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

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 contain a reference to the device and the new RuleName introduces in lates version of Sysmon. 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

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

Foreign Key

The **AllEvents** table is used to reference all events, this is a relational data model, referencing all events (for example, it is used in Sysmon View to build the timeline) requires an entity that can group those events with common attributes, to track back to teh original event, the FID is used

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

NetworkConnection contains additional fields to geo locate IP addresses, it also separates the exeutable (ImageExe) from the full path (Image).

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

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

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

AllIPAddresses
- FID
- UtcTime
- IPAddress
- Direction
- Initiated

AllPorts
- FID
- UtcTime
- Port
- PortName
- Direction

AllRegTargets
- FID
- UtcTime
- TargetObject

AllHosts
- FID
- UtcTime
- Hostname

Foreign Key