRate - int - Telemetry Sample Rate. 0 means no samples, all values indicate sample 1 every N occurrences (average randomized occurrence) sfsVersion - int64 - File version of the SFS executable used to gather the ReputationData configVersion - string - SHA256 hash of the configuration items used to produce the local reputation reputationData - JSON string - the intermediate results of a Local Reputation Analysis
localRep	integer	The machine learning local reputation. -1 is unknown, 0-100 is the local reputation
globalRep	integer	The machine learning global reputation. -1 is unknown, 0-100 is the global reputation
coreFileInfo	text	Hidden The file info as a json structure containing: isSavWinPE - if it is scanned by sav isWinPE - if it is scanned with ML version - the version

Example

```
SELECT
    *
FROM
    sophos_file_properties
WHERE
    sha256 = 'f29a448b780745bf2e10667f46c442b102e75e76a46a1fff969641866225ab56'

SELECT
    *
FROM
    sophos_file_properties
WHERE
    pathname = 'C:\Windows\System32\cmdl32.exe'
```

sophos_http_journal

Description

Http events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
PID	unsigned_bigint	The ID of the process that produced the http event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the http event
sophosPID	text	The ID of the process that produced the http event and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread that produced the http event This field may not be populated
sophosTID	text	Hidden The ID of the thread that produced the http event and its start time creating a unique identifier This field may not be populated
source	text	The source IP address of the http event
sourcePort	integer	The source port of the http event
destination	text	The destination IP address of the http event
destinationPort	integer	The destination port of the http event

Column	Type	Description
protocol	integer	The protocol used in the http event Unsupported(0), ICMP(1), ICMPv4(1), TCP(6), UDP(17), ICMPv6(58)
url	text	The requested url
headers	text	The request headers associated with the http event

Example

```
SELECT
    *
FROM
    sophos_http_journal
WHERE
    time > 1559641265
```

sophos_image_journal

Description

Process events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: loaded(0)
PID	unsigned_bigint	The ID of the process that produced the image event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the image event
sophosPID	text	The ID of the process that produced the image event and its start time creating a unique identifier
loadTime	unsigned_bigint	The time (unix epoch) when the image loaded
imageBase	unsigned_bigint	Set to the virtual base address of the image
imageSize	unsigned_bigint	The size of the image in bytes May never be populated
pathname	text	The path name of the image

Example

```
SELECT
    *
FROM
    sophos_image_journal
WHERE
    time > 1559641265
```

sophos_ip_journal

Description

ip events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
PID	unsigned_bigint	The ID of the process that produced the ip event
sophosPID	text	The ID of the process that produced the ip event and its start time creating a unique identifier
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the ip event
TID	unsigned_bigint	The ID of the thread that produced the ip event This field may not be populated Hidden
sophosTID	text	The ID of the thread that produced the ip event and its start time creating a unique identifier This field may not be populated
source	text	The source ip address of the ip event
sourcePort	integer	The source port of the ip event
destination	text	The destination ip address of the ip event
destinationPort	integer	The destination port of the ip event
protocol	integer	The protocol used in the ip event: Unsupported(0), ICM(1), ICMPv4(1), TCP(6), UDP(17), ICMPv6(58)

Column	Type	Description
redirectionState	integer	The current state of redirection if the ip event is redirected This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateInProgress(1), RedirectionStateRedirected(2)
originalDestination	text	The original destination of the ip event before redirection This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateInProgress(1)
originalDestinationPort	integer	The port of the original destination for the ip event before redirection This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateInProgress(1)
targetPID	unsigned_bigint	The PID of the process used to redirect the ip event This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateInProgress(1)
targetProcessStartTime	unsigned_bigint	The start time (unix epoch) of the process used to redirect the ip event This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateInProgress(1)
targetSophosPID	text	The Sophos PID of the process used to redirect the ip event as a combination of the PID and its start time This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateInProgress(1)
originalProcessPath	text	The original process path associated with the ip event This will only be populated if the ip event has been redirected and redirectionState contains: RedirectionStateRedirected(2)

