# Phương pháp kiểm tra an toàn thông tin hệ thống

**Kiểm tra các văn bản, tài liệu của hệ thống**

Đánh giá các chính sách, quy trình kỹ thuật hiện tại nhằm đánh giá tổng quan hiện trạng an toàn thông tin của hệ thống.

Xác định các thiếu sót, điểm yếu trong các kiểm soát an toàn thông tin đang triển khai.

**Kiểm tra nhật ký, sự kiện của hệ thống**

Xác định xem các biện pháp kiểm soát bảo mật có ghi lại thông tin thích hợp hay không và tổ chức có tuân thủ các chính sách quản lý nhật ký hay không.

**Kiểm tra chính sách, luật của hệ thống**

Việc kiểm tra chính sách, tập luật này nhắm tới hai mục tiêu:

* O1 (Security): Tăng cường bảo mật của hệ thống kiểm soát
* O2 (Performance): Cải thiện hiệu năng hoạt động của hệ thống kiểm soát

Các chính sách, luật trên các loại hệ thống khác nhau được phân loại như sau:

* Chính sách kiểm soát truy cập (Access rule)
* Chính sách kiểm soát nội dung (Content rule)
* Chính sách kiểm soát hành vi (Behavior rule)

Do đặc điểm của từng loại chính sách khác nhau, việc rà soát, kiểm tra, tối ưu những chúng theo từng mục tiêu khác nhau cũng cần áp dụng các phương pháp khác nhau. Chi tiết được mô tả trong bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Access rule** | | **Content rule** | | **Behavior rule** | |
| **Định nghĩa, phân loại** | - Kiểm tra siêu dữ liệu (metadata) của đối tượng để thực hiện permit/deny/inspect  - Thường nằm ở lớp dưới (lớp đầu tiên) và có thể quyết định có tiếp tục kiểm tra sâu hơn ở các lớp trên hay không | | - Kiểm tra nội dung (content) của đối tượng để phát hiện ra các mối đe dọa  - Sử dụng các bộ mẫu, cơ sở dữ liệu có sẵn (từ nhà cung cấp hoặc do người dùng định nghĩa) | | - Kiểm tra hành vi (behavior) của đối tượng để phát hiện ra các trường hợp bất thường  - Sử dụng các bộ mẫu, cơ sở dữ liệu có sẵn (từ nhà cung cấp hoặc do người dùng định nghĩa) | |
| **Thiết bị điển hình** | FW, DBFW, WebGW: URL/category filter, MailGW: mail flow policy, MailGW: spam by reputation, PIM, Encryption, NAC, Authentication, VPN | | AV, IPS, WAF, Mail/WebGW: content filter, MailGW: spam by content, App Scanning | | DDOS, Sandbox, APT, SIEM | |
| **Thiết bị áp dụng được trong phạm vi dự án** | Switch, Firewall, VPN, ESG | | WAF, ESG, AV | | Không có | |
| **Đặc điểm** | - Bộ luật có thứ tự (first match). Do vậy sẽ có thể tồn tại các loại luật bao trùm, trùng lặp, sai logic, không cần thiết  - Luật là dạng nhị phân (permit/deny) do vậy không có cán cân bảo mật / hiệu năng | | - Bộ luật không có thứ tự. Tất cả luật đều được kiểm tra  - Luật có các trường hợp khẳng định hoặc phủ định sai, do vậy có cán cân bảo mật / hiệu năng | | - Bộ luật không có thứ tự. Tất cả luật đều được kiểm tra  - Luật có các trường hợp khẳng định hoặc phủ định sai, do vậy có cán cân bảo mật / hiệu năng | |
|  | **Tiêu chí** | **Phương pháp** | **Tiêu chí** | **Phương pháp** | **Tiêu chí** | **Phương pháp** |
| **Phương pháp đạt O1 - Security** | 1. Loại bỏ các trường hợp phủ định sai (false negative) | Áp dụng mô hình quyền tối thiểu (least privilege)  + Sử dụng luật từ chối mặc định (implicit deny) ở dưới cùng  + Chỉ cho phép những gì thực sự cần thiết | 1. Loại bỏ các trường hợp phủ định sai (false negative) mà hệ thống không phát hiện ra | Kiểm thử bộ signature/database bằng cách sử dụng:  + Các mẫu tấn công cũ/mới nhất  + Các mẫu tấn công nguy hiểm nhất  + Các mẫu tấn công có liên quan đến môi trường, hệ thống đích | 1. Loại bỏ các trường hợp phủ định sai (false negative) mà hệ thống không phát hiện ra | Kiểm thử bộ signature/database bằng cách sử dụng:  + Các mẫu tấn công cũ/mới nhất  + Các mẫu tấn công nguy hiểm nhất  + Các mẫu tấn công có liên quan đến môi trường, hệ thống đích |
|  |  | 2. Loại bỏ các trường hợp đối tượng cần kiểm tra bị bỏ sót | Rà soát thủ công cấu hình, chính sách để đảm bảo toàn bộ các đối tượng cần kiểm tra đã được đưa vào các luật để kiểm tra | 2. Loại bỏ các trường hợp đối tượng cần kiểm tra bị bỏ sót | Rà soát thủ công cấu hình, chính sách để đảm bảo toàn bộ các đối tượng cần kiểm tra đã được đưa vào các luật để kiểm tra |
| **Phương pháp đạt O2 - Performance** | 1. Loại bỏ các luật bao trùm | Đưa các luật chi tiết hơn lên trên | 1. Giảm số trường hợp cảnh báo sai | Rà soát thủ công các cảnh báo đã sinh ra | 1. Giảm số trường hợp cảnh báo sai | Rà soát thủ công các cảnh báo đã sinh ra |
| 2. Loại bỏ các luật trùng lặp | Rà soát thủ công các luật | 2. Loại bỏ các trường hợp kiểm tra thừa | - Whitelist các đối tượng chắc chắn là tin cậy  - Blackslist các đối tượng chắc chắn là độc hại | 2. Loại bỏ các trường hợp kiểm tra thừa | - Whitelist các đối tượng chắc chắn là tin cậy  - Blackslist các đối tượng chắc chắn là độc hại |
| 3. Loại bỏ các luật sai logic | Rà soát thủ công các luật |  |  |  |  |
| 4. Loại bỏ các luật thừa | Tuân theo khuyến nghị khi viết luật (\*) |  |  |  |  |

