SOPHOS
Security made simple.

SDR Exporter tool for EDR Early Access Phase 0

For admins looking to do more detailed investigations than Threat Cases (formerly RCA) currently allow, the SDR Exporter utility is a tool which can convert Sophos Data Recorder snapshots on an endpoint into a format where advanced queries can be run. For the EDR Phase 0 Private Early Access Program customers will require direct access to existing snapshots on endpoints. The snapshots can then be converted to a SQLite database using the SDR Exporter tool.

Downloading the SDR Exporter:

The tool is available from the Sophos Downloads. There is a 64 bit version and 32 bit version of the tool available:

Download 64 bit version here
Download 32 bit version here

Accessing Snapshots and Converting to a SQLite DB using the SDR Exporter:

Notes:

- If tamper protection is enabled admins must be running from an elevated command prompt to get access to saved snapshots
- Endpoints store the last 10 snapshots in the *%PROGRAMDATA%\Sophos\Endpoint Defense\Data\Saved Data* directory

The minimal usage for the tool would be to specify the path and filename of the snapshot to be converted with path and filename of the output file as seen below:

SDRExporter.exe –i <path to snapshot tgz> -o <path to output file>

The resulting DB can be interpreted using many different SQLite tools, click here to download the official sqlite3 command-line tool.

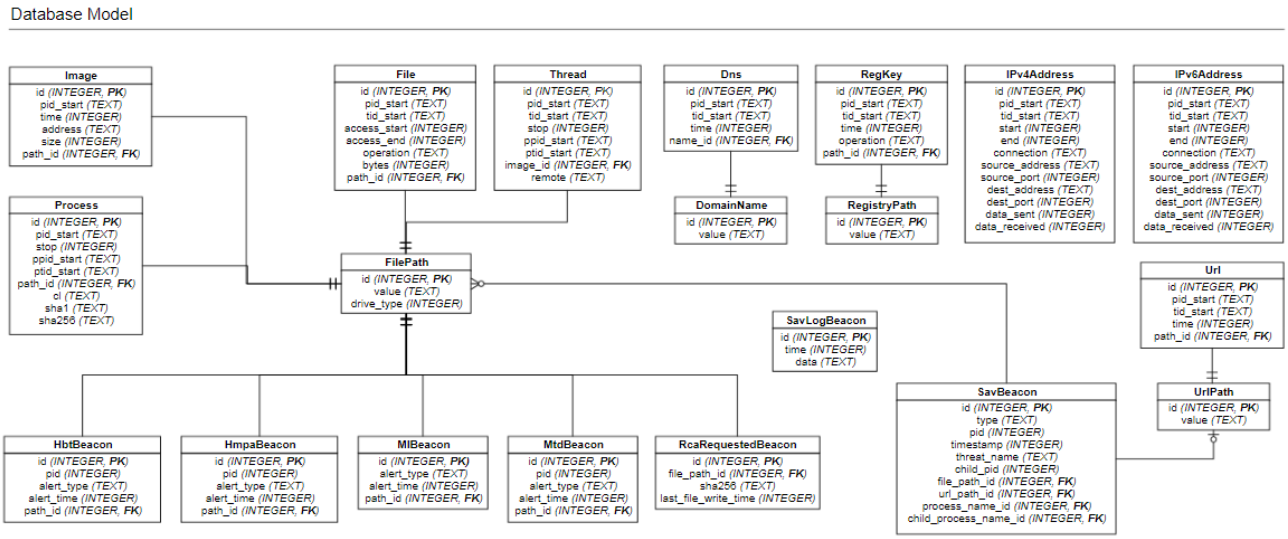
SDR Exporter Help:

Help for the tool can be seen by running the command '*SDRExporter.exe –h'* command:

Options:

-h [--help]	Print help message
-i [--input-path] arg	Path to input snapshot container file
-o [--output-path] arg	Path to output file
-f [--output-format] arg (=sqlite)	Output format (choices: sqlite only for EAP0)
-v [--output-version] arg	Output version - default is latest

EAP 0 database Schema of an exported snapshot:



EAP 0 Schema Descriptions:

