회의록

8월 20일 화요일

1. 주제 정하기
   - 팀 주제 구체화하기

➡️ Suricata를 활용한 네트워크 빅데이터 분석 및 리포트 작성 자동화

2. 팀명 정하기

➡️ No-Way (as 'not gateway')

3. 1주차 업무 - Suricata 심화 (~ 8/21)
- 프로그램의 이해, 활용, 로그 data 들여다 보기

8월 21일 수요일
- Suricata 심화 계속 진행

8월 26일 월요일

1. 엘라스틱 서치 / 키바나 시각화 관련 선정 (~28일)

➡️ - 기본 +- @
- Custom 화 +?? / 리포트 작성 진행

2. 프로젝트 개발 문서화 작업 관련

➡️ - 필요성 : 개발 역량 확대 / 팀 방향성 x
- 진행?? : 참고 자료 역할로

8월 28일 수요일

1

멘토링

8월 21일 수요일

1. Suricata rule 기반 탐지 리포트 업무 추가

➡️ 엘라스틱 서치를 활용한 데이터 가공 가능 > 리포트 작성 / 추출 가능한 '파이프라인' 필요

2. 정책 범위, 종류 확실하게... ex. 보안뉴스 사이트 - 웹서버

➡️ 템플릿 : craigs
서비스 : 메인페이지 / 공지게시판(관리자계정) / 이벤트(개인정보수집)

3. 네이버 로그 수집 필요, 가능 > 보류!

8월 22일 목요일

1. 설정, 로그 파일 관련 Suricata + 엘라스틱 서치 자료 공유

➡️ 메뉴얼이 대부분! / 커뮤니티 활용

2. 최종 리포트 작성 위치

➡️ 보안은 거버넌트 → 결정권자의 의사결정이 중요함.

- 얼마나 준비하였는지가 보여지면 결정권자가 의사 결정할 때 좀 더 긍정적으로 설득될 수 있음
- 보안 리포트에는 내용도 중요하지만 언변, 화려한 시각화도 중요함 (차트 등) > 모든게 아우러진 분야

결론) 텍스트만 x, 화려한 문서화 필요! as is to be... best!! / 엘라스틱 활용 하려면... ...
> 웹서버로 구현??!!

3. 설치 스크립트 작성 필요!
> 네이버클라우드 서버 스냅샷 활용...

4. 현업... 보안 솔루션 활용만! / 기본 역량 부족 대부분.

8월 23일 금요일

1. Elasticsearch 리포트 기능 (유료?) - 구현 어떻게;;
> Elastic 데이터 활용!!

2. Suricata Manual 커스텀 / 샘플 패킷 학습
> 보류!

3. 프로젝트 개발 양식 진행 : 유연성 필요

➡️ 1. 플로우 차트 - 요구사항 명세서 (1장~2장) / ~ 축약본
2. WBS
3. 기능/기술 명세서
4. ERD (데이터베이스 설계도, 모식도)

8월 26일 월요일

1. 프로젝트

➡️ 범위 특화 / 엘라스틱에서 icmp 등등 보안 특화된 샘플 지원!

2. 프로젝트 개발 문서화 필요!! :

➡️ 단순히 코딩 내용 추가 x > 자세한 기능 구현 설정 > ERD로 연결
> 모든 업무에서 필수로 활용! / 각각의 업무량 산출 가능 > 전체 진행 상황 예측 가능!!

8월 27일 화요일

1. API 기능 활용 > 추출 후 편집 가능!!

2. Flowchart 추가 기능

➡️ 충분한 내용 > 차후 내용 추가 및 part별 분할 관리 필요!!

3. 문서화 워드로 작업 필요!

➡️ + 기능 명세서 엑셀화 추가 필요!! (한눈에 확인)

8월 28일 수요일(멘토링)

1. 프로젝트 산출물 방향성

우리 프로젝트 특징 : 메이저 도구들의 결합과 활용을 통해 결과를 도출하고 보여주는 것이어서 전달력이 있음 → 이 부분을 강화하는 것이 중요

➡️ - 패키지가 너무 크기 때문에(범위가 넓음) 무엇을 보여줄지 명확하게 정립하고 전달해야함
- 아키텍처를 그리는 등 블럭구조를 사용하여 설명해주는 방법 고려

2. 인사이트 찾아보기 (지니어스, 미디움 등)

한국 보안 시장의 한계 : 침입차단에 대한 적용이 떨어짐, 실질적으로 제대로 활용하는 시장은 아님. 기능은 있는데 안쓰고 있음 → 우리가 생각한 프로젝트의 강점들을 잘 전달해야함

➡️ 찾아본 인사이트를 가지고 이들은 어떤 결과를 제시했고 그 결과를 통해서 시장에서 어떤 가능성을 가지고 있는지 효과들을 충분히 확인하는 작업 필요

3. 메뉴얼에 필요한 내용

➡️ 1) 기능을 구현하면서 생기는 시행착오
2) 설정법

4. Flowchart > ERD

➡️
- 시간적, 논리적 위치 흐름도
- 데이터 흐름도 잘 보이게
- 실행하면 다음동작, 다음동작 스텝들 잘 보일 수 있게