한국컴퓨터정보학회 하계학술대회 논문집 제31권 제2호 (2023. 7)

인공지능을 활용한 EDR 시스템 발전 동향

김대형*, 박재경O
*한국폴리텍대학교 사이버보안과,
O한국폴리텍대학교 사이버보안과
e-mail: yj4004h23@hanmail.net*, jakypark@kopo.ac.krO

A Survey on the Development of EDR System Uisng Artificial Intelligence

Dae-Hyung Kim*, Jae-Kyung ParkO
*Dept. of Cybersecurity, Korea-Polytechnics University,
ODept. of Cybersecurity, Korea-Polytechnics University

● 요 약 ●

본 논문에서는 인공지능을 결합한 EDR(Endpoint Detection and Response) 시스템을 확인하고, 그 현황을 파악하는 것을 목적으로 한다. 현대에는 점차 보안 위협이 더욱 증가하면서 기존의 방식으로는 대응하기 어려운 상황이 발생하고 있으며, 위협에 대한 예측과 선제적인 대응력을 강화하기 위해 스스로 학습해 감시 및 공격에 대응하는 인공지능 기반의 보안 시스템에 대한 관심이 증가하고 있다. 본 논문은 AI 기반 EDR 시스템과 그 현황에 대해 살펴보고자 한다.

키워드: 인공지능(artificial intelligence), 엔드포인트(Endpoint), EDR(Endpoint Detection and Response)

I. Introduction

기술 발전에 따라 보안 위협의 정교함과 구성 수준도 증가하고 있다. 보안 환경은 전례 없는 속도로 진화하고 있으며, 보안 인력이 이러한 위협에 다르게 대응해야 할 필요성이 그 어느 때보다 시급해졌다. 이러한 맥락에서 인공지능(AI) 기술을 보안 시스템에 적용하는 것이 보안 위협을 탐지하고 대응할 수 있는 잠재적 솔루션으로 급부상하고 있으며 보안 시스템에 AI 기술을 활용하면 보안 전문가가 악성코드와 같은 위협을 빠르게 식별하고 대응할 수 있어 보안 위협 대응의 효율성과 속도를 높일 수 있다. 따라서 AI를 활용한 보안 시스템의 개발 및 구현은 현재와 미래의 보안 환경에서 점차 필수적인 요소로 변화하고 있다.

II. EDR System

EDR 시스템은 컴퓨터, 서버 및 모바일 장치와 같은 엔드포인트에서 발생하는 보안 위협 및 사건을 탐지, 조사 및 대응하도록 설계된 보안 솔루션 유형이다. 해당 시스템은 엔드포인트 활동을 지속적으로 모니터링하고, 데이터를 수집하고, 의심스럽거나 악의적인 행동의 징후를 분석하여 작동하게 된다. 이에 따른 주요 이점 중 하나는 엔드포인트 활동에 대한 실시간 가시성과 제어를 제공하는 가능인데 이를 통해 보안 팀은 위협과 사건에 신속하게 대응하고 심각한 피해를 받기 전에 억제하고 해결할 수 있다. 더불어 조직이 공격의 범위와 영향을 이해하고 향후 유사한 사고를 방지하기 위한 조치를 취하는데 도움이 되는 귀중한 포렌식 데이터를 제공할 수도 있다. 때문에 EDR 시스템은 기존의 방화벽, 침입탐지시스템 등 다른 보안 솔루션들과 함께 사용될 때 최상의 효과를 발휘할 수 있다. 전반적으로 EDR 시스템은 포괄적인 보안 전략의 필수 구성 요소로 위협 환경이 계속 진화함에 따라 자산 및 데이터를 보호하려는 조직에게 중요한 도구로 그림 1처럼 그 수요가 늘어갈 것이다.

