IDMEF gồm nhiều class con. Mỗi class con gồm nhiều class con khác.

IDMEF có 1 attr là version chỉ version của rfc.

IDMEF chứa các class

* Class Alert
  + Attr: messageid: optional
  + Chỉ 1 analyzer: thông tin về analyzer của alert
  + CreateTIme: chỉ 1.
  + Classification: chỉ 1. “name” của alert hay các thông tin khác mà manager có thể xác định đc alert
  + DetectTime: 0 hoặc 1. Thời gian mà sự kiện dẫn đến alert xảy ra
  + AnalyzerTime:0 hoặc 1. Thời gian hiện tại trên analyzer
  + Source: >=0. Nguồn của event
  + Target:>=0. Đích của event
  + Assessment: 0-1. Thông tin về ảnh hưởng của event, các hành động mà analyzer đã làm xử lý event, độ chắc chắn của analyzer
  + AdditionalData:0-1. Các thông tin ko chứa đc trong model.
  + ToolAlert: tool dùng để tấn công nếu analyzer phát hiện đc tool này. Dùng để group các alert lại với nhau. Chứa các class
    - Name:chỉ 1. Dạng string
    - Command:0-1. String. Hành động mà tool đó đã làm
    - Alertident:>=0. String. Các alert liên quan tới tool này.
  + CorrelationAlert: các thông tin liên quan tới việc kết hợp các alert
    - Name: 1.string. lí do hợp các alert lại
    - Alertident.>=0.string.các alert liên quan tới alert này.
  + OverflowAlert: các thông tin về bufferoverflow attack
    - Program:1.String. Chương trình mà attack dự định sẽ chạy(ko phải cái bị attack)
    - Size:0-1.Int.Size in bytes of the overflow
    - Buffer:0-1.Byte[]. Dự liệu bị overflow
* Class Heartbeat: analyzer gửi tình trạng của mình đến manager bằng hearbeat. Gửi theo chu kỳ.
  + Analyzer:1. Nguồn của heartbeat
  + CreateTime: 1. Time mà heartbeat đc tạo
  + HeartbeatInterval:0-1. Chu kì heartbeat.
  + AnalyzerTime:0-1.Giờ hiện tại cảu analyzer.
  + AdditionalData:>=0. Thông tin của analyzer mà ko chứa đc torng model.
* Thông tin về các core class
  + Analyzer
    - Node: 0-1. Thông tin về host và device mà analyzer chạy trên nó.
    - Process.0-1. Thông tin về process mà analyzer đang chạy.
    - Analyzer:0-1.Thông tin về analyzer mà message có thể đi qua (dạng cây phân cấp)
  + Classification
    - Reference:>=0. Thông tin về message, chỉ tới tài liệu tham khảo.
      * Name
      * URL
      * Origin:attr
        + Unknown
        + Vendor-specific
        + User-specific
        + Bugtraquid: securityfocus vulnerability DB Id
        + Cve
        + osvdb
  + Source: chu7ac1 thông tin về các source có thể có của event tạo ra alert (DDOS…). Source có chứa thuộc tính spoofed xác định Node đó là giả hay thật.
    - Node:host,router,switch. Chứa các class và attr sau
      * Location:0-1.String.
      * Name:0-1.String.
      * Address:>=0. Chứa các class
        + Address: định dạng theo category của class này

Category: atm,ipv4-addr…

Vlan-num:address này thuộc vlan nào

* + - * + Netmask
      * Category:attr. Optional. Chứa domain mà Class name có thể có.
    - User :thông tin user tạo ra event. Chỉ chứa class UserID. Có thể chứa 1 hay nhiều class userID để chỉ rằng có thể có nhiều người nhận hoặc gửi. Hoặc là cùng 1 user hay process nhưng với nhiều quyền.
      * UserID:>=1. Identification của user.
        + Chứa các class

Name

Number

* + - * + Chứa các attr

Ident

Type: kiểu thông tin của user.

original-user:user hiện đang sử dụng

current-user:user mà hệ thống ghi nhận(thường là login id)

target-user:user id mà user đó mún thành. Vd: user thường mún thành su

user-privs:user khác mà user này có quyền đc dùng

current-group

group-privs

other-privs:đối với file permission

* + - * Ident: attr
      * Category:attr.unknow,application,os-device:user là OS hay device user
    - Process: process tạo event hoặc đc chạy trên source,target,analyzer tùy vào nó thuộc node nào trong IDMEF
      * Chứa các classs
        + Name:1. Tên dạng short ko chứa path và arg
        + Pid:INT.0-1.
        + Path:full path
        + Arg:>=0. Các arg đc dùng với program
        + Env:các biến môi trường liên quan tới process
    - Service: liên quan tới event trên cả source và target. Đc xác định ba82ng2 tên port hoặc protocol.
      * Chứa các class
        + Name
        + Port
        + Portlist:list các port đang đc sử dụng. Format ở 3.2.8
        + Protocol
      * Chứa các attr
        + Ident
        + Ip\_version
        + Iana\_protocol\_number
        + Iana\_protocol\_name
      * Webservice class: chứa các thông tin liên quan đến web.
        + Chứa các class

url:1.

Cgi:0-1.CGI script

http-method:0-1. PUT or GET

arg:argument của CGI script

* + - * SNMPService:chứa các thông tin liên quan đến traffic của SNMP(simple network management protocol)
        + Không rõ về SNMP lắm!!!
  + Target: ngoài các class của source còn chứa class
    - File: chứa các thông tin liên quan tới file và các đối tượng dạng file.
      * Chứa các class
        + Name
        + Path:full path
        + Create-time
        + Modify-time: last modified
        + Access-time:last accessed
        + Data-size:size tính theo byte
        + Disk-size: size trên đĩa
        + FileAccess: access permission

UserID: mà có những quyền này

Permission:>=0.

noAcccess

read

write

execute

search

delete

executeAs

changPermissions

takeOwnership

* + - * + Linkage: các đối tượng đc link tới file này
        + Inode:Unix Inode
        + Checksum:0-1.
      * Chứa các attr
        + Ident
        + Category: ngũ cảnh của thông tin

Current:thông tin đc thu thập sau khi thay đổi xảy ra

Original:thông tin đc thu thập trc khi thay đổi xảy ra

* + - * + Fstype: thông tin về file system như ntfs, fat32,fat16…
        + File-type: Mime-type
  + Assessment
    - Impact: chứa các attr (đều là optional)
      * Severity: informational,love,medium,high. Đc sắp xếp theo độ nguy hiểm.
      * Completion:failed,succeeded
      * Type: kiểu của event:admin,dos,file,recon,user,other. Default là other
    - Action
      * Category: block-installed (block attack), notification-sent,taken-offline(hệ thống bị shutdown),other
    - Confidence:low,medium,high,numeric(dạng confidence biểu diễn ở dạng số)
      * Các analyzer có thể có giá trị này khác nhau nên ko thể so sánh đc.
      * Dữ liệu numeric 0.0->1.0
  + AdditionalData: có thể chứa dữ liệu nhỏ như string,int hoặc cả 1 packet header tùy vào config của DTD
    - Chứa các rank và keyword tương ứng: 0-boolean, 1-byte
  + Time có 3 loại CreateTime, DetectTime, AnalyzerTime