Example

```
SELECT
    *
FROM
    sophos_ip_journal
WHERE
    time > 1559641265
```

sophos_network_journal

Description

Network events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: tcpIPv4Connect(0), tcpIPv4Accept(1), tcpIPv4(2), udpIPv4(3), tcpIPv6Connect(4), tcpIPv6Accept(5), tcpIPv6(6), udpIPv6(7)
PID	unsigned_bigint	The ID of the process that produced the network event
sophosPID	text	The ID of the process that produced the network event and its start time creating a unique identifier
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the network event
TID	unsigned_bigint	The ID of the thread that produced the network event This field may not be populated
sophosTID	text	Hidden The ID of the thread that produced the network event and its start time creating a unique identifier This field may not be populated
startTime	unsigned_bigint	The start time (unix epoch) of the network event
source	text	The source IP address of the network event
sourcePort	integer	The source port of the network event
destination	text	The destination IP address of the network event
destinationPort	integer	The destination port of the network event
dataSent	unsigned_bigint	The number of bytes sent in the network event
dataRecv	unsigned_bigint	The number of bytes received in the network event
flags	unsigned_bigint	The flags field of the network event: SG_EVT_JRN_TCP_CONNECTION_ACTIVE(0x00000001)

Example

```
SELECT
    *
```

```
FROM
    sophos_network_journal
WHERE
    time > 1559641265
```

sophos_powershell_events

Description

Windows powershell script block event logs from the Microsoft-Windows-PowerShell/Operational channel
This table requires script block logging to be enabled.

Columns

Column	Type	Description
time	unsigned_bigint	Timestamp of the windows powershell event (unix epoch) If no time constraint is given the table will be queried for events in the last day
datetime	text	System time at which the Powershell script event occurred
script_block_id	text	The unique GUID of the powershell script to which this block belongs
script_block_count	integer	The total number of script blocks for this script
script_text	text	The text content of the Powershell script
script_name	text	The name of the Powershell script
script_path	text	The path for the Powershell script

Example

```
SELECT
    *
FROM
    sophos_powershell_events
WHERE
    time > 1574500000;
```

sophos_process_activity

Description

Process activity events from the Sophos journals.

Columns

Column	Type	Description

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal event was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
sophosPID	text	The ID of the process that produced the event and its start time creating a unique identifier
subject	text	The subject of the process activity event can be: DirectoryChanges, Dns, FileBinaryChanges, FileBinaryReads, FileDataChanges, FileDataReads, FileOtherChanges, FileOtherReads, Http, Image, Ip, Network, Process, Registry, Thread, Url Supported with multiple equals operators for known subjects.
action	text	The action of the event can be (depending on the subject): DirectoryChanges: --Created --Renamed --Deleted --PermissionsModified --OwnershipModified --Unknown Dns: --Request --Unknown File: --Created --Renamed --Deleted --Modified --HardLinkCreated --TimestampsModified --PermissionsModified --OwnershipModified --Accessed --BinaryFileMapped

Column	Type	Description
		--Unknown Http: --Request Image: --Loaded --Unknown Ip: --Connected --Redirecting --Redirected --Unknown Network: --TCP IPv4 Connect --TCP IPv4 Accept --TCP IPv4 --UDP IPv4 --TCP IPv6 Connect --TCP IPv6 Accept --TCP IPv6 --UDP IPv6 --Unknown Process: --Start --End --Unknown Registry: --Key Created --Key Renamed --Key Deleted --Key Permissions Modified --Key Ownership Modified --Value Set --Value Deleted --Unknown Thread: --Start --End --Unknown Url: --Request --Unknown

Column	Type	Description
object	text	The object of the event is (depending on the subject): DirectoryChanges: the path of the directory Dns: the host name of the DNS request File: the path of the file Http: the URL of the HTTP request Image: the path of the image Ip: the source and destination of the request --format: [SOURCE_ADDRESS]:SOURCE_PORT -> [DESTINATION_ADDRESS]:DESTINATION_PORT Network: the source and destination of the request --format: [SOURCE_ADDRESS]:SOURCE_PORT -> [DESTINATION_ADDRESS]:DESTINATION_PORT Process: the command line of the process Registry: the path of the registry key or value Thread: the path of the thread image Url: the URL of the event
fileId	text	The fileId of the directory or file
pathname	text	The pathname that the event relates to
fileSize	unsigned_bigint	The file size in bytes
targetPathname	text	The target pathname of the file.
url	text	The requested url
source	text	The source IP address of the http event
sourcePort	integer	The source port of the http event
destination	text	The destination IP address of the http event
destinationPort	integer	The destination port of the http event
originalDestination	text	The original destination of the ip event before redirection
originalDestinationPort	integer	The port of the original destination for the ip event before redirection
protocol	integer	The protocol used in the event
targetSophosPID	text	The Sophos PID of the target process
cmdLine	text	The command line arguments
keyName	text	The registry key path and name
valueName	text	The name of the registry value. Will only be set for valueSet(5) or valueDeleted(6) event types
value	text	The stored registry value, can be truncated if too large
sophosTID	text	The ID of the thread and its start time creating a unique identifier

