Enterprise Strategy Group | Getting to the bigger truth.™

ESG 백서

Managed Detection and Response: 보안 프로그램의 급성장을 위한 경로

Dave Gruber, Principal Analyst

2022년 8월

목차

요약

디지털 혁신 가속화, 신속한 클라우드 도입, 더욱 복잡한 위협 환경, 지속적인 보안 기술 부족으로 보안 팀은 한계에 부딪히고 있습니다. 현재의 보안 솔루션으로는 요구 사항에 대처할 수 없으므로 많은 기업에서 기술과 프로세스를 개편하기 위해 SOC 현대화 이니셔티브의 우선 순위를 설정해야만 합니다. 제로 트러스트(zero trust)와 XDR(Extended Detection and Response)을 중심으로 하는 업계 메가트렌드는 새로운 비전을 제시합니다. 그러나 많은 기업들이 이러한 전략을 효과적으로 구현하고 운영하는 데 어려움을 겪고 있습니다. MDR(Managed Detection and Response) 서비스는 많은 조직이 이 격동하는 환경에서 보안 프로그램을 강화하는 데 필요한 인력, 프로세스 및 기술을 제공하여 부담을 완화합니다.

소개

사이버 공격이 손상을 입힐 위험이 증가하며 핵심 비즈니스 목표의 인지도와 예산을 빼앗김에 따라 조직은 사이버 보안 프로그램을 강화하여 대응해야 합니다. 일부 조직의 경우 내부 리소스를 사용하여 전체 보안 프로그램을 구축하는 것이 타당하지만, 대부분의 경우 프로그램 규모를 빠르게 확장하기 위해 타사 리소스가 필요합니다.

모든 사이버 보안 프로그램의 핵심은 보안 운영(SecOps)으로, 이는 디지털 공격 지점의 모든 측면을 모니터링하고 보호하는 일을 담당합니다. 네트워크, 엔드포인트, 클라우드, ID, 애플리케이션 및 데이터를 모두 포함하고 보안 운영과 관련된 보안 텔레메트리 및 알림의 양이 증가하여 조직은 한계에 부딪히고, 이로 인해 많은 조직에서 부담을 줄이기 위해 MDR 서비스 공급업체를 선택하고 있습니다.

MDR 서비스 공급업체는 인시던트 대응, 연중무휴 모니터링, 프로그램 관리 및 위험 관리와 같은 다양한 보안 서비스 오퍼링을 제공하여 이러한 조직에게 중요한 메커니즘으로 자리잡았습니다. ESG(Enterprise Strategy Group) 연구에 따르면 MDR 서비스는 규모와 보안 성숙도를 불문하고 모든 조직을 위한 최신 사이버 보안 전략의 메인스트림 구성 요소가 되었습니다.

