DELL Technologies

백서

DELL MANAGED DETECTION AND RESPONSE

중간 규모 및 소규모 조직을 위한 완벽한 관리형 보안 솔루션.

핵심 요약

기업에 대한 사이버 공격이 증가세에 있습니다. 2021년 FBI Internet Complaint Center의 보고에 따르면 전년 대비 69% 증가했으며 총 42억 달러의 손실을 기록했습니다.[1] 대기업에 대한 공격이 1페이지 헤드라인을 장식하지만 실제로는 모든 규모의 기업이 취약한 상태입니다. 대기업의 광범위한 리소스가 부족한 소규모 기업은 특히 위험에 노출되어 있습니다.

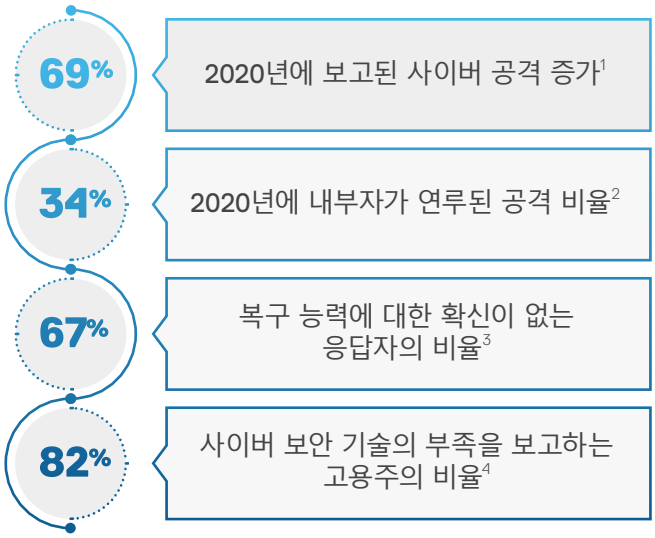
사이버 보안은 데이터 자산, 운영 및 비즈니스 연속성을 보호하는 데 매우 중요합니다. 대기업에는 최신 기술, 방법 및 인텔리전스를 갖춘 전담 보안 팀이 있는 경우가 많습니다. 그러나 중소 규모 기업에서는 점점 더 복잡해지는 보안 어플라이언스 및 소프트웨어 툴을 관리하고 운영해야 하는 보안 전문가를 불과 한두 명만 보유하는 경우도 있습니다.

증가하는 IT 당면 과제

엔드포인트, 서버, 애플리케이션, 네트워크 및 클라우드에 대한 공격이 다량 발생하면 보안 및 IT 팀을 빠르게 압도하는 엄청난 양의 알림이 생성됩니다. 이와 동시에 위협 행위자들은 기술을 계속 발전시키면서 과거의 효과적인 방어 수단을 재빠르게 회피하고 있습니다. 2020년대에 IT 환경을 철저히 보호하려면 전담 전문가의 24x7, 365일 모니터링 및 대응이 필요합니다.

중간 규모 및 소규모 기업의 IT 리더가 충분한 IT 인력과 예산을 사이버 보안에 할당하면 애플리케이션 개발 및 DevOps와 같은 중요한 영역에서 어려움을 겪게 됩니다. 오늘날의 위협 행위자로부터 기업을 보호하려면 많은 조직이 감당할 수 없는 규모의 인재, 툴 및 운영에 투자해야 하는 것이 사실입니다.

갈수록 심각해지는 사이버 공격의 위협



관리형 탐지 및 대응 솔루션으로 대응

결과적으로 더 많은 기업이 외부 서비스 공급업체의 MDR (Managed Detection and Response) 솔루션을 고려하고 있습니다. IT 의사 결정권자는 뛰어난 MDR 파트너를 어떻게 식별할까요?

실행 가능한 MDR 솔루션 공급업체는 알려진 위협 유형을 탐지하고, 거짓 양성을 최소화하며, 이벤트 상관 관계를 파악하고, 침입자의 활동 순서를 추적하며, 억제 및 예방 조치를 자동화하는 기술을 구현해야 합니다. 공급업체는 고도로 숙련되고 경험이 풍부한 보안 전문가로 구성된 팀이 알림을 분석하고 위협을 24x7x365 해결하며 새로운 위협 유형을 찾아야 합니다.

