Alert

OverflowAlert
- [STRING] program (1)
- [INTEGER] size (0..1)
- [BYTE[]] buffer (0..1)

ToolAlert
- [STRING] name (1)
- [STRING] command (0..1)
- [STRING] alertident (1..*)

CorrelationAlert
- [STRING] name (1)
- [STRING] alertident (1..*)

Address
- [STRING] address (1)
- [STRING] netmask (0..1)
- [STRING] ident (Optional)
- [ENUM] category (Optional)
- [STRING] vlan-name (Optional)
- [INTEGER] vlan-num (Optional)

Process
- [STRING] name (1)
- [INTEGER] pid (0..1)
- [STRING] path (0..1)
- [STRING] arg (0..*)
- [STRING] env (0..*)
- [STRING] ident (Optional)

SNMPService
- [STRING] oid (0..1)
- [INTEGER] messageProcessingModel (0..1)
- [INTEGER] securityModel (0..1)
- [STRING] securityName (0..1)
- [INTEGER] securityLevel (0..1)
- [STRING] contextName (0..1)
- [STRING] contextEngineID (0..1)
- [STRING] command (0..1)

Analyzer
- [STRING] analyzerid (Optional)
- [STRING] name (Optional)
- [STRING] manufacturer (Optional)
- [STRING] model (Optional)
- [STRING] version (Optional)
- [STRING] class (Optional)
- [STRING] ostype (Optional)
- [STRING] osversion (Optional)

Node
- [STRING] location (0..1)
- [STRING] name (0..1)
- [STRING] ident (Optional)
- [ENUM] category (Optional)

Service
- [STRING] name (0..1)
- [INTEGER] port (0..1)
- [PORTLIST] portlist (0..1)
- [STRING] protocol (0..1)
- [STRING] ident (Optional)
- [INTEGER] ip_version (Optional)
- [INTEGER] iana_protocol_number (Optional)
- [STRING] iana_protocol_name (Optional)

WebService
- [STRING] url (1)
- [STRING] cgi (0..1)
- [STRING] http-method (0..1)
- [STRING] arg (0..*)

Source
- [STRING] ident (Optional)
- [ENUM] spoofed (Optional)
- [STRING] interface (Optional)

Target
- [STRING] ident (Optional)
- [ENUM] decoy (Optional)
- [STRING] interface (Optional)

User
- [STRING] ident (Optional)
- [ENUM] category (Optional)

Inode
- [DATETIME] change-time (0..1)
- [INTEGER] number (0..1)
- [INTEGER] major-device (0..1)
- [INTEGER] minor-device (0..1)
- [INTEGER] c-major-device (0..1)
- [INTEGER] c-minor-device (0..1)

Alert
- [STRING] messageid (Optional)

Transaction
- [Enum] direction (Optional)

File
- [STRING] name (1)
- [STRING] path (1)
- [DATETIME] create-time (0..1)
- [DATETIME] modify-time (0..1)
- [DATETIME] access-time (0..1)
- [INTEGER] data-size (0..1)
- [INTEGER] disk-size (0..1)
- [STRING] ident (0..1)
- [ENUM] category (0..1)
- [STRING] file-type (0..1)

Checksum
- [STRING] value (1)
- [STRING] key (0..1)
- [ENUM] algorithm (Required)

UserId
- [STRING] name (0..1)
- [INTEGER] number (0..1)
- [STRING] ident (Optional)
- [ENUM] type (Optional)
- [STRING] tty (Optional)

CreateTime

Classification
- [STRING] ident (Optional)
- [STRING] text (Required)

Linkage
- [STRING] name (1)
- [STRING] path (1)
- [ENUM] category (Optional)

DetectTime

AnalyzerTime

Reference
- [STRING] name (1)
- [STRING] url (1)
- [ENUM] origin (Required)
- [STRING] meaning (Optional)

Stream
- [ENUM] offsetunit (Optional)
- [INTEGER] offset (Optional)
- [DATA] Data (Required)

Impact
- [ENUM] severity (Optional)
- [ENUM] completion (Optional)
- [ENUM] type (Optional)

Assessment

FileAccess
- [ENUM] Permission (1..*)

AdditionalData
- [STRING] meaning (Optional)

Action
- [ENUM] category ()

Confidence
- [ENUM] rating ()