보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

EDR 도입 후 달라지는 것

AhnLab 2021-09-06

코로나19 역학조사는 감염자의 감염 경로, 이동 동선 등 인과관계를 파악하여 추가적인 확산을 막기 위해 실시된다. 이후, 수집한 정보를 분석해 인사이트를 도출하면 적합한 대응 방안을 수립할 수 있다.

사이버 보안에서도 유사한 개념을 적용한 솔루션이 각광을 받고 있다. 바로, 위협 탐지 & 대응 솔루션 'EDR'이다. 시장조사기관 가트너에 따르면, 글로벌 EDR 시장 규모는 2015년 2억 3800만 달러(한화 약 2,795억 원)에서 2020년 15억 달러(한화 약 1조 7,615억 원)까지 성장했다. 특히 연 평균 성장률 45.3%는 주목할만한 수치다.

조직들이 EDR을 올바르게 사용하고 도입 효과를 극대화하기 위해서는 EDR에 대한 근본적인 이해가 선행되어야 한다. 이번 글에서는 공격의 고도화와 방어 기법 발전 현황을 살펴보고, EDR이 필요한 이유와 도입 후 달라지는 보안 체계에 대해 설명한다.

EDR의 이론적인 배경을 이해하려면 먼저 공격의 고도화와 방어 기법의 발전이 어떤 식으로 이뤄지고 있는지 살펴봐야 한다. 참고로, 공격과 방어의 기술에는 여러가지가 있지만 이번 글에서는 가장 핵심적인 ▲사회공학적 기법 ▲파일리스 공격 ▲행위기반 탐지에 대해 설명한다.

사회공학적 기법으로 교묘하게 유입되는 공격

오랜 기간 변하지 않는 해커들의 공통적인 특징을 꼽자면, 보안이 취약한 지점을 찾아 집요하게 공격을 감행한다는 것이다. 더 쉽게 큰 이득을 취하기 위해서다. 이 관점에서 최근 공격자들이 가장 많이 선택하는 공격 경로는 웹, 이메일, 그리고 취약점이다. 예를 들면 보안 패치가 되지 않은 응용 프로그램, 취약한 웹 사이트 접속

등을 통한 악성코드 감염을 들 수 있다. 이 경로들은 과거에도 공격에 많이 활용되어 왔지만 시간이 지남에 따라, 그리고 공격 지점이 분산됨에 따라 고도화 및 조직화되고 있다.

해당 공격 방어가 쉽지 않은 이유는 공격자들이 주로 '사회공학적' 기법을 사용하기 때문이다. 사회공학적 기법이란 사람의 심리를 이용하는 공격 방법으로, 공격 대상을 속여 공격자가 원하는 행위를 하게 하는 방법이다. 사냥을 할 때 덫을 놓고 미끼로 유인하는 것과 같은 맥락이다. 만약 공격 대상이 덫에 걸리면 공격자는 원하는 결과를 손쉽게 얻을 수 있다.

대표적인 사례가 악성 이메일을 전송해 첨부 파일을 실행하게 하거나, 악성 URL을 클릭하도록 유도하는 것이다. 이러한 공격은 대상이 공격자가 원하는 행위를 해준다는 전제 하에 이뤄진다. 사람은 누구나 실수를 할 가능성이 있고, 특히 위급하거나 어려운 상황에서 잘못된 판단을 할 가능성이 더욱 높아진다는 사실을 공격에 이용하는 것이다. 공격자들은 공격 경로를 설정할 때 '사람'이 보안에 있어 가장 취약한 부분이라는 전제를 하고 공격을 감행한다.

공격 방법의 고도화, 파일리스 공격 증가

이처럼 최근의 공격들은 교묘한 방법을 동원해 보안이 취약한 지점을 노린다. 뿐만 아니라, 공격의 동작 형태도 탐지를 우회하고 흔적을 남기지 않도록 진화를 거듭하고 있다.