MDR 서비스를 제공하려면 보안 운영 구축과 프로세스 설정 및 개선이 필요합니다. 나아가, 분석가는 최신 위협과 기술을 최신 상태로 유지하기 위해 지식 공유 툴과 정기적인 교육이 필요합니다.

많은 서비스 공급업체가 관리형 탐지 및 대응 서비스를 제공하는 점을 광고하지만, 그 중 소수만이 탁월한 성능을 제공하는 데 필요한 용량과 기능을 보유하고 있습니다.

Dell Managed Detection and Response는 조직의 전체 IT 환경에서 위협을 모니터링, 감지, 조사 및 대응하는 포괄적인 완벽한 관리형 24x7 솔루션입니다. 엔터프라이즈를 구성하는 엔드포인트가 50개든 수천 개든 관계없이 Dell MDR은 IT 직원의 부담을 줄이면서 회사의 보안 태세를 빠르게 대폭 개선합니다. Dell MDR은 인력, 프로세스 및 툴에 투자하는 Dell의 역량을 활용하여 중간 규모 및 소규모 기업에 엔터프라이즈급 사이버 보안 모니터링 및 대응 기능을 제공합니다.

기업에서 MDR(Managed Detection and Response) 솔루션을 사용하는 주요 이유

- **찾기 힘든 사이버 보안 전문가 활용**
- **포괄적인 모니터링, 탐지 및 대응 범위**
- **IT 직원의 부담을 경감하여 DevOps에 집중하도록 지원**

오늘날의 위협 환경

현대의 위협 행위자는 체계적으로 몇 주 또는 몇 달을 투자해 귀중한 애플리케이션과 데이터에 대한 액세스 권한을 획득하는 방법을 숙고합니다. 기회를 식별하면 구멍을 악용하거나 피싱 이메일을 보내 사용자가 악의적인 첨부 파일을 열도록 유도할 수 있습니다. 탐지 및 대응은 직원 교육, 사이버 보안 평가, 취약성 및 침투 테스트, 회복탄력성 및 복구 계획 등과 함께 포괄적인 사이버 보안 프로그램의 필수 요소입니다.

행위자가 액세스 권한을 획득되면 처음에는 공격 범위를 넓힐 기반을 설정하려고 합니다. 또한 회사의 인프라스트럭처 내에서 자신의 입지를 공고히 하는 데 시간을 들입니다. 예를 들어 랜섬웨어 공격은 비즈니스 시스템을 공격할 뿐만 아니라 회사의 백업 시스템을 오프라인으로 전환하고 백업에 대한 액세스를 차단하는 것을 목표로 하는 경우가 많습니다. 이에 따라 회사의 복구 능력이 사라지면 랜섬 비용을 지불하는 것만이 비즈니스를 정상화할 수 있는 유일한 선택지가 됩니다.

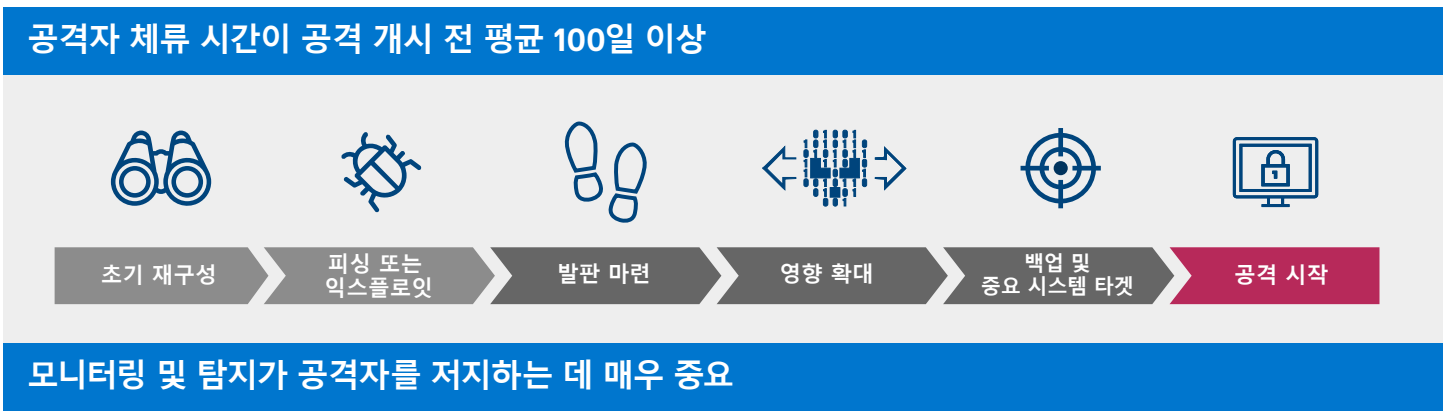
정교하고 지속적으로 업데이트되는 탐지 및 대응 기능은 공격 및 기타 단서를 인식하는 데 매우 중요합니다. 조기 경고는 조직에 공격이 더 확산되기 전에 피해를 줄일 수 있는 기회를 제공합니다.