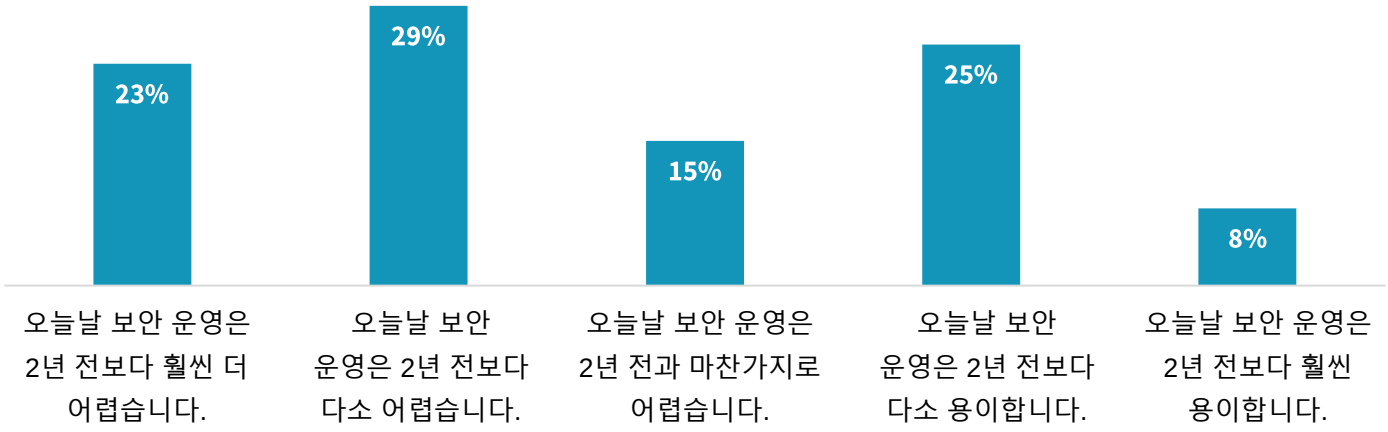
증가하는 보안 운영 당면 과제

ESG 조사에 따르면(그림 1 참조) 대부분의 조직이 전체 보안 운영 시나리오가 2년 전보다 현재 더 어렵다는 사실을 인정합니다.[1]

[1] 출처: ESG 전체 설문조사 결과, *SOC Modernization and the Role of XDR*, 2022년 8월. 이 백서의 모든 ESG 참고 자료 및 차트는 달리 명시되지 않는 한 이 설문조사 결과에서 가져왔습니다.

그림 1. 절반 이상이 보안 운영이 더 어렵다고 느낌

다음 중 귀사의 보안 운영에 대한 귀하의 의견을 가장 잘 반영한 답변은 무엇입니까? (응답자 비율, N=376)

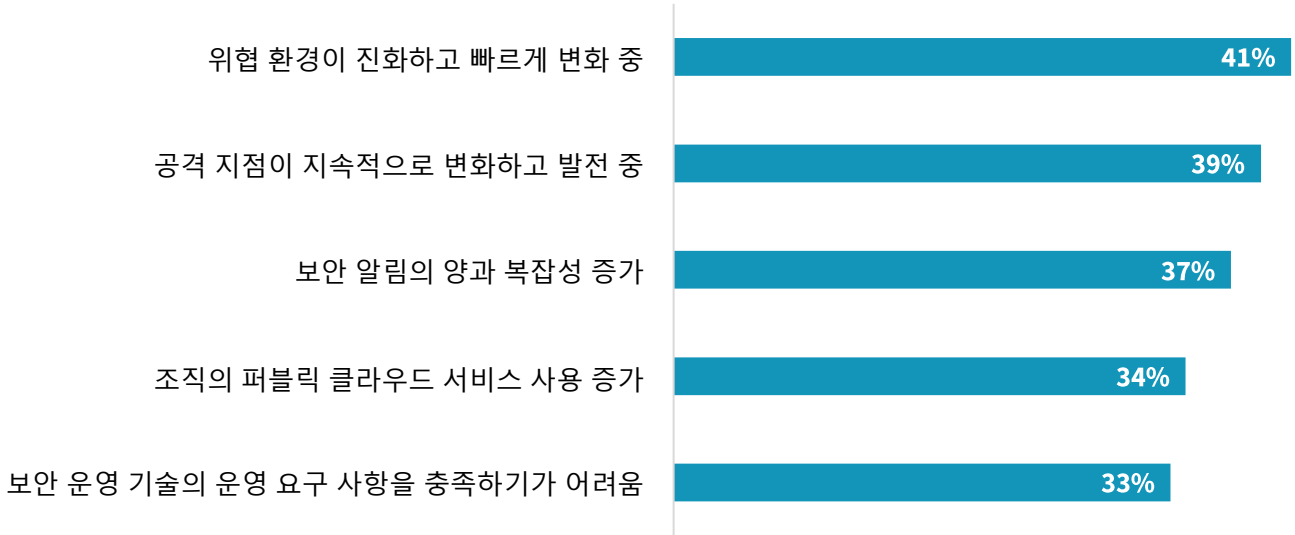


출처: ESG, TechTarget, Inc. 사업부

또한 그림 2에서와 같이 ESG 연구에서는 공격 지점 확대, 위협 환경의 증가 및 다양성, 더 광범위한 애플리케이션 및 활용 사례에 클라우드 서비스 이용 확대 등 탐지 및 대응을 그 어느 때보다 어렵게 만드는 다른 당면 과제도 지적합니다.

