ESG 쇼케이스

MDR이 모던 사이버 보안 전략의 핵심 요소가 된 이유

날짜: 2022년 8월 **작성자:** Dave Gruber, ESG Principal Analyst

요약: 사이버 보안 프로그램에서 탐지 및 대응 기능의 중요성에 대해 누구도 이의를 제기하지 않습니다. 중요한 문제는 대부분의 조직이 적응하기 어려울 정도로 빠르게 위협이 증가하고 복잡성이 변모할 때, 시기적절하며 정확하고 신뢰할 수 있으며 일관된 탐지 및 대응을 보장하는 최상의 방법을 찾는 일입니다. 타사 매니지드 서비스로서 MDR(Managed Detection and Response)은 조직이 보조를 맞출 수 있는 접근 방식입니다.

소개: MDR의 등장

모든 조직은 엄연한 현실에 직면해 있습니다. 사이버 보안 위협이 급속히 증가하고, 공격 지점이 확대되고 있으며, 위협을 탐지하고 대응하기 위한 기존의 프로세스와 툴은 더 이상 충분하지 않습니다. 위협 그 자체와 이러한 위협을 가하는 악의적 행위자는 모두 더 능숙하고 민첩하며 끈질기므로 기업 자산을 보호하는 임무를 맡은 보안 및 IT 전문가는 디지털 표적을 잡아내기 어려워졌습니다.

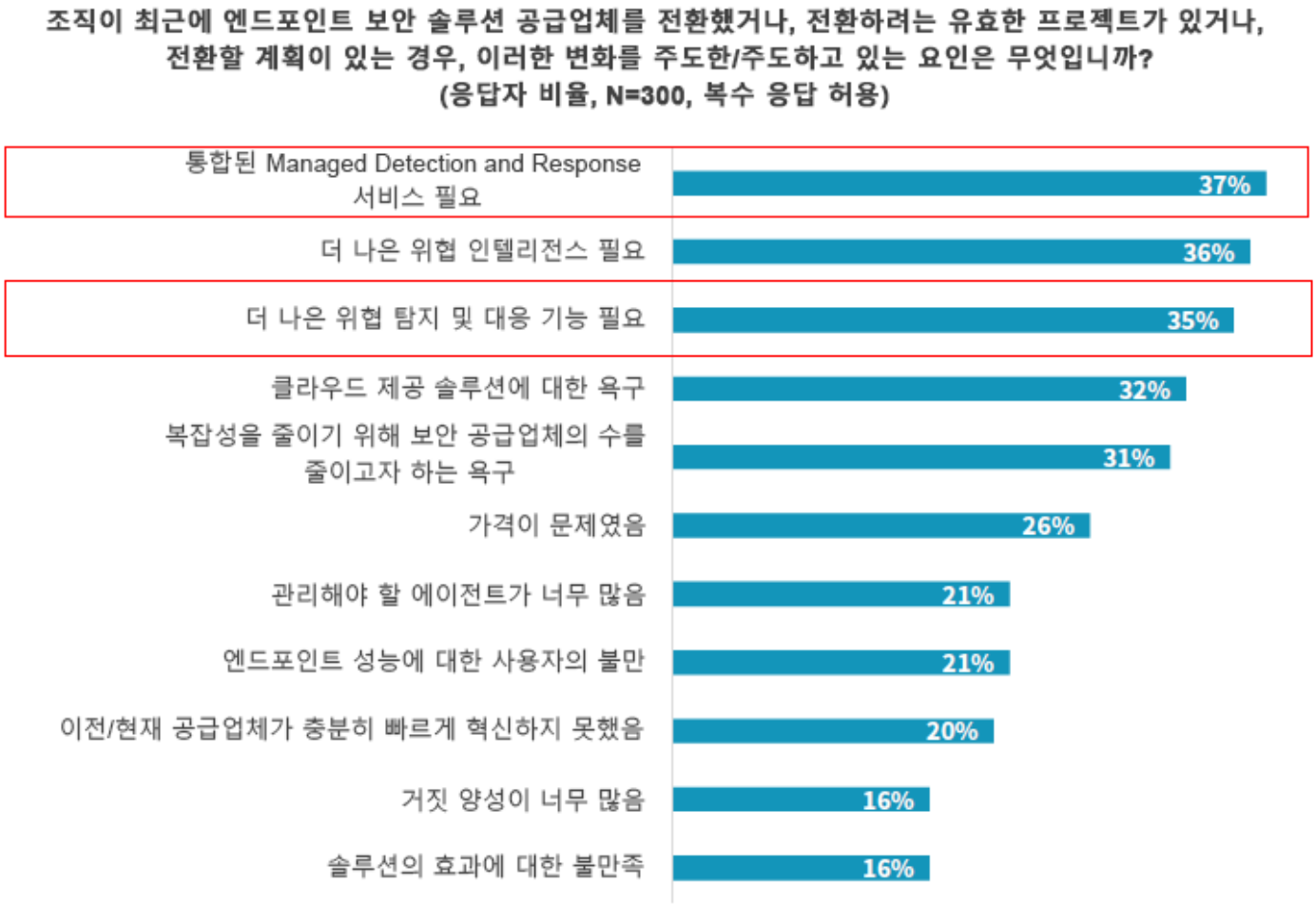
수많은 보안 제어는 보안 팀이 거짓 양성으로부터 유효한 위협을 가려내고자 끊임없이 쏟아져 들어오는 알림을 수동으로 분류해야 하기 때문에 탐지 및 대응 작업의 비용과 복잡성을 가중시킵니다. 더 큰 규모로 SOC(Security Operations Center)를 구축하고 여기에 더 많은 툴과 더 많은 보안 엔지니어를 채우려면 비용이 많이 듭니다. 또한 이 방법은 또한 점점 커지는 막대한 사이버 보안 기술 격차에 직면하여 조직에서 보안 전문가를 충분히 식별하고 고용할 수 있다는 전제에서 가능합니다.