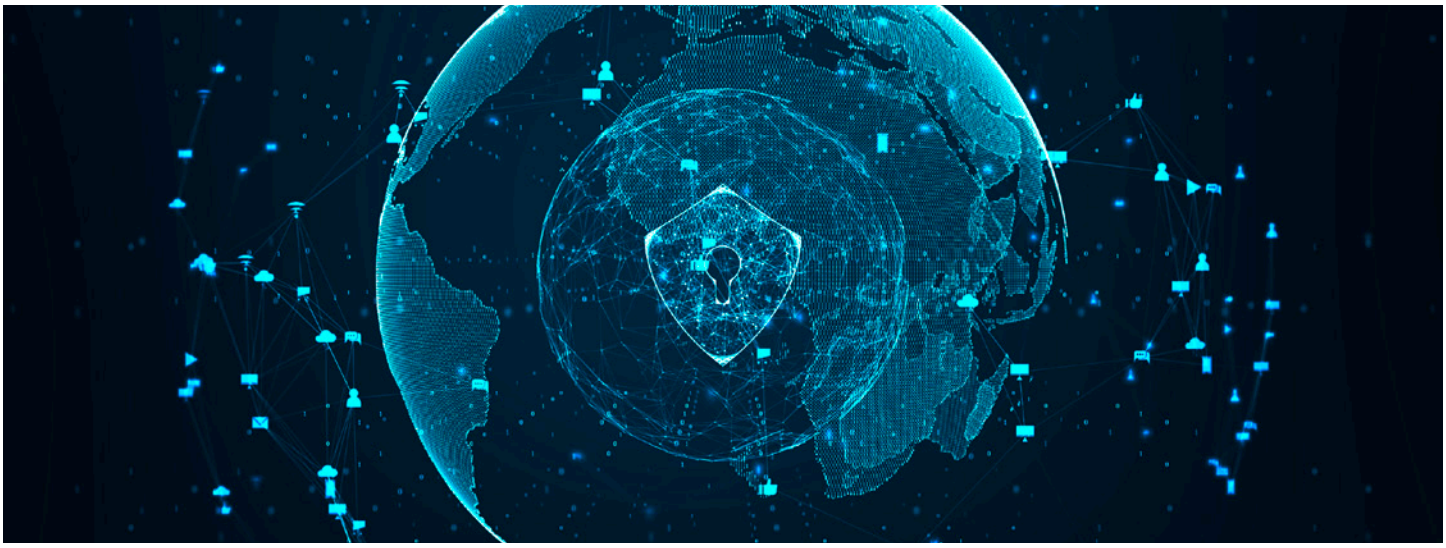
조직은 암호 감사, 네트워크 테스트, 취약성 검사, 암호화, 모니터링 및 위협 탐지와 같은 광범위한 사이버 보안 툴을 구축했습니다. 이러한 모든 툴에서 IT에 알림이 발생하여 알림의 볼륨 자체가 문제가 되고 툴 전반에서 이벤트의 상호 관계를 파악하는 것이 어렵다는 점을 감안하면 문제는 더욱 커집니다. 또한 IT 보안 담당자는 이러한 모든 기술에 대한 숙련도를 유지하기 위해 상당한 시간을 할애해야 할 과제를 안게 됩니다.