Image

Column Name	Type	Description
Id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that loaded the image, which can uniquely identify the process in the **Process** table - e.g. *2608:130883139897447781*
Time	INTEGER	The load time of the image (as Windows Filetime) - e.g. *130883139897447781*
address	TEXT	The load address of the image - e.g. *0x0000000076DB0000*
Size	INTEGER	The size of the image - e.g. *1740800*
path_id	INTEGER	The ID of the file path, to identify a row in the **FilePath** table

Process

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process - e.g. *2608:130883139897447781*

Column Name	Type	Description
stop	INTEGER	The stop time of the process (as Windows Filetime), or 0 if still running - e.g. *130883139897603781*
ppid_start	TEXT	The PID and start-time (as Windows Filetime) of the parent process, which can uniquely identify another row in the **Process** table - e.g. *544:130883139857667711*
ptid_start	TEXT	The TID and start-time (as Windows Filetime) of the parent thread, which can uniquely identify a row in the **Thread** table - e.g. *1156:130883139857667711*
path_id	INTEGER	The ID of the executable file path, to identify a row in the **FilePath** table
cl	TEXT	The command-line parameters -e .g. *C:\Windows\system32\wermgr.exe –queuereporting*
sha1	TEXT	The SHA1 hash of the process's executable file - e.g. *0df224fc2785f656c821792d594545cd4689ea91*
sha256	TEXT	The SHA256 hash of the process's executable file - e.g. *2ae00de49d51186c88014f382878c2abc9195a8db811715909c37ca9*

Dns

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that performed the DNS query, which can uniquely identify a row in the **Process** table - e.g. *10916:130928601588610841*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that performed the DNS query, which can uniquely identify a row in the **Thread** table - e.g. *10848:130928601596731305*
time	INTEGER	The time (as Windows Filetime) that the DNS query was performed - e.g. *130928601718008242*
name_id	INTEGER	The ID of the domain name, to identify a row in the **DomainName** table

File

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that performed the file operation, which can uniquely identify a row in the **Process** table - e.g. *2888:130895661806716096*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that performed the file operation, which can uniquely identify a row in the **Thread** table - e.g. *908:130895661806716096*
access_start	INTEGER	The time (as Windows Filetime) that the file operation started - e.g. *130895661807184097*
access_end	INTEGER	The time (as Windows Filetime) that the file operation ended - e.g. *130895661830696214*
operation	TEXT	The type of file operation performed ("*FileRead*" or "*FileWrite*")

Column Name	Type	Description
bytes	INTEGER	The number of bytes read or written
path_id	INTEGER	The ID of the file path, to identify a row in the **FilePath** table

Thread

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that the thread was created in, which can uniquely identify a row in the **Process** table - e.g. *2888:130895661806716096*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that was created - e.g. *908:130895661806716096*
stop	INTEGER	The stop time of the process (as Windows Filetime), or 0 if still running - e.g. *130883139897603781*
ppid_start	TEXT	The PID and start-time (as Windows Filetime) of the parent process that created the thread, which can uniquely identify another row in the **Process** table -e.g. *544:130883139857667711*
ptid_start	TEXT	The TID and start-time (as Windows Filetime) of the parent thread that created this thread, which can uniquely identify a row in the **Thread** table - e.g. *1156:130883139857667711*
image_id	INTEGER	The ID of the image that the thread was started in, to identify a row in the **FilePath** table
remote	TEXT	If present, can have the value "RemoteThread" to indicate that the thread was created by a process other than the parent process and the process itself

Url

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that accessed the URL, which can uniquely identify a row in the **Process** table - e.g. *10916:130928601588610841*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that accessed the URL, which can uniquely identify a row in the **Thread** table - e.g. *10848:130928601596731305*
time	INTEGER	The time (as Windows Filetime) that the URL was accessed - e.g. *130928601718008242*
path_id	INTEGER	The ID of the URL path, to identify a row in the **UrlPath** table

