SOMANSA

우리나라는 왜 아직까지 EDR 도입이 더딜까?

2020.08.14 소만사

세계최대의 정보보안전시회 RSAC, 블랙햇(Black Hat)에 참가한 보안솔루션 기업들이 전면적으로 내세운 제품은 EDR(Endpoint Detection and Response: 엔드포인트 위협탐지 및 대응)이었다.

2013 년 처음 언급된 보안기술은 어느덧 1 조 8 천억원 규모의 큰 시장을 만들어냈다. [1][2](글로벌 시장조사기관 '리서치앤마켓'에서는 EDR 시장이 2026 년까지 8 조 5 억원 규모로 성장할 것이라 예상하고 있다.[3]) 이제는 '차세대 엔드포인트 보안'이라는 수식어를 떼어내도 될 정도로 'EDR'은 정보보안의 상징적인 기술이 되었다.

해외 EDR 기업 '크라우드스트라이크'는 작년 시가총액 13 조원 공개 이후 단숨에 메이저 위치를 차지했다. 'VM 웨어'는 '카본블랙'을 인수했다. '엘라스틱서치'도 '엔드게임'을 인수하면서 EDR 시장에 진입했다. 가상화, 검색엔진 등 보안과 관련이 없는 글로벌 기업이 인수합병을 통해 EDR 시장에 진입했다는 것은 그만큼 EDR 시장 잠재성이 무궁무진하다는 의미일 것이다.

그러나 국내에서는 효과적으로 EDR 을 사용하고 있는 기업을 찾아보기 어렵다. 세가지 부정적인 인식이 있어, 도입을 망설이고 있기 때문이다.

첫번째, '엔드포인트 위협탐지 및 대응' 솔루션이라고 하지만 '전문가의 판단'이 최종적으로 필요한 솔루션이라는 인식이 있어서 일 것이다.

자동화 솔루션인 것처럼 포장하지만 사람이 개입하는 구조라고 생각하기 때문이다. EDR 솔루션이 엔드포인트 단에서 악성행위를 탐지하는 것은 맞다. 하지만 악성행위가 '맞다/아니다'로 알려주지 않고 강수확률처럼 100% 기준 퍼센테이지로 나타내기 때문에, EDR 에이전트가 보안담당자에게 "악성확률 60%의 행위를 탐지했습니다"라고 안내했을 경우 보안담당자는 곤란해진다. 결국 최종결정은 사람이 해야 한다. 책임은 결국 사람이 지게 된다.

---

[1] https://www.etnews.com/20190930000091 전자신문 EDR 보도자료

[2] https://blogs.gartner.com/avivah-litan/2017/03/15/morphing-edr-market-grows-to-1-5-billion-in-2020/ 가트너 EDR 시장 보고서

[3] https://www.researchandmarkets.com/reports/4704049/endpoint-detection-and-response-global-market , Endpoint Detection and Response - Global Market Outlook (2017-2026)

EDR 관제 인력을 자체 고용하는 것도 어려운 일이다. 검증되고 숙련된 위협탐지 전문가를 구하기란 '하늘의 별 따기'이다. 어렵게 한사람을 구하더라도 24 시간 보안관제가 필요한 상황에서는 한두사람으로 커버할 수 없다. 구축비용도 비싼데 인건비도 만만치 않게 든다. 수십억을 투입하여 구매할 때도 경영진 눈치가 보이는데, 구축 후에도 유지비가 꾸준히 발생하기 때문에 선뜻 도입하기 망설여진다.

두번째, 망분리에 대한 무조건적인 믿음이 EDR 의 도입을 막아서고 있다.

2010 년 기점으로, 해커들이 내부전산망으로 침입하여 피해가 발생하다보니 다수의 기업과 기관은 이에 대한 방어대책으로 '망분리'를 적용했다.
2012 년에는 전자금융감독규정 제 15 조, 정보통신망법 시행령 15 조(2020 년 8 월 5 일 기점으로 개인정보보호법 시행령으로 이관)에 이용자수 일평균 100 만명 이상이거나 매출액 100 억원 이상인 정보통신 서비스 제공자 대상으로 망분리 규정이 신설되었다. 의무사항인 것이다.

한 대의 PC 에서 내부망과 외부망을 분리해 외부보안 위협이 원칙적으로 들어올 수 없도록 구축했기 때문에 보안위협이 발생할 확률을 대부분 제거했다는 것이 망분리의 장점이다. 그래서 EDR 도입을 강력히 주장할 설득력이 떨어지게 된다.

세번째, 인건비는 인건비대로 들어가는 상황에서, 망분리가 잡지 못하는 잔존위험을 해결하려는 목적으로 수십억원 이상을 투입해 구축하는 것은 비효율적이라고 생각한다.