MDR의 인적 측면에는 시스템 관리, 사이버 포렌식, 위협 조사 및 침투 테스트와 같은 다년간의 사이버 보안 경험과 기술을 갖춘 전문가 그룹이 필요합니다. 이러한 전문가들은 찾기 어렵고, 고용 비용이 높으며, 더 유명하고 지출 규모가 큰 조직에 지속적으로 채용되고 있습니다. 2021년 CIO 설문조사 결과 사이버 보안 직책이 모든 IT 직책 중에서 충원하기가 가장 어려운 것으로 확인되었습니다.[5] 보안 분석가를 유지하고 퇴사하는 인원을 다시 충당하는 것은 IT 리더가 마주하는 끝없는 싸움입니다.

필수 툴과 인재를 확보한 후에도 기업은 24x7 보안 운영 및 시설을 구축해야 합니다.

그림 1. 위협 행위자 전략





Dell Managed Detection and Response 서비스를 통해 최고 수준의 기능 활용

중간 규모 기업 및 소규모 기업이 스스로를 적절하게 방어하는 데 어려움을 겪는 경우가 많다는 것은 놀라운 일이 아닙니다. 사이버 보안 환경은 변화무쌍한 위협의 요지경으로 변모되었습니다. 활동이 쇄도하여 인력 요건이 확대되고 공격의 복잡성으로 인해 필요한 인재의 수준도 높아졌습니다.

Dell Managed Detection and Response는 규모가 가장 큰 기업에 맞먹는 사이버 보안 전문가, 툴 및 운영 역량으로 보안 팀을 확장합니다. Dell MDR은 IT 팀의 부담을 줄이고, 위험을 완화하며, 회사의 보안 태세를 크게 개선하여 비즈니스 우선 순위에 집중할 수 있도록 합니다.

Dell Managed Detection and Response는 기술, 전문 지식 및 운영이 완벽하게 통합된 조합입니다. 이 서비스는 수년간 전 세계 기업들이 운영을 더 잘 보호할 수 있도록 지원해 온 Dell Technologies 보안 분석가의 지식을 활용합니다. Dell MDR은 20년 이상 검증된 노하우, 실제 위협 인텔리전스 및 연구, 정교한 위협 탐지 및 대응에 대한 전문 지식의 산물로서 고급 보안 분석 소프트웨어 플랫폼인 Secureworks® Taegis™ XDR의 성능을 활용합니다.

Secureworks Taegis XDR

Secureworks Taegis XDR은 보안 우려 사항에 대해 규모가 큰 데이터 스케일 솔루션을 제공하는 특별히 설계된 사이버 보안 플랫폼입니다. 클라우드 네이티브 플랫폼인 Taegis XDR은 완전한 위협 정보로 강화된 다양한 공격 벡터의 텔레메트리 및 이벤트에 대한 지속적인 머신 러닝 및 딥 러닝 기반 평가를 포함합니다.

Dell Managed Detection and Response를 선택해야 하는 이유

인력

- **경험이 많은 사이버 보안 전문가**
- **Taegis XDR 인증 분석가**
- **CEH, GIAC SANS, CISSP 및 CompTIA도 포함하는 인증**

기술

- **업계를 선도하는 Secureworks Taegis XDR 보안 분석 플랫폼**
- **광범위한 엔드포인트, 네트워크 및 클라우드의 텔레메트리를 활용하는 지속적이고 포괄적인 위협 모니터링**

프로세스

- **문제 해결 시간 단축**
- **24x7/365 지원**
- **에이전트 롤아웃 지원 포함**
- **분기당 40시간의 원격 문제 해결 지침**
- **연간 40시간의 인시던트 대응 시작**

신뢰할 수 있는 파트너

- **디바이스 및 인프라스트럭처 지원에 대한 전 세계적 신뢰**
- **20년 이상의 비즈니스 회복탄력성 혁신**
- **인력, 프로세스, 툴에 지속적으로 투자**

그림 2. Threat Intelligence

정교한 공격을 식별하고 대응할 수 있는 유일한 방법은 먼저 악의적인 행위자가 어떻게 기능하고 어떤 동기를 갖는지 이해하는 것입니다. 매년 XDR을 뒷받침하는 Secureworks 팀은 약 1,000건의 인시던트 대응 계약을 수행합니다. 그에 따라 클라이언트 비즈니스에 효과적으로 침투하는 위협 행위자 전략, 기술 및 프로세스가 정기적으로 어떻게 변화하는지 확인하는 데 뚜렷한 이점을 갖습니다.