RegKey

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that accessed the registry key, which can uniquely identify a row in the **Process** table - e.g. *10916:130928601588610841*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that accessed the registry key, which can uniquely identify a row in the **Thread** table - e.g. *10848:130928601596731305*
time	INTEGER	The time (as Windows Filetime) that the registry key was accessed - e.g. *130928601718008242*
operation	TEXT	The type of registry operation that was performed (can be "*Create*", "*Delete*", "*SetValue*", "*DeleteValue*")
path_id	INTEGER	The ID of the registry path, to identify a row in the **RegistryPath** table

IPv4Address

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that connected to the IP address, which can uniquely identify a row in the **Process** table - e.g. *10916:130928601588610841*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that connected to the IP address, which can uniquely identify a row in the **Thread** table - e.g. *10848:130928601596731305*
start	INTEGER	The time (as Windows Filetime) that the connection was established - e.g. *130896042083063327*
end	INTEGER	The time (as Windows Filetime) that the connection was closed - e.g. *130896042083063327*
connection	TEXT	If present, the type of the connection (can be "TCP_IPv4_Connect", "TCP_IPv4_Accept", "TCP_v4", "UDP_v4")
source_address	TEXT	The source IP address of the connection - e.g. *192.168.183.128*
source_port	INTEGER	The source port of the connection - e.g. *52699*
dest_address	TEXT	The target IP address of the connection - e.g. *204.79.197.200*
dest_port	INTEGER	The target port of the connection - e.g. *80*
data_sent	INTEGER	The number of bytes sent over the connection
data_received	INTEGER	The number of bytes received over the connection

IPv6Address

Column Name	Type	Description
id	INTEGER	Unique row ID
pid_start	TEXT	The PID and start-time (as Windows Filetime) of the process that connected to the IP address, which can uniquely identify a row in the **Process** table - e.g. *10916:130928601588610841*
tid_start	TEXT	The TID and start-time (as Windows Filetime) of the thread that connected to the IP address, which can uniquely identify a row in the **Thread** table - e.g. *10848:130928601596731305*
start	INTEGER	The time (as Windows Filetime) that the connection was established - e.g. *130896042083063327*
end	INTEGER	The time (as Windows Filetime) that the connection was closed - e.g. *130896042083063327*
connection	TEXT	If present, the type of the connection (can be "TCP_IPv6_Connect", "TCP_IPv6_Accept", "TCP_v6", "UDP_v6")
source_address	TEXT	The source IP address of the connection - e.g. *0000:0000:0000:0000:0000:0000:0000:0001*
source_port	INTEGER	The source port of the connection - e.g. *52699*
dest_address	TEXT	The target IP address of the connection - e.g. *fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff*
dest_port	INTEGER	The target port of the connection - e.g. *80*
data_sent	INTEGER	The number of bytes sent over the connection
data_received	INTEGER	The number of bytes received over the connection

DomainName

Column Name	Type	Description
id	INTEGER	Unique row ID
value	TEXT	The domain name, e.g. *acroipm.adobe.com*

FilePath

Column Name	Type	Description
id	INTEGER	Unique row ID
value	TEXT	The canonicalized file path (converted to a DOS path if possible), e.g. *c:\windows\fonts\staticcache.dat*
drive_type	INTEGER	The identified drive type that the path resides on - can have one of the following integer values: 0 - unknown 1 - fixed 2 - removable

Column Name	Type	Description
		3 - network 4 - CD-ROM

RegistryPath

Column Name	Type	Description
id	INTEGER	Unique row ID
value	TEXT	The full registry path, e.g. *\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters*

UrlPath

Column Name	Type	Description
id	INTEGER	Unique row ID
value	TEXT	The full URL path, e.g. *http://msdn.microsoft.com/*

HbtBeacon

Column Name	Type	Description
id	INTEGER	Unique row ID
pid	INTEGER	The PID of the process that triggered the Heartbeat alert, e.g. *908* - to associate with a process in the **Process** table, query the pid_start and path_id, e.g. *"pid_start LIKE "908:%" AND path_id=2"*
alert_type	TEXT	The name of the alert - e.g. *C2/Generic-C*
alert_time	INTEGER	The time (as Windows Filetime) of the alert - e.g. *130928601718008242*
path_id	INTEGER	The ID of the process path that triggered the alert, to identify a row in the **FilePath** table

