비용이 많이 드는 인력을 추가하지 않고 보안 보호 조치 개선

미국 남서부의 한 대형 카운티에서는 사이버 보안을 대폭 강화하기 위해 Dell Managed Detection and Response를 선택했습니다.

고객 프로파일

미국 카운티

주 및 지방 정부 | 미국

"우리는 보안 태세를 강화해야 한다는 것을 알았습니다. Dell Managed Detection and Response를 사용하니 추가 인력 없이 작업을 완수할 수 있었습니다."

정보 시스템 부문 이사
미국 남서부의 대형 카운티

비즈니스 요구

주 정부와 지방 정부를 노리는 랜섬웨어 및 기타 사이버 위협이 급속도로 증가함에 따라, 미국 남서부에서 성장세를 보이는 어느 대형 카운티에서는 보안 태세를 강화하고 추가 보안 전문가를 채용하고 교육하는 데 필요한 비용과 노력 없이 위협을 탐지하고 대응하는 능력을 향상하고자 했습니다.

솔루션 요약

- Managed Detection and Response

비즈니스 성과

- 인력 증가 없이 카운티의 보안 태세를 강화합니다.
- IT 팀의 지식, 기술, 확장 능력을 보완합니다.
- 직원의 24x7 위협 모니터링 및 대응 부담을 해소합니다.
- 서버 침해 탐지를 간소화하고 신속하게 문제를 해결합니다.
- 카운티가 의지할 수 있는 숙련된 전문가로 편안한 서비스를 제공합니다.

미국 남서부에서 급성장 중인 어느 대형 카운티는 수십만 명의 주민에게 서비스를 제공하고 있으며, 활발한 의료, 바이오테크, 제조업체부터 필수적인 농업과 영농 운영에 이르기까지 다양한 비즈니스 기반을 갖춘 것으로 알려져 있습니다.

최근 몇 년 동안 주 정부와 지방 정부에 대한 사이버 보안 위협이 크게 증가했습니다. 2020년 미국에서는 79건에 달하는 랜섬웨어 공격이 발생하여 전국 각계각층의 정부 기관에 거의 190억 달러에 달하는 다운타임과 복구 비용이 발생했습니다.[1]

미국 남서부의 이 카운티에서는 기존에 거래하던 다른 공급업체의 서비스에 실망한 경험이 있어, 이번에는 Secureworks® Taegis™ XDR 보안 분석 소프트웨어 기반의 Dell Managed Detection and Response를 선택했습니다. 이 솔루션은 카운티의 전체 IT 환경에서 위협을 모니터링, 탐지, 조사 및 대응하는 포괄적인 24x7 매니지드 서비스입니다.

카운티의 정보 시스템 부문 이사는 "보안 태세를 개선해야 한다는 것을 알았습니다."라고 말합니다. "Dell Managed Detection and Response를 사용하니 추가 인력 없이 작업을 완수할 수 있었습니다."

두 가지 핵심 기능 결합

이 솔루션은 강력한 보안 태세를 구성하는 가장 중요한 요소 두 가지를 하나로 결합합니다.

- 보안 분석가 한 명과 시스템 관리자 겸 엔지니어 한 명으로 구성된 소규모 카운티 팀을 보완하는 Dell Technologies 보안 분석가의 전문 지식

- Secureworks Taegis XDR의 광범위한 기능. 가장 지능형 공격을 탐지하도록 설계된 클라우드 네이티브 보안 분석 플랫폼을 통해 MDR 분석가가 카운티와 협력하여 효과적으로 조사하고 궁극적으로 적절한 조처를 통해 영향을 완화할 수 있습니다.

"Dell Technologies 전문가의 도움이 필요할 때 바로 담당자가 투입돼 1주일에서 10일 가량 지원해 줬기 때문에 저희는 안심할 수 있었습니다."

정보 시스템 부문 이사
미국 남서부의 대형 카운티

[1] Bischoff, Paul, "Ransomware attacks on US government organizations cost $18.9bn in 2020", Comparitech, 2021년 3월 17일. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

"Dell Technologies 전문가들은 소프트웨어 에이전트를 모든 서버와 워크스테이션에 설치하도록 지원해 주었고, 위협이 탐지되면 서비스를 중지하거나 컴퓨터 또는 계정을 강제 종료한 후 우리에게 알려주는 트리거를 선택하도록 도와주었습니다."라고 정보 시스템 부문 이사는 말합니다. "Dell Technologies 전문가는 우리에게 귀중한 조언을 해주고 모든 것을 구현하는 90일 동안 우리가 어떤 단계부터 우선적으로 처리해야 할지 알려주었습니다."

보안 침해 시도의 신속한 완화

이 솔루션은 가장 복잡한 상황에서도 위협에 대응하고 해결할 명확한 지침 설명을 분기별로 최대 40시간 제공하며, 필요한 경우 매년 40시간을 추가로 제공하여 활동을 조사하고 심각한 보안 인시던트로부터 복구를 시작할 수 있도록 지원합니다.

"솔루션에 대해 확신을 가지게 된 것은 실제 보한 침해 시도가 발생했을 때였습니다."라고 정보 시스템 부문 이사는 회상합니다. "어떤 해킹 그룹이 Microsoft Exchange 이메일 서버에서 취약점을 발견했습니다. Microsoft와 주를 담당하는 사이버 보안 기관으로부터 통보를 받은 후 3대의 서버 중 하나가 공격당한 사실을 알게 되었습니다. Dell Technologies 팀은 매우 철저하게 보안 침해를 조사하고 서버를 복구하도록 지원했습니다."

그는 계속해서 말합니다. "저는 모든 카운티의 CIO에게 일개 안티바이러스 소프트웨어 공급업체의 솔루션이 아닌 Dell Managed Detection and Response와 같은 엔터프라이즈급 보안 솔루션을 사용할 것을 권합니다. Dell Technologies 전문가의 도움이 필요할 때 바로 담당자가 투입돼 1주일에서 10일 가량 지원해줬기 때문에 저희는 안심할 수 있었습니다. 우리는 서로 더 현명하게 일했고, 팀끼리 많은 시너지 효과를 낼 수 있었습니다."