Taegis XDR은 엔드포인트, 네트워크, 클라우드 시스템 및 온프레미스 비즈니스 시스템에서 수집된 보안 관련 데이터를 분석하여 위협을 탐지합니다. XDR은 기존 보안 인프라스트럭처를 보완하여 포괄적인 적용 범위를 보장하고 이전 투자를 보호하는 완전한 개방형 플랫폼입니다.

XDR은 자동화된 대응, 문제 해결 및 통찰력을 제공하여 보안 운영의 효율성을 높이고 대응 팀이 위협에 직면했을 때 조치를 취하는 데 필요한 가시성을 제공합니다. Dell MDR 고객은 고객 및 공유 인텔리전스 서비스에 걸쳐 컴파일된 수십만 개의 데이터 포인트를 사용하여 개발된 위협 인텔리전스의 이점을 누릴 수 있습니다.

최고 수준의 보안 전문가 활용

고도로 숙련된 보안 분석가로 구성된 글로벌 팀은 항상 시스템 내의 문제를 경계하고 있습니다. Dell의 숙련된 사이버 보안 전문가는 위협 조사, 위협 추적, 엔드포인트 보안, 인시던트 대응 및 복구를 비롯한 모든 단계의 위협 탐지 및 완화에 대한 경험을 보유하고 있습니다. Dell 분석가는 XDR 인증을 획득했으며 CEH, GIAC SANS, CISSP 및 CompTIA를 포함하는 다양한 정부 및 업계에서 인정받는 기타 인증을 보유하고 있습니다. Dell MDR의 분산된 'FTS(Follow-the-sun)' 보안 운영 센터는 연간 24x7/365일 운영됩니다.

Dell MDR 팀은 회사의 운영 및 IT 인프라스트럭처를 파악합니다. XDR을 통해 제공되는 수천 개 IT 환경의 선별된 위협 정보와 머신 러닝을 사용하여 환경을 모니터링합니다. Dell MDR 팀은 경고가 나타나면 즉시 행동에 돌입하여 알림 데이터 조사를 통해 숙련되고 경험이 많은 보안 분석가만이 인식할 수 있는 연결 및 패턴을 발견합니다. 그 후 조직의 대응 팀원에게 최선의 조치에 대해 조언합니다.