Example

```
SELECT
    *
FROM
    sophos_process_activity
```

sophos_process_journal

Description

Process events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: start(0), end(1)
PID	unsigned_bigint	The ID of the process event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process event
sophosPID	text	The ID of the process and its start time creating a unique identifier
parentPID	unsigned_bigint	The parent process ID
parentProcessStartTime	unsigned_bigint	The start time (unix epoch) of the parent process
parentSophosPID	text	The parent process ID and its start time creating a unique identifier
parentTID	unsigned_bigint	The thread ID of the parent process
parentSophosTID	text	Hidden The thread ID of the parent process and its start time creating a unique identifier
inheritPID	unsigned_bigint	The process inherited from the process ID
inheritProcessStartTime	unsigned_bigint	The start time (unix epoch) of the process inherited from the process ID
inheritSophosPID	text	The process inherited from process ID and its start time creating a unique identifier
endTime	unsigned_bigint	The time (unix epoch) the process stopped
fileSize	unsigned_bigint	The file size of the process in bytes
flags	unsigned_bigint	The Windows process creation flags as a bit mask: SG_EVT_JRN_PROCESS_IS_SYSTEM(0x00000001), SG_EVT_JRN_PROCESS_IS_SERVICE(0x00000002), SG_EVT_JRN_PROCESS_IS_SOPHOS(0x00000004), SG_EVT_JRN_PROCESS_IS_WOW64(0x00000008), SG_EVT_JRN_PROCESS_IS_PROTECTED(0x00000010), SG_EVT_JRN_PROCESS_IS_SECURE(0x00000020), SG_EVT_JRN_PROCESS_IS_WSL(0x00000040)
sessionId	unsigned_bigint	The session ID
sid	text	The user SID
pathname	text	The path name of the process
processName	text	The name of the process
cmdLine	text	The command line arguments This field may not be populated

Column	Type	Description
sha256	text	The SHA-256 hash of the file This field may not be populated
sha1	text	The SHA-1 hash of the file This field may not be populated
pesha256	text	The PESHA-256 hash of the file This field may not be populated
pesha1	text	The PESHA-1 hash of the file This field may not be populated

Example

```
SELECT
    *
FROM
    sophos_process_journal
WHERE
    time > 1559641265
```

sophos_process_properties

Description

Gets Sophos properties for a process using either the SPID or PID, using the SPID will get any data on the process event with that SPID. Using the PID will get data for current process which is using that PID.

Columns

Column	Type	Description
sophosPID	text	The ID of the process and its start time creating a unique identifier
pid	unsigned_bigint	The process ID
processStartTime	unsigned_bigint	The start time of the process
appId	text	Hidden The app ID as a json structure containing: status - enum: unknown(0), invalid(1), undetermined(2) ruleId - string category - int - a unique identifier that classifies the type of application name - string - appId name
pathname	text	The pathname of the process
fileSize	unsigned_bigint	The size of the file (in bytes)
sha256	text	The SHA-256 hash of the file

Column	Type	Description
sha1	text	The SHA-1 hash of the file
mlScoreData	text	Hidden The ml scores as a json structure containing: version - int - the version of the structure peMalwareScore - int - -1 is unknown, 0-100 is the score from a successful ML PE Malware scan pePuaScore - int - -1 is unknown, 0-100 is the score from a successful ML PE PUA scan vdlFlags - int - VDL flags providing additional data about the ML scores expireTime - int64 - the time ML scores expire (zero is never) configVersion - string - SHA256 hash of the configuration items used to produce the ML scores
mlScore	integer	The machine learning malware score. -1 is unknown, the score from a successful ML PE PUA scan is 0-100
puaScore	integer	The machine learning PUA score. -1 is unknown, the score from a successful ML PE PUA scan is 0-100
globalRepData	text	Hidden The global reputation as a json structure containing: version - int - the version of the structure reputation - int - -1 is unknown, 0-100 is the local reputation LookupType - enum - Lookup Type used for the Local Reputation score: unknown(0), sha256(1), sha1(2), expireTime - int64 - the time ML scores expire (zero is never) sampleRate - int - Telemetry Sample Rate. 0 means no samples, all values indicate 1 sample every N occurrences (average randomized occurrence) reputationData - JSON string - the intermediate results of a Local Reputation Analysis

