# Parsed 1 File

Reset

Collapse All

schema.json 1 items Download JSON

{97}

arp_cache {8}

description:

"Gets cached ARP replies to enumerate layer-2 network neighbors."

| | Description | Id | Type |
|---|---|---|---|
| 1 | IPv4 address target | address | string |
| 2 | MAC address of broadcasted address | mac | string |
| 3 | Interface of the network for the MAC | interface | string |

interval: 3600

name: "arp_cache"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

browser_plugins {8}

description:

"Gets the list of C/NPAPI browser plugins in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The local user that owns the plugin | uid | long |
| 2 | Plugin display name | name | string |
| 3 | Plugin identifier | identifier | string |
| 4 | Plugin short version | version | string |
| 5 | Plugin description text | description | string |
| 6 | Path to plugin bundle | path | string |

interval: 14400

name: "browser_plugins"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ changed_files_windows_sophos {8}

description:

"Lists hashes for files which have changed in the last 10 mins."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Name of the file that has changed | filename | string |
| 2 | Full path of the file that has changed | path | string |
| 3 | Time of the change event | ctime | long |
| 4 | SHA1 of the file now | sha1 | string |
| 5 | SHA256 of the file now | sha256 | string |
| 6 | File size now | fileSize | long |
| 7 | The machine learning malware scor... | mlScore | int |
| 8 | All ML score data | mlScoreData | string |
| 9 | The machine learning PUA score now | puaScore | int |
| 10 | The machine learning global reputa... | globalRep | int |
| 11 | All global reputation data | globalRepData | string |
| 12 | The machine learning local reputati... | localRep | int |
| 13 | All local reputation now | localRepData | string |
| 14 | Core file info | coreFileInfo | string |

interval: 300

name: "changed_files_windows_sophos"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ chrome_extensions {8}

description:

"Gets the list of extensions for Chrome in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The local user that owns the extension | uid | long |
| 2 | Extension display name | name | string |
| 3 | Extension identifier | identifier | string |
| 4 | Extension-supplied version | version | string |
| 5 | Optional extension author | author | string |
| 6 | Path to extension folder | path | string |
| 7 | Extension-supplied update URI | update_url | string |

interval: 14400

name: "chrome_extensions"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ deb_packages {8}

description:

"Gets all the installed DEB packages in the target Linux system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Package name | name | string |
| 2 | Package version | version | string |
| 3 | Package architecture | arch | string |
| 4 | Package revision | revision | string |

interval: 14400

name: "deb_packages"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ firefox_addons {8}

description:

"Gets the list of add-ons for Firefox in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The local user that owns the addon | uid | long |
| 2 | Addon display name | name | string |
| 3 | Addon identifier | identifier | string |
| 4 | Addon-supplied version string | version | string |
| 5 | Addon-supplied description string | description | string |
| 6 | Path to plugin bundle | path | string |
| 7 | URL that installed the addon | source_url | string |
| 8 | Addon-supported creator string | creator | string |

interval: 14400

name: "firefox_addons"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ homebrew_packages {8}

description:

"Gets the list of brew packages installed in the target macOS system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Package name | name | string |
| 2 | Package install path | path | string |
| 3 | Current 'linked' version | version | string |

interval: 14400

name: "homebrew_packages"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ host_sensor_heartbeat_check {8}

description:

"Gets the current host time information,checking whether queries are running."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Current timestamp (log format) in th... | timestamp | string |
| 2 | Current date and time (ISO format) i... | datetime | string |
| 3 | Current local UNIX time in the system | local_time | int |
| 4 | Current UNIX time in the system, co... | unix_time | int |
| 5 | Current local timezone in the system | local_timezone | string |

interval: 3600

name: "host_sensor_heartbeat_check"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ host_sensor_version_darwin {8}

description: "Gets the current host sensor version."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Version of the host sensor | host_sensor_version | string |
| 2 | The build commit hash | commit_hash | string |
| 3 | The event timestamp | event_timestamp | string |

interval: 14400

name: "host_sensor_version_darwin"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ host_sensor_version_linux {8}

description: "Gets the current host sensor version."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Version of the host sensor | host_sensor_version | string |
| 2 | The build commit hash | commit_hash | string |
| 3 | The event timestamp | event_timestamp | string |

interval: 14400

name: "host_sensor_version_linux"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ host_sensor_version_windows {8}

description: "Gets the current host sensor version."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Version of the host sensor | host_sensor_version | string |
| 2 | The build commit hash | commit_hash | string |
| 3 | The event timestamp | event_timestamp | string |

interval: 14400

name: "host_sensor_version_windows"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ ie_extensions {8}

description:

"Gets the list of extensions for Internet Explorer in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Extension display name | name | string |
| 2 | Version of the executable | version | string |
| 3 | Path to executable | path | string |

interval: 14400

name: "ie_extensions"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ installed_applications {8}

description:

"Gets all the currently installed applications in the target macOS system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Name of the Name.app folder | name | string |
| 2 | Absolute and full Name.app path | path | string |
| 3 | Info properties CFBundleExecu... | bundle_executable | string |
| 4 | Info properties CFBundleIdentif... | bundle_identifier | string |
| 5 | Info properties CFBundleName... | bundle_name | string |
| 6 | Info properties CFBundleVersio... | bundle_version | string |
| 7 | Info properties CFBundleShort... | bundle_short_version | string |
| 8 | Info properties CFBundleDispla... | display_name | string |
| 9 | Info properties NSHumanRead... | copyright | string |
| 10 | The UTI that categorizes the a... | category | string |
| 11 | Info properties CFBundleGetInf... | info_string | string |

interval: 120

name: "installed_applications"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ ioc_windows_registry_malware_sdbot {8}

description:

"Retrieves a registry key used by sdbot malware persistence mechanism."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The time (unix epoch) the value was set | event_time | long |
| 2 | The registry key path and name | keyName | string |
| 3 | The stored registry value | value | string |
| 4 | The event type | eventType | int |
| 5 | The process ID that produced the regis... | sophosPID | string |
| 6 | The name of the value that was set | valueName | string |
| 7 | Static REG_BINARY | valueType | string |
| 8 | Static descrption for the events | description | string |

interval: 600

name: "ioc_windows_registry_malware_sdbot"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ launchd_md5 {8}

description:

