https://doi.org/10.33778/kcsa.2020.20.1.041

Smart EDR 시스템구축을 위한 보안전략과 발전방안★

유 승 재*

ABSTRACT

기업 시스템 환경에서 실제업무의 적용단계인 단말(Endpoint)에서 발생하는 의심스러운 행위를 탐지하고 통제하는 것은 조직의 비즈니스 환경을 안전하게 하는 가장 핵심적인 영역이라 할 것이다. 내외부로부터의 위협을 정확하게 탐지하고 차단하기 위해서는 조직 내 모든 단말의 모든 영역을 모니터링하고 관련 정보를 수집할 수 있어야 한다. 즉 끊임없는 악성코드의 도전으로부터 기업조직의 안전한 비즈니스 환경을 유지하기 위해서는 기존 보편화 되었던 알려진 패턴이나 시그니처, 정책, 룰 기준의 탐지와 방어 중심의 클라이언트 보안을 넘어 PC등 업무용 단말에서 발생하는 모든 일을 파악하고 모니터링 할 수 있도록 하는 EDR 솔루션 도입은 이제 보안의 필수적인 요소가 되고 있다. 이에 본 연구에서는 EDR솔루션에 요구되는 필수적인 기능을 살펴보고, 보안문제에 대한 능동적인 선행적 탐지를 기반으로 하는 지능적인 EDR시스템의 설계와 발전방안에 대해 연구하고자 한다.

A Study on Smart EDR System Security Development

Seung Jae Yoo*

ABSTRACT

In the corporate information system environment, detecting and controlling suspicious behaviors occurring at the end point of the actual business application is the most important area to secure the organization's business environment. In order to accurately detect and block threats from inside and outside, it is necessary to be able to monitor all areas of all terminals in the organization and collect relevant information. In other words, in order to maintain a secure business environment of a corporate organization from the constant challenge of malicious code, everything that occurs in a business terminal such as a PC beyond detection and defense-based client security based on known patterns, signatures, policies, and rules that have been universalized in the past. The introduction of an EDR solution to enable identification and monitoring is now an essential element of security. In this study, we will look at the essential functions required for EDR solutions, and also study the design and development plans of smart EDR systems based on active and proactive detection of security threats.

Key words : EDR, Endpoint Security, Security Policy

접수일(2020년 12월 09일), 수정일(1차: 2020년 12월 26일), 게재확정일(2020년 03월 22일)

★이 논문은 2019년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임.

* 중부대학교 정보보호학과

1. 서론

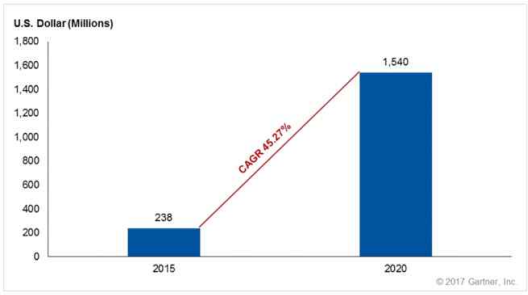
기업의 업무형태로 보편화되어 있는 BYOD(Bring Your Own Device)환경은 많은 보안 이슈를 생산해 왔다. 실제로 포브스(Forbes)에 따르면, 미국의 경우 2007년 대비 2019년 원격 근무 비율이 159% 증가했으며, 영국은 인력의 50%가 원격 근무를 하는 것으로 추정되어 업무용이 아닌 개인용 데스크톱이나 노트북을 회사의 업무에 사용하는 비율도 함께 증가하고 있다.[6]

개인 소유 장치를 업무에 사용하는 것의 위험성을 제거하기 위해 우선 소유자 개인의 정보가 기업 보안 인프라의 일부로 관리되어야 할 것이며 이 과정에는 상호 수용 가능한 보안모델이 필요함을 이미 잘 알려진 보안이슈이다.

또한 기업업무 환경을 구성에 있어서 이러한 BYOD 장치(PC, 노트북, 휴대폰, 각종 모바일 디바이스 등)들은 단말(Endpoint)에 해당되며 이곳에서 수많은 위협요소와 취약점이 노출되고 있어 어에 대한 대응이 중요한 이슈로 자리매김하고 있다.