사이버 보안 프로그램이 재설계됨에 따라 조직은 도움을 받기 위해 Managed Detection and Response 공급업체에 더 빈번하게 의존하고 있습니다.

사이버 보안 프로그램이 재설계됨에 따라 조직은 프로세스를 개선하고 리소스 및 기술 격차를 해소하며 보안 운영 툴을 현대화하기 위해 Managed Detection and Response 공급업체에 더 빈번하게 의존하고 있습니다. ESG 연구에서 통합 MDR 서비스의 필요성이 조직이 엔드포인트 보안 솔루션 공급업체를 변경하도록 유도하는 주요 요인으로 밝혀졌듯이 많은 이들이 MDR을 엔드포인트 보안과 연관짓습니다.(그림 1 참조).[1]

[1] 출처: ESG Complete Survey Results, *Endpoint Security Trends*, 2021년 12월. 이 쇼케이스의 모든 ESG 연구 참고 자료 및 차트는 이 설문조사 결과에서 가져왔습니다.

그림 1. 엔드포인트 보안 공급업체 변경을 유도하는 동인



출처: ESG, TechTarget, Inc. 사업부

그러나 보안 팀이 탐지 및 대응 프로그램을 확장하여 보다 종합적인 XDR(Extended Detection and Response) 솔루션으로 업그레이드함에 따라 MDR 오퍼링은 조직에서 보다 포괄적인 공격 지점 적용 범위와 지능형 공격 탐지를 제공할 수 있는 기술 및 운영 모델을 모두 업데이트하는 경로를 조직에 제공하고 있습니다. 연중무휴 모니터링, 실시간 글로벌 위협 인텔리전스, 자동화 및 고급 머신 러닝 분석이 결합된 새로운 접근 방식이 필요합니다. 모두 신속한 탐지 및 위협 추적을 지원하는 방대한 양의 보안 텔레메트리를 다룰 수 있습니다. XDR은 계속해서 진화하고 성숙해지며, MDR 서비스를 통해 모든 조직은 규모와 보안 성숙도 수준을 불문하고 탐지 및 대응을 운영할 수 있으므로 지능형 공격을 완화할 수 있습니다. 이는 조직이 데이터 센터에서 엣지, 클라우드에 이르는 사이버 보안 경계의 범위와 규모를 재정립함에 따라 특히 중요합니다. MDR은 분산 엔터프라이즈 전반에서 위협 탐지 및 대응 활용 사례를 확장하는 데 필요한 인력, 프로세스 및 기술을 하나로 통합합니다.

MDR 도입의 주요 동인

MDR 서비스의 사용이 증가함에 따라 서비스 범위를 확장하고 인력 격차를 해소하며 전반적인 프로그램 목표를 강화할 수 있는 방법을 보안 팀에 제공하고 있습니다. 활용 사례는 다양하지만 기본적인 동인은 다음과 같습니다.