"Lists auto-start, non-Apple launch daemons including binary hashes."

| | Description | Id | Type |
|---|---|---|---|

| | Description | Id | Type |
|---|---|---|---|
| 1 | Key describes the intended pur… | process_type | string |
| 2 | Should the program run on laun… | run_at_load | string |
| 3 | Path to daemon or agent plist | name | string |
| 4 | Daemon or agent service name | label | string |
| 5 | Command line arguments passe… | program_arguments | string |
| 6 | Path to daemon or agent plist | path | string |
| 7 | Path to target program | program | string |
| 8 | Deprecated key, replaced by ke… | on_demand | string |
| 9 | Should the process be restarted… | keep_alive | string |
| 10 | SHA1 hash of provided filesyste… | sha1 | string |
| 11 | SHA256 hash of provided filesy… | sha256 | string |

```
interval: 14400
name: "launchd_md5"
namespace: "com.sophos.central.data.xdr.query.avro"
tag: "DataLake"
type: "record"
version: "1.1.17"
```

▼ listening_ports {8}

```
description: "Gets all the listening ports in the target system."
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | The process path or shorthand argv[0] | name | string |
| 2 | Specific address for bind | address | string |
| 3 | Transport layer port | port | int |
| 4 | Process (or thread) ID | pid | long |
| 5 | Path to executed binary | path | string |

```
interval: 3600
name: "listening_ports"
namespace: "com.sophos.central.data.xdr.query.avro"
```

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ network_interfaces {8}

description:

"Lists all the IP addresses on attached network interfaces."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Network MTU | mtu | int |
| 2 | Interface name | interface | string |
| 3 | MAC of interface (optional) | mac | string |
| 4 | Interface netmask | mask | string |
| 5 | Specific address for interface | address | string |
| 6 | Broadcast address for the interface | broadcast | string |
| 7 | Input bytes | ibytes | long |
| 8 | Output bytes | obytes | long |

interval: 43200

name: "network_interfaces"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ open_sockets {8}

description:

"Gets all the open sockets for each process in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The process path or shorthand argv... | name | string |
| 2 | Command line passed to process | cmdline | string |
| 3 | Process (or thread) ID | pid | long |
| 4 | Process parent's PID | parent | long |

| | Description | Id | Type |
|---|---|---|---|
| 5 | Path to executed binary | path | string |
| 6 | Socket remote address | remote_address | string |
| 7 | Socket remote port | remote_port | int |
| 8 | Socket local address | local_address | string |

interval: 30

name: "open_sockets"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ opera_extensions {8}

description:

"Gets the list of extensions for Opera in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The local user that owns the extension | uid | long |
| 2 | Extension display name | name | string |
| 3 | Extension identifier | identifier | string |
| 4 | Extension-supplied version | version | string |
| 5 | Extension-optional description | description | string |
| 6 | Extension-supplied update URI | update_url | string |
| 7 | Optional extension author | author | string |
| 8 | Path to extension folder | path | string |

interval: 14400

name: "opera_extensions"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ osquery_process {8}

description:

"Retrieves Osquery and MTR process information on all platforms."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Process (or thread) ID | pid | long |
| 2 | The process path or shorthan... | name | string |
| 3 | Returns elapsed time that all ... | percent_processor_time | long |
| 4 | Total number of handles that t... | handle_count | long |
| 5 | Elapsed time in seconds this ... | elapsed_time | long |
| 6 | Process start time in seconds ... | start_time | long |
| 7 | Bytes read from disk | disk_bytes_read | long |
| 8 | Bytes written to disk | disk_bytes_written | long |
| 9 | CPU time in milliseconds spen... | user_time | long |
| 10 | CPU time in milliseconds spen... | system_time | long |
| 11 | Total virtual memory size | total_size | long |
| 12 | Percentage of total CPU time | cpu_percent | long |

interval: 14400

name: "osquery_process"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osquery_query_schedule {8}

description:

"Retrieves the Osquery scheduled query performance metrics for all platforms."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The given name for this query | name | string |
| 2 | The interval in seconds to run this... | interval | int |

| | Description | Id | Type |
|---|---|---|---|
| 3 | Number of times the query was e... | executions | long |
| 4 | 1 if the query is blacklisted else 0 | blacklisted | int |
| 5 | Total number of bytes generated ... | output_size | long |
| 6 | Total wall time spent executing | wall_time | long |
| 7 | Total user time spent executing | user_time | long |
| 8 | Total system time spent executing | system_time | long |
| 9 | Average private memory left after ... | average_memory | long |
| 10 | Average time per execution | average_time | long |

interval: 14400

name: "osquery_query_schedule"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osquery_rocksdb_error_osx {8}

description:

"Retrieves the Osquery RocksDB stalling write events indicating bac
ked up process_events on MacOS."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The path that was searched | path | string |
| 2 | Path to the files found | filepath | string |
| 3 | The search pattern | pattern | string |
| 4 | Line of content from the file | line | string |

interval: 86400

name: "osquery_rocksdb_error_osx"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osquery_rocksdb_size_linux {8}

description: "Retrieves the size of Osquery RocksDB on Linux."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Number of files in the directory | number_of_files | long |
| 2 | Total size of the files in the directory | total_size | long |
| 3 | Total size of the files in MB | mb | long |

interval: 86400

name: "osquery_rocksdb_size_linux"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osquery_rocksdb_size_osx {8}

description: "Retrieves the size of Osquery RocksDB on MacOS."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Number of files in the directory | number_of_files | long |
| 2 | Total size of the files in the directory | total_size | long |
| 3 | Total size of the files in MB | mb | long |

interval: 86400

name: "osquery_rocksdb_size_osx"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osquery_rocksdb_size_windows {8}

description: "Retrieves the size of Osquery RocksDB on Windows."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Number of files in the directory | number_of_files | long |

| | Description | Id | Type |
|---|---|---|---|
| 2 | Total size of the files in the directory | total_size | long |
| 3 | Total size of the files in MB | mb | long |

interval: 86400

name: "osquery_rocksdb_size_windows"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osquery_watchdog_logs_windows {8}

description: "Retrieves the Osquery watchdog logs for Windows."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The path that was searched | path | string |
| 2 | Path to the files found | filepath | string |
| 3 | The search pattern | pattern | string |
| 4 | Content of the file | line | string |

interval: 86400

name: "osquery_watchdog_logs_windows"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ osx_updates_patch {8}

description:

"Gets all the installed updates from the Apple software update serv

ice"

| | Description | Id | Type |
|---|---|---|---|
| 1 | Label packageIdentifiers | package_id | string |
| 2 | Label packageIdentifiers | time | long |

| | Description | Id | Type |
|---|---|---|---|
| 3 | Package display name | name | string |
| 4 | Package display version | version | string |
| 5 | Install source: usually the installer pro... | source | string |
| 6 | Package content_type (optional) | content_type | string |

interval: 43200

name: "osx_updates_patch"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ pending_osx_updates_patch {8}

description:

"Gets all the pending updates from the Apple software update service"

| | Description | Id | Type |
|---|---|---|---|
| 1 | Title of the update | title | string |
| 2 | Update package ID | package_id | string |
| 3 | restart | restart | string |
| 4 | recommended | recommended | string |
| 5 | size | size | long |
| 6 | version | version | string |
| 7 | uid from package ID and version | uid | long |

interval: 43200

name: "pending_osx_updates_patch"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ pending_windows_updates_patch {8}

description:

"Gets all the pending updates from the Windows Update Service."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Title of the update | title | string |
| 2 | Support URL provided in the update | support_url | string |
| 3 | Severity of the update | msrc_severity | string |
| 4 | Is the update installed | installed | string |
| 5 | Is the update mandatory | mandatory | string |
| 6 | Size of the update | size | long |
| 7 | The kb article ID for the update | hotfix_id | string |

interval: 43200

name: "pending_windows_updates_patch"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ rpm_packages {8}

description:

"Gets all the installed RPM packages in the target Linux system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | RPM package name | name | string |
| 2 | Package version | version | string |
| 3 | Package release | release | string |
| 4 | Source RPM package name (optional) | source | string |
| 5 | Architecture(s) supported | arch | string |

interval: 14400

name: "rpm_packages"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ running_processes_linux_events {8}

description:

"Retrieves the list of running processes in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | List of PIDs | pids | string |
| 2 | Name of the process | name | string |
| 3 | Process command line | cmdline | string |
| 4 | List of parent PIDs | parents | string |
| 5 | Path of executed file | path | string |
| 6 | Group ID at process start | gid | long |
| 7 | User ID at process start | uid | long |
| 8 | Effective user ID at process start | euid | long |
| 9 | Effective group ID at process start | egid | long |
| 10 | SHA1 hash of provided filesystem data | sha1 | string |
| 11 | SHA256 hash of provided filesystem data | sha256 | string |
| 12 | Time of execution in UNIX time | time | long |

interval: 10

name: "running_processes_linux_events"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ running_processes_osx_events {8}

description:

"Retrieves the list of running processes in the target system."

| | Description | Id | Type |
|---|---|---|---|

| | Description | Id | Type |
|---|---|---|---|
| 1 | Process (or thread) ID | pid | long |
| 2 | Process name | name | string |
| 3 | Process command line | cmdline | string |
| 4 | Path of executed file | path | string |
| 5 | Process parent's PID, or -1 if cannot be ... | parent | long |
| 6 | Group ID at process start | gid | long |
| 7 | User ID at process start | uid | long |
| 8 | Effective user ID at process start | euid | long |
| 9 | Effective group ID at process start | egid | long |
| 10 | SHA1 hash of provided filesystem data | sha1 | string |
| 11 | SHA256 hash of provided filesystem data | sha256 | string |
| 12 | Time of execution in UNIX time | time | long |


