사이버 보안에서 사람의 중요성

최악의 시나리오를 상상해 보십시오.

정교한 랜섬웨어 공격으로 데이터 센터 전체가 마비되었습니다. 영업, 고객 서비스, 재무 부서는 운영이 불가능합니다. 여러분은 시스템 복원을 담당하는 선임 IT 리더인데, 해결책을 찾기 어려운 것으로 파악되었습니다.

여러분의 팀은 이미 인력이 부족한 상태로 몇 주 내내 휴식이나 휴무가 거의 없이 일해 왔습니다. 일부 실무자들은 **무려 36시간 동안 한숨도 못 자고 일했습니다.** 여러분은 피로로 인해 잘못된 의사 결정이 내려져 복구 작업 자체가 위험해질까 봐 걱정하고 있습니다.

즉시 투입되어 문제 해결을 지원할 수 있는 추가 인력이 절실히 필요한데, 그런 인력을 어디서 찾을 수 있을까요?

이 시나리오는 소설의 시작처럼 들릴지 모르지만, Dell 고객의 실제 경험을 바탕으로 합니다. 오늘날 사이버 보안 환경의 심각한 문제인 인적 요소를 드러내는 것입니다.

최근 데이터에 따르면 업계는 거의 500만 명의 보안 전문가 부족을 겪고 있습니다. 자원의 필요성은 인시던트가 발생하는 동안에 가장 크게 느껴지지만 해결책은 훨씬 이전 단계에서 시작됩니다.

인재 파이프라인 구축 및 육성에서 출발

필요한 리소스를 확보하기 위한 첫 번째 단계는 인재 파이프라인을 구축하는 것입니다.

대학 채용 및 인턴십

지역 대학 및 실업학교와의 협력을 통해 신진 인재를 꾸준히 확보할 수 있습니다. 이들은 시간이 지남에 따라 영향력 있는 팀원으로 성장할 수 있습니다.

지속적인 교육 및 개발

시간과 예산에 대한 압박이 지속적인 상황에서, 사이버 보안 전문가는 툴과 위협의 변화에 발맞춰 나가야 합니다.

유지에 집중

뛰어난 실무자, 특히 공격 대응 경험이 있는 인재에 대한 수요가 높습니다. 최고의 인재를 유지하지 못하면 다른 누군가가 대신하게 됩니다.

경험이 풍부한 팀일지라도 공격에 대응할 때 스트레스를 관리하기 힘들 수 있으므로 사전에 추가 지원을 파악하여 미리 계획하십시오.

타사 리소스 평가

사이버 보안 컨설팅 및 인력 증강 회사는 지속적인 운영 및 인시던트 발생 시 귀사의 팀을 지원할 수 있습니다. 당장은 필요하지 않더라도 이러한 회사와 관계를 구축하여 필요할 때 해당 리소스에 접근할 수 있도록 하십시오.

Dell Technologies는 vCISO(virtual CISO), 인시던트 대응, 사이버 보안 자문 등 기존 팀을 보강할 수 있는 다양한 서비스를 제공합니다.

AI 활용

로그 분석, 이상 징후 탐지, 저수준 알림 분류 또는 전문 교육 등 사이버 보안 툴에 내장된 새로운 AI 기능을 활용하여 리소스 격차를 해소하고 운영상의 필요를 충족함으로써 팀원들이 더 중요한 업무에 집중할 수 있는 시간을 확보할 수 있습니다.

사이버 공격 발생 시 가장 큰 어려움은 자원 확보

초기 시나리오에서 볼 수 있듯이, 대규모 사이버 공격은 조직을 무력화하여 주요 시스템과 비즈니스 운영을 마비시킬 수 있습니다. 매 순간 회사 자금이 소진되고, 사이버 보안 팀은 문제 해결에 엄청난 압박을 받게 됩니다.

팀이 가능한 한 최신 상태를 유지하도록 하는 것은 인시던트 대응과 팀에 가해지는 관련 스트레스에 직접적인 영향을 미칩니다.

교육은 보안 전문가뿐만 아니라 모든 직원에게까지 확대되어야 합니다. 모든 직원이 1차 방어선이기 때문입니다.

이 사례에서는 핵심 과제를 강조합니다. 사이버 방어자는 결국 인간입니다. 인간은 한계가 있으며, 그 한계를 넘어서면 가장 능숙한 전문가라도 실패할 수 있습니다. 정신적 피로, 스트레스, 그리고 번아웃은 이제 사이버 보안 태세에 있어 중요한 요소입니다.

이 과제에 대한 단 하나의 해결책은 없을지 모르지만, 다음과 같은 전략들이 큰 도움이 될 수 있습니다.

강력한 팀과 인재 파이프라인 구축

이 문제의 가장 근본적인 해결책은 이를 긴급 상황이 되지 않게 하는 것입니다. 백업 인력을 갖춘 강력한 팀을 구축하십시오.

공격의 인적 측면에 대한 계획
인시던트 대응 계획은 매우 중요하며, 여기에는 직원 관리, 일정 계획, 직원의 휴식 시간 처리 계획이 반드시 포함되어야 합니다.

타사 리소스 활용
외부 사이버 보안 컨설턴트가 팀을 보강하는 데 도움을 줄 수 있습니다. 예를 들어 Dell Technologies의 인시던트 대응 서비스는 즉시 평가, 격리하고 문제 해결을 시작할 수 있는 전문가 팀을 몇 시간 내에 현장에 파견할 수 있습니다. Dell Technologies는 많은 고객이 사이버 공격을 극복할 수 있도록 지원해 왔습니다.