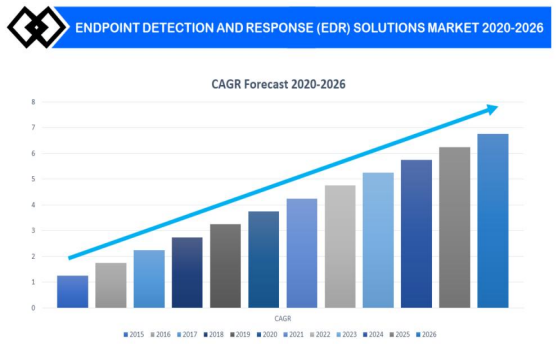
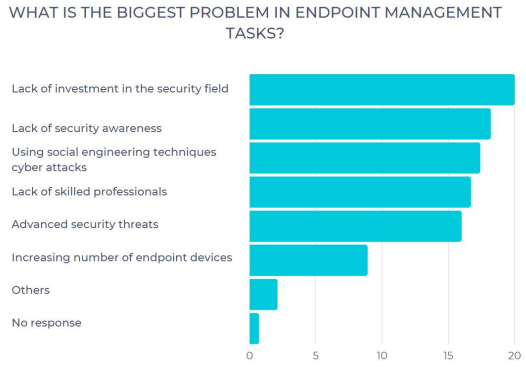


Fig. 1. EDR CAGR forecast 2020-2026

III. The Status of AI-based EDR

사실상 EDR 시스템의 AI 활용은 스마트 EDR 시스템이라는 이름으로 이전부터 주목을 받아왔던 분야라 할 수 있다. 그럼에도 불구하고 스마트 EDR 시스템의 실용적 구현에 대해서는 미흡한 부분이 존재하는데 구체적인 원인은 기술적인 부분도 있겠지만 그보다는 그림 2에서 나타나듯 보안 예산 부족이 가장 큰 원인으로 꼽힌다.



Flg. 2. A survey on awareness and selection criteria of EDR solutions

또한 반복되는 개인정보유출, 사내 중요 정보 탈취와 같은 사례와 그림 3에서 알 수 있듯 해마다 급격하게 증가하는 데이터 트래픽을 대입해보면 향후 해당 분야에 대한 투자는 선택이 아니라 필수인바, 스마트 EDR 시스템의 구현을 위해 보다 폭넓은 수준의 학술적, 기술적 교류를 기대해 볼 수 있다.

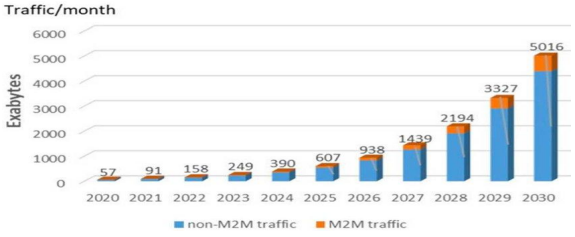


Fig. 3. Prediction of growth global data traffic in year 2020 to 2030

IV. Conclusions

현재의 EDR 시스템은 규모가 있는 기업 중심의 엔터프라이즈 보안에 그치고 있지만 기술과 산업 환경의 변화가 극심한 현재, 수요의 증가 추이로 볼 때 앞으로는 더욱 경량화와 최적화된 환경으로의 전환이 요구될 것이며 그에 따라 발전된 스마트 EDR 시스템에 대한 요구도 증가할 것이다. 또한, 방대한 정보들이 실시간, 유기적으로 생산되는 현대 사회에서 수많은 단말들을 일일이 관리하고 안전하게 처리하는 문제는 현재가 아닌, 미래에도 가장 중요한 이슈가 될 것이므로 인공지능을 활용한 스마트 EDR 시스템의 구축 및 발전은 현재 보안 영역에서의 최우선 과제로서 해결해야 할 것이라고 판단한다.

REFERENCES

[1] Korea Internet & Security Agency, "EDR solution report", November 2022.

[2] Jhhong, "Artificail Intelligence-based Security Contro l Construction and Countermeasures", Journal of The Korea Contents Association, Vol. 21, No. 1, pp. 531-540, Jan. 2021.

[3] Ksryu, "Trends in Research on Artificial Intelligence Security Attacks and Countermeasures", Journal of The Korea Institute of Information Security & Cryptology, pp.93-99, Oct. 2020.

[4] Ysjae, "A Study on Smart EDR System Security Development", Journal of The Korea Convergence Security Association, pp.41-47, Mar. 2020.

[5] Mjkim, "A Study Of Mining ESM based on Data-Mining", Journal of The Korea Convergence Security Association, pp.3-8, Dec. 2011.

[6] Bgan, "Malicious Packet Detection Technology Using Machine Learning and Deep Learning", Journal of The Korea Convergence Security Association, pp.109-115, Oct. 2021.