그림 2. 보안 운영이 더 어려운 5가지 이유

조직의 보안 운영이 2년 전보다 더 어렵다고 말씀하셨습니다. 그와 같이 생각하는 주된 이유는 무엇입니까? (응답자 비율, N=194, 복수 응답 허용)



출처: ESG, TechTarget, Inc. 사업부

탐지 및 대응 프로그램 현대화

공격 지점과 위협 환경은 규모와 복잡성 모두 증가했고, 따라서 더 많은 보안 제어 기능을 활용하여 수천 개의 알림과 방대한 양의 보안 데이터가 생성됩니다. 보안 팀은 알림 및 인시던트 분류와 조사를 지원하기 위해 이 데이터를 집계하고 상관 관계를 파악하고 분석해야 하므로 엄청난 수동 처리가 필요한 경우가 많습니다. 하지만 알림 및 보안 데이터의 캡처 및 분석 외에도 더 많은 것이 필요합니다.

보안 팀은 전반적인 프로그램 운영을 재구성하여 IT 및 LOB(Line of Business) 팀의 자산 및 위험 데이터를 추가로 통합하고 조직 목표에 가장 큰 위험을 초래하는 위협에 집중하고 있습니다. 예를 들어, 도메인 관리 자격 증명을 도난당하면 단기 및 장기적으로 조직의 운영, 재무 및 브랜드 평판에 광범위한 부정적 영향을 미칠 수 있습니다.

보안 책임자가 전략을 재구상함에 따라 점점 더 많은 조직이 보다 전략적인 보안 활동에 내부 리소스를 다시 집중하면서 일상적인 운영 활동을 타사에 오프로드하고 있습니다. 내부 보안 리소스가 보안 운영 프로세스를 재설계하는 데 집중함에 따라 MDR 서비스 공급업체는 인시던트 탐지, 분류 및 대응을 처리하여 손상을 방지하고 잠재적인 운영 업무 중단을 최소화하기 위한 신속한 조치를 취합니다.

다른 조직은 전반적인 프로그램 개발 지침을 위해 MDR 공급업체를 찾고 있으며 결과를 최적화하기 위해 전문가와 검증된 보안 운영 프로세스를 활용하고 있습니다.

또한 XDR 이동으로 탐지 및 대응 프로그램을 현대화하는 데 필요한 비전과 로드맵이 창출됨에 따라 다른 조직에서는 MDR 공급업체를 활용하여 XDR 등급 솔루션의 구축을 지원하려 모색합니다.