```
interval: 10
name: "running_processes_osx_events"
namespace: "com.sophos.central.data.xdr.query.avro"
tag: "DataLake"
type: "record"
version: "1.1.17"
```


▼ running_processes_windows_sophos {8}

description:
"Retrieves the list of running processes in the target system using the sophos_process_journal table."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The command line arguments | cmdline | string |
| 2 | The process ID | pid | long |
| 3 | The parent process ID | parent | long |
| 4 | Parent process name | parent_name | string |

| | Description | Id | Type |
|---|---|---|---|
| **5** | The parent process path | parent_path | string |
| **6** | Path of the process | path | string |
| **7** | Process name | name | string |
| **8** | The SHA-1 hash of the file | sha1 | string |
| **9** | The SHA-256 hash of the file | sha256 | string |
| **10** | The start time (unix epoch) of the… | time | long |
| **11** | The ID of the process and its star… | sophosPID | string |
| **12** | The ID of the parent process and … | parentSophosPID | string |
| **13** | The file size of the process execu… | fileSize | long |
| **14** | The machine learning malware sc… | mlScore | int |
| **15** | The ml scores as a json structure | mlScoreData | string |
| **16** | The machine learning PUA score. | puaScore | int |
| **17** | The machine learning global repu… | globalRep | int |
| **18** | The global reputation as a json st… | globalRepData | string |
| **19** | The machine learning local reput… | localRep | int |
| **20** | The local reputation as a json str… | localRepData | string |
| **21** | Username running the process | username | string |
| **22** | User ID of the user running the pr… | uid | long |
| **23** | Group ID (unsigned) of the user r… | gid | long |


```
interval:  20
name:    "running_processes_windows_sophos"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:     "DataLake"
type:    "record"
version:  "1.1.17"
```


▼ sophos_events_darwin {8}


