<Suricata 설정>

- yaml 파일 주요 설정 항목 및 내용(기본만)

- (추후) 실제 설정한 내용만 추가작성 -> 나오는 이슈들 정리

1. 들어가며

보안 리포트에 사용할 JSON 파일을 Suricata로 생성하려면, Suricata의 YAML 파일(suricata.yaml)을 적절하게 설정하여 Suricata가 네트워크 트래픽을 분석한 결과를 eve.json 파일에 기록하도록 구성해야 한다.

1. Suricata YAML 파일 설정

구성 파일을 수정한 후엔 새로운 설정이 적용되도록 Suricata를 재시작 해야한다.

-> sudo systemctl restart suricata

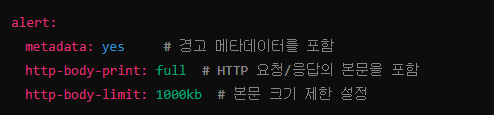
1. **outputs 섹션 수정**:

* Suricata가 로그를 JSON 형식으로 저장하도록 eve-log 출력 설정
* 로그에 포함될 이벤트 유형을 지정한다. 일반적으로 보안 리포트에 필요한 이벤트는 alert, http, dns, tls, fileinfo 등이 있다.



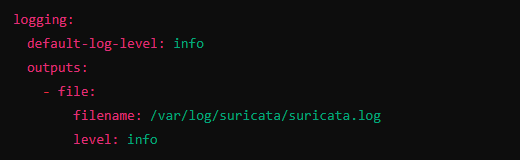
1. **alert 설정**:

* Suricata가 경고(alert)를 생성할 때 포함할 내용을 설정
* 모든 경고에 대한 세부 정보가 포함되도록 metadata와 http 필드를 추가로 설정할 수 있다.



1. **logging 설정**:

* Suricata 자체 로그의 레벨과 저장 위치를 설정한다. Suricata의 동작을 모니터링하는 데 유용하다.



1. **네트워크 인터페이스 설정**:

* Suricata가 분석할 네트워크 인터페이스를 지정한다. 올바른 네트워크 트래픽을 캡처하고 분석할 수 있다.