과거 행해지던 사이버 공격들은 대부분 파일 형태의 악성코드를 활용했다. 우리가 흔히 알고 있는 실행 파일, 스크립트 파일, 문서 파일 등 개별 파일에 악성코드를 포함시키는 방식이다. 그리고 방어자는 안티바이러스(AV) 솔루션을 활용하여 디스크 내에 파일 형태로 존재하는 악성코드를 진단 및 차단해 시스템을 보호해왔다.

하지만 공격자들은 AV 솔루션의 탐지 & 차단을 우회하기 위해 다양한 방법을 개발하기 시작했다. 대표적인 예가 파일리스(Fileless) 악성코드다. 직역하면 '파일이 없다'는 뜻의 파일리스 악성코드, 정확한 정의는 '악의적인 기능을 수행하는 코드를 메모리에서만 실행시키면서 시스템에 피해를 입히는 유형의 공격'이다.

파일리스 악성코드는 메모리에서만 동작하는 인 메모리 멀웨어(in-memory malware)와 LOL(Living Off The Land) 도구를 사용해 타깃 시스템 내 공격 흔적을 최소화하는 것이 특징이다. 참고로, LOL은 자급자족을 뜻하는 표현으로 공격자가 공격 과정에서 외부 도구가 아닌 파워쉘(PowerShell) 등 대상 시스템 내 정상 도구를 사용한다는 의미다.

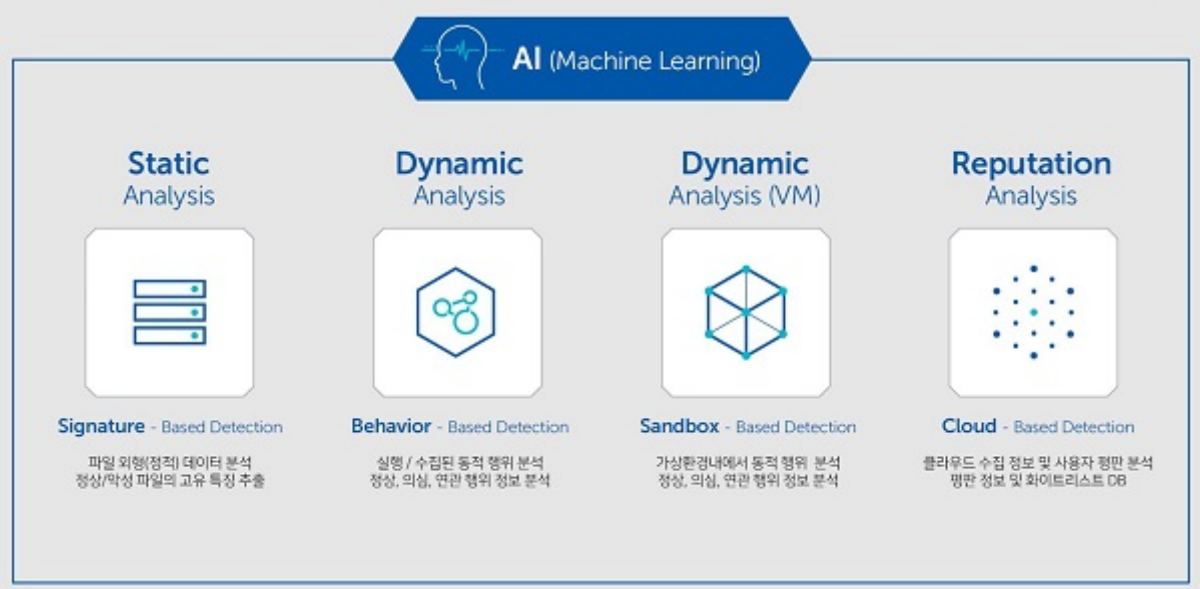
해커가 파일리스 공격을 성공시켰다고 가정해보자. 방어자 입장에서는 악성코드가 파일 형태로 존재하지 않아 스캔할 대상이 없기 때문에 파일을 모니터링하는 AV 솔루션으로 탐지해 차단하기 어렵다. 공격을 당한 이후에도 파일이 없기 때문에 파일의 해시(Hash)를 구할 수 없다. 결국 공격을 추적할 단서가 부족해져 피해를 복구하고 향후 대응 체계를 수립하는 데에도 한계에 부딪히게 된다.