즉 기존 방화벽, IDS, 접근제어시스템 등 대부분의 보안제품들은 외부에서 내부로의 트래픽에 대한 보안강화가 목적이므로 내부 사용자들의 다양한 단말 디바이스 이용으로 인해 발생할 수 있는 보안위협에 대해서는 적절한 대응이 어렵다는 문제점을 갖고 있다. 한편 엔드포인트에서의 위협 탐지 및 대응 솔루션으로 일려진 EDR은 내부 사용자들의 단말기에서 발생하는 여러 상황을 탐지하고 대응할 수 있는 행위 위주의 보안솔루션으로서 사용자 어플리케이션을 통한 악성코드 유입, 제로데이와 같은 패치되지 않은 신규 취약점에 대한 능동적인 대처에 최적화된 대응으로 평가되어 지난 해 세계 보안 분야에서 가장 핫 했던 솔루션으로 평가되고 있다.[8]

Gartner에서는 EDR의 핵심적 역할을 다른 보호기술을 회피한 위협을 탐지하는 것으로 정의하고 있듯이 기업보안의 측면에서 EDR 솔루션 도입은 이제 보안의 필수적인 요소가 되고 있고, (그림 1)에서 볼 수 있듯이 그 시장규모도 45.27%의 연평균 성장률을 보이고 있다.



(그림 1) 글로벌 EDR시장 규모[12]

이 연구에서는 이미 보편화 되었던 미리 만들어진 패턴이나 시그니처, 정책, 룰 기준의 탐지와 방어 중심의 클라이언트보안에서 보안문제에 대한 능동적인 선행적 탐지를 기반으로 하는 스마트 EDR시스템으로의 발전방안에 대해 연구하고자 한다.

2. 관련연구

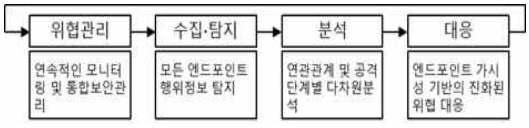
앞에서 언급된 바와 같이 EDR은 사용자 어플리케이션을 통한 악성코드 유입, 제로데이와 같은 패치되지 않은 신규 취약점에 대한 능동적인 대처에 최적이며 최근에는 인공지능이 탑재되어 능동적이고 유연한 대응이 가능한 솔루션으로 그 성능이 지속적으로 진화하고 있다.[1][2] 실제로 STIX(The Structured Threat Information eXpression;사이버위협정보표현규격), TAXII (Trusted Structured Threat Indicator Information ; 사이버위협 정보전송규격), YARA, IOC(Indicator of Compromise;침해지표)등의 위협정보 공유 포맷을 활용하고 또한 행위분석이나 머신러닝 등 인공지능 기술을 활용하여 알려지지 않은 위협을 탐지하고 있다. 또한 엔드포인트에서 발생하는 다양한 이벤트로 위협을 탐지해 기존 APT 방지를 위한 샌드박스 유형의 제품들의 약점을 보완하고 있다.

기본적으로 EDR이 갖춰야 할 기본기능으로는 첫째, 사용자, 엔드포인트 및 네트워크 수준에서 잠재적인 또는 발견된 위협을 탐지(Detection) 둘째 연관분석, 추적조사 & 클라우드나 샌드박스 등과 연동 조사(Investigation) 그리고 셋째는 운영 중인 보안솔루션 및 대응프로세스와 연계, 대응, 예방, 치료와 복구를 위한 통제와 복구(Containment & Remediation)라 할 수

있고 이와 더불어 위협에 의한 재발과 확산 방지라 할 수 있다. [8]

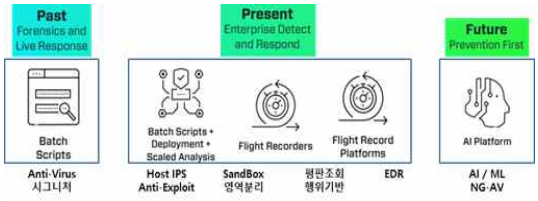
다음은 국내외 대표적인 EDR 솔루션에 대해 특징과 구성을 살펴본 것이다.

