체크리스트

확장된 탐지 및 대응 솔루션을 선택해야 할 때 가장 중요한 5가지 항목

필요한 비용이나 직원을 줄이면서도 위험 대비와 보안 관제를 개선하기 위해 보안 공급업체를 통합하려는 기업이 많습니다. 확장된 탐지 및 대응(XDR) 솔루션은 이런 목표를 달성하기에 좋은 옵션입니다. Gartner에 따르면, "XDR의 기본적 장점은 3가지가 있습니다.

- 보호, 탐지 및 대응 기능
- 전반적인 관제 보안 인력 생산성 향상
- 총소유비용(TCO)을 낮추어 효과적인 탐지 및 대응 기능 구성[1]"

그러나 아무 XDR 솔루션이나 선택해서는 안 됩니다. Gartner의 말을 빌리자면, "XDR 제품은 상당히 유망하지만, 공급업체를 옮기지 못하는 등의 위험도 안고 있습니다. XDR 시장은 불안정하고 각 공급업체와 제품마다 기능 차이가 크기 때문입니다."[2] 솔루션을 평가할 때는 다음과 같은 질문을 고려해야 합니다.

☑ XDR 솔루션에서 공격 벡터가 커버됩니까?

XDR 솔루션으로 커버되지 않는 공격 영역은 사이버 범죄자에게 악용되기만을 기다리는 구멍입니다. XDR 솔루션에서 기능을 제공하지 않는다면 포인트 제품을 통합하거나 독립적으로 운영해야 할 수도 있습니다. 엔드포인트(관리형 및 비관리형 최종 사용자 기기, 헤드리스 사물 인터넷[IoT], 산업용 사물 인터넷[IIoT]기기), 액세스(유무선), 자격 증명, 네트워크(홈, 지점, 기업), 클라우드(퍼블릭, 프라이빗, 서비스형 소프트웨어[SaaS]), 이메일, 웹 애플리케이션 기능을 제공하는지 평가하세요.

☑ XDR 솔루션에서 사이버 킬 체인이 커버됩니까?

Lockheed Martin의 사이버 킬 체인 모델(MITRE ATT&CK 프레임워크와 유사)에서는 정찰, 무기화, 전달, 익스플로잇, 설치, 명령 및 제어, 목표 실행의 7가지 단계를 설명합니다. 일반적으로 사이버 공격은 이 단계를 거쳐 목표를 수행합니다. 그 단계 중 하나만 끊어도 사이버 방어에 성공하기 때문에 사이버 보안으로 많은 단계를 차단할수록 공격을 멈출 기회도 늘어납니다.

☑ XDR 솔루션 구성 요소가 얼마나 효과적입니까?

표면적으로 기능을 갖춘다고 해서 보안이 보장되지는 않습니다. 보안 효과는 기술, 제품, 공급업체마다 큰 차이가 있습니다. 그래서 보안 효과를 정기적으로 평가하는 권위 있는 독립적 테스트 기관이 많이 있는 것입니다. 제품에서 알림과 원격 측정 데이터를 제공하고, XDR 솔루션의 대응이 권위 있는 독립적인 기관(예: AV Comparatives, SE Labs, Virus Bulletin, ICSA Labs)에 테스트를 받고 한 번이 아니라 정기적으로 보안 효과의 우수성이 검증되었는지 확인하십시오.

☑ 직원이 얼마나 편리하게 XDR 솔루션을 사용할 수 있습니까?

기업마다 보안 부서의 규모, 구조, 기술 수준이 다릅니다. 또한, 각 XDR 솔루션은 통합과 자동화 수준이 다릅니다. XDR 솔루션이 (기존 보안 정보 및 이벤트 관리[SIEM]처럼) 단순히 보안 정보의 상관관계만을 파악하는지, 상관관계, 탐지, 조사, 대응 기능을 완전히 자동화하는지 알아보세요.

☑ XDR 솔루션이 공급업체 하나로 제한됩니까, 개방되어 있습니까, 혼합되어 있습니까?

공급업체가 정해진 XDR 솔루션은 일반적으로 통합 기능은 우수하지만, 공급업체 포트폴리오에서 제품을 선택해야 합니다. 개방형 XDR 시스템은 효과적인 것 같지만, 데이터를 정규화하고 상관관계를 파악하는 데만 지속적인 엔지니어링 노력이 많이 필요한 경우가 많아서 시간이 지나면서 탐지와 조사 기능이 부족해집니다. 자동화하는 대신 공급업체 포트폴리오가 얼마나 제한되어도 괜찮은지 고려해보십시오.

보안 공급업체 통합을 통해 보호 효과와 효율을 높이려면 기업에 알맞은 XDR 솔루션을 선택하는 것이 중요합니다.

[1] Peter Firstbrook and Craig Lawson, "Innovation Insight for Extended Detection and Response," Gartner, 2020년 3월 19일.

[2] 상게서

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화**: 080-559-8989 **Email**: kr-callcenter@fortinet.com

830153-0-0-KO