반대로 공격자 입장에서 파일리스 공격은 악성 파일을 활용했던 기존 방식 대비 AV 솔루션 탐지를 우회해 공격 성공률은 높이면서 추적 당할만한 흔적은 최소화하는, 말 그대로 '일석이조'의 효과가 있는 셈이다.

보안 기술 발전, 핵심은 '행위 기반' 탐지

공격의 고도화에 대응해 보안 기술은 어떻게 발전했는지 살펴보자. 보안에서 공격과 방어는 쫓고 쫓기는 관계에 있다. 특정 보안 기술이 등장하면 공격자들은 이를 우회할 수 있는 공격 기법을 개발하고, 다시 이를 탐지해 방어할 수 있는 신기술이 등장하는 식이다.

사이버 공격을 탐지하는 기술을 정리해보면 크게 ▲시그니쳐 기반 탐지 ▲행위 기반 탐지 ▲가상 환경에서 동적 분석을 진행하는 행위 기반 탐지 ▲평판 분석을 통한 클라우드 기반 탐지 등 네 가지를 꼽을 수 있다. 최근에는 이 네 가지 탐지 기법에 머신러닝 기법을 적용하기도 한다.



[그림 1] 사이버 공격에 대한 네 가지 탐지 기술

시그니처 기반 탐지는 파일에 존재하는 데이터 패턴을 확인해 악성 여부를 진단한다. 예를 들면, 파일에 블루크랩(BlueCrab) 랜섬웨어에서 발견되는 데이터 패턴이 존재하면 블루크랩 랜섬웨어로 진단하는 것이다. 다만, 공격자는 데이터 패턴을 변경하는 방법을 통해 탐지를 우회할 수 있다. 전통적인 시그니처 기반 AV 솔루션만으로 최신 공격을 방어하는데 한계가 있는 이유이기도 하다.

공격자들이 시그니처 기반 탐지를 다양한 방법을 통해 우회하자 보안 기업들은 악성코드의 행위 자체는 동일하다는 점에 착안해 '행위 기반 탐지' 기법을 개발했다. 예를 들면 특정 파일을 생성하고, 레지스트리에 어떤 값을 기록하거나 네트워크 접속 행위를 하면 악성으로 탐지하는 방식이다.

또한, 기업/조직에 유입되는 파일의 행위 분석을 가상 환경에서 진행해 악성코드를 차단하는 기법도 많이 활용되고 있다. 흔히 '샌드박스(Sandbox) 기반 탐지'로도 알려져 있는데 가상 환경에서 이뤄지는 동적 행위의 연관 정보를 분석하여 정상 여부를 판단하는 것이다.

이 밖에, 각 파일에 대해 수집된 정보를 기반으로 진단하는 '클라우드 기반 진단'도 있다. 얼마나 많은 사용자가 사용하고 있는 파일인지, 코드 서명은 되어 있는지, 사용자 평판은 어떤지 등의 정보를 종합해서 악성 여부를 판단한다.

EDR의 역할: 기존 보안 체계의 한계 보완

공격의 고도화와 보안 기술의 발전을 종합하면 공격자들은 교묘한 방법으로 보안이 취약한 지점을 노리고 공격 흔적을 최소화해 방어자의 대응을 어렵게 한다. 이에, 보안은 악성 파일이 아닌 공격자의 행위에 초점을 두고 기술을 발전시켜왔다.

앞서 설명한 파일리스 공격이 이제 여러 종류의 악성코드에 일관되게 나타나면서, 행위 기반 진단이 굉장히 중요한 역량으로 부각되고 있다. 특히, 기업과 기관을 노리는 지능적인 공격자들은 다양한 진단 기술을 회피

할 수 있는 상당한 기술력을 갖추고 있기 때문에, 신속한 침해 대응을 위해서는 알려지지 않은 위협까지 탐지하고 추적(Threat Hunting)하는 것이 중요해졌다.