(그림 2)와 같이 엔드포인트 영역에 대한 연속적인 모니터링을 통해 위협 탐지 및 분석, 대응을 제공하는 엔드포인트 위협 탐지 및 대응솔루션인 AhnLab EDR은 자체개발한 MDP(Multi-Dimensional Protection) 엔진에 의한 행위분석기술과 MITRE ATT&CK 사이버보안 프레임워크를 결합하여 고도화된 위협탐지 성능과 정밀한 위협가시성을 추구하였다 평가된다. 또한 EPP(Endpoint Protection Platform) 기반의 제3 솔루션과의 연동을 통한 인텔리전스 강화를 그 특징으로 들 수 있다.[13]



(그림 2) 안랩 EDR 위협대응 프로세스(13)

Cylance 의 EDR솔루션으로 인공지능 및 머신러닝 기반 모델링을 내장하고 있는 CylancePROTECT는 엔드포인트에서 위협을 탐지하고 보고하는 단순기능을 넘어 파일 기반의 악성코드 공격, 파일 기반이 아닌 공격, 스크립트 공격, 메모리 기반 공격 등이 실제로 실행되기 이전에 능동적으로 위협을 격리 및 차단하고 보안 담당자와 엔터프라이즈 보안 부서를 위해서 내부에 존재했던 위협 가시성에 대한 실질적인 대응 정보를 제공함으로써 예측-차단-보호 단계적 과정을 수행하며 엔터프라이즈 네트워크를 보호하는 솔루션이다. 아래 그림은 EDR의 기능과 특징에 대한 변천과정을 설명한 것이다. 과거 안티바이러스나 시그니처 기반으로 알려진 위협만 대응하는 수준에서 오늘날 보안 분석가가 선별할 수 있는 유용한 데이터를 생성하고 Hunting기능과 SE-마이그레이션, 지능형탐지 등이 가능한 수준이다. 미래의 EDR은 (그림 3)에서 보는 바와 같이 AI플랫폼을 통해 멀웨어나 랜섬웨어 등 악성코드를 pre-execution으로 실행 이전에 차단하는 것과 또한 탐지-조사-차단-치료 EDR단계에 완전 자동화된 AI에 적용되는 것이 기대되고 있다.



(그림 3) EDR 변화과정 [7]

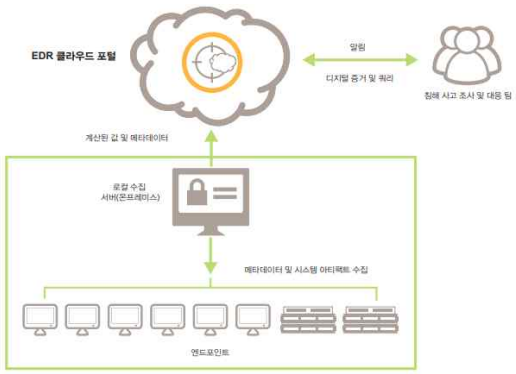
차세대 엔드포인트보안, 위협정보 및 대응서비스 분야 대표적인 기업인 CrowdStrike에 의하면 기업은 시스템 리소스를 낭비하지 않고 보안 팀에 가치를 추가하면서 최소한의 노력과 투자를 요구하면서 최고 수준의 보호 기능을 제공 할 수 있는 EDR 소프트웨어를 찾는 것이 중요하다는 것을 강조하고 있다. 이를 위한 EDR의 주요 핵심요소 6가지를 제시하고 있다.[9]