- **위협 환경:** 사이버 공격 수가 증가하고 이러한 공격이 갈수록 정교해짐에 따라 조직이 더 빠르고 확실하게 탐지하고 대응해야 하는 부담이 커졌습니다.
- **적대적 의도:** 공격자는 공격을 계획하고 이행하는 방식에서 더욱 스마트하고 끈질기며 특히 전략적으로 변모했습니다. 악의적인 행위자가 전술을 공유하고 심지어 공격에 있어 협력하는 강력한 "범죄 생태계"가 나타났습니다.
- **경제적 문제:** SOC를 구축하고 확장하기 위한 CapEx의 노력은 대개 백만대 지출이며 때로는 더 많은 비용이 소요됩니다.
- **사이버 보안 기술 교체:** 사내 보안 운영 활동을 전부 또는 대부분 수행하는 조직을 위해 사이버 보안 제어 스택을 보다 빈번하게 새로 고쳐야 합니다. 여기에는 1세대 엔드포인트 탐지 및 대응에서 보다 포괄적인 XDR/MDR 프레임워크로의 전환이 포함됩니다.
- **기술 부족:** 많이 논의되는 사이버 보안 기술 격차는 계속 반복되는 문제입니다. 사내 사이버 보안 직위에 제대로 된 인력을 충원하지 못하면 대부분 탐지 및 대응 목표에 차질이 생기고 자산이 위험해집니다.

사이버 공격은 무차별적으로 발생합니다. 인력, 예산이 제한되고 이전에 모든 유형의 공격에 노출된 적 있는 소규모 및 중간 규모 조직은 위험에 처해 있습니다. 대규모 조직이라도 진화하는 위협 환경을 탐지하고 대응하기 위한 추가 인력, 확장 가능한 제어 및 경영진 수준 컨설팅이 필요합니다.

MDR 서비스 및 MDR 서비스 공급업체에서 모색해야 할 사항

MDR 서비스를 평가하는 조직에는 다음과 같은 몇 가지 중요하고 까다로운 요구 사항이 있습니다.

- **컨텍스트 기반 위협 인텔리전스:** 위협을 식별하거나 거짓 양성을 해소하기 위해 여러 지표의 상관 관계를 포함한 실시간 위협 인텔리전스 및 탐지를 지원합니다.
- **사전 예방적 활용 사례:** 알려진 위협에 대한 능동적인 추적을 지원합니다.

- **풍부한 텔레메트리:** 새로운 위협을 식별하는 데 특히 중요한 심층적인 포렌식 조사와 정교한 분석을 수행합니다.
- **문제 해결:** 상황에 맞는 AI 기반 문제 해결 지침을 제공합니다.
- **위험 완화:** 취약성 평가 및 관리를 제공합니다.

MDR 서비스 공급업체를 선택하는 경우 조직은 다음과 같은 구체적이고 입증된 기능을 제공할 수 있는 파트너를 찾아야 합니다.

- **24/7 적용 범위:** 24/7 연중무휴 지속적인 모니터링을 제공합니다.
- **예측 시나리오** 계획 및 컨설팅
- 서비스 공급업체의 **인간 전문 지식** 및 경험
- 최고 경영진 및 이사회 구성원을 위한 **지침**.
- 거버넌스, 규정 준수 및 비즈니스 연속성 **보장 능력**.

또한 조직은 잠재적인 MDR 파트너에게 서비스 수준 목표에 대해 질문해야 합니다. 이러한 기능에는 알림에서 조사 개시에 이르기까지 대응하는 평균 시간, 조사 개시에서 인시던트 분석이 조직에 제공되는 시점까지 평균 응답 시간, 조사 개시에서 완전한 해결이 수행된 시점까지 평균 해결 시간이 포함됩니다.

MDR에 대한 Dell Technologies 접근 방식

MDR 서비스 공급업체를 식별하고, 평가하고 파트너십을 구축하기 위해 조직은 위협을 탐지하고 대응하는 데 필요한 현재의 요구 사항뿐만 아니라 향후에 이러한 요구 사항이 어떻게 진화하고 확장될 가능성이 있는지에 대해서도 집중해야 합니다. 어떤 조직도 사이버 보안 위협의 미래를 예측하는 마법의 수정 구슬은 없지만, 조직은 혁신적인 기술, 검증된 프로세스 및 인력의 입증된 전문 지식을 바탕으로 시간이 지남에 따라 서비스를 확장할 수 있는 검증된 능력을 갖춘 MDR 파트너를 찾아야 합니다.