이에, 기존 보편화된 AV와 네트워크 기반 보안 체계에 진일보한 탐지 & 대응 역량이 추가로 요구되고 있다. AV와 네트워크 중심의 대응으로는 실제 감염이 일어난 엔드포인트에 대한 충분한 정보(로그)를 확보하지 못해 감염 경로와 잠재적인 위협을 파악하는 것이 어렵기 때문이다.

이 한계를 보완해주는 것이 바로 EDR(Endpoint Detection & Response)이다. 가트너가 정의한 바에 따르면, EDR은 엔드포인트에서 지속적인 모니터링과 대응 역량을 제공하는 보안 솔루션이다. EDR은 기본적으로 ▲보안 침해 탐지 ▲보안 침해 조사 ▲엔드포인트에서의 보안 통제 ▲조치와 해결을 위한 가이드 및 대응 등의 기능을 제공한다. 핵심은 사용자에게 로그를 포함한 상세한 위협 정보와 공격 흐름도를 제공해, 위협 종류, 행위 및 공격 단계에 따라 적절한 대응 방안을 제시한다는 것이다.

EDR의 개념과 필요성을 보다 직접적으로 알 수 있는 두 가지 설명을 보충한다.

첫 번째는 기존 보안 체계에 대한 자문이다. 새로운 것의 필요성을 이해하고자 할 때 적합한 기준을 세운 뒤 수학에서 역산을 하듯 현재 상황에서부터 거슬러 올라가면 올바른 답을 찾을 수 있다. 이 관점에서 기존 보안 체계의 한계점을 정리한 [표 1]을 살펴보자.

#	한계점
1	수집할 수 없는 대상은 분석할 수 없다
2	분석하지 못하면 악성 또는 정상 여부를 확인할 수 없다.
3	악성으로 확인하지 못했다면 대응도 할 수 없다.
4	분석 결과를 패턴화하지 못하면 동일한 위협을 자동 탐지할 수 없다.
5	패턴화하는 작업 자체를 자동화할 수 없다면 신종 위협에 실시간으로 대응할 수 없다.

[표 1] 기존 보안 체계의 한계점

EDR은 다양한 위협 경로 모니터링과 탐지 & 대응의 패턴화와 자동화를 통해 [표 1]에 서술된 기존 보안 체계의 한계로 인한 부정문을 긍정문으로 바꿔준다. 이를 통해 EDR의 가치와 필요성을 자연스럽게 알 수 있다. 기업 입장에서는 [표 1]의 내용을 자문해보고 근본적인 EDR의 필요성에 대해 가늠해 볼 수도 있다.

두 번째는 실생활에서의 비유로, EDR은 범죄 현장에 CCTV를 설치하는 것과 비슷하다. 서두에 소개한 코로나 19 역학조사와 유사한 개념으로, 모든 경로에서 이상 행위를 탐지하고 축적된 정보를 분석해 범인을 추적하는 실제 수사에 활용하는 것이다. 또한, 분석을 통해 도출한 인사이트를 바탕으로 잠재적인 위협에 대한 대응 전략을 수립해 사전에 예방할 수도 있다.

EDR은 엔드포인트에서 일어나는 다양한 행위들을 얼마나 신속하게 포괄적으로 탐지할 수 있는지가 중요하다. 탐지된 단말 이외에 피해가 전이되었는지 등 엔드포인트 영역에서 발생한 침해 행위를 추적할 수 있는 가시성

(Visibility)을 제공해야 한다. 또한 추가 피해가 발행하지 않도록 감염된 단말을 격리하거나 네트워크를 차단, 취약점을 찾아서 패치를 적용하는 등 대응이 가능해야 한다. 이 모든 행위의 목적은 위협의 잠복 기간과 피해를 최소화하는 것이다.