- 모든 엔드포인트에 대한 실시간 가시성을 통해 환경을 위반하려고 시도하더라도 악의적 인 활동을 보고 즉시 중지 할 수 있는 가시성 확보
- 다양한 분석 기술로 공격 징후를 탐지 할 수 있도록 엔드포인트에서 수집되고 컨텍스트가 강화 된 방대한 양의 원격감시에 요구되는 위협 데이터베이스
- 시그니처 기반 방법이나 IOC (Indication of Indication)에만 의존하지 않고, 효과적인 엔드포인트 탐지 및 대응을 위해 공격 지표 (IOA)를 검색하는 행동 방식의 행위보호
- 위협 인텔리전스가 통합된 엔드포인트 탐지 및 대응 솔루션은 공격자나 공격에 관한 세부 정보를 포함한 컨텍스트를 제공 할 수 있는 인사이트와 인텔리전스 제공
- 침입이 발생하기 전에 공격을 중단하고 신속하게 비즈니스에 복귀 할 수 있도록 하는 빠른 응답
- 엔드포인트에 미치는 영향을 최소화하는 방법으로서 검색, 분석 및 조사와 같은 기능을 정확하고 실시간으로 수행 할 수 있도록 하는 클라우드 기반 솔루션

시만택의 EDR Cloud의 특징은 엔터프리이즈 환경 전반에서 기존 환경에 속하지 않은 이상 요소 발견하

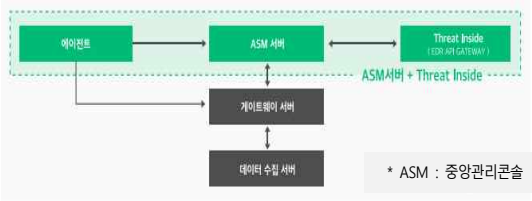
는 탐지와 베스트 프랙티스를 활용한 자동화 그리고 방대한 양의 사이버 데이터에서 실행 가능한 결과를 창출하고 시각화하는 것으로 정리된다.

구체적으로 보면, (그림 4)에서 참고할 수 있듯이. 소프트웨어 이상요소, 메모리 이상요소, 사용자이상요소, 네트워크 이상요소 뿐만 아니라 신경망머신러닝 기반 탐지와 보안위협 인텔리전스 소스기반 탐지를 수행한다. 시각적 링크 분석을 통해 서로 다른 데이터 유형 간의 복잡한 관계를 분석하고 개념적으로 연결하는 기능을 수행한다. 자동화(Automation)로는 자동화된 침해 사고 플레이북 규칙에 따른 분석, 자동화된 아티팩트 수집으로 엔드포인트 활동에 대한 심도 있는 가시성 확보 등 숙련된 조사 팀의 베스트 프랙티스 활용하는 기능이다. 시각화(Visualization) 측면을 보면 방대한 양의 사이버 데이터에서 실행 가능한 결과를 창출하고 방대한 엔드포인트 텔레메트리를 대화형 그래픽으로 변환 제공하는 기능으로 설명된다.[5]



(그림 4) Symantec의 EDR Cloud[5]

알약 EDR은 (그림 5)와 같이 이스트시큐리티의 엔드포인트보안 위협대응 솔루션으로서 엔드포인트 내의 위협정보 선별하고 모니터링하며 위협프로세스를 차단한다. 이 솔루션의 특징으로는 악성/의심 프로세스를 흐름도로 제공하여 가시성을 높였고, 행위기반 의심탐지 및 상세위협 인텔리전스(연관성분석, 리얼머신 분석, 유사도분석, 평판분석, 네트워크분석, 샌드박스 분석, 정적분석 등) 운영 그리고 커널 로깅 기능 등 안정적인 운용을 지원한다.



(그림 5) 알약 EDR 구성타입[11]

글로벌 기업 C사에서는 조사 발표한 2016 NSS Labs BDS테스트보고서에 포함된 엔드포인트보안솔루션 성능비교를 제시하였는데, 이 자료는 4개의 솔루션 (자사솔루션1, 경쟁사 솔루션3개)에 대해 탐지(12), 대응(5), 아키텍처(4), 위협인텔리전스(7) 등 4개의 영역에서 28개의 항목에 대한 성능과 기능을 비교 평가하였다.[14]