```
description:
"Retrieves a list of detections from sophos_mac_event_store table w
```

ith attached details. Reference 'https://wiki.sophos.net/display/savmaceng/MTR+Schema+Change%3A+Sophos+Extension+for+macOS+v1.0.0'"

| | Description | Id | Type |
|---|---|---|---|
| 1 | Unique event ID (uuid) for threat | event_id | string |
| 2 | Event update time (unix epoch) | event_time | long |
| 3 | JSON collection of event details | details_json | string |
| 4 | Severity of the event | severity | int |
| 5 | Name of the event | event_name | string |
| 6 | Numeric value indicating event type | event_type | int |
| 7 | Numeric value indicating an action whi... | resolved | int |
| 8 | Logged in user when the event occurred | user_name | string |

interval: 600

name: "sophos_events_darwin"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ sophos_events_windows {8}

description:

"Retrieves a list of detections from sophos_events_summary table with attached details"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The familyId of the events | family_id | string |
| 2 | The time the event took place as ... | event_timestamp | string |
| 3 | The raw JSON string containing a... | summary_json | string |
| 4 | All raw JSON string containing th... | details_json | string |
| 5 | The severity of the summary event | severity | int |
| 6 | The application | app | string |

| | Description | Id | Type |
|---|---|---|---|
| 7 | resource ID for the summary evet | resource_id | string |
| 8 | Component ID from the summary ... | component_id | string |
| 9 | HMPA type from the summary event | hmpa_type | string |
| 10 | Threat name from the summary e... | threat_name | string |
| 11 | Threat type from the summary ev... | threat_type | string |
| 12 | Username from the summary event | user_name | string |
| 13 | User SID from the summary event | user_sid | string |

```
interval: 600
name: "sophos_events_windows"
namespace: "com.sophos.central.data.xdr.query.avro"
tag: "stream"
type: "record"
version: "1.1.17"
```

▼ sophos_ips_windows {8}

```
description:
"Gets all network connections to and from this device with a number
of exclusions"
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | List of PIDs connected to the same ... | pids | string |
| 2 | List of SophosPIDs connected to th... | sophosPIDs | string |
| 3 | The source IP address of the IP event | sourceIp | string |
| 4 | The destination ip address of the ip ... | destinationIp | string |
| 5 | The destination port of the ip event | destinationPort | int |
| 6 | The protocol used in the ip event | protocol | int |
| 7 | List of times for the events | timestamps | string |

```
interval: 600
name: "sophos_ips_windows"
namespace: "com.sophos.central.data.xdr.query.avro"
```

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ sophos_urls_windows {8}

description:

"Gets all URLs accessed by this device with a number of exclusions"

| | Description | Id | Type |
|---|---|---|---|
| 1 | List of PIDs that accessed the same ... | pids | string |
| 2 | List of sophosPIDs that accessed to t... | sophosPIDs | string |
| 3 | The accessed domain | domain | string |
| 4 | List of Clean URLs accessed | cleanUrls | string |
| 5 | List of source IPs | sourceIps | string |
| 6 | List of destination IPs | destinationIps | string |
| 7 | List of times the URLs were accessed | timestamps | string |

interval: 600

name: "sophos_urls_windows"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ stopped_processes_windows_sophos {8}

description:

"Lists the stopped processes which have ended in target system from sophos_process_journal table."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The ID of the process and its start time ... | sophosPID | string |
| 2 | The process ID | endTime | long |

interval: 20

name: "stopped_processes_windows_sophos"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ threat_osx_hidden_users {8}

description:

"Detect users that do not appear on the login screen on macOS."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Username | username | string |
| 2 | User ID | uid | long |
| 3 | User's configured default shell | shell | string |

interval: 43200

name: "threat_osx_hidden_users"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ threat_pass_the_hash {8}

description:

"Detect login events that indicate a pass-the-hash attack."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The type of logon which was perf… | logon_type | int |
| 3 | The name of the trusted logon pr… | logon_process | string |
| 4 | IP address of machine from whic… | remote_address | string |
| 5 | Source port which was used for l… | remote_port | int |
| 6 | The process name that caused th… | name | string |
| 7 | The account that reported the log… | subject_username | string |
| 8 | The domain or computer name fo… | subject_domain | string |

| | Description | Id | Type |
|---|---|---|---|
| 9 | The name of the account that wa... | target_username | string |
| 10 | The domain or computer name fo... | target_domain | string |
| 11 | SID of account for which logon w... | target_sid | string |
| 12 | The length of NTLM Session Sec... | key_length | int |
| 13 | The Windows event provider | provider_name | string |
| 14 | The Windows event source | source | string |

```
interval:  3600
name:  "threat_pass_the_hash"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```

▼ threat_promisc_interfaces_linux {8}

```
description:  "Return all promiscuous network interfaces on Linux."
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | Interface name | interface | string |
| 2 | MAC of interface (optional) | mac | string |
| 3 | Flags (netdevice) for the device | flags | int |
| 4 | Promiscuous interface | promisc | long |
| 5 | Loopback interface | loopback | long |

```
interval:  43200
name:  "threat_promisc_interfaces_linux"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```

▼ threat_space_after_filename {8}

```
description:  "Detect files that have a space after the extension."
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | The path associated with the event | path | string |
| 2 | Change action (UPDATE, REMOVE, etc) | action | string |
| 3 | Owning user ID | uid | long |
| 4 | Owning group ID | gid | long |
| 5 | Permission bits | mode | string |
| 6 | Size of file in bytes | size | long |
| 7 | Last access time | atime | long |
| 8 | Last modification time | mtime | long |
| 9 | Last status change time | ctime | long |
| 10 | The SHA1 of the file after change | sha1 | string |
| 11 | The SHA256 of the file after change | sha256 | string |

interval: 43200

name: "threat_space_after_filename"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ threat_stickykeys_registry_backdoor {8}

description:

"Searches for the presence of the 'Debugger' registry key for common Windows accessibility tools. More info: (https://blogs.technet.microsoft.com/jonathantrull/2016/10/03/detecting-sticky-key-backdoors/)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | Name of the key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value, or 'subkey' if ite… | type | string |

| | Description | Id | Type |
|---|---|---|---|
| 5 | Data content of registry value | data | string |
| 6 | timestamp of the most recent registry write | mtime | long |

interval: 43200

name: "threat_stickykeys_registry_backdoor"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ user_accounts {8}

description: "Gets the list of active users in the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | User ID | uid | long |
| 2 | Group ID | gid | long |
| 3 | Username | username | string |
| 4 | Optional user description | description | string |
| 5 | User's home directory | directory | string |
| 6 | User's configured default shell | shell | string |
| 7 | Whether the account is roaming (domai... | type | string |
| 8 | User's UUID (Apple) or SID (Windows) | uuid | string |

interval: 43200

name: "user_accounts"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ user_events_linux {8}

description:

