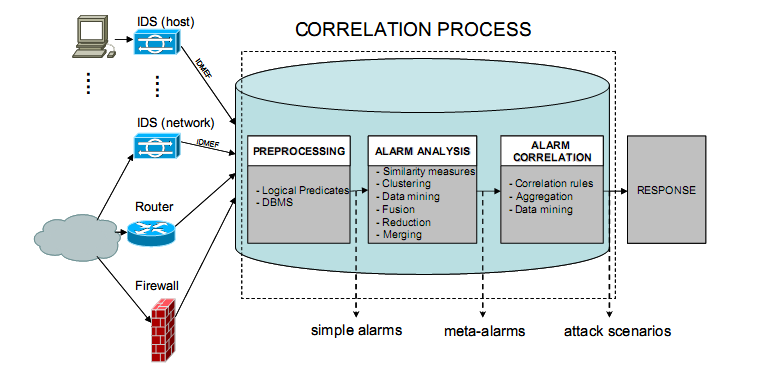
Intrusion detection alarm correlation: A survey

Trong survey này, quá trình alert correlation bao gồm các giai đoạn như hình vẽ sau:



**Preprocessing**: giai đoạn này các alert sẽ được chuyển sang các fact và các logical predicate.

* Ning: Predicates được dùng như “hyper-alert” gồm có : fact (attributes), prerequisite, consequence.
* Julich: tạo các tập alarm bằng cách tổng quát hóa các thuộc tính của các alarm con.

**Alarm analysis**: tạo các high level alarm, giảm các false alarm.

* T.Bass: dùng data fusion (anomaly detection).
* Manganaris & Clifton, Gengo: dùng data mining.
* Valdes, Skinner: áp dụng xác suất giống nhau giữa các alert.
* Debar, Wespi: correlate dựa vào relationship giữa các alert (rules algorithm)
* Cuppens’s framework: dùng 1 system để tính toán sự giống nhau, quan hệ giữa các alert. Sau đó alerts được gán vào các cluster phù hợp.
* Julisch: xây dựng một attribute oriented induction data mining heuristic.
* Ning: hyper alert .

**Alarm correlation**:

* Vades, Skinner: dựa vào xác suất để tạo attack scenario.
* Dain, Cunninghan: dùng naïve (clustering), heuristic, data mining để xác định xác suất 1 alert.
* Debar, Wespi: correlate dựa vào relationship giữa các alert (rules algorithm).
* Cuppens: dựa vào các predicate để tạo correlation rules (Lambda language).
* Ning: hyper alert, dựa vào tiền điều kiện, hậu điều kiện.

Hạn chế:

* Không biết được nguyên nhân của các alert được correlate
* Khi dùng rules hoặc data mining chỉ phát hiện được các scenario đã biết và tốn nhiều công sức (vấn đề real time)

Questions:

1. Tại sao lại có kiến trúc này? kIến trúc này có phải là kiến trúc duy nhất của quá trình này hay không?
2. Alarm với Alert ở đây sử dụng nghĩa khác nhau ntn?