<표 1> EDR 솔루션 성능측정 결과

매우우수3, 우수(미공개):2 보통: 1, 미흡:0

구분	항목	평가값	비고 (C1,C2,C3,C4)
탐지 (12)	통합된 탐지 기술 수	8	(3,2,2,1)
	지속적 분석과 회귀적 탐지	11	(3,2,3,3)
	디바이스 경로 분석	8	(3,3,0,2)
	탐지 수단	10	(3,3,3,1)
	동적 파일분석	4	(3,1,0,0)
	파일분석구축모델	6	(3,1,2,0)
	API 지원	10	(3,3,3,1)
	파일경로분석	8	(3,2,2,1)
	화이트리스트/블랙리스트	12	(3,3,3,3)
	소프트웨어 취약점	6	(3,1,2,0)
	통합형 ATP(공격 디토네이션)	7	(3,1,2,1)
	샌드박스 인식형 악성코드	8	(3,2,2,1)
	소계	**98**	**68.05**
대응 (5)	악성코드 치료	10	(3,2,2,3)
	악성코드 게이트웨이 확인	8	(3,2,3,0)
	맞춤형 탐지	12	(3,3,3,3)
	파일 검색 및 가져오기	8	(3,3,2,0)
	취약한 애플리케이션 가시성	6	(3,1,1,1)
	소계	44	73.33
아키텍처 (4)	운영 체제 지원	9	(3,3,2,1)
	구축 모델	10	(3,3,2,2)
	오프라인 지원	12	(3,3,3,3)
	폐쇄 루프형 탐지, 다른 플랫폼과의 통합	11	(3,2,3,3)
	소계	**42**	**87.50**
위협 인텔리전스 (7)	일일 고유 악성코드 샘플	9	(3,2,2,2)
	매일 차단되는 위협 수	9	(3,2,2,2)
	매일 검사된 이메일 메시지 수	6	(3,1,1,1)
	매일 모니터링되는 웹 요청 수	6	(3,1,1,1)
	매일 모니터링 및 처리되는 URL	6	(3,1,1,1)
	자동화된 인텔리전스 피드	12	(3,3,3,3)
	위협 인텔리전스 공유	6	(3,1,1,1)
	소계	54	64.29
총계 (통합)		238	70.83

앞의 <표 1>은 2016 NSS Labs BDS테스트보고서의 측정 자료를 토대로 측정항목간의 가중치는 두지 않고 각각을 3점 척도로 계량한 것이다

이 비교평가 자료는 C사의 자사제품을 강조할 목적으로 측정된 것임을 감안할 때 비교 제품의 특성을 충분히 반영하였다고 보기 어려운 면이 있음을 전제로 한다. 다만 조사 시기를 기준으로 EDR제품의 특성을 이해하기 위한 참고자료로는 무리가 없다고 판단된다.

3. 스마트 EDR 구성요소

CONCERT(한국침해사고대응팀협의회)는 한국CPO포럼과 공동으로 발표한 Security Consumer Report에서 EDR솔루션의 필요성과 도입의 효과성을 통해 EDR솔루션을 운영하고 있거나 향후 도입을 계획하는 기업에게 유용한 정보를 제공하기 위해 주요 제품들에 대한 비교평가를 실시하고 그 결과를 발표하였다.

EDR솔루션이 제공하는 탐지와 대응, 엔드포인트단에서의 가시화부분에 초점을 맞추어 EDR 솔루션의 평가항목으로 탐지엔진 및 기술(9), 인스턴트 분석정보(24), EDR Endpoint(13), 인스턴트 처리(6), 관리(3), 리포팅(3) 등의 6개 영역에서 총 58개의 항목을 세분화 하여 제시하고 사이버리즌, 시만텍, 엔피코어, 지니언스, 카스퍼스키, 트렌드마이크로, 파이어아이, 팔로알토 등 8개 업체의 제품을 대상을 평가를 실시하여 EDR의 도입 운영에 대한 주요한 참고정보를 제공하였다. 그리고 EDR솔루션이 반드시 가져야 할 기능으로서 엔드포인트 시스템레벨 동작으로 이벤트를 기록하고 중앙데이터베이스에 저장하고, 알려진IOC(침해지표)와 행위분석기술을 사용하여 침해를 조기에 식별하기 위한 지속적인 검색을 수행하며 공격의 범위를 신속하게 조사하고 빠른 대응 등을 제시하고 있다. [15]