"Retrieves the user login events from the target system."

| | Description | Id | Type |
|---|---|---|---|
| 1 | User ID | uid | long |
| 2 | Process ID | pid | long |
| 3 | Message from the event | message | string |
| 4 | The file description for the process socket | audit_type | int |
| 5 | Supplied path from event | path | string |
| 6 | The Internet protocol address or family ID | address | string |
| 7 | The network protocol ID | terminal | string |
| 8 | Time of execution in UNIX time | time | long |

interval: 43200

name: "user_events_linux"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_app_compatibility {8}

description:

"Applications with special compatibility set for an executable"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_app_compatibility"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_app_disabled_exception_chain_validation {8}

description:

"Applications avoiding SEHOP. Anything other than 0 will disable Exception Chain Validation for this specific file. Seems to be disabled for a number of windows apps"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the data | analysis | string |

interval: 3600

name: "vulnerability_app_disabled_exception_chain_validation"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_app_mitigation_options {8}

description:

"Special exceptions for MitigationOptions - (https://docs.microsoft.com/en-us/windows/security/threat-protection/override-mitigation-options-for-app-related-security-policies)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |

| | Description | Id | Type |
|---|---|---|---|
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_app_mitigation_options"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_applocker_ruleset_enforcement_mode {8}

description:

"Check Applocker rule set configuration. 0 = Audit, 1 = Enforce, missing = Disabled"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_applocker_ruleset_enforcement_mode"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_audit_special_groups {8}

description:

"Special Logon Audit configuration too lax (https://blogs.technet.microsoft.com/jepayne/2015/11/26/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts/)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_audit_special_groups"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_certificate_padding {8}

description:

"Certificate Padding is disabled - (https://docs.microsoft.com/en-us/security-updates/securityadvisories/2014/2915720)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |

| | Description | Id | Type |
|---|---|---|---|
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_certificate_padding"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_dep {8}

description:

"DEP is not Admin Opt-out or Always-on - (http://www.maxi-pedia.com/noexecute+DEP+parameter+optin+optout)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_dep"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_developer_mode {8}

description: "Developer mode enabled"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_developer_mode"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_disallowed_paths {8}

description: "SRP path rule is missing"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_disallowed_paths"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_disallowed_paths_item_data {8}

description: "SRP blacklist rule is missing"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_disallowed_paths_item_data"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_fontblocking {8}

description: "FontBlocking is disabled"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_fontblocking"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_kernel_null_page_access {8}

description: "Kernel Null page access is allowed"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_kernel_null_page_access"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_opentype_font {8}

description:

"Determines if Adobe Type Manager Font Driver is disabled (https://technet.microsoft.com/en-us/library/security/ms15-078)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |

| | Description | Id | Type |
|---|---|---|---|
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |


```
interval:  3600
name:  "vulnerability_opentype_font"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```


▼ vulnerability_outlook_flags {8}

description:

"Checks if specific Outlook security patches have been disabled (https://www.fireeye.com/blog/threat-research/2019/12/breaking-the-rules-tough-outlook-for-home-page-attacks.html)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON string containing extra data | analysis | string |


```
interval:  3600
name:  "vulnerability_outlook_flags"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
```

version: "1.1.17"

▼ vulnerability_safer_flags_missing {8}

description: "SRP rule is missing"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON string containing extra data | analysis | string |

interval: 3600

name: "vulnerability_safer_flags_missing"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_safer_flags_not_enforcing {8}

description: "SRP rule is not enforcing"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_safer_flags_not_enforcing"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_secureboot {8}

description: "Secure boot supported but not enabled"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_secureboot"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_sehop {8}

description:

"Structured Exception Handling Overwrite Protection is disabled - (https://support.microsoft.com/en-ca/help/956607/how-to-enable-structured-exception-handling-overwrite-protection-sehop)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |

| | Description | Id | Type |
|---|---|---|---|
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_sehop"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_sehop_validation {8}

description:

"Structured Exception Handling Overwrite Protection is disabled - (https://support.microsoft.com/en-ca/help/956607/how-to-enable-structured-exception-handling-overwrite-protection-sehop)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_sehop_validation"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_spectre_meltdown {8}

description:

"Determines if patch for Spectre and Meltdown vulnerabilities is in stalled."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Count of patches | count | long |

interval: 3600

name: "vulnerability_spectre_meltdown"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_srp_default_level {8}

description:

"Checks Software Restriction Policies state. 0 = allow-only. 262144 (40000 Hex) = overrides that policy allowing all programs that are not specifically banned to execute"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_srp_default_level"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_srp_exclude_local_admin {8}

description:

"Checks Software Restriction Policies state. 0 = all users, 1 = all users except local admin"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_srp_exclude_local_admin"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_srp_transparent {8}

description:

"Software Restriction Policies enforcement disabled. if present and 0, indicates that Software Restriction Policies is turned off"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |

| | Description | Id | Type |
|---|---|---|---|
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

interval: 3600

name: "vulnerability_srp_transparent"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_uac_disabled {8}

description:

"UAC registry entry where 0 indicates that UAC is disabled."

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |

interval: 3600

name: "vulnerability_uac_disabled"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ vulnerability_unrestricted_paths {8}

description: "SRP path rules missing"

| | Description | Id | Type |
|---|---|---|---|

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

```
interval:  3600
name:  "vulnerability_unrestricted_paths"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```

▼ vulnerability_unrestricted_paths_item_data {8}

```
description:  "SRP allow list rule is missing"
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |
| 7 | JSON object representing the analysis | analysis | string |