Managed Detection and Response에 대한 Dell Technologies의 접근 방식은 유연하고 지능적이며 확장 가능한 기술과 숙련된 사이버 보안 전문가의 역량을 결합합니다. 구독 기반 서비스는 필요한 경우 비용 예측 가능성과 더 높은 수준의 서비스로의 원활한 전환을 제공하도록 설계되었습니다.

Dell Managed Detection and Response를 위한 기술 플랫폼은 Dell 사업부인 Secureworks에서 개발한 완벽하게 관리되는 클라우드 네이티브 서비스인 Taegis XDR입니다. Taegis XDR은 분산되고 다각화된 공격

영역 전반에서 완벽하게 확인된 위협을 탐지, 분석하고 조치를 취하여 대규모 글로벌 기업에서 비교적 소규모 기업에 이르기까지 조직을 보호합니다.

Taegis XDR은 Dell의 대규모 보안 분석가 및 엔지니어 그룹의 기술을 통해 극대화됩니다. 이 그룹의 집단 지성은 알려진 위협과 지금까지 알려지지 않은 위협으로부터 조직을 보호하는 데 도움이 되는 수십 년에 걸쳐 축적된 전문 지식에 바탕을 두고 있습니다. 이 조합은 대부분 지속적으로 업데이트되는 위협 인텔리전스 데이터베이스를 통해 전체 IT 아키텍처에서 탐지 및 대응을 효율적으로 통합할 수 있는 방법을 제공합니다. 또한 Dell Managed Detection and Response는 악의적인 행동을 모니터링, 분석 및 식별하여 탐지 및 대응에 소요되는 평균 시간을 단축합니다.

Dell Managed Detection and Response는 또한 악의적인 행동을 모니터링, 분석 및 식별하여 탐지 및 대응에 소요되는 평균 시간을 단축합니다.

마지막으로, Dell Managed Detection and Response는 매니지드 서비스이므로 이미 업무가 과다한 사내 IT 및 보안 운영 팀을 위해 보안 전문가를 찾고 충원해야 하는 조직의 필요성을 크게 줄여줍니다. Dell Managed Detection and Response는 비용 효율적이면서도 전략적인 방식으로 조직의 역량을 보완하고 확장하도록 설계되었습니다.

더 중요한 사실

조직이 위협 탐지 및 대응 프로그램을 현대화함에 따라 빠르게 증가하는 공격 지점, 반복적인 랜섬웨어 공격 및 일반적으로 더 복잡한 위협 환경은 XDR 및 MDR에 대한 투자와 추진력을 높이는 요인이 되고 있습니다. 개별 보안 전략은 다양하지만, 공격 지점을 보다 폭넓게 파악해야 할 필요성과 이를 보호하는 개별 보안 제어에서 방대한 양의 보안 데이터를 집계, 상관 관계 파악 및 분석할 수 있는 능력이 제어 확보에서 중요한 단계입니다.

Managed Detection and Response 서비스는 보안 팀이 MDR 공급업체를 활용하여 기술, 프로세스 및 보안 기술을 강화하므로 효과적이고 쉽게 사용할 수 있습니다. ESG 연구에 따르면 XDR에 투자하는 조직은 이러한 솔루션을 구현하고 운영하는 데 도움이 되는 동반 MDR 서비스를 원합니다. 즉, 보안 솔루션과 서비스를 모두 제공하는 데 있어 검증된 실적을 보유한 솔루션 공급업체와 협력해야 합니다. 시간이 지남에 따라 적용되어 IT 및 보안 팀이 보안 프로그램을 개발하고 확장하는 데 도움이 될 수 있습니다.

ESG는 조직이 이러한 목표를 달성할 수 있도록 인력, 프로세스 및 기술과 함께 제공되는 Dell Technologies와 같은 기업의 MDR 솔루션을 탐색할 것을 권장합니다.

Enterprise Strategy Group은 글로벌 IT 커뮤니티에 마켓 인텔리전스, 실행 가능한 통찰력 및 GTM(Go to Market) 콘텐츠 서비스를 제공하는 통합 기술 분석, 연구 및 전략 회사입니다.

www.esg-global.com contact@esg-global.com 508.482.0188