Alert Correlation Process: gồm các bước

1. Normalization
   * IDMEF (rfc <http://www.ietf.org/rfc/rfc4765.txt>) (Đã report)
2. Aggregation
   * Julisch:Clustering intrusion alert to support root cause analysis
     + Tác giả có kiến thức sâu. Nghiên cứu kĩ.
     + Alert chuẩn được nhiều người cite lại
     + Gom cụm alert dựa trên generalization hierachies
     + Phương pháp đơn giản. Có chứng minh và nêu bài toán rõ ràng
     + Tuy nhiên chưa thực tế vì các alert tạo ra có lúc quá abstract
   * Intrusion alarm reduction using root cause analysis and clustering
     + Cải tiến của julisch.
     + Gom cụm dựa trên khoảng cách và generalization hierachies
     + Paper tương đối tốt
     + Nhiều phần có vẻ như copy của Julisch quá nhiều
   * Using an Intrusion Detection Alert Similarity Operator to Aggregate and Fuse Alerts
     + Áp dụng generalization hierachies để tính khoảng cách giữa 2 alert
     + Có thể dùng khoảng cách này cho việc clustering
     + Paper tương đối cũ và đọc cũng không thấy hay lắm!
3. Correlation
   * 2 paper về correlate đã đọc: sử dụng prepost và dùng attack graph để predict
   * Correlation of intrusion Symptoms: an application of chronicles
     + Khái niệm chronicle tương đối hấp dẫn
     + Trong slide báo cáo DAMH1 có nói về paper này
     + Ứng dụng trong correlate thì không rõ ràng
   * *Discovering Novel Attack Strategies from INFOSEC Alerts*
     + Đây là phương pháp sử dụng thống kê
     + Granger Causality Test là cái gì thì đọc không hiểu vì nói không rõ
     + Có thể phát hiện được lỗi mới
4. Visualization
   * Phần Visualization thì đã đọc được nhiều cái nhưng không report lại nên cũng không nhớ
   * Phần này có thể sử dụng tool.

Các paper khác:

1. Kiến trúc:
   * A comprehensive approach to intrusion detection alert correlation
     + Phát thảo 1 process khác
     + Xây dựng chủ yếu dựa trên sliding window
     + Có rất nhiều step trong quá trình correlate
       - Nhiều step thật sự không rõ tính thực tế như Focus Analysis
   * A mission-impact based approach to INFOSEC
     + Quá trình correlate chỉ đến mức aggregate
       - Xây dựng 1 giải thuật aggregate khác (không chắc phù hợp)
     + Việc tính toán các giá trị như relevance ... không rõ ràng
   * A survey of Alert Fusion Techniques for Security Incident
     + Quá trình correlate tương tự như của mình
       - Chỉ có thêm phần Verification
       - Phần Verification như đã nói sử dụng HIDS
     + Survey phân loại các giải thuật aggregate, correlate rõ ràng
   * Alert correlation in a cooperative intrusion detection framework
     + Quá trình correlate tương tự của mình
       - Phần aggregate được chia ra làm 2 phần merging và clustering
       - Có thể xem các giải thuật aggregate liên quan đến clustering
     + Paper tương đối cũ, không rõ ràng. Tác giả có nghiên cứu sâu về intrusion detection
2. Đánh giá mức độ ảnh hưởng
   * Success Likelihood of Ongoing Attacks for IDPS
     + Sử dụng Markov Model
     + Tính toán dựa trên xác suất
     + Sử dụng đối với các phương pahp1 dùng pre-post
     + Paper có vẻ tốt. Các công thức rõ ràng

Một số note:

1. Phần verification nên tìm hiểu kĩ xem nó có cần thiết trong quá trình hay không. Không hay có gì cũng phải chứng minh.
2. Phần Visualization cho packet có thể sử dụng tool vì thầy cũng không quá quan trọng phần này
3. Phần prediction và prevention và reaction chưa tìm hiểu vì chưa tìm thấy paper nào. Có thể đây là 1 hướng đi.
4. Các paper về quá trình correlate thì đa số chỉ có bấy nhiêu :| Trong paper A survey of Alert Fusion Techniques for Security Incident, paper này ra đời năm 2008 nên survey cũng tương đối đầy đủ. Không cần quá lo lắng về phần đọc paper và research. :D
5. Về phần ý tưởng, tốt nhất nên dành time để suy nghĩ. Ý tưởng tốt nhất nên đơn giản không nên quá abstract.
6. Paper nếu không down được có thể vào đây <http://www.updatesofts.com/forums/showthread.php?p=1903895#post1903895> để tải.