```
interval:  3600
name:  "vulnerability_unrestricted_paths_item_data"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
```

version: "1.1.17"

▼ vulnerability_weak_algorithms {8}

description:

"Determines if Windows is configured to log certificates with weak crypto (https://technet.microsoft.com/library/dn375961(v=ws.11).aspx)"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The registry key | key | string |
| 2 | Full path to the value | path | string |
| 3 | Name of the registry value entry | name | string |
| 4 | Type of the registry value | type | string |
| 5 | Data content of registry value | data | string |
| 6 | time of the most recent registry write | mtime | long |

interval: 3600

name: "vulnerability_weak_algorithms"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_accessibility_md5 {8}

description: "Return hashes of Windows accessibility binaries."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Path to the hashed file | path | string |
| 2 | The directory of the hashed file | directory | string |
| 3 | SHA1 hash of provided filesystem data | sha1 | string |
| 4 | SHA256 hash of provided filesystem data | sha256 | string |

interval: 14400

name: "windows_accessibility_md5"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ windows_disk_md5 {8}

description:

"Return hashes of binaries running from Downloads folder."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Name of the file | filename | string |
| 2 | Last status change time | ctime | long |
| 3 | Absolute file path | path | string |
| 4 | The SHA-1 of the file | sha1 | string |
| 5 | The SHA-256 of the file | sha256 | string |
| 6 | The size of the file (in bytes) | fileSize | long |
| 7 | The machine learning malware score. | mlScore | int |
| 8 | The ml scores as a json structure | mlScoreData | string |
| 9 | The machine learning PUA score. | puaScore | int |
| 10 | The machine learning global reputa... | globalRep | int |
| 11 | The local reputation as a json struc... | globalRepData | string |
| 12 | The machine learning local reputati... | localRep | int |
| 13 | The local reputation as a json struc... | localRepData | string |
| 14 | The file info as a json structure | coreFileInfo | string |

interval: 14400

name: "windows_disk_md5"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ windows_event_audit_log_cleared {8}

description: "Retrieves a list of audit log clearing events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The user that cleared the events | subject_username | string |
| 3 | The domain of the user | subject_domain | string |
| 4 | Static description of the event | description | string |
| 5 | The Windows event provider | provider_name | string |
| 6 | The Windows event source | source | string |

```
interval:  3600
name:  "windows_event_audit_log_cleared"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```

▼ windows_event_audit_policy_changed {8}

```
description:  "Retrieves a list of audit policy changed events"
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The name of the account that m... | subject_username | string |
| 3 | the domain of the account that ... | subject_domain | string |
| 4 | The name of auditing Category ... | category | string |
| 5 | The name of auditing Subcateg... | subcategory | string |
| 6 | Changes that were made. | audit_policy_changes | string |
| 7 | Static description of the event | description | string |
| 8 | The Windows event provider | provider_name | string |
| 9 | The Windows event source | source | string |

```
interval:  3600
name:  "windows_event_audit_policy_changed"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
```

type: "record"

version: "1.1.17"

▼ windows_event_disallowed_credentials {8}

description: "Retrieves a list of disallowed credentials events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The name of the account that ma... | subject_username | string |
| 3 | the domain of the account that m... | subject_domain | string |
| 4 | The name of Security Package w... | package | string |
| 5 | UPN of the account for which del... | user_upn | string |
| 6 | SPN of the target service for whi... | target_server | string |
| 7 | Types of credentials which were ... | cred_type | string |
| 8 | Static description of the event | description | string |
| 9 | The Windows event provider | provider_name | string |
| 10 | The Windows event source | source | string |

interval: 3600

name: "windows_event_disallowed_credentials"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_dos_attack_detected {8}

description: "Retrieves a list of dos attack detected events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | Type | type | string |
| 3 | Static description of the event | description | string |
| 4 | The Windows event provider | provider_name | string |
| 5 | The Windows event source | source | string |

```
interval:  3600
name:  "windows_event_dos_attack_detected"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```

▼ windows_event_invalid_logon {8}

```
description:  "Retrieves a list of invalid logon events"
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The account that reported the ... | subject_username | string |
| 3 | The domain or computer nam... | subject_domain | string |
| 4 | The name of the account that ... | target_username | string |
| 5 | The domain or computer nam... | target_domain | string |
| 6 | The reason the logon failed | status | string |
| 7 | Textual explanation of Status f... | failure_reason | string |
| 8 | Additional information about l... | sub_status | string |
| 9 | The type of logon which was p... | logon_type | int |
| 10 | The name of the trusted logon... | logon_process | string |
| 11 | The authentication package | authentication_package | string |
| 12 | The transmitted services | transmitted_services | string |
| 13 | The length of NTLM Session ... | key_length | int |
| 14 | The process name that cause... | name | string |
| 15 | IP address of machine from w... | remote_address | string |
| 16 | Source port which was used f... | remote_port | int |
| 17 | Static description of the event | description | string |
| 18 | The Windows event provider | provider_name | string |
| 19 | The Windows event source | source | string |

```
interval:  3600
name:  "windows_event_invalid_logon"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```

▼ windows_event_invalid_logon_brute_force {8}

```
description:  "Retrieves a list of brute force events"
```

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The account that reported the ... | subject_username | string |
| 3 | The domain or computer nam... | subject_domain | string |
| 4 | The name of the account that ... | target_username | string |
| 5 | The domain or computer nam... | target_domain | string |
| 6 | The reason the logon failed | status | string |
| 7 | Textual explanation of Status f... | failure_reason | string |
| 8 | Additional information about l... | sub_status | string |
| 9 | The type of logon which was p... | logon_type | int |
| 10 | The name of the trusted logon... | logon_process | string |
| 11 | The authentication package | authentication_package | string |
| 12 | The transmitted services | transmitted_services | string |
| 13 | The length of NTLM Session ... | key_length | int |
| 14 | The process name that cause... | name | string |
| 15 | IP address of machine from w... | remote_address | string |
| 16 | Source port which was used f... | remote_port | int |
| 17 | Static description of the event | description | string |
| 18 | The Windows event provider | provider_name | string |
| 19 | The Windows event source | source | string |

interval: 3600

name: "windows_event_invalid_logon_brute_force"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_replay_attack {8}

description: "Retrieves a list of event replay attack events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The subject user | subject_username | string |
| 3 | The subject domain | subject_domain | string |
| 4 | The target user | target_username | string |
| 5 | The target domain | target_domain | string |
| 6 | The request type | request_type | string |
| 7 | The logon process | logon_process | string |
| 8 | The authentication package | authentication_package | string |
| 9 | The transmitted services | transmitted_services | string |
| 10 | The process name that cause... | name | string |
| 11 | Static description of the event | description | string |
| 12 | The Windows event provider | provider_name | string |
| 13 | The Windows event source | source | string |

