Managed Detection and Response로 보안 태세 강화

IT 환경 전반의 지능형 공격 탐지, 조사 및 대응

Dell Managed Detection and Response

귀사가 선택한 업계를 선도하는 엄선된 XDR 보안 분석 플랫폼과 Dell Technologies의 보안 전문 지식 및 IT 환경에 대한 심도 깊은 지식 결합

비즈니스 보안 방식

IT 팀은 끊임없이 진화하며 늘어나는 보안 위협에 대응하는 데 어려움을 겪고 있습니다. 2022년에만 전 세계적으로 55억 건의 멀웨어 공격이 발생했는데, 이는 2021년보다 1억 건이 증가한 수치입니다.[1]

조직을 완전하게 보호하려면 환경 전반에서 신종 위협을 신속히 탐지하고 효과적으로 대응해야 합니다. 하지만 이렇게 하기란 쉽지 않습니다. 왜냐하면 한 가지 문제만 해결하는 제품과 툴 때문에 총체적으로 상황을 파악하기가 힘들고, 자격을 갖춘 보안 전문가를 찾고 유지하기도 힘들며, IT 팀은 이미 중대한 요구 사항과 일상 작업에 완전히 매몰되어 있기 때문입니다.

관리형 위협 탐지 및 대응

Dell Managed Detection and Response는 전체 IT 환경에서 위협을 모니터링하고 감지, 조사 및 대응하는 포괄적인 완전 관리형 24/7 연중무휴 서비스로, 50개 이상의 엔드포인트를 보유한 조직은 이를 통해 IT에 대한 부담을 줄이면서 보안 태세를 신속하고 대폭 개선할 수 있습니다.

본 서비스는 다음과 같은 두 가지 주요 기능을 활용합니다.

- 수년간의 경험을 바탕으로 전 세계 조직이 비즈니스를 보다 효과적으로 보호할 수 있도록 지원하는 Dell Technologies 보안 분석가의 전문 지식
- 여러 공격 벡터의 이벤트 및 텔레메트리에 대한 AI 지원 분석을 통합하는 기능으로 업계를 선도하는 XDR(Extended Detection and Response) 보안 분석 플랫폼

주요 이점:

- 전체 생태계에서의 통합 탐지 및 대응
- 지속적으로 업데이트되는 위협 데이터베이스로 최신 보호 상태 유지
- 가장 은밀한 위협 행위자 전술까지 탐지 가능
- 공격자의 전체 활동을 포괄적으로 파악
- 보안, 고급 인프라스트럭처, 클라우드 등에 대한 전문 지식을 갖춘 Dell Technologies 보안 전문가 팀
- 클라우드 네이티브 SaaS XDR 구현에 대한 전문가 지원
- 침해 발생 시 신속한 사이버 인시던트 대응
- 서비스 공급업체를 위한 최고 수준의 보안 규정을 지속적으로 준수

전체 서비스 솔루션

Dell Technologies 보안 분석가가 예측 가능한 단일 가격으로 초기 설정, 모니터링, 탐지, 문제 해결, 대응을 모두 지원합니다. 이들은 IT 팀과 긴밀하게 협력하면서 환경을 이해하고, 보안 태세 강화 방법을 조언하며, XDR 소프트웨어 에이전트를 엔드포인트에 배포하도록 지원합니다.

알림은 24/7 모니터링 및 검토됩니다. 조사가 필요한 알림인 경우 분석가는 적절한 대응 방법을 결정하고 수행합니다. 위협이 악의적이거나 조치가 필요한 경우 사용자에게 알리고 필요한 경우 단계별 지침을 제공합니다.

보안 인시던트가 발생하는 경우 Dell Technologies는 비즈니스 운영을 재개하는 프로세스를 시작하도록 지원합니다.

XDR 플랫폼 선택

보안과 기술 요구 및 선호도는 모두 다릅니다. 따라서 업계를 선도하는 세 가지 옵션이라는 유연한 선택지를 제공합니다. Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR, Microsoft Defender XDR 중에서 요건에 맞는 XDR 플랫폼을 선택할 수 있습니다.[2]

주요 기능

신뢰할 수 있는 지원

- 긴밀한 파트너십으로 환경을 이해하고 조사한 문제를 해결하고 보안 태세 강화 방법을 조언
- 귀사가 선택한 엄선된 XDR 플랫폼으로 여러 공격 벡터의 이벤트 및 텔레메트리에 대한 AI 지원 분석을 통합하여 24/7 모니터링 진행
- XDR 플랫폼 배포 및 구성에 대한 전문가 조언

위협 대응 및 보안 구성

- Dell SOC 팀은 XDR 기능을 활용하여 문제 해결을 자동화하거나 귀사와 협력하여 모니터링 시 발견한 위협 해결
- 복잡한 상황에서도 위협을 억제하기 위해 이해하기 쉬운 세부 지침 제공
- 분기당 최대 40시간의 서비스 관련 보안 구성 포함

24/7 탐지 및 조사

- 조직의 보안 환경에 맞게 조정되고 효율적인 일상 작업을 위해 자동화된 프로세스 및 알림
- 각 고객의 환경에 맞춰 보안 시스템을 회피하는 새로운 위협 또는 이미 알려졌지만 변형된 위협을 발견하는 사전 예방적인 위협 추적
- 덜 중요한 알림의 일일 요약으로 Dell SOC 팀은 중요한 알림에 집중 가능
- 조사, 알림 추세 분석, 보안 태세 지침을 제공하는 분기별 보고서

사이버 인시던트 대응 시작

- 연간 40시간의 원격 인시던트 대응 지원을 통해 조사 활동에 신속하게 착수
- 모든 규모의 조직이 심각한 보안 이벤트로부터 복구하도록 지원하는 공인 보안 전문가의 지침 제공

지금부터 Dell과 함께 환경 보호 시작

랜섬웨어 침해로 인한 평균 총 비용이 2022년보다 13% 증가한 513만 달러에 달하는 지금이 바로 Dell Managed Detection and Response가 귀사에 적합한지 자세히 알아볼 때입니다.[3]

지금 바로 영업 담당자에게 문의하십시오.

1. Statista, Annual number of malware attacks worldwide from 2015 to 2022
2. Microsoft Defender XDR을 사용하는 데 최소 500개의 엔드포인트 필요
3. IBM, Cost of a Data Breach Report 2023