elastic

Search. Observe. Protect.

EDR과 XDR 비교

두문자어로는 한 글자 차이밖에 나지 않지만, 엔드포인트 탐지 및 대응(Endpoint Detection & Response, EDR)과 확장 탐지 및 대응(Extended Detection & Response, XDR)은 사이버 보안 팀에 상당히 다른 결과를 제공합니다. 여기서는 팀이 이 두 가지 솔루션에서 기대할 수 있는 것을 세분화해보겠습니다.

EDR	XDR
• 엔드포인트에 대한 집중적인 보호	• 엔드포인트, 클라우드, 사용자, 네트워크 및 기타 벡터에 걸친 다양한 통합 세트를 통한 광범위한 탐지
• 머신 러닝을 사용하여 Malware 및 랜섬웨어 탐지 및 예방	• EDR 기능 + 활동을 상호 연관시키고 위협을 식별하기 위한 머신 러닝 기반 분석
• 최소한의 통합 기능을 갖춘 독립형 도구	• 다른 도구들 간에 하나로 합쳐진 통합 보안 플랫폼으로서 분석가를 위한 단일 기준점 역할을 함
• 고급 보안 성숙도가 필요하지 않음	• 고급 보안 성숙도/확립된 보안 팀이 필요함
• 엔드포인트에서의 공격 차단과 탐지 경보, 호스트 분리, 자동 대응 기능 제공	• EDR 기능 + 여러 위협 벡터, 환경 및 솔루션에 걸쳐 확장된 중앙 집중식 관리 및 실행 기능

EDR은 보안 팀의 기존 툴셋에 보다 쉽게 구현되지만, XDR은 조직의 전체 공격 표면에서 모니터링, 탐지 및 대응 능력을 향상시키는 데 훨씬 더 효과적입니다.

조직의 요구사항에 가장 적합한 솔루션이 어느 것인지 궁금하신가요? 둘 다 이용하면 안될까요? Elastic Security의 Limitless XDR을 사용하는 EDR은 SIEM 및 클라우드 보안과 함께 포괄적인 솔루션의 핵심 구성 요소입니다.
보다 자세한 내용은 elastic.co/kr/security에서 확인하세요

