2021 산업별 주요 현황 : 보건의료

작년 한 해 동안 보건의료 산업을 표적으로 하는 사이버 공격이 활발히 이루어졌습니다 . 업무 역량을 최대로 끌어올리면서도 랜섬웨어와 같이 빠르게 확산하는 위협에 대응하면서 , 많은 기관에서 자가 학습 Cyber AI 를 활용해 기계 속도로 움직이는 공격을 탐지하고 자율적으로 이를 차단했습니다 .

한눈에 보기

- ✔ 전 세계 280 곳 이상의 보건의료 기관 보호
- ✔ 자가 학습 AI 기술로 정교한 신종 위협 탐지
- ✔ 빠르게 확산하는 공격을 몇 초만에 자율적으로 차단
- ✔ 분류 시간을 최대 92% 단축

빠르게 확산하는 공격과 제로데이 취약점 차단

사이버 범죄자들은 지난해 사회적 격변기를 틈타 빠르게 움직였습니다 . WHO 는 팬데믹이 시작된 이후 공격이 5 배 늘었다고 발표했으며 , FBI 는 “병원과 의료 기관에 사이버 범죄 위협이 임박” 했다고 경고해왔습니다 .

특히 우려되는 것은 랜섬웨어입니다 . 2020 년 9 월 , 미국의 병원 체인인 UHS(United Health Services) 의 250 개 이상의 병원이 공격을 받은 후 2 주간 업무가 마비되면서 , 구급차는 타 병원으로 연결되고 진료 예약은 연기됐으며 검진 결과는 늦어졌습니다 . 같은 달 사이버 공격의 직접적인 결과로 , 독일에서는 첫 사망자가 나왔습니다 . 그처럼 치명적인 결과가 나타나자 보건의료 기관에서는 더 이상 사이버 범죄자들이 악용하도록 다운타임을 두고 볼 수 없게 됐습니다 .

일선 근무자들이 사용하는 디지털 시스템과 데이터를 보호해야 하는 보안 팀의 과제는 점점 늘어나고 있습니다 . 디지털 인프라에 SaaS 애플리케이션 , 이메일 플랫폼 , MRI 장비 및 원격 환자 모니터링 기기 등 각종 요소가 포함되면서 , 조직의 디지털 환경과 이를 방어하기 위해 설계된 보안 스택은 그 어느 때보다도 단편화되었습니다 .

뿐만 아니라 , 효율성과 치료 결과를 개선하기 위해 구현한 IoT 디바이스는 보안 설정이나 암호화가 되지 않을 때가 많으며 , 보안 팀이 인식하지 못하는 경우도 흔합니다 . 미 식품의약국 (FDA) 은 치명적인 제로데이 취약점으로 인해 10 번 넘게 의료 IoT 디바이스의 86% 를 리콜했습니다 . 그러한 결함은 위협이 은밀히 침투하기에 적합한 발판이 됩니다 .

혁신을 거듭하는 공격자에 맞서기 위해서는 의료기관도 자가 학습 AI 를 활용해 새로운 지능형 사이버 위협을 자율적으로 탐지하고 대응해야 합니다 .

> “자율 대응 (Autonomous Response) 은 예측할 수 없이 빠르게 움직이는 위협을 차단해 피해 발생을 사전에 방지하는 새로운 보안 표준이 될 것입니다 .”
>
> Milton Keynes Hospital, CTO, Craig York

자율적으로 방어하는 보건의료 기관

세계 최고 수준의 혁신성을 자랑하는 미래지향적인 의료 기관에서 사용하는 Darktrace Cyber AI 는 전체 디지털 에코시스템을 보호합니다 . 자가 학습 방식의 AI 기술은 사전 공격 데이터에 의존하지 않고도 기계 속도로 움직이는 공격과 내부자 위협을 실시간으로 식별하고 대응할 수 있습니다 .

Darktrace 는 인간의 면역 체계를 응용해 조직 내 모든 사용자와 디바이스의 디지털 DNA 와 이들 간 모든 연결 상태를 학습합니다 . AI 는 그러한 '고유 환경' 에 대한 이해를 바탕으로 , 눈에 거의 띄지 않는 새로운 위협의 징후까지 탐지해 악의적인 활동을 무력화할 수 있습니다 . 클라우드 , SaaS, 의료 IoT, 이메일 , 엔드포인트 디바이스 및 기존 네트워크 전반에서 실행되는 Darktrace 는 조직의 민감한 환자 데이터와 디지털 시스템을 어느 위치에서나 보호할 수 있습니다 .

오늘날 새로운 위협의 시대에 , 기계 속도로 움직이는 사이버 위협을 자율적으로 차단할 수 있는 Darktrace 는 DDos 공격과 랜섬웨어 발생 시 특히 중요한 역할을 합니다 . 자율 대응 (Autonomous Response) 기술은 신속한 표적 대응을 통해 정상적인 활동을 중단시키지 않고도 새로운 위협을 차단합니다 . 매우 비정상적이고 의심스러운 디바이스와 직원 행동만 금지됩니다 . 생명과 직결되는 환자 진료는 평소처럼 지속할 수 있으며 그동안 전방위적인 사이버 범죄 활동은 신속히 무력화됩니다 .

위협 발견 : 암호화가 일어나기 전 Maze 랜섬웨어 탐지

Darktrace Cyber AI 는 의료 기관을 표적으로 한 메이즈 (Maze) 랜섬웨어를 탐지해 피해 발생 전 보안 팀에 이 사실을 알렸습니다 .

네트워크 스캔 활동 및 열거 (enumeration) 로 공격이 시작된 후 관리자 수준의 자격 증명과 비정상적인 RDP 활동 및 다양한 Kerberos 인증 시도가 이어졌습니다 . 그러자 Darktrace 는 일괄 처리 파일이 여러 파일 공유에 쓰여지기 전에 공격자가 도메인 컨트롤러를 업로드하는 것을 발견했습니다 .

그런 후 감염된 디바이스가 mazedecrypt[.] top 에 연결됐고 , TOR 브라우저 번들이 다운로드되면서 R&D 서브넷의 대량의 민감한 데이터가 희귀 도메인에 업로드되었습니다 .

Darktrace AI 는 이러한 공격의 각 단계를 탐지해 보안 팀에 정확도가 높은 여러 건의 경고를 발령함으로써 암호화가 시작되기 전에 위협을 차단할 수 있었습니다 .

"Darktrace 의 완벽한 가시성 , 조기 위협 탐지 , 이상 징후에 대한 스마트한 우선순위 설정 기능을 활용해 아주 미세한 사이버 공격까지도 차단할 수있었습니다 ."

Swope Health Services, CIO, Brian Thomas