주요위협을 스스로 판단하여 알아서 차단하는 것도 아니고, 큰 위협을 탐지하는 것도 아닌데 비용은 수십억이 투입된다. 높은 비용이 투자되는 만큼 구축/안정화기간도 오래 소요되는 EDR 은 속칭 '가성비가 떨어진다'고 여기는 것이다.

해당 포스팅에서는 전산, 보안담당자가 EDR 에 관해 가지고 있는 세 가지 편견에 대해 해소해보고자 한다.

첫번째, EDR 은 'Detection' 중심 솔루션이기 때문에 사용자 개입이 반드시 필요하다.

X. 결론은 아니다.

과거에는 그랬다. 하지만 2018 년 'Mitre(마이터)'사의 'ATT&CK Matrix' (이후 마이터어택) 공개이후 Detection 에서 Response 로 중심축이 이전되었다. 마이터어택은 실제 관측에 기반하여 분석한 자료를 토대로 최신공격방법, 대응방법, 관련 솔루션을 망라한 '사이버 킬체인 보고서'이다. EDR 업체들이 해당 보고서를 활용, 반영하기 시작하면서 사람의 최종 결정이 없더라도 공격에 대한 예측과 '대응'이 용이해졌다. EDR 솔루션이 엔드포인트 단에서 혼자 탐지도 하고 해결방법도 찾고, 알아서 차단할 수 있게 된 것이다.

'마이터어택'을 기반으로 대응까지 자동화하는데 성공했기에 이제 보안담당자는 과거 EDR 을 사용할 때처럼 빈번하게 최종결정을 하지 않아도 된다. 대부분 자동화되어 EDR 에게 맡겨도 된다.

회사 PC 에 랜섬웨어 파일이 유입되었다면 EDR 이 알아서 차단할 것이다. 제로데이어택이 발생할 경우에는 백엔드에서 일어나는 행위를 기준으로 위협을 판단하고, EDR 서버에 전송하여 사내 모든 EDR 에이전트에 해당 위협을 업데이트, 적용시킬 것이다. 이후 해당 정보를 TI(Threat Intelligence, 위협 인텔리전스)에 공유하고, TI 는 EDR 을 도입한 다른 기업/기관의 EDR 서버에 동일한 내용을 배포하여 확산을 막아줄 것이다.

기계학습(Machine Learning: 머신러닝) 도 꾸준히 발전하고 있다. 시간이 흐를수록 탐지/대응능력은 더욱 정교해질 것이다.

기술발전과 사례가 늘어남에 따라, EDR 전문기업에서 관제, 분석 서비스를 제공하기 시작했다. 보안위협분석 전문가를 고용하기 위해 찾아 나서지 않아도 된다. 내부에서 직접 EDR 관련 업무를 수행하지 않아도 된다. 전문화된 서비스를 이용하면 되기에, 많은 유지관리 비용을 투입하지 않아도 충분히 활용할 수 있다.

두번째, 망분리 적용기관은 굳이 EDR 을 도입하지 않아도 된다.

X. 아니다.

망분리는 내부 정보자산을 보호하기 위해 외부망과 내부망을 분리시켜서 악성코드, 랜섬웨어, 바이러스, 웜 등 외부 위협요소의 유입을 아예 막아버리는 방식이다.

하지만 아래 4 가지 문제로 인하여 망분리는 점차 축소되거나 제한될 것이다.

일부직원들은 우회경로를 만들어 쥐구멍으로 몰래 외부 네트워크를 이용하기도 한다.
보안담당자가 모르는 곳에 허점이 생기고, 그 경로를 통해 보안사고가 발생한다면 아주 빠르게 내부망은 초토화될 것이다. 망분리에 대한 믿음이 있기에 그 이외에는 조치하지 않았을 것이 분명하니까. 상황을 깨닫게 되었을 때는 이미 해결할 수 없을 정도로 걷잡을 수 없이 커져버린 상태일 것이다.

외부 디바이스로 인해 감염될 경우 막을 방법이 없다. 대만 반도체기업 TSMC(타이지덴)는 생산설비 업데이트를 위해 바이러스 검사가 완료되지 않은 USB 를 연결했다가 생산설비가 바이러스에 감염됐다. 하루동안 생산라인 3 곳의 가동이 중단되었으며 이로 인해 손실액은 한화 2,800 억 정도일 것으로 추산했다. 생산설비에 망분리를 구축하여 네트워크와 멀리 떨어뜨려 놓아도 이렇게 외부요인에 의해 감염되고 손실을 일으킬 수 있다. 무균실에 떨어진 세균 하나는 방해요소가 없다는 걸 아는 순간 순식간에 세력을 확장한다.

시대의 흐름 역시 망분리에서 벗어나고 있다. 망분리는 내부에서만 적용된다. 코로나 19 의 영향으로 임직원의 안전을 위해 재택근무를 도입하고 활용한 곳이 늘어났다. 클라우드/모바일 컴퓨팅 비중이 증가했다. 견고하던 '안전한 내부망'의 개념이 점점 줄어들고 있는 것이 지금의 현실이다.