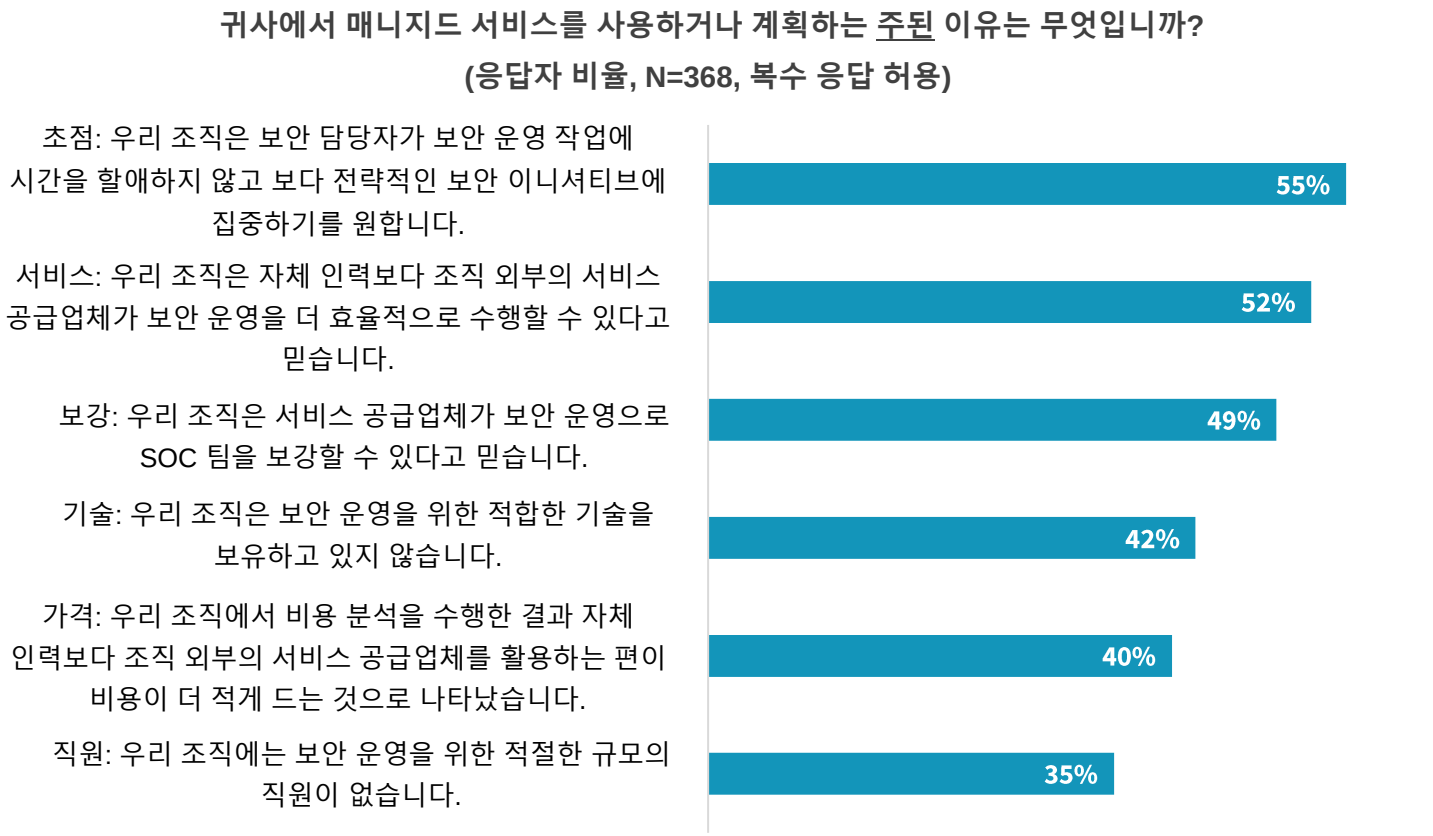
MDR 활용 사례

많은 MDR 공급업체가 광범위한 보안 서비스를 제공하지만, 알림을 모니터링, 분류 및 조사하는 핵심 탐지 및 대응 서비스는 대개 초기 개입이 시작되는 단계입니다. 운영 모델은 MDR 공급업체에 따라 다르므로 보안 책임자는 특정 목표를 충족할 수 있는 MDR 공급업체와 신중하게 개별 조직의 요구 사항을 조율해야 합니다. 예를 들어 일부 보안 책임자는 보안 운영을 완전히 아웃소싱하여 MDR 공급업체와의 협력을 통해 전체 공격 지점 적용 범위, 위협 모니터링 및 문제 해결을 제공하도록 선택합니다. 이 모델에서 MDR 공급업체는 일반적으로 서비스를 렌더링하는 데 필요한 기술 스택, 프로세스 및 보안 전문가를 제공합니다. 다른 경우, MDR 서비스는 사내 보안 운영 기능의 확장으로, 기술 스택 및 운영 프로세스를 주로 담당하는 사내 팀에 근무 시간 외 서비스 또는 추가 보안 전문가를 추가합니다. 이는 MDR 서비스를 활용하는 많은 활용 사례 중 두 가지 예에 불과합니다.

