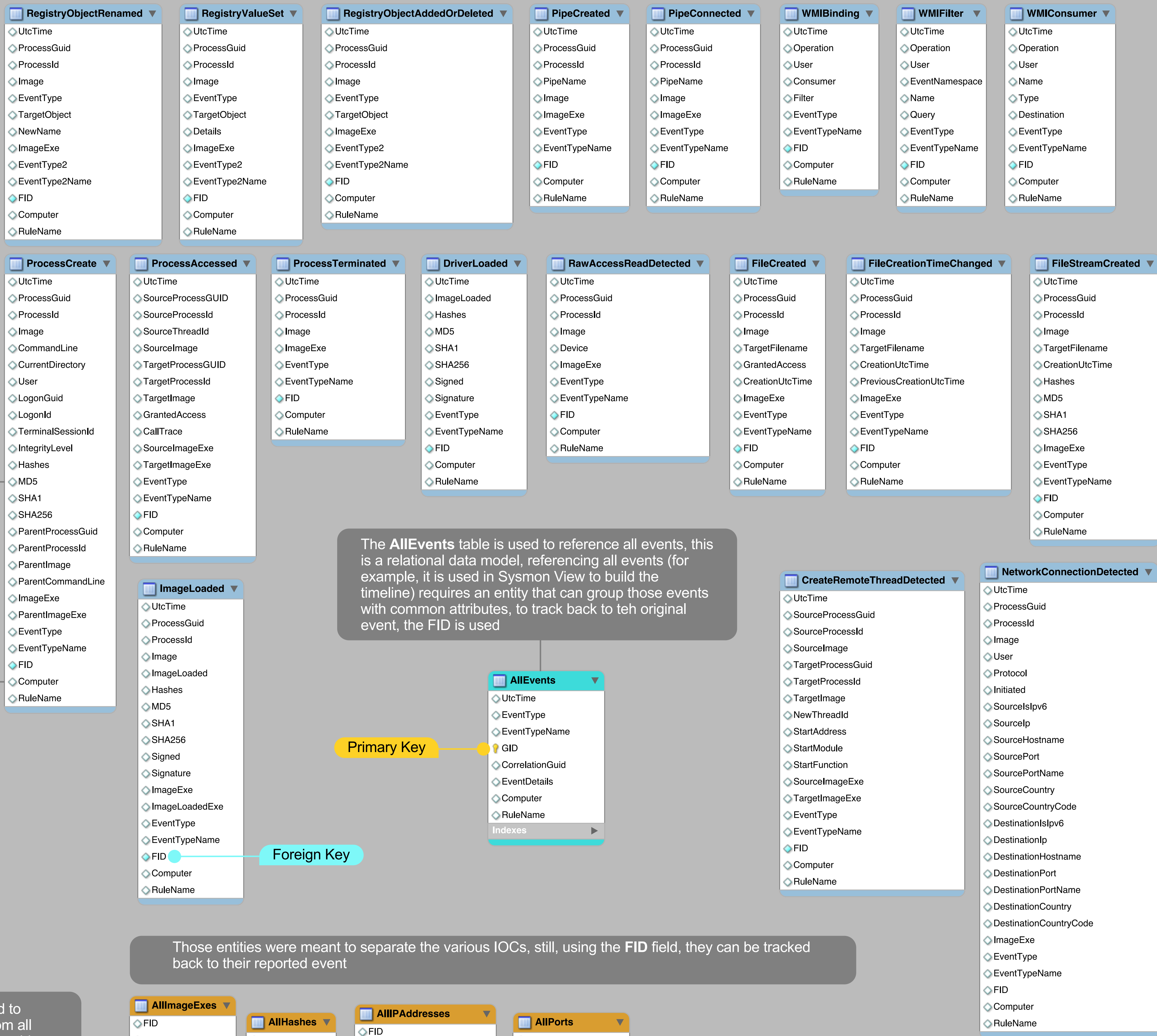


# Sysmon View Data Model

nader@nosecurecode.com

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



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