* Data model
  + GraphResult
    - AddImplication để làm gì ?
    - GraphResult constructor sẽ load graph từ file hay còn cách nào khác để khởi tạo ?
    - Lưu graph ntn (ghi cái này để sau này research)
    - <http://discovery.csc.ncsu.edu/software/correlator/ver1.0/Abstraction.xml>
    - Kết quả sẽ được lấy từ cơ sở dữ liệu lên, file đưa vào là tên file để extract ra thôi. File này sau đó sẽ được đưa về cho client.
    - Link trên là ví dụ 1 graphresult. Dtd của nó

<!ELEMENT Abstractions (Abstraction+)>

<!ELEMENT Abstraction (Abstraction\*)>

<!ATTLIST Abstraction Type CDATA #REQUIRED>

Đã chỉnh sửa lại 1 số method.

* + Alert
    - AlertValues chứa các thông tin về alert trong các phần tử của mảng ? (không tên)
    - Đã chỉnh lại
  + Fact:
    - Type ?
    - Kiểu dữ liệu tương ứng với Fact (int, varchar,….)
  + HyperAlert
    - Hình như thiếu facts.
    - HyperAlert được tạo từ HyperAlertType ? Nếu vậy thì thiếu 1 hàm để tạo nó.
    - Các predicate ở trong HyperAlert là các encoded predicate, nên lúc này không cần lưu fact nữa.
    - HyperAlert đơn thuần chỉ là một cấu trúc dữ liệu để chứa thông tin 1 hyper alert lấy lên từ trong db để tiện trong lúc xử lý thôi.
  + Implication
    - Constructor khởi tạo bằng string ? String này là tên của predicate ? ID ?
    - String này là tên của predicate.
  + HyperAlertType
    - Fact trong này chưa được gán giá trị ?
    - Giá trị này lấy từ bang HATFact trong DB.
  + Predicate
    - Predicate có ID ? ID này được lấy từ đâu ? Hay chỉ là argID thôi ?
    - Predicate được phân biệt bởi tên. Các ID này sẽ được tạo ra thêm trong chương trình để tiện cho việc tìm kiếm và so sánh vì thực hiện so sánh trên String chi phí quá lớn.
* DataProcess
  + AlertHandler
    - Xử lí alert mới xuất hiện lưu vào DB ?
    - Class này sẽ được register vào NotificationCenter, nếu như có alerts mới xuất hiện thì nó sẽ được gọi để xử lý.
  + AlertDBPreparation
    - Constructor ?
    - Kiểm tra những thứ cần thiết (table in DB, file input, alert db,…) để throw lỗi hoặc tạo những cái còn thiếu.
    - Dùng để tạo DB mới từ file hoặc IDMEF ?
    - Chuyển những data có được từ IDMEF file hoặc trong các DB thành data DB của chương trình.
  + KnowledgebasePreparation
    - PrepareDB để làm gì ?
    - Cũng để kiểm tra như trên.
* Correlation
  + Analysis: cần thì làm. Giảm scope.
  + Correlation
    - getAttackGraph dùng để làm gì ?
    - gọi tới để extract graph vào file.
* Notification
  + NotificationCenter
    - newEventArrive làm gì ?
* WebService
  + ConfigService
    - changeConfigConfiguration : dùng configuration ở Correlate ?
    - changeConfigInformation: information này là những thông tin ở trên server.
  + CorrelateService
    - Có nhiều graph ?
    - Trong 1 lúc sẽ có nhiều graph tách biệt nhau, mỗi graph sẽ có ID riêng.
  + CommandExecuteService:
    - Command ở dạng string ? YES, it is.
  + Không có phần gửi cho client ? Xem thêm về WEB service để biết thêm chi tiết ☺.
  + Dùng HTTPS có đủ ? đủ gì?
  + ReportService: nhận reports từ servers ? dựa theo log của service có được, service sẽ trả gửi log file theo những định dạng định trước về cho người dùng.

Nhiều project ? hỏi gì đây?

Coding

+ERD ?

+ERD -> DB và dữ liệu giả.

+KnowledgeBase : KB lưu trong DB ?

-ERD -> KnowledgebasePreparation -> KnowledgeBase

+AlertHandler viết được liền ? chưa.