차세대 사이버 보안 동향

이예인

Summary

문제점 : 핵심 기술(IoT, 5G, Cloud, Bigdata, AI 등)이 주도하는 4차 산업혁명이 국가의 사회-경제적 인프라의 스마트 융합을 촉진하면서, 새로운 형태의 사이버 공격이 증가하고 있다.

연구목표 : 최근 사이버 공격의 발전을 조사하고, 사이버 보안의 개념적 변화(SOAR, Zero Trust 등)를 기반으로 차세대 사이버 보안 기술의 동향을 파악하여 새로운 형태의 사이버 공격에 대비한다.

내용요약

- 최근 사이버 공격 동향 (IoT 보안, 랜섬웨어, 공급망 공격, GDPR 등)
- 사이버 보안 개념적 변화 기반의 차세대 보안 기술 (Zero Trust, SOAR로 자동화, AI 방어 기술 개발, 국가 차원의 Cyber Kill Chain, SRS)
- 하이프 사이클 기반의 영역별 차세대 보안 기술
    - IT 영역 (악성 웹사이트 탐지, 멀웨어 감염 탐지, 봇 프로파일링, 도메인 평가 기술 고도화)
    - IoT/OT 영역 (인증/인가, 보안 프레임 관리, 탐지/대응)
    - 중요 정보 통신 시설 영역 (리스크 관리 기술)

Strengths

- 기술 용어를 제시하는 방식으로 차세대 보안기술 동향을 명확하게 소개했다.
- 차세대 보안 기술 동향을 파악하여 새로운 형태의 사이버 공격에 대응하겠다는 연구 목표가 명확하다.

Weakness

- SynoLocker의 개념이 잘못 설명되어 있다. Synology의 NAS를 대상으로 하는 랜섬웨어라는 설명이 옳다.
- 차세대 보안기술 동향을 파악하는 데 있어 사이버 공격 동향에서 내린 결론들이 거의 활용되지 않았다. 차세대 보안기술을 소개하는 데 있어, 최근의 사이버 공격 동향을 조사한 목적이 불분명하다.
- '사이버 공격 동향 분석'보다 '사이버 보안 이슈 동향 분석'이라는 소제목이 적합해 보인다. 내용에서 제시한 GDPR은 사이버 공격이 아닌 개인정보 보호 법령이다.

Thoughts / Ideas

- 기존의 사이버 보안 기술까지 소개하여, 차세대 보안 기술로 어떻게 변화하는지 설명하면 보안 개념 변화를 더 자세히 이해할 수 있어보인다.