또한, EDR은 독자적으로 기능하는 것이 아닌 AV 등 기존 보안 솔루션과 연계했을 때 최상의 효과를 발휘한다. 현 시장에서는 EPP(Endpoint Protection Platform)와 EDR을 융합해 플랫폼으로 제공하는 추세이며, 이와 같은 형태로 위협 탐지, 대응, 차단 및 치료 역량을 유기적으로 지원하는 기업들이 강세를 보이고 있다.

안랩 역시 AhnLab EDR을 AhnLab EPP와 통합해 플랫폼 형태의 엔드포인트 보안 역량을 제공한다. AV 솔루션 'V3'를 비롯해 EPP를 구성하고 있는 여러 엔드포인트 보안 솔루션들과 연동해 사용자들이 '알려진 위협'부터 신종 악성코드나 제로데이 취약점을 악용한 '알려지지 않은 위협', 내재해 있으나 언제 발현될 지 예측할 수 없는 '보이지 않는 위협'까지 효과적으로 대응할 수 있도록 한다.

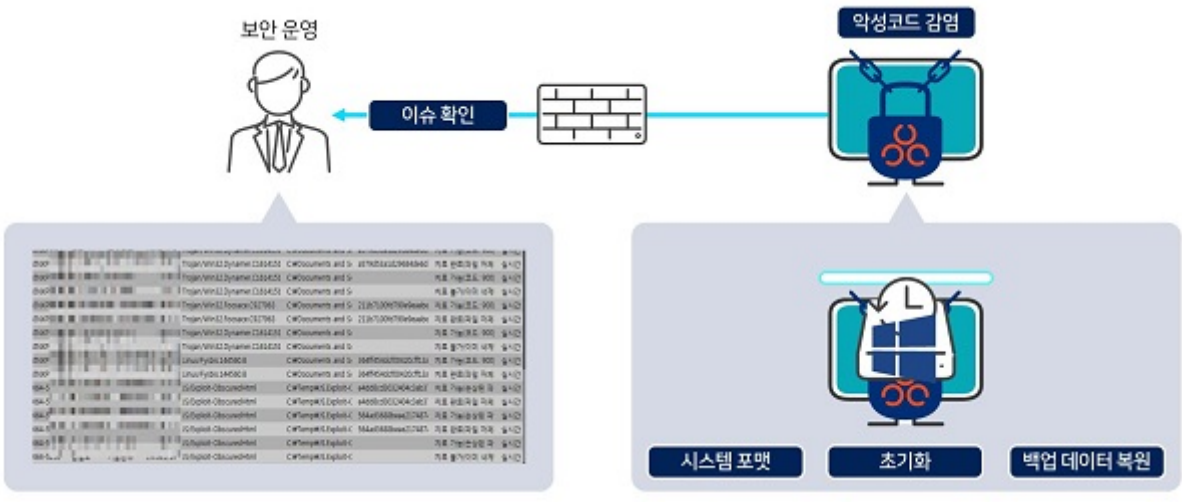
아울러, AhnLab EDR은 보다 효과적이고 선제적인 대응을 위해 필요에 따라 운영 중인 보안 솔루션들과 연계해 운영하는 것도 가능하다. AhnLab EPP 서버에서 수집되는 데이터와 AhnLab EDR 서버에서 단말의 이상 행위로 분석된 로그를 운영 중인 APT 솔루션과 함께 SIEM(Security Information & Event Management)에서 통합 관리한다. 위협 정보 통합 관리시스템에서는 EPP에서 활용 가능한 API를 통해 공지사항 보내기, 악성코드 검사, 파일 수집 & 삭제 등 다양한 명령을 전달한다. 이와 같은 통합 보안 시스템 구성을 통해 잠재적인 피해를 예방할 수 있다.

AhnLab EDR의 특장점과 주요 기능에 대한 자세한 내용은 웨비나 영상을 참고하면 된다.

EDR 도입 전 vs 도입 후

그렇다면, EDR을 도입하기 전과 후 조직의 위협 대응 프로세스는 어떻게 달라질까? EDR을 도입해 운영하고 있는 A사의 사례를 통해 그 차이를 살펴보자.

