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.
  + 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:
    - User :thông ti user tạo ra event
    - Process: process tạo event
    - Service: liên quan tới event
  + Target: ngoài các class của source còn chứa class
    - File: liên quan tới event
  + Assessment
    - Impact: chứa các attr
      * Severity: informational,love,medium,high
      * Completion:failed,succeeded
      * Type: kiểu của event:admin,dos,file,recon,user,other
    - Action
    - Confidence