따라서 MDR은 "한 가지로 모든 것을 충족하는" 솔루션이 아닙니다. 그보다 개별 조직의 요구 사항에 적용할 수 있는 맞춤 구성 가능한 기능 세트를 나타내는 경우가 많습니다.

다양한 조직에서 사내 리소스와 기술에 따라 탐지 및 대응의 다른 측면을 위해 MDR 파트너를 선택할 수 있습니다. ESG 조사는 그림 3에서 주요 이유를 살펴봅니다.

그림 3. 조직이 MDR 파트너를 선택하는 이유



출처: ESG, TechTarget, Inc. 사업부

MDR 계약을 위한 주요 가치 동인

보안 프로그램 개발은 효율성과 효과 모두에 초점을 맞춰야 하고 MDR 서비스는 각각에 긍정적인 영향을 미칠 수 있습니다.

- **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.

최신 MDR 솔루션 공급업체에서 찾아야 할 사항

MDR 솔루션은 일반적으로 새로운 솔루션이 아니라는 점을 기억하십시오. 실제로 MDR 솔루션은 꽤 오래되었고 성공적인 실적을 보여주었습니다. 그러나 많은 "1.0세대" MDR 솔루션은 데이터의 수량과 위협의 빈도가 적고 탐지도 간단한 이전 시대에 맞게 설계 및 구현되었습니다. 차세대 MDR 솔루션과 이를 배포하고 관리하는 타사에서는 탐지 및 대응을 그 어느 때보다 중요하고 더 어렵게 만드는 더 광범위하고 심층적이며 복잡한 당면 과제를 고려해야 합니다.

MDR 솔루션을 평가할 때 조직은 다음과 같은 기능을 모색해야 합니다.

- 24/7 이벤트 및 로그 모니터링, 볼륨, 위치 및 유형별로 의심스러운 활동 및 알림에 대한 빠르고 높은 가시성 정보 산출.
- 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.
- 풍부한 텔레메트리.
- 조직의 지리적 적용 범위 영역, 업종별 시장 및 규제 프로필에서 검증된 실적.
- 위협 추적 기능 시연.
- 멀티클라우드 및 하이브리드 클라우드 환경의 광범위한 기능, 제로 트러스트, 클라우드 보안의 공동 책임 모델을 갖춘 클라우드 기반 MDR에 대한 장기적 노력.
- 혁신적인 기술, 검증된 프로세스 및 인력의 입증된 전문 지식을 바탕으로 시간이 지남에 따라 서비스를 확장할 수 있는 검증된 능력.

MDR에 대한 Dell Technologies 접근 방식

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 Technologies 회사인 Secureworks에서 개발한 완벽하게 관리되는 클라우드 네이티브 서비스인 Taegis XDR입니다. Taegis XDR은 분산되고 다각화된 공격 지점에서 완벽하게 확인된 위협을 탐지, 분석하고 조치를 취하여 대규모 글로벌 기업부터 비교적 소규모 기업에 이르는 조직을 보호하도록 돕습니다.

Taegis XDR의 강점은 Dell의 대규모 보안 분석가 및 엔지니어 그룹의 전문 지식과 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.

구독 기반 매니지드 서비스로 구성 및 구축된 Dell Managed Detection and Response는 보안 전문가를 찾아내고 모집하여 더 많은 위협, 더 많은 공격 및 더 많은 알림을 처리해야 하는 조직의 필요성을 크게 줄여줍니다. Dell Managed Detection and Response는 조직의 내부 기능을 효율적, 효과적으로 보완하고 확장합니다. 결과적으로 사내 보안 운영 담당자는 다른 보안 관련 작업에 더 많은 시간과 에너지를 집중할 수 있습니다.