한편 엔드포인트보안플랫폼 EPP(Endpoint Protection Platform)는 바이러스 백신, 멀웨어 방지, 데이터 암호화, 개인 방화벽, 침입방지시스템(IPS) 및 데이터 손실 방지(DLP)등과 같이 디바이스 레벨에서 위협을 탐지하고 차단하도록 설계된 통합 보안 솔루션이다.

기본적으로 EPP와 EDR을 구분해 본다면, EPP는 알려진 위협을 차단하는 데 효과적인 1차 방어 메커니즘이라면 EDR은 그 다음 보안 계층으로, 위협을 찾고, 포렌식으로 침입을 분석하고, 신속하고 효과적으로 공격에 대응할 수 있는 추가 도구를 제공한다 할 수 있다. [10]

이전까지 엔드포인트보안의 메인이었던 백신은 한 번의 설치로 관리자 개입 없이 자동으로 시그니처를 업데이트하는 편의성을 장점으로 하였지만, 이는 알려진 위협을 차단하는 것으로 정해진 패턴, 시그니처 분석으로 탐지하므로 실상 사전예방이 아닌 사후조치에 해당된다고 볼 수 있다. 능동적이고 적절한 사전대응을 위해서는 엔드포인트에서 발생하는 행위를 모니터링하고 발견된 이벤트의 위협 수준에 따라 적절하게 대응하는 관리자 단에서 적극적인 개입이 필요하며 이 역할을 EDR이 담당하는 것이다.

한편 PC에서 일어나는 이벤트 로그 등을 분석해서 이상행위를 탐지하고 대응함에 있어서, EDR 운영의 복잡성으로 인하여 실제 기업의 업무성격에 따라서 유의할 수준의 오탐(과탐)이 발생할 수도 있다는 것은 큰 난제로 존재한다.[3][4]

이에 대해 EaaS(EDR as a service))개념의 형태인 MDR (Managed Detection &Response)은 부분적인 대안으로 제시되고 있다.

아울러 엔드포인트 자체에서 일어나는 이벤트를 분석하는 차원을 넘어 엔드포인트, 네트워크, 클라우드, 파일 등 IT 전체에서 발생하는 위협을 탐지하고 연계 분석하는 개념인

XDR(everything Detection &Response) 등장은 네트워크와 클라우드 등 모든 영역을 포괄하는 매우 이상적인 형태로 평가된다.

다양한 국내외 EDR 솔루션의 기능과 특징을 분석하면 EDR 선택기준으로 다음가 같은 기능을 정리할 수 있다.

- 빈틈없는 위협탐지 기능 : 시그니처, IOC(침해사고지표), IOA(침해공격지표), 샌드박스, 머신러닝 등 file기반 악성코드 탐지 및 행위기반, 비정형탐지 권한관리 등 file-less기반 위협탐지 구현
- 단말정보기반 기능수행 : Agent에 의한 정보수집 빈도와 수준을 고려하여 사용성과 효율성의 균형 유지
- 수집된 정보분석 위협탐지 : 탐지운영과 역량에 따라 클라우드형, 하이브리드형, 독립/단말 형

으로 구분하여 운영

또한 EDR솔루션 도입의 효과를 극대화 위해서 관리자가 반드시 고려해야 사항으로 다음을 제시하고 있다.[6]

- 시스템 내 모든 위협요소와 엔드포인트 전체와의 연관성을 한눈에 파악할 수 있는 위협가시성을 확보하는 것이다.
- 기존 보안솔루션과의 연동 및 지능형 공격 대응을 위해 필수적으로 부가되는 운영 리소스를 줄이는 전략이 요구된다.
- 낮은 보안전문성을 보완할 수 있는 대안으로 위협 인텔리전스 운영이 요구되는데, 이 경우 기존 보안솔루션과의 상승효과를 높이기 위해 공유체계의 표준이 지원되도록 하는 것이 필요하다.

