Sysmon View Data Model

nader@nosecurecode.com

Sysmon Events
Parsed data fields (IPs, Hashes, Registry Keys, etc.)
Entity used to reference all events in one table

ProcessGUID field represents the unique identifier reported by Sysmon and used to describe a run-session, it is reported by all events except the *DriveLoaded* event.

The **AllEvents** table references this field too as *CorrelationGUID*, check the sample queries later to see how to build a timeline for Sysmon events using this data field

RegistryObjectRenamed: UtcTime, ProcessGuid, ProcessId, Image, EventType, TargetObject, NewName, ImageExe, EventType2, EventType2Name, FID, Computer, RuleName

RegistryValueSet: UtcTime, ProcessGuid, ProcessId, Image, EventType, TargetObject, Details, ImageExe, EventType2, EventType2Name, FID, Computer, RuleName

RegistryObjectAddedOrDeleted: UtcTime, ProcessGuid, ProcessId, Image, EventType, TargetObject, ImageExe, EventType2, EventType2Name, FID, Computer, RuleName

PipeCreated: UtcTime, ProcessGuid, ProcessId, PipeName, Image, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

PipeConnected: UtcTime, ProcessGuid, ProcessId, PipeName, Image, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

WMIBinding: UtcTime, Operation, User, Consumer, Filter, EventType, EventTypeName, FID, Computer, RuleName

WMIFilter: UtcTime, Operation, User, EventNamespace, Name, Query, EventType, EventTypeName, FID, Computer, RuleName

WMIConsumer: UtcTime, Operation, User, Name, Type, Destination, EventType, EventTypeName, FID, Computer, RuleName

ProcessCreate: UtcTime, ProcessGuid, ProcessId, Image, CommandLine, CurrentDirectory, User, LogonGuid, LogonId, TerminalSessionId, IntegrityLevel, Hashes, MD5, SHA1, SHA256, ParentProcessGuid, ParentProcessId, ParentImage, ParentCommandLine, ImageExe, ParentImageExe, EventType, EventTypeName, FID, Computer, RuleName

All events tables contain a reference to the source device and the new RuleName introduced in Sysmon version 8.0. The events hashes are also parsed into seprate fields (MD5, SHA1 and SHA256)

ProcessAccessed: UtcTime, SourceProcessGUID, SourceProcessId, SourceThreadId, SourceImage, TargetProcessGUID, TargetProcessId, TargetImage, GrantedAccess, CallTrace, SourceImageExe, TargetImageExe, EventType, EventTypeName, FID, Computer, RuleName

ProcessTerminated: UtcTime, ProcessGuid, ProcessId, Image, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

DriverLoaded: UtcTime, ImageLoaded, Hashes, MD5, SHA1, SHA256, Signed, Signature, EventType, EventTypeName, FID, Computer, RuleName

RawAccessReadDetected: UtcTime, ProcessGuid, ProcessId, Image, Device, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

FileCreated: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, GrantedAccess, CreationUtcTime, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

FileCreationTimeChanged: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime, PreviousCreationUtcTime, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

FileStreamCreated: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime, Hashes, MD5, SHA1, SHA256, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

AllEvents: This is a relational data model, referencing all events types requires a special entity that can group those events with common attributes (for example, in Sysmon View, this table is used to build a timeline of events). The FID field is used to track back to the original event (for example, to retrive the original event details)

ImageLoaded: UtcTime, ProcessGuid, ProcessId, Image, ImageLoaded, Hashes, MD5, SHA1, SHA256, Signed, Signature, ImageExe, ImageLoadedExe, EventType, EventTypeName, FID, Computer, RuleName

Foreign Key

AllEvents: UtcTime, EventType, EventTypeName, GID, CorrelationGuid, EventDetails, Computer, RuleName, Indexes

Primary Key

CreateRemoteThreadDetected: UtcTime, SourceProcessGuid, SourceProcessId, SourceImage, TargetProcessGuid, TargetProcessId, TargetImage, NewThreadId, StartAddress, StartModule, StartFunction, SourceImageExe, TargetImageExe, EventType, EventTypeName, FID, Computer, RuleName

NetworkConnectionDetected: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated, SourceIsIpv6, SourceIp, SourceHostname, SourcePort, SourcePortName, SourceCountry, SourceCountryCode, DestinationIsIpv6, DestinationIp, DestinationHostname, DestinationPort, DestinationPortName, DestinationCountry, DestinationCountryCode, ImageExe, EventType, EventTypeName, FID, Computer, RuleName

NetworkConnectionDetected contains additional fields to *Geo-locate* IP addresses (Country and Country Code)

Those entities were meant to separate the various IOCs, still, using the **FID** field, they can be tracked back to their reported event, check the following ***Sample Queries***

AllImageExes is used to aggergate binaries from all related Sysmon events, this helps in faster search and detection of anomolies of binary file path. Additionally, the table is used to separate the full binary path (Image field) from the executable (ImageExe).

AllImageExes: FID, UtcTime, Image, ImageExe, ProcessGuid, EventType, EventTypeName

AllHashes: FID, UtcTime, ReportedByVT, MD5, SHA1, SHA256

AllIPAddresses: FID, UtcTime, IPAddress, Direction, Initiated

AllPorts: FID, UtcTime, Port, PortName, Direction

AllRegTargets: FID, UtcTime, TargetObject

AllHosts: FID, UtcTime, Hostname

Foreign Key

AllHashes contains all reported hashes, with addtional field to highlight if the hash was reported by VT

Sample Query: Produce a summary of all Sysmon reported Network ports.

```
SELECT PortName, COUNT(*) AS Total FROM AllPorts GROUP BY PortName;
```

Sample Query: List all registry events reported by Sysmon involving a registry key containing ‘Start’ string in it.

```
SELECT FID, TargetObject FROM AllRegTargets WHERE TargetObject LIKE ‘%Start%’;
```

The reason for selecting FID, is to track back to the event details. For example, having the FID, we can find the event CorrelationGUID as follows:

```
SELECT CorrelationGuid FROM AllEvents WHERE GID = 223;
```

If we have the CorrelationGUID, we can retrieve a timeline of all the events associated with this session GUID

```
SELECT * FROM ALLEvents WHERE CorrelationGuid IS '{C748F056-5753-58F7-0000-0010AB870100}' ORDER BY UtcTime;
```