성공 사례: 실제 환경에서 MDR의 작동 방식

ESG는 Dell MDR 고객의 IT 및 보안 책임자들과 대화를 나누면서 특정 활용 사례, 운영 모델 및 결과에 대한 통찰력을 얻었습니다.

예 #1: 중간 규모 지방 정부

지방 정부의 IT 및 사이버 보안 리소스가 민간 부문 상대의 리소스와 맞먹는 경우는 드물지만, 그렇다고 해서 같은 종류의 문제에 직면하지 않는다는 의미는 아닙니다. 이 예에서 미국 남서부 주에 있는 중간 규모 카운티는 증가하는 보안 위협에 대처하고 극복하는 데 어려움을 겪고 있었지만 빡빡한 제약 조건 이내로 지출을 유지하는 문제로도 힘들어 하고 있었습니다.

새로운 IT 책임자가 고용되었고, 그는 소규모 팀이 직면한 위협 증가하는 환경을 즉시 인식하고 탐지 및 대응 기능의 잠재적 취약성을 발견했습니다. 그는 "우리의 보안 태세는 사태를 파악할 뿐만 아니라 경영진 의사

결정권자에게 매우 민감한 주제인 급여 확대 없이 역량을 확장할 수 있어야 했습니다"라고 말했습니다. "하지만 재정적으로 절감해야 한다는 경영진의 우려 사항에 호소하면서도 취약성을 해결해야 할 필요성을 지적할 수 있다는 것을 알았습니다."

먼저, 탐지 및 대응 개선을 위해 당시 90일간의 소프트웨어 업그레이드 "무료 평가판"을 홍보하던 카운티의 엔드포인트 보안 공급업체를 평가하는 일에 착수했습니다. 하지만 소프트웨어가 요구 사항에 맞는 기능이 부족하고 공급업체의 커뮤니케이션이 기대에 못 미친다는 점을 발견하자 보다 포괄적인 MDR 솔루션으로 결정했습니다.

"다행히 우리는 Dell과 가상 CSO(Chief Security Officer)를 제공하는 계약을 맺고 있었기 때문에, 카운티 책임자는 매니지드 서비스, 이 경우 탐지 및 대응 접근 방식을 사용할 때 얻을 수 있는 이점을 알고 있었습니다." 그는 Dell 팀이 카운티에서 보유한 사내 보안 및 IT 전문가 팀을 대신한다기 보다 보완하는 역할을 맡았다고 덧붙였습니다. "Dell 팀원들은 우리 팀의 확장이었고 직원들과 매우 원활하게 협력했습니다."

이 계약의 실질적인 이점은 글로벌 해킹 캠페인이 카운티를 비롯한 다양한 조직에서 사용하는 인기 있는 플랫폼인 Microsoft Exchange 웹 메일을 타겟으로 했을 때 곧 명확해졌습니다. "Microsoft는 공격을 발견한 즉시 패치를 개발하고 전송했지만, 0일 차 공격은 아마도 한 달 전인 것 같았습니다."라고 카운티 IT 책임자는 말했습니다. "우리는 몇 시간 후 Dell 가상 CSO에게 연락을 받았고 Dell MDR 팀은 바로 작업에 돌입했습니다. 스크립트를 전송하여 서버를 확인했고 서버 중 하나가 손상되었다는 것을 빠르게 발견했습니다."

"Dell(그리고 Dell의 Secureworks 파트너)은 무슨 일이 일어나고 있는지 실제로 파악했습니다. 우리는 보안 침해 시도를 처리하는 동안 매일 하루에 2번, 3번 통화했습니다." 그는 인시던트 대응 팀이 카운티 담당자와 함께 조사 결과를 검토하여 코드 정보와 기타 보안 침해 시도 조짐, 손상의 증거를 보여주했다고 덧붙였습니다.

마지막으로, 보안 침해 시도의 잠재적 영향을 해결할 뿐만 아니라 광범위한 관점과 기간에 걸쳐 카운티의 사이버 보안 프로파일을 강화하는 여러 기술 및 비기술적 권장 사항을 제공했습니다.