먼저, EDR 도입 전 A사는 사용자 PC에서 악성코드 감염 이력이 확인되면 관리자가 사용자의 불편함을 줄이기 위해 시스템 포맷 혹은 초기화를 진행하고 백업된 데이터가 있다면 복원해 업무를 재개했다. 이 과정에서, 백신 관리 서버에 사용자 PC 악성코드 감염 이력이 존재하지만 악성코드가 어디로부터 감염되어 어디로 전파되었는지 등은 확인할 수 없었다. 단지, 저장된 로그를 통해 감염 이력이 있는 것만 확인 가능했다.

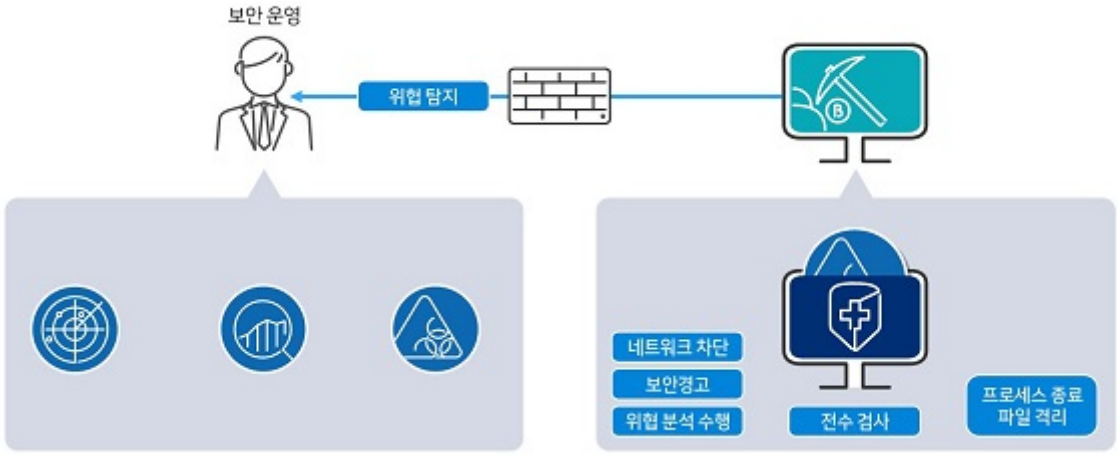


[그림 2] EDR 도입 전 위협 대응 프로세스

즉, 위협 분석을 통한 방지 대책 수립이 불가능했고, 사후 조치 이력만 관리가 가능했다. 뿐만 아니라 차단된 위협에 대해서도 차단된 맥락을 정확히 분석할 수 없어 지속가능한 보안 전략 수립 대신 상시적인 방어에 의존할 수 밖에 없었다.

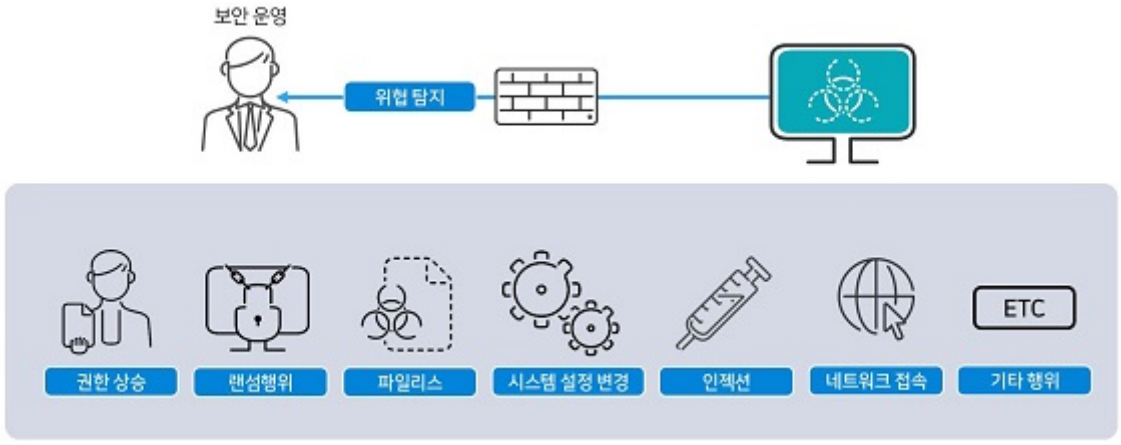
하지만 EDR을 도입한 이후에는 상황이 많이 달라졌다.

