IODEFv2 : Indicator

AlternativeIndicatorID
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

IndicatorReference

Indicator
[ML_STRING] Description (0..*)
[DATETIME] StartTime (0..1)
[DATETIME] EndTime (0..1)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

ObservableReference

Reference
[] (0..1)
[URL] URL (0..*)
[ML_STRING] Description (0..*)
[ID] observable-id (0..1)

IndicatorExpression
[EXTENSION] AdditionalData (0..*)
[ENUM] operator (0..1)
[STRING] ext-operator (0..1)

IndicatorID

IndicatorData

Confidence

AttackPhase
[STRING] Specified (0..*)
[URL] URL (0..*)
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)

HistoryItem
[DATETIME] DateTime (1..1)
[ML_STRING] Description (0..*)
[STRING] DefinedCOA (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] action (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

History
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

Incident
[DATETIME] DetectTime (0..1)
[DATETIME] StartTime (0..1)
[DATETIME] EndTime (0..1)
[DATETIME] RecoveryTime (0..1)
[DATETIME] ReportTime (0..1)
[DATETIME] GenerationTime (1..1)
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)
[STRING] purpose (0..1)
[ENUM] status (0..1)
[STRING] ext-status (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

AlternativeID
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

IncidentID

Method
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

RelatedActivity
[URL] URL (0..*)
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

ThreatActor
[STRING] ThreatActorID (0..*)
[URL] URL (0..*)
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

Campaign
[STRING] CampaignID (0..*)
[URL] URL (0..*)
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

NodeRole
[ML_STRING] Description (0..*)
[STRING] category (0..1)

Contact
[ML_STRING] ContactName (0..*)
[ML_STRING] ContactTitle (0..*)
[ML_STRING] Description (0..*)
[TIMEZONE] Timezone (0..1)
[EXTENSION] AdditionalData (0..*)
[STRING] role (0..1)
[STRING] type (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

Email
[EMAIL] EmailTo (1..1)
[ML_STRING] Description (0..*)
[ENUM] type (0..1)
[STRING] ext-type (0..1)

Telephone
[PHONE] TelephoneNumber (1..1)
[ML_STRING] Description (0..*)
[ENUM] type (0..1)
[STRING] ext-type (0..1)

SystemImpact
[ML_STRING] Description (0..*)
[ENUM] severity (0..1)
[ENUM] completion (0..1)

BusinessImpact
[ML_STRING] Description (0..*)
[ENUM] severity (0..1)
[STRING] ext-restriction (0..1)
[STRING] type (0..1)

Expectation
[ML_STRING] Description (0..*)
[STRING] DefinedCOA (0..*)
[DATETIME] StartTime (0..1)
[DATETIME] EndTime (0..1)
[ENUM] action (0..1)
[STRING] ext-action (0..1)
[ENUM] severity (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

TimeImpact

MonetaryImpact

PostalAddress
[POSTAL] PAddress (1..1)
[ML_STRING] Description (0..*)
[ENUM] type (0..1)
[STRING] ext-type (0..1)

DomainContacts
[STRING] SameDomainContact (0..1)

Discovery
[ML_STRING] Description (0..*)
[ENUM] source (0..1)
[STRING] ext-source (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

DetectionPattern
[SOFTWARE] Application (1..1)
[ML_STRING] Description (0..*)
[STRING] DetectionConfiguration (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

Node
[ML_STRING] Location (0..*)

Counter

RegistryHandle

EventData
[ML_STRING] Description (0..*)
[DATETIME] DetectTime (0..1)
[DATETIME] StartTime (0..1)
[DATETIME] EndTime (0..1)
[DATETIME] RecoveryTime (0..1)
[DATETIME] ReportTime (0..1)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

Assessment
[ML_STRING] IncidentCategory (0..*)
[] IntendedImpact (0..*)
[ML_STRING] MitigatingFactor (0..*)
[ML_STRING] Cause (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] occurrence (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

System
[SOFTWARE] OperatingSystem (0..*)
[STRING] AssetID (0..*)
[ML_STRING] Description (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] category (0..1)
[STRING] ext-category (0..1)
[ENUM] interface (0..1)
[ENUM] spoofed (0..1)
[ENUM] virtual (0..1)
[ENUM] ownership (0..1)
[STRING] ext-ownership (0..1)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

DomainData
[STRING] Name (1..1)
[DATETIME] DateDomainWasChecked (0..1)
[DATETIME] RegistrationDate (0..1)
[DATETIME] ExpirationDate (0..1)
[EXTENSION] RelatedDNS (0..*)
[ENUM] system-status (0..1)
[STRING] domain-status (0..1)
[ID] observable-id (0..1)

Nameservers
[STRING] Server (1..1)

Address

Observable
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

Service
[INTEGER] Port (0..1)
[PORTLIST] Portlist (0..1)
[INTEGER] ProtoCode (0..1)
[INTEGER] ProtoType (0..1)
[INTEGER] ProtoField (0..1)
[SOFTWARE] Application (0..1)
[INTEGER] ip-protocol (0..1)
[ID] observable-id (0..1)

ServiceName
[STRING] IANAService (0..1)
[URL] URL (0..*)
[ML_STRING] Description (0..*)

ApplicationHeader
[EXTENSION] ApplicationHeaderField (1..*)

Record
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)

RecordData
[DATETIME] DateTime (0..1)
[ML_STRING] Description (0..*)
[SOFTWARE] Application (0..1)
[EXTENSION] RecordItem (0..*)
[URL] URL (0..*)
[EXTENSION] AdditionalData (0..*)
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

RecordPattern

Key
[STRING] KeyName (1..1)
[STRING] KeyValue (0..1)
[ENUM] registryaction (0..1)
[STRING] ext-registryaction (0..1)
[ID] observable-id (0..1)

WindowsRegistryKeysModified

BulkObservable
[STRING] BulkObservableList (1..1)
[EXTENSION] AdditionalData (0..*)
[ENUM] type (0..1)
[STRING] ext-type (0..1)

BulkObservableFormat
[EXTENSION] AdditionalData (0..*)

FileData
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

File
[STRING] FileName (0..1)
[INTEGER] FileSize (0..1)
[STRING] FileType (0..1)
[URL] URL (0..*)
[SOFTWARE] AssociatedSoftware (0..1)
[EXTENSION] FileProperties (0..*)
[ID] observable-id (0..1)

Hash
[] (0..1)
[SOFTWARE] Application (0..1)

HashData
[STRING] HashTargetID (0..1)
[STRING] scope (0..1)

EmailData
[EMAIL] EmailTo (0..*)
[EMAIL] EmailFrom (0..1)
[EMAIL] EmailSubject (0..1)
[STRING] EmailX-Mailer (0..1)
[EXTENSION] EmailHeaderField (0..*)
[STRING] EmailHeaders (0..1)
[STRING] EmailBody (0..1)
[STRING] EmailMessage (0..1)
[ID] observable-id (0..1)

SignatureData

Signature
[] (1..*)

CertificateData
[ENUM] restriction (0..1)
[STRING] ext-restriction (0..1)
[ID] observable-id (0..1)

Certificate
[] (1..1)
[ML_STRING] Description (0..*)
[ID] observable-id (0..1)

FuzzyHash
[EXTENSION] FuzzyHashValue (1..*)
[SOFTWARE] Application (0..1)
[EXTENSION] AdditionalData (0..*)