interval: 3600

name: "windows_event_replay_attack"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_scheduled_task_created {8}

description: "Retrieves a list of scheduled task created events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The name of the account that cre… | subject_username | string |
| 3 | The domain of the account that cr… | subject_domain | string |
| 4 | The task name of the new task | task_name | string |
| 5 | The XML content of the new task | task_content | string |
| 6 | Static description of the event | description | string |
| 7 | The Windows event provider | provider_name | string |
| 8 | The Windows event source | source | string |

interval: 3600

name: "windows_event_scheduled_task_created"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_successful_logon {8}

description: "Retrieves a list of successful logon events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | List of times for the same logo… | event_timestamps | string |
| 2 | The Windows event ID | eventid | int |
| 3 | The name of the account that … | subject_username | string |
| 4 | The domain of the account tha… | subject_domain | string |
| 5 | The account for which the log… | target_username | string |
| 6 | The target domain | target_domain | string |
| 7 | Hexadecimal value for the ne… | target_logon_id | string |
| 8 | Hexadecimal value for the log… | subject_logon_id | string |
| 9 | The type of logon which was p… | logon_type | int |

| | Description | Id | Type |
|---|---|---|---|
| 10 | The name of the trusted logon... | logon_process | string |
| 11 | The name of the authenticatio... | authentication_package | string |
| 12 | The list of transmitted services | transmitted_services | string |
| 13 | The length of NTLM Session ... | key_length | int |
| 14 | full path and the name of the ... | name | string |
| 15 | IP address of machine from w... | remote_address | string |
| 16 | Source port which was used f... | remote_port | int |
| 17 | Static description of the event | description | string |
| 18 | The Windows event provider | provider_name | string |
| 19 | The Windows event source | source | string |

interval: 3600

name: "windows_event_successful_logon"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_uac_bypass_journal {8}

description:

"Gets a list of uac bypass events from Sophos registry journal"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The time (unix epoch) the key was crea... | event_time | long |
| 2 | The registry key path and name | keyName | string |
| 3 | The stored registry value | value | string |
| 4 | The event type | eventType | int |
| 5 | The process ID that produced the regist... | sophosPID | string |
| 6 | Static description based upon the regist... | description | string |

interval: 480

name: "windows_event_uac_bypass_journal"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_uac_bypass_registry {8}

description: "Retrieves a list of uac bypass events from registry"

| | Description | Id | Type |
|---|---|---|---|
| 1 | Timestamp of the most recent registry … | event_time | long |
| 2 | The registry key path and name | keyName | string |
| 3 | Data content of registry value | value | string |
| 4 | Static description based upon the regist… | description | string |

interval: 3600

name: "windows_event_uac_bypass_registry"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_user_account_changed {8}

description: "Retrieves a list of user account changed events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | hexadecimal value that can he… | subject_logon_id | string |
| 3 | Internet-style login name for t… | user_principal_name | string |
| 4 | The list of user privileges whic… | privilege_list | string |
| 5 | Logon name for account used … | sam_account_name | string |
| 6 | It is a name, displayed in the … | display_name | string |
| 7 | User's home directory. | home_directory | string |
| 8 | | home_path | string |
| 9 | Specifies the path of the acco… | script_path | string |

| | Description | Id | Type |
|---|---|---|---|
| 10 | Specifies a path to the accoun... | profile_path | string |
| 11 | Contains the list of NetBIOS o... | user_workstations | string |
| 12 | The date when the account ex... | account_expires | string |
| 13 | The list of SPNs to which this ... | allowed_to_delegate_to | string |
| 14 | Shows the list of changes in u... | uac | string |
| 15 | If you change any setting usin... | user_parameters | string |
| 16 | The name of the account that ... | subject_username | string |
| 17 | Subjectâ€™s domain or comp... | subject_domain | string |
| 18 | The name of the account that ... | target_username | string |
| 19 | Last time the accountâ€™s pa... | password_last_set | string |
| 20 | Target accountâ€™s domain o... | target_domain | string |
| 21 | Static description of the event | description | string |
| 22 | The Windows event provider | provider_name | string |
| 23 | The Windows event source | source | string |

interval: 3600

name: "windows_event_user_account_changed"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_user_account_created {8}

description: "Retrieves a list of user account created events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The name of the account that ... | subject_username | string |
| 3 | The domain of the account tha... | subject_domain | string |
| 4 | The name of the account that ... | target_username | string |

| | Description | Id | Type |
|---|---|---|---|
| 5 | The domain of the account tha… | target_domain | string |
| 6 | The list of user privileges whic… | privilege_list | string |
| 7 | Logon name for account used … | sam_account_name | string |
| 8 | The value of displayName attr… | display_name | string |
| 9 | Internet-style login name for t… | user_principal_name | string |
| 10 | User's home directory. | home_directory | string |
| 11 | User's home path. | home_path | string |
| 12 | Specifies the path of the acco… | script_path | string |
| 13 | Specifies a path to the accoun… | profile_path | string |
| 14 | Contains the list of NetBIOS o… | user_workstations | string |
| 15 | The date when the account ex… | account_expires | string |
| 16 | The list of SPNs to which this … | allowed_to_delegate_to | string |
| 17 | Shows the list of changes in u… | uac | string |
| 18 | For new local accounts this fie… | user_parameters | string |
| 19 | Static description of the event | description | string |
| 20 | The Windows event provider | provider_name | string |
| 21 | The Windows event source | source | string |

interval: 3600

name: "windows_event_user_account_created"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_event_user_account_deleted {8}

description: "Retrieves a list of user account deleted events"

| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |

| | Description | Id | Type |
|---|---|---|---|
| 2 | The name of the account that req... | subject_username | string |
| 3 | The domain of the account that re... | subject_domain | string |
| 4 | The name of the account that was... | target_username | string |
| 5 | The domain of the account that w... | target_domain | string |
| 6 | The list of user privileges which w... | privilege_list | string |
| 7 | Static description of the event | description | string |
| 8 | The Windows event provider | provider_name | string |
| 9 | The Windows event source | source | string |


```
interval:  3600
name:  "windows_event_user_account_deleted"
namespace:  "com.sophos.central.data.xdr.query.avro"
tag:  "DataLake"
type:  "record"
version:  "1.1.17"
```