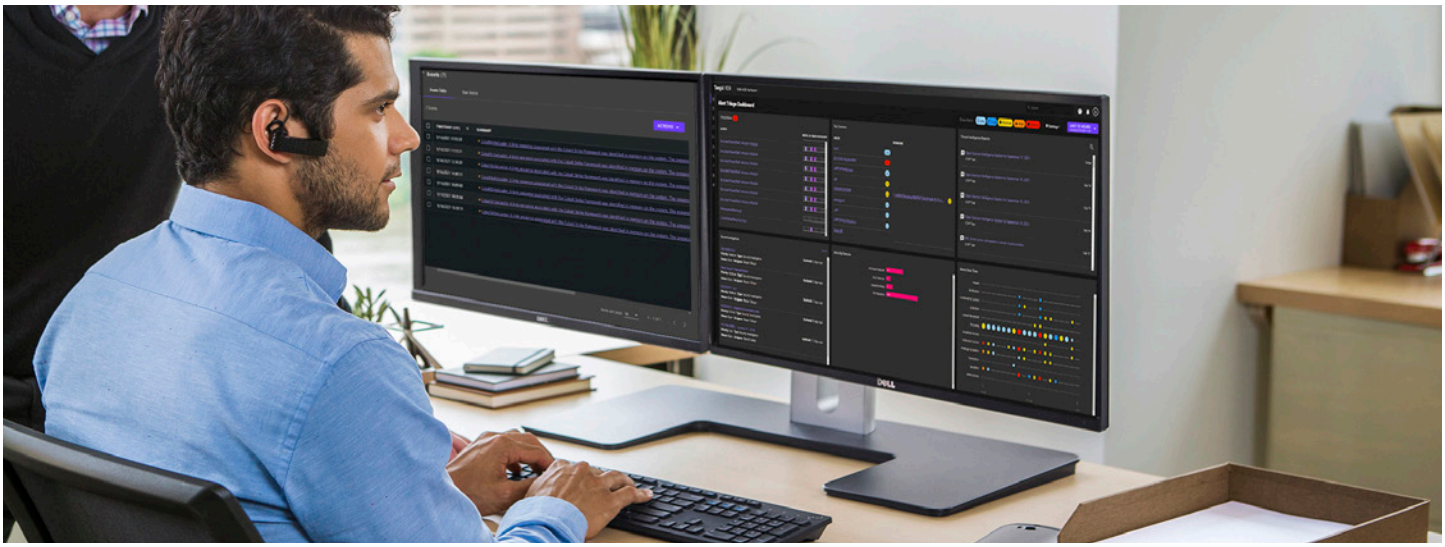
Dell MDR은 세계적 수준의 IT 서비스 조직을 개발하기 위해 Dell이 다년간 기울인 노력의 일환입니다. 즉, Dell MDR 사이버 보안 전문가는 위협을 해결하는 데 탁월한 지침을 제공할 뿐만 아니라 어떤 조직을 위해서도 이를 관리할 수 있는 기술과 노하우도 보유합니다.

위협 추적 - 자동화된 시스템을 회피할 수 있는 위협 식별

위협 행위자는 자동화된 탐지 시스템을 알고 있으므로 이러한 시스템을 우회하기 위해 새로운 공격 유형 또는 기존 공격 유형의 변형을 개발하고자 노력합니다. Taegis XDR과 같은 시스템에서는 쉽지 않지만 불가능하지 않습니다.

보안 분석가는 위협 추적을 사용하여 이러한 '은밀한' 위협을 식별합니다. 위협 추적은 계정 로그인에 계속 여러 번 실패한 후 로그인에 성공하는 경우 또는 일반적인 업무 시간 외와 같은 비정상적인 로그인 시도 또는 짧은 시간 내에 파일에 대한 반복적인 변경과 같은 손상 지표를 찾습니다.

효과적인 위협 추적은 기술과 인력의 산물입니다. Taegis XDR 플랫폼은 침입자의 활동에 대한 엄청난 양의 세부 정보를 제공합니다. Dell MDR 분석가는 이 세부 정보를 조사하여 철저히 숨겨진 활동도 파악합니다.



DELL MDR 알아보기

뉴스 미디어는 사이버 보안 위협을 억제하려는 정부 및 글로벌 기업의 어려움에 대해 보도했습니다. 중소 규모 기업은 더 이상 해당 당면 과제에 단독으로 직면하지 않아도 됩니다. Dell MDR을 사용하면 귀사를 보호하는 데 전념하는 고도로 숙련된 보안 전문가와 업계를 선도하는 보안 플랫폼인 Secureworks Taegis XDR을 활용할 수 있습니다. 조직에서는 인력, 프로세스 및 툴에 투자하는 Dell의 역량을 활용하여 조직의 요구 사항에 맞게 구성된 관리형 보안 서비스를 구축할 수 있습니다. Dell Managed Detection and Response 서비스는 모든 고객이 액세스할 수 있는 세계적 수준의 사이버 보안 서비스입니다.

Dell MDR에 대해
자세히 보기

MDR 전문가에게
문의

1. FBI 공격 69% 증가: https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html
2. 34% 내부자: https://www.verizon.com/business/resources/reports/dbir/
3. 파괴적인 사이버 공격 후 복구 능력에 대한 확신이 없는 67%: www.delltechnologies.com/gdpi
4. 사이버 보안 기술의 부족을 보고하는 고용주의 82%: https://www.csis.org/analysis/cybersecurity-workforce-gap
5. 충원하기 가장 어려운 13개 IT 직무. https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html

DELL Technologies