4. 결론

현재의 EDR 솔루션은 기업 시스템을 사용하는 사용자들을 위한 엔터프라이즈 보안으로 분류되지만 점차 개인사용자에 준하는 소규모 창업기업이나 개인사업자들의 수효가 늘어나면서 이들의 환경에 적용할 수 있도록 보안솔루션의 커스터마이징 이슈가 부각되어 왔다. 이러한 현상으로 EDR 솔루션은 악성코드 탐지, APT 공격 탐지, 해킹 방지 등 주로 탐지와 대응에 초점을 두고 경량화와 최적화된 환경으로의 전환이 강조되고 있어, 보다 능동적인 선행적 탐지를 기반으로 하는 진화된 스마트 EDR솔루션에 대한 구현방안의 제시가 필요하다.

즉 능동적인 탐지와 대응을 통해 이전의 오진 및 오탐으로 인한 피해와 부작용 최소화하고, 기존 악성코드로부터 새로운 악성코드로의 변형을 예측하는 과정에서의 발생되는 오탐과 에러를 줄이기 축적된 많은 악성코드 로-데이터를 빅데이터 시스템과 인공지능 머신러닝과 결합하여 엔드포인트 공격의 요소를 보완하고 취약점을 해결하며, 개인 이용자와 소규모 기업에 적합한 환경으로 구현하도록 제공해야 할 것이다. 더 나아가 초연결사회를 지향하는 지능정보사회에서 수많은 디바이스들 간의 연결로 생산되는 엄청난 양의 정보를 안전하게 관리하는 문제는 미래의 중요한 보안이슈를 고려하여 단말의 부하를 최소화한 수집과 탐지가 가능하며 기 알려진 위협은 물론 비정상적인 행위(위협 의심파일 및 File-less 공격 기반 등)분석과 네트워크상의 위협 의심 정보와의 연동하여 네트워크상의 이상이 엔드포인트에서의 악성행위나 악성파일 생성으로 이어졌는지 분석 & 반대 상황도 분석이 가능하도록 구현되어야 할 것이다. 아울러

인공지능머신러닝 기술을 기반으로 진화하는 엔드포인트보안은 실시간 탐지와 선제적 차단을 가장 우선으로 하고 있으며 그 기법의 안정적 운용과 적합성에 대해 명확하게 수학적모델과 알고리즘으로의 증명이 필수적인 요건이라 할 것이다.

참고문헌

[1] Seung Jae Yoo, “Study on Improving Endpoint Security Technology”, 융합보안논문지 제18권 제3호 pp.19-25, 2018.

[2] John R. Vacca, Computer and Information Security Handbook, Elsevier, 2013

[3] 박원형 외 3인, “보안관제 위협 이벤트 탐지규칙 표준 명명법 연구”, 융합보안논문지 제15권 제4호 pp.89-96, 2015.

[4] 김귀남 외1명, “데이터 마이닝 기반 보안관제 시스템”, 정보보안논문지 제11권 6호, 3-8, 2011.

[5] 시만텍 인터넷 보안 위협 보고서(ISTR), 제22호, 2017.

[6] 이스트시큐리티 보안동향보고서 No.126 2020.

[7] The Evolution of ED_Acceleration of Intelligence and Actions, 2019. www.cylance.com.

[8] Genian Insights E v2.0, http://genians.co.kr/

[9] What is Endpoint Detection and Response (EDR)? 2019. www.crowdstrike.com/

[10] EPP VS EDR - WHAT'S THE DIFFERENCE?, 2019, https://www.redscan.com/

[11] 이스트시큐리티, www.estsecurity.com

[12] 가트너, www.gartner.com

[13] 안랩, www.ahnlab.com

[14] 2016 NSS Labs BDS 테스트보고서, 2016, Cisco

[15] “Security Consumer Report-EDR 솔루션”, CONCERT & 한국CPO포럼, 2019.

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교
정보보호학과 교수
email : sjyoo@joongbu.ac.kr