AI는 도움이 될 수 있지만, 만병통치약은 아님

AI는 사이버 보안 툴과 프로그램을 개선할 수 있는 엄청난 가능성을 제시합니다. AI의 역량은 궁극적으로 예측 분석부터 맞춤형 교육 프로그램 개발, 심지어 위협 확산 전에 사전 예방적으로 해결하는 것까지 아우를 것입니다.

더 중요한 것은 AI가 인시던트 발생 시 방어자에게 실시간 지원 시스템을 제공할 수 있다는 점입니다. 과거 공격 데이터를 기반으로 학습된 머신 러닝 모델은 유사한 과거 이벤트를 기반으로 조치를 추천할 수 있습니다.

자연어 처리가 사이버 보안 툴에 적용됨에 따라 분석가는 시스템에 직접 접속하여 위협을 식별하고 솔루션을 구축할 수 있게 될 것입니다.

AI는 또한 행동 패턴을 모니터링하여 인간 분석가가 피로 등으로 인해 반복적으로 실수를 저지르는 경우에 대해 플래그를 지정하고, 근무 교대 또는 새로운 시각으로 업무를 할 사람을 유도할 수 있습니다.

사이버 보안 툴이 더욱 정교한 AI 툴을 빠르게 통합하고 있지만, 가장 강력한 기능 중 상당수는 아직 개발 단계에 있습니다. 현재로서는 AI가 경험이 풍부한 실무자, **특히 이전에 공격을 경험한 실무자**의 기술을 대체할 수는 없다는 점을 명심하십시오.

AI 활용을 위한 권장 사항:

툴이 보안 운영에 어떻게 도움이 될 수 있는지 이해
AI 툴에 대한 상세한 분석을 수행하고 가장 효과적인 곳에 툴을 구현합니다. 손쉽게 효과를 볼 수 있는 조치로는 지능형 공격 탐지, 반복 작업 자동화, ID 관리에 AI 활용 등이 있습니다.

AI의 미래 계획
새로운 기능이 언제 출시되는지, 팀에 어떤 이점을 제공하는지 파악하고 구현 계획을 수립합니다.

인력 계획에 AI 통합
자동화로 수동 작업이 감소함에 따라 보안 팀의 구성도 변화해야 할 수 있습니다. 보안 정보를 수집하는 것이 아니라 분석하고 조치를 취할 수 있는 더 높은 수준의 인력이 필요할 수 있습니다. 채용 및 개발 전략을 이에 따라 조정합니다.

> "인시던트 대응, 문제 해결 및 복구를 상시 계약 형태로 수행하는 파트너를 확보하는 것이 모범 답안입니다."
>
> ***Jason Rosselot***
> *Dell Technologies, Cybersecurity and Business Unit Security Officer* 부사장

AI가 아직은 그렇지 않더라도, 앞으로는 사이버 보안 운영에 있어 중요한 부분이 될 것입니다. 하지만 숙련되고 경험이 풍부한 실무자를 대체할 수 있는 것은 없다는 점을 명심하십시오. AI를 활용하여 운영을 자동화하고 인적 자원의 효율성을 높여 궁극적으로 공격을 예방하고 공격 발생 시 그 영향을 최소화하는 것이 목표여야 합니다.

사이버 보안 성숙도 향상: 한 번에 한 단계씩

사이버 보안을 구성하는 모든 것이 그렇듯이 인적 요소를 다루는 것은 목적지가 아닌 여정입니다. 점진적인 노력, 그리고 진보를 향한 사소한 과정도 차이를 만들고 시간이 지남에 따라 누적됩니다. 중요한 것은 최고의 기술과 보안 툴이 있어도 궁극적으로는 이것을 운영하는 사람이 잘 해야만 제 효과를 발휘한다는 것입니다.

DELL Technologies

도움이 될 수 있는 Dell 제품 및 솔루션

주요 Dell 솔루션	설명
인시던트 대응 서비스	사이버 공격 발생 시 신속한 대응을 위해 업계 공인 사이버 보안 전문가 팀이 대기하고 있습니다. Dell Technologies는 정상 운영이 재개될 때까지 위협을 제거하기 위해 고객과 긴밀히 협력합니다.
Cybersecurity Advisory Services	보안 전략의 사각지대를 찾아 해결하고, 자산과 데이터를 보호하고, 지속적인 경계와 거버넌스를 구현하는 데 도움이 되는 전문가 지침입니다.
vCISO	가상 최고 정보 보안 책임자이자 사이버 보안 전문가로, 위험을 식별하고 관리하는 데 도움을 줄 수 있으며 전략적 의사 결정을 안내할 수 있습니다.
Managed Detection and Response	엔드포인트, 네트워크 및 클라우드 전반에 걸쳐 모니터링, 위협 탐지, 조사 및 신속한 대응을 제공하여 수동 작업을 줄이고 일상적인 보안 운영을 간소화합니다. 고객은 선호하는 XDR 플랫폼(Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR 또는 Microsoft Defender XDR)을 선택하여 전문가 지침, 분기별 보고서, 그리고 연간 최대 40시간의 인시던트 대응 서비스를 제공받습니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.