Column	Type	Description
		Hidden
localRepData	text	The local reputation as a json structure containing: version - int - the version of the structure reputation - int - -1 is unknown, 0-100 is the local reputation lookupType - enum - Lookup Type used for the Local Reputation score: unknown(0), customerHash(1), customerCertThumbprint(2), customerSigner(3), customerPath(4), sophosHash(5), sophosCertThumbprint(6), sophosSigner(7) cryptoStrength - int - Cryptographic security strength of Lookup Type used for the Local Reputation score sampleRate - int - Telemetry Sample Rate. 0 means no samples, all values indicate 1 sample every N occurrences (average randomized occurrence) sfsVersion - int64 - File version of the SFS executable used to gather the ReputationData configVersion - string - SHA256 hash of the configuration items used to produce the local reputation reputationData - JSON string - the intermediate results of a Local Reputation Analysis
localRep	integer	The machine learning local reputation. -1 is unknown, the local reputation is 0-100
globalRep	integer	The machine learning global reputation. -1 is unknown, the global reputation is 0-100

Example

```
SELECT
    *
FROM
    sophos_process_properties
WHERE
    sophosPID = "12596:132075140530000000"
```

sophos_registry_journal

Description

Registry events from Sophos journals.

Columns

Column	Type	Description

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: keyCreated(0), keyRenamed(1), keyDeleted(2), keyPermissionsModified(3), keyOwnershipModified(4), valueSet(5), valueDeleted(6)
PID	unsigned_bigint	The ID of the process that produced the registry event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the registry event
sophosPID	text	The process ID that produced the registry event and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread that produced the registry event
sophosTID	text	Hidden The ID of the thread that produced the registry event and its start time creating a unique identifier
keyName	text	The registry key path and name
sid	text	The owner of the registry key as a sid
valueName	text	The name of the registry value. Will only be set for valueSet(5) or valueDeleted(6) event types
valueType	bigint	Will only be set for the valueSet(5) event type The type of the registry value: None(0), String(1), ExpandString(2), Binary(3), Dword(4), DwordBigEndian(5), SymbolicLink(6), MultiString(7), ResourceList(8), FullResourceDescriptor(9), Qword(11)
valueSize	bigint	The size of the registry value in bytes, always correct even if value field is truncated Only populated for events with eventType(s): valueSet(5)
value	text	The stored registry value, can be truncated if too large Only populated for events with eventType(s): valueSet(5)
dacl	text	The file discretionary access control list of the key as a string Only populated for events with eventType(s): keyPermissionsModified(3)

Column	Type	Description
owner	text	The owner of the key as a SID string. Only populated for events with eventType(s): keyOwnershipModified(4)
newKeyName	text	The new name of the registry key. Only populated for events with eventType(s): KeyRenamed(1)

Example

```
SELECT
    *
FROM
    sophos_registry_journal
WHERE
    time > 1559641265
```

sophos_system_journal

Description

System events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: shutdown(0), timeChange(1)
osVersion	text	The version of the os
flags	unsigned_bigint	Flag containing additional details about the OS and boot mode as a bit mask: SG_EVT_JRN_SYSTEM_IS_64_BIT(0x00000001), SG_EVT_JRN_SYSTEM_IS_SERVER(0x00000002), SG_EVT_JRN_SYSTEM_BOOTED_WITH_SAFE_BOOT(0x00000004), SG_EVT_JRN_SYSTEM_KERNEL_DEBUGGER_ACTIVE(0x00000008), SG_EVT_JRN_SOPHOSED_LOADED_AT_BOOT(0x00000010)