그는 "우리는 경험을 통해 향상된 탐지 및 대응 방법을 모색할 경우 EDR 소프트웨어를 업그레이드하는 저렴한 방법을 찾기보다, 이 문제를 해결한 경험이 있는 신뢰할 수 있고 검증되었으며 믿음직스러운 MDR 전문가를 찾는 것이 방법임을 깨달았습니다."라고 말했습니다. "보안 침해 시도의 여파가 있을 때뿐만 아니라 정기적으로 협력하면서 저는 우리를 안전하게 지키는 데 도움을 줄 수 있는 좋은 팀이 있다는 편안한 안도감이 들었던 기억이 납니다."

예 #2: 중간 규모 학군

학군은 지금까지 일반적으로 IT, 특히 사이버 보안에 대한 투자가 부족했습니다. 그러나 학군에 대한 랜섬웨어와 기타 사이버 공격이 증가함에 따라 지역 공교육 공무원은 취약성으로부터 보호하는 더 신뢰할 수 있고 경제적인 더 나은 방법을 마련하기 위해 분주히 움직이고 있었습니다.

예를 들어, 미국의 한 중간 규모 학군은 랜섬웨어의 공격을 받아 전체 기술 중심 운영이 중단되었다는 것을 발견했습니다. 21개 시설에 8,500명의 학생과 직원이 분산되어 있는 이 학군은 100개의 물리적 서버와 또 다른 63개의 가상 서버를 갖추고 학생과 직원을 위한 11,000대 이상의 디바이스에 연결된 합리적인 규모의 IT 프로필을 보유하고 있었습니다. 분명히 이 학군은 악의적인 행위자가 보기에 많은 잠재적 진입점이 있었고 신속하게 조치를 취할 수 있는 파트너가 필요했습니다.

랜섬웨어 공격이 실제이며 즉시 해결되어야 한다는 것을 판단한 후 학군의 IT 팀은 Dell Managed Detection and Response에 문의했습니다. "공격 2일 차까지 Dell에서 10명의 직원이 참여했습니다."라고 학군의 IT 책임자는 말했습니다. "우리는 Dell 팀과 매우 신뢰할 수 있는 관계를 맺었으며, Dell에서는 곧바로 담당 업무에 착수했습니다."

다행히 실질적인 결과는 학군에 긍정적이었습니다. IT 책임자는 "시스템에 있는 600만 개 이상의 파일 중 손실된 것은 단 6개였습니다."라고 언급했습니다. "위협 행위자에게 전혀 지불하지 않았습니다. 우리는 랜섬웨어에서 살아남고 안전하게 작업을 지속하는 실제 사례입니다.

"Dell과 협력하는 것은 긍정적인 경험이었습니다. 현장 보안 분석가는 Dell 팀원들과 대화를 나눈 후에 항상 만족하고 있으며, Managed Detection and Response에 대해 Dell과 협력하기 전보다 현재 95% 더 나은 태세를 갖추고 있습니다."

더 중요한 사실

사이버 공격이 손상을 입힐 위험이 증가하여 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.

MDR 서비스 공급업체는 보안 전문가, 검증된 프로세스, 확장 가능하고 구축이 간편한 보안 기술을 비롯하여 성공적인 보안 프로그램을 구축하는 데 있어 인식되는 많은 당면 과제를 극복할 수 있는 방법을 제공합니다.

Dell Technologies는 조직이 거의 실시간으로 위협을 탐지하고 대응할 수 있도록 긴밀하게 통합된 기술, 숙련된 보안 전문가 및 모범 사례를 종합했습니다. 이 백서의 사례 연구에서 볼 수 있듯이, Dell Technologies는 다양한 산업 및 리소스 프로필에 걸친 광범위한 조직을 지원하여 기업 전반에서 새로운 위협이 미치는 영향을 저지하는 데 도움을 주었습니다.

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