Enterprise Strategy Group | Getting to the bigger truth.™

MDR을 통한 보안 운영 격차 해소

사이버 공격이 손상을 입힐 위험이 증가하며 핵심 비즈니스 목표의 인지도와 예산을 빼앗김에 따라 조직은 사이버 보안 프로그램을 강화하여 대응해야 합니다. 모든 사이버 보안 프로그램의 핵심은 SecOps(Security Operations)으로, 이는 디지털 공격 지점의 모든 측면을 모니터링하고 보호하는 일을 담당합니다.

투자에도 불구하고 더 어려운 보안 운영

응답자의 절반 이상이 2년 전보다 현재 SecOps가 더 어렵다고 생각합니다.

» SecOps가 더 어려운 5가지 이유

1. **41%** 위협 환경이 지속하고 빠르게 변화 중
2. **39%** 공격 지점이 지속적으로 변화하고 발전 중
3. **37%** 보안 알림의 양과 복잡성 증가
4. **34%** 조직의 퍼블릭 클라우드 서비스 사용 증가
5. **33%** 보안 운영 기술의 운영 요구 사항을 충족하기가 어려움

프로그램 전략의 재구성

공격 지점과 위협 환경은 규모와 복잡성 모두 증가했고, 따라서 보안 제어 기능을 활용하여 수천 개의 알림과 방대한 양의 보안 데이터가 생성됩니다. 보안 팀은 전반적인 프로그램 운영을 재구성하여 IT 및 LOB(Line of Business) 팀의 자산 및 위협 데이터를 추가로 통합하고 조직 목표에 가장 큰 위험을 초래하는 위협에 집중하고 있습니다.

조직의 **98%**는 이미 MDR 공급업체와 협력하고 있거나 향후 12개월 이내에 협력할 계획입니다.

이러한 조직의 **88%**는 향후 12개월 동안 MDR 활용을 늘릴 계획입니다.

» MDR 계약을 위한 주요 가치 동인

운영 개선 및 효율성.
MDR은 조직이 인프라스트럭처, 인력 및 관리와 같은 여러 가지 방법으로 보안 운영의 총 비용을 절감하도록 지원할 수 있습니다. 또한 "알림 피로" 문제를 해결하고 거짓 양성을 크게 감소시킬 가능성을 높일 수 있습니다.

사이버 보안 효과 개선 및 위험 감소.
MDR은 조직이 이미 진행 중인 위협을 차단하고, 잠재적 위협 및 지속적인 지능형 공격 탐지를 개선하고, 사전 예방적 위협 추적을 활성화하며, 더 강력한 제어를 체계화하여 향후 공격을 식별 및 방지하도록 지원할 수 있습니다.

» 귀사에서 매니지드 서비스를 사용하거나 계획하는 주된 이유

55%
초점:
우리 조직은 보안 담당자가 보안 운영 작업에 시간을 할애하지 않고 보다 전략적인 보안 이니셔티브에 집중하기를 원합니다.

52%
서비스:
우리 조직은 자체 인력보다 조직 외부의 서비스 공급업체가 보안 운영을 더 효율적으로 수행할 수 있다고 믿습니다.

49%
보강:
우리 조직은 서비스 공급업체가 보안 운영으로 SOC 팀을 보강할 수 있다고 믿습니다.

42%
기술:
우리 조직은 보안 운영을 위한 적합한 기술을 보유하고 있지 않습니다.

> "많은 '1.0세대' MDR 솔루션은 데이터의 수량과 위협의 빈도가 적고 탐지도 간단한 **다른 시대에 맞게 설계 및 구현되었습니다."**
>
> *- Dave Gruber, ESG Principal Analyst*

MDR에 대한 새로운 요구 사항.

많은 '1.0세대' MDR 솔루션은 데이터의 수량과 위협의 빈도가 적고 탐지도 간단한 다른 시대에 맞게 설계 및 구현되었습니다. 차세대 MDR 솔루션은 보다 다양한 공격 지점을 보호하고, 더 복잡한 위협을 탐지하며, 우선 순위 지정 및 완화에 대한 보다 위험 중심적인 접근 방식을 활용할 수 있어야 합니다.

- 24/7 이벤트 및 로그 모니터링
- 불륨, 위치 및 유형별로 의심스러운 활동 및 알림에 대한 빠르고 높은 가시성 정보
- 지속적이고 확장 가능한 네트워크 모니터링 및 위협 분석
- 상황에 맞는 응답 옵션을 위한 AI 기반 권장 사항
- 규정 준수 보고
- 사내 팀과 직접 접촉하는 "인간" 보안 조언자
- 위협 탐지, 분류, 조사 및 포렌식에 기반한 상세 실시간 분석
- 취약성 진단, 우선 순위 지정 및 완화 지침

아웃소싱 MDR 기능을 일부, 대부분 또는 모두 제공할 수 있는 수많은 잠재적 서비스 공급업체를 **고려할 때 조직은 다음을 제공할 수 있는 파트너를 찾아야 합니다.**

- 사이버 위협 인텔리전스
- 조직의 지리적 적용 범위 영역, 업종별 시장 및 규제 프로필에서 검증된 실적
- 위협 추적 기능 시연
- 클라우드 기반 MDR에 대한 장기적 노력
- 멀티클라우드 및 하이브리드 클라우드 환경의 광범위한 기능, 제로 트러스트(zero trust), 클라우드 보안의 공동 책임 모델
- 혁신적인 기술, 검증된 프로세스 및 인력의 입증된 전문 지식을 바탕으로 시간이 지남에 따라 서비스를 확장할 수 있는 검증된 능력

더 중요한 사실

사이버 공격을 손상시킬 위협이 증가하며 핵심 비즈니스 목표의 인지도와 예산을 빼앗김에 따라 조직은 사이버 보안 프로그램을 강화해야 합니다. 활용 사례는 다양하지만 대부분은 MDR 서비스 공급업체를 활용하여 프로그램을 증대하고 확장하고 있습니다. Managed Detection and Response에 대한 Dell Technologies의 접근 방식은 유연하고 지능적이며 확장 가능한 기술과 숙련된 사이버 보안 전문가의 역량을 결합하여 모든 규모의 조직과 리소스 프로파일이 보안 프로그램을 가속화 및 강화하도록 지원합니다.

자세히 보기

DELL Technologies

출처: ESG 전체 설문조사 결과, SOC Modernization and the Role of XDR, 2022년 8월.