먼저 악성코드 감염 경보가 발생하면 EDR 시스템을 통해 위협을 분석하여 유입 경로, 유입 이후 생성된 파일, 파일의 네트워크 통신 이력 등 악성코드의 행위 이벤트를 모두 분석에 활용했다. 그리고 분석 정보를 활용해 취약점을 해결하고 사용자 PC의 보안성을 강화할 수 있었다.



[그림 3] EDR 도입 후 위협 대응 프로세스

또 기존 알려지지 않은 위협에 대해서도, 사용자 PC에서 이상 행위가 발생하면 EDR을 통해 관리자가 경고 알림을 수신했다. 이후 EDR은 사전 정의된 규칙을 바탕으로 위협을 분석하고 전체 사용자 대상 검사를 수행했으며, 악성으로 '의심'되는 파일에 대해서는 파일 수집 및 프로세스 종료를 진행했다. 또 필요할 경우, 악성코드의 네트워크 전파 방지를 위해 사용자 PC의 네트워크를 격리해 고립시키는 것도 가능해졌다.



[그림 4] EDR의 행위 탐지

파일 형태의 악성코드 이외에도, 앞서 주요 위협으로 소개한 파일리스 악성 행위, 의심되는 파일들의 권한 상승(Privilege Escalation) 행위, 문서나 사진 파일을 검색해 암호화를 시도하는 랜섬웨어 행위, 기존 시스템의 설정

을 임의로 변경하려 하는 시스템 설정 변경 행위 등 다양한 행위 탐지를 통한 분석과 대응을 단일 콘솔에서 수행할 수 있게 됐다.

결론: EDR 도입, 기성복이 아닌 맞춤 정장으로

지금까지 EDR의 필요성을 다양한 보안 개념과 도입 사례를 통해 살펴봤다. 위협의 고도화를 고려했을 때 EDR은 분명 필요한 솔루션이지만 도입 시 획일적인 자세로 접근하는 것은 지양해야 한다.

예컨데, 우리는 옷을 구매할 때에도 다양한 요소들을 고려한다. 옷이 필요한지부터 시작해 브랜드, 사이즈, 현재 보유하고 있는 아이템들과 어울리는지 등 여러가지를 생각해보고 종합하여 구매 결정을 내린다. 그 이유는? 나 자신과 맞지 않으면 효용 가치가 떨어지기 때문이다. 아무리 마음에 드는 디자인의 명품 브랜드 옷이라도, 내 사이즈가 M인데 XL을 산다면 그 옷은 어울리지 않고 가치가 낮아지게 된다.

EDR도 마찬가지다. EDR 도입을 고려하고 있다면 현 조직의 규모와 비즈니스 및 IT 현황, 도입 목적, 비용 등 여러가지 요소들을 명확히 해야 한다. 특히 EDR은 탐지 및 분석할 정보가 많은 본질적으로 '무거운' 솔루션이기 때문에 활용 방안도 면밀히 생각해봐야 한다. 만약 현실적인 한계로 명확한 답을 내릴 수 없다면 안랩과 같은 외부 전문 기업의 컨설팅을 받는 것도 좋은 방법이다.

점점 더 지켜야할 것이 많아지는 현재, 그리고 미래에 보다 많은 기업들이 EDR을 '지능적으로' 활용해 안전한 비즈니스 환경을 조성하길 바란다.

AhnLab 콘텐츠기획팀 신재만 대리