HmpaBeacon

Column Name	Type	Description
id	INTEGER	Unique row ID
pid	INTEGER	The PID of the process that triggered the HMPA alert, e.g. *908* - to associate with a process in the **Process** table, query the pid_start and path_id, e.g. *"pid_start LIKE "908:%" AND path_id=2"*
alert_type	TEXT	The name of the alert - e.g. *StackPivot*

Column Name	Type	Description
alert_time	INTEGER	The time (as Windows Filetime) of the alert - e.g. *130928601718008242*
path_id	INTEGER	The ID of the process path that triggered the alert, to identify a row in the **FilePath** table

MtdBeacon

Column Name	Type	Description
id	INTEGER	Unique row ID
pid	INTEGER	The PID of the process that triggered the MTD alert, e.g. *908* - to associate with a process in the **Process** table, query the pid_start and path_id, e.g. *"pid_start LIKE "908:%" AND path_id=2"*
alert_type	TEXT	The name of the alert - e.g. *C2/Generic-B*
alert_time	INTEGER	The time (as Windows Filetime) of the alert - e.g. *130928601718008242*
path_id	INTEGER	The ID of the process path that triggered the alert, to identify a row in the **FilePath** table

MlBeacon

Column Name	Type	Description
id	INTEGER	Unique row ID
alert_type	TEXT	The name of the alert (which represents a SAV, ML or reputation-based detection on a PE file) - e.g. *ML/PE-A*
alert_time	INTEGER	The time (as Windows Filetime) of the alert - e.g. *130928601718008242*
path_id	INTEGER	The ID of the file path that the alert was triggered on, to identify a row in the **FilePath** table

RcaRequestedBeacon

Column Name	Type	Description
id	INTEGER	Unique row ID
file_path_id	INTEGER	The ID of the file path that the alert was triggered on, to identify a row in the **FilePath** table
sha256	TEXT	If present, the SHA256 hash of the file, e.g. *2ae00de49d51186c88014f382878c2abc9195a8db811715909c37ca977653513*
last_file_write_time	INTEGER	If present, the time (as Windows Filetime) of the most recent file write to the file - e.g. *130928601718008242*

SavBeacon

Column Name	Type	Description
id	INTEGER	Unique row ID
type	TEXT	The type of the SAV alert - can be one of the following: "on_access_file", "on_demand_file", "on_create_key", "on_delete_key", "set_reg_key_value", "on_create_or_delete_process", "on_close_modified_file_of_interest", "on_create_remote_thread", "web_scan", "bops", "phenotype", "app_control", "network_threat", "heartbeat"
pid	INTEGER	The PID of the process, or *0* if not applicable - e.g. *908*
timestamp	INTEGER	The time (as Windows Filetime) of the alert - e.g. *130928601718008242*
threat_name	TEXT	The SAV detection name - e.g. *EICAR-AV-Test*
child_pid	INTEGER	The PID of the target process for "on_create_or_delete process" and "on_create_remote_thread" beacons, or *0* if not applicable - e.g. *908*
file_path_id	INTEGER	If applicable, the ID of the file/process path that the alert was triggered on, to identify a row in the **FilePath** table
url_path_id	INTEGER	ID of the URL path for "web_scan" and "heartbeat" beacons, to identify a row in the **UrlPath** table
process_name_id	INTEGER	If applicable, the ID of the process path, to identify a row in the **FilePath** table
child_process_name_id	INTEGER	The ID of the target process path for "on_create_or_delete process" and "on_create_remote_thread" beacons, to identify a row in the **FilePath** table

SavLogBeacon

Note: these beacons are only generated by older versions of the endpoint

Column Name	Type	Description
id	INTEGER	Unique row ID
time	TEXT	The time (as Windows Filetime) of the alert - e.g. *130928601718008242*
data	INTEGER	The raw data associated with the detection - e.g. *20151124 230357 File "\\192.168.183.1\M$\Sysadmin\....*

SDR Exporter Feedback:

Sophos is keen to capture customer feedback in regards to formats customers would like the SDR Exporter to support and preferred methods for generating and getting access to snapshots so that direct access to the endpoint is not required.