▼ windows_event_user_account_locked_out {8}


```
description:  "Retrieves a list of user account locked out events"
```


| | Description | Id | Type |
|---|---|---|---|
| 1 | The Windows event ID | eventid | int |
| 2 | The name of the account that perf... | subject_username | string |
| 3 | The domain of the account that pe... | subject_domain | string |
| 4 | The name of the account that was... | target_username | string |
| 5 | the name of computer account fro... | target_domain | string |
| 6 | Static description of the event | description | string |
| 7 | The Windows event provider | provider_name | string |
| 8 | The Windows event source | source | string |


```
interval:  3600
name:  "windows_event_user_account_locked_out"
namespace:  "com.sophos.central.data.xdr.query.avro"
```

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_powershell_script_blocks {8}

description: "Retrieves powershell script blocks"

| | Description | Id | Type |
|---|---|---|---|
| 1 | Timestamp of the windows pow... | time | long |
| 2 | The unique GUID of the powers... | script_block_id | string |
| 3 | The total number of script block... | script_block_count | int |
| 4 | Truncated script text | script_text | string |
| 5 | Is the script text truncated | script_text_truncated | int |
| 6 | The name of the Powershell script | script_name | string |
| 7 | The path for the Powershell script | script_path | string |

interval: 600

name: "windows_powershell_script_blocks"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_programs {8}

description:

"Get all the installed programs on the target machine."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Commonly used product name | name | string |
| 2 | Product version information | version | string |
| 3 | The language of the product | language | string |
| 4 | The installation source of the pro... | install_source | string |
| 5 | Name of the product supplier | publisher | string |
| 6 | Product identification such as a s... | identifying_number | string |

| | Description | Id | Type |
|---|---|---|---|
| 7 | Date that this product was install... | install_date | string |

interval: 14400

name: "windows_programs"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_services_md5 {8}

description:

"Lists auto-start, non-system services including binary hashes."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Service name | name | string |
| 2 | Service Display name | display_name | string |
| 3 | Service Description | description | string |
| 4 | Service start type | start_type | string |
| 5 | Path to Service Executable | path | string |
| 6 | SHA1 hash of the service executable | sha1 | string |
| 7 | SHA256 hash of the service executable | sha256 | string |

interval: 14400

name: "windows_services_md5"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_shell_md5 {8}

description: "Return hashes of Windows shell binaries."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Path to the shell binary | path | string |

| | Description | Id | Type |
|---|---|---|---|
| 2 | Directory of the shell binary | directory | string |
| 3 | SHA1 hash of the binary | sha1 | string |
| 4 | SHA1 hash of the binary | sha256 | string |

interval: 86400

name: "windows_shell_md5"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "stream"

type: "record"

version: "1.1.17"

▼ windows_startup_items {8}

description: "Shows descriptions of startup items."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Source of the startup item | source | string |
| 2 | Command line of the startup item | cmdline | string |
| 3 | Path to the startup item | path | string |
| 4 | Name of the startup item | NAME | string |
| 5 | Startup status; either enabled or disabled | status | string |
| 6 | The authenticode signature of the startup ... | result | string |
| 7 | The SHA-256 hash of the startup item | sha256 | string |

interval: 14400

name: "windows_startup_items"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_startup_programs_md5 {8}

description: "Lists hashes of binaries running at startup."

| | Description | Id | Type |
|---|---|---|---|

| | Description | Id | Type |
|---|---|---|---|
| 1 | Path to the startup item | mod_path | string |
| 2 | Name of startup item | name | string |
| 3 | Path to the startup item | path | string |
| 4 | Startup Item or Login Item | type | string |
| 5 | Startup status; either enabled or di... | status | string |
| 6 | The user associated with the startu... | username | string |
| 7 | The SHA-1 hash of the startup item | sha1 | string |
| 8 | The SHA-256 hash of the startup item | sha256 | string |
| 9 | The size of the file (in bytes) | fileSize | long |
| 10 | The machine learning malware score | mlScore | int |
| 11 | The ml scores as a json structure | mlScoreData | string |
| 12 | The machine learning PUA score | puaScore | int |
| 13 | The machine learning global reputa... | globalRep | int |
| 14 | The global reputation as a json stru... | globalRepData | string |
| 15 | The machine learning local reputation | localRep | int |
| 16 | The local reputation as a json struc... | localRepData | string |
| 17 | The file info as a json structure | coreFileInfo | string |

```
interval: 14400
name: "windows_startup_programs_md5"
namespace: "com.sophos.central.data.xdr.query.avro"
tag: "DataLake"
type: "record"
version: "1.1.17"
```

▼ windows_updates_patch {8}

```
description:
"Gets all the installed updates from the Windows Update Service."
```

| | Description | Id | Type |
|---|---|---|---|

| | Description | Id | Type |
|---|---|---|---|
| 1 | The KB ID of the patch | hotfix_id | string |
| 2 | Short description of the patch | caption | string |
| 3 | Full description of the patch | description | string |
| 4 | The system context in which the patch... | installed_by | string |
| 5 | The date when the patch was installed | installed_on | string |

interval: 43200

name: "windows_updates_patch"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

version: "1.1.17"

▼ windows_wsl_installed {8}

description:

"Lists all devices that have WSL (Windows Subsytem for Linux) installed."

| | Description | Id | Type |
|---|---|---|---|
| 1 | Name of the file | filename | string |
| 2 | Absolute file path | path | string |
| 3 | Last access time | atime | long |
| 4 | Last modification time | mtime | long |
| 5 | Last status change time | ctime | long |
| 6 | File product version | product_version | long |
| 7 | The SHA-256 hash of the file after ... | sha256 | string |

interval: 86400

name: "windows_wsl_installed"

namespace: "com.sophos.central.data.xdr.query.avro"

tag: "DataLake"

type: "record"

```
        version:  "1.1.17"
```