(\*) khuyến nghị khi xây dựng và quản lý access rule: (cùng áp dụng cho mục tiêu thứ 3 (O3): Operation)

* Documenting, description:
  + Purpose, owner, service/system
* Expire whenever possible
* Change procedure/management
* Logging action: is it necessary?

# QRadar rule tuning

- Mục đích & quy trình tuning rule

**O1: Security**

1. Rà soát lại logic của rule **so với ý tưởng, yêu cầu ban đầu**

(việc này đã làm từ giai đoạn 1 => logic chắc chắn phải là đúng)

2. **Rule match ít** (gồm cả không match) => khả năng bỏ sót false negative

=> mục tiêu: bắt thêm được false negative, để biến nó thành true positive

* trường hợp lý tưởng: rule chạy đúng, chỉ toàn true negative, ít hoặc không có true positive

- kiểm tra lại logic, ngưỡng để xem có bỏ sót thật không

* logic: đáng ra phải match với traffic đó nhưng thực tế lại không match.VD:
  + logic sai:
    - các test phủ định nhau
    - test ở trên lọc mất traffic mà đáng ra phải ăn vào test ở dưới
    - tham số test sai:
      * chọn sai trường same xxx, different xxx
      * sai AQL syntax
  + logic đúng nhưng đầu vào sai:
    - custom property không có (chưa tạo, bị xóa, bị đổi tên...)
    - custom property không parse được (value là N/A, blank...)
    - refset không có (chưa tạo, bị xóa, bị đổi tên...)
    - refset sai kiểu (IP, numeric, alphanumeric...)
    - refset không có dữ liệu, thiếu dữ liệu
* ngưỡng:
  + số trường hợp match chưa đủ => ngưỡng quá cao so với thực tế

=> điều chỉnh & theo dõi

- kiểm tra flow thực tế trên network activity để tìm false negative

3. **Rule match nhiều** => khả năng bắt nhầm quá nhiều false positive

=> mục tiêu: giảm bớt số trường hợp bắt phải false positive mà vẫn giữ nguyên true positive

* trường hợp lý tưởng: rule chạy đúng, rất nhiều true positive

- kiểm tra lại logic, ngưỡng để xem có đúng là nhiều false positive không

* logic:
  + test để tham số quá rộng
  + tham số test sai:
* ngưỡng
  + số trường hợp match quá nhiều => ngưỡng quá thấp so với thực tế

=> điều chỉnh & theo dõi

- kiểm tra flow thực tế trên network activity để tìm ???

**O2: Performance**