Example

```
SELECT
    *
FROM
    sophos_system_journal
WHERE
    time > 1559641265
```

sophos_thread_journal

Description

Thread events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: start(0), end(1)
PID	unsigned_bigint	The ID of the process that produced the thread event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the thread event
sophosPID	text	The ID of the process that produced the thread event and its start time creating a unique identifier
parentPID	unsigned_bigint	The parent process ID
parentProcessStartTime	unsigned_bigint	The start time (unix epoch) of the parent process
parentSophosPID	text	The ID of the parent process and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread
sophosTID	text	Hidden The ID of the thread and its start time creating a unique identifier
parentTID	unsigned_bigint	The thread ID of the parent process
parentSophosTID	text	Hidden The thread ID of the parent process and its start time creating a unique identifier
endTime	unsigned_bigint	The time (unix epoch) the thread stopped
startAddress	text	The address of the thread at start
flags	unsigned_bigint	The Windows process creation flags as a bit mask: SG_EVT_JRN_THREAD_IS_SYSTEM(0x00000001), SG_EVT_JRN_THREAD_START_REMOTE(0x00000002), SG_EVT_JRN_THREAD_START_KERNEL(0x00000004), SG_EVT_JRN_THREAD_IS_WOW64(0x00000008)
imageName	text	The image that has the start address for the thread

Example

```
SELECT
    *
FROM
    sophos_thread_journal
WHERE
    time > 1559641265
```

sophos_url_journal

Description

Url events from Sophos journals.

Columns

Column	Type	Description
time	unsigned_bigint	The event time (unix epoch) the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type: request(0)
PID	unsigned_bigint	The ID of the process that produced the url event
processStartTime	unsigned_bigint	The start time (unix epoch) of the process that produced the url event
sophosPID	text	The ID of the process that produced the url event and its start time creating a unique identifier
TID	unsigned_bigint	The ID of the thread that produced the url event
sophosTID	text	Hidden The ID of the thread that produced the url event and its start time creating a unique identifier
url	text	The url that was requested
flags	unsigned_bigint	Flags as a bitmask Set if the connection is currently active (0x00000001)

Example

```
SELECT
    *
FROM
    sophos_url_journal
WHERE
    time > 1559641265
```

sophos_windows_events

Description

Windows events logs
Events for the windows "System", "Application", "Setup" and "Security" source channels will be gathered by default. These can be overriden by specifying event source channels using the "source" field.

Columns

Column	Type	Description
time	unsigned_bigint	Timestamp of the windows event (unix epoch) If no time constraint is given the table will be queried for events in the last day
datetime	text	System time at which the event occurred
source	text	Source or channel of the event
provider_name	text	Provider name of the event
provider_guid	text	Provider guid of the event
eventid	integer	Event ID of the event
task	integer	Task value associated with the event
task_message	text	Message describing the windows event task type
level	integer	The severity level associated with the event
keywords	text	A bitmask of the keywords defined in the event
executing_pid	unsigned_bigint	Executing process ID
executing_tid	unsigned_bigint	Executing thread ID within the executing process
data	text	Data associated with the event
eid	text	Unique event ID

Example

```
SELECT
    *
FROM
    sophos_windows_events
WHERE
    time > 1574500000;
```

sophos_winsec_journal

Description

Windows Security (WinSec) events from Sophos journals

Columns

Column	Type	Description

Column	Type	Description
time	unsigned_bigint	The event time the journal was created If no time constraint is specified the default constraint will be to retrieve events starting at 'now - 15 minutes' The only constraints supported for time are: - EQUAL - GREATER THAN - GREATER THAN OR EQUAL - LESS THAN - LESS THAN OR EQUAL
eventType	integer	The event type The audit log was cleared = 1102 For data relating to this event see: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102 An account was successfully logged on = 4624 For data relating to this event see: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624 An account failed to log on = 4625 For data relating to this event see: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625 NOTE - Logon failure events are only generated if the following audit policy command has been run: "auditpol /set /subcategory:logon /failure:enable"
data	text	The data relating to the WinSec event as a json string. The data fields will vary depending on the event type. See the Microsoft Docs pages above for more information on the contained data fields. Note - the json field names are camelCased to be consistent with the sophos journals example data json extract: "select JSON_EXTRACT(data, '$.targetUserSid') as tus from sophos_winsec_journal where time > 0 and eventType = 4624;"

Example

```
SELECT
    *
FROM
    sophos_winsec_journal
WHERE
    time > 1559641265
```