핀테크 스타트업계에서도 망분리에 대해 부정적인 입장이다. '전자금융'으로 성장한 핀테크 기업들은 망분를 **'외부 오픈소스코드를 반영하여 개발하는 연구소의 업무생산성을 저해하는 요인'**이라고 주장하고 있다.

모 CISO 는 "망분리 방식에서 협업을 통한 업무를 진행할 경우 업무생산성이 50% 이하로 떨어진다."고 이야기했다. 이어 "핀테크 기업 특성상 업데이트가 필요한 오픈소스 라이브러리 관리를 위해서는 인터넷 연결이 필수적이지만 망분리 규정을 따르면 반드시 차단해야 한다. 별도의 불필요한 작업이 수행되기에 작업속도는 현저히 떨어질 수밖에 없다. "라고 덧붙였다.

핀테크 기업은 기존 금융, 민간대기업과 다르게 적은 수의 인원으로 꾸려지기 때문에 사업규모도 작다. 그럼에도 불구하고 망분리, 망연계를 위해 몇 억을 투자해야 한다면 비효율적일 것이다. 과도한 규제 때문에 성장 가능성이 높은 사업을 경영자들이 외면하고 다른 산업으로 눈을 돌리게 된다면 국가적으로도 큰 손실일 것이다.

망분리는 시대의 흐름에 따라 점차 중요성이 줄어들게 될 것이다. 2010 년 초반, 그 때는 전산서비스의 안전을 위해 반드시 필요했던 규제였지만 10 년이 지난 지금은 다른 기술로도 충분히 보호할 수 있기 때문이다.

결국 엔드포인트(PC) 자체에서 보안을 강화하는 것은 거스를 수 없는 추세이다.

세번째, 구매하기에는 가격도 비싸고 가격대비 그렇게 효과적으로 사용할지 의문이다.

△. 어느정도는 동의한다.

당장 도입하기에는 구축비용이 부담스럽다. 구축과 안정화에 필요한 기간 역시 길다.
현재도 충분히 망분리를 통해 주요 보안위협을 막고 있는데, 자잘한 잔존위협을 보안하기 위해 수십억을 투자하는 것은 '가성비'가 떨어진다고 여길 수도 있다.

그렇다고 해서 도입을 안 할 수는 없다. EDR 이 보안 트렌드인 것은 모두가 인정하는 사실이기 때문이다.

이 경우에는 선택할 수 있는 방법이 두 가지가 있다.

1) 수십억을 투입하여 1 년 프로젝트로 기획하고 전면적으로 구축한다.
2) 기존 에이전트에 EDR 기능을 추가하면서 점진적으로 차츰차츰 적용, 고도화 한다.

2) 번의 경우 비용이 상대적으로 저렴하고 구축/안정화 시간이 짧다는 장점이 있다. 1 차로 적용을 해보고 향후 구축방향을 결정할 수도 있기 때문에 도입사 입장에서는 부담이 적다. 국내에는 기존 보안솔루션을 중심으로 EDR 기능을 개발, 적용한 솔루션이 많다. 소만사는 DLP 솔루션을 중심으로, 안랩은 안티바이러스 솔루션 중심으로, 지니언스는 NAC 을 중심으로 EDR 기능을 접목하여 개발, 고도화하고 있다.

미국에 CWT 라는 기업이 있다. B2B 전문 여행사인데 직원수만 1 만 8 천명이며, 연간매출은 1.8 조원 수준의 큰 기업이다. 이 회사가 7 월, 회사 PC 3 만대가 Ragnar Locker 랜섬웨어에 감염되어 해커에게 한화 약 53 억원 상당의 비트코인을 지불하고 해결했다. (관련기사

https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W)

재미있는 점은, 해커가 복호화 비용을 받은 후 CWT 에게 보안 관련 어드바이스를 해줬다는 것이다.

해커가 조언해준 보안사항은 다음과 같다.

1. 로컬 암호는 꺼라
2. 관리자 세션은 강제로 종료시켜라
3. 그룹정책에서 WDigest 값을 0 으로 설정해라. 값이 0 이면 메모리에 저장을 안한다.
4. 암호는 매달 바꿔라
5. 사용자에게 준 권한은 최소설정해라. 필요한 앱에서만 접근하도록 엄격하게 관리해라.
6. 대부분 Applocker 정도면 다 지킬 수 있다.
7. 필요한 어플리케이션만 허가해라.
8. 안티바이러스 믿지마라.
9. **EDR(Endpoint Detection& Respones) 설치하고 보안관리자들에게 사용하도록 알려라.**
10. 적어도 3 명의 관리자가 24 시간 일하는 것을 추천한다. 여유있으면 4 명의 관리자가 하루에 8 시간씩 3 교대하면 더 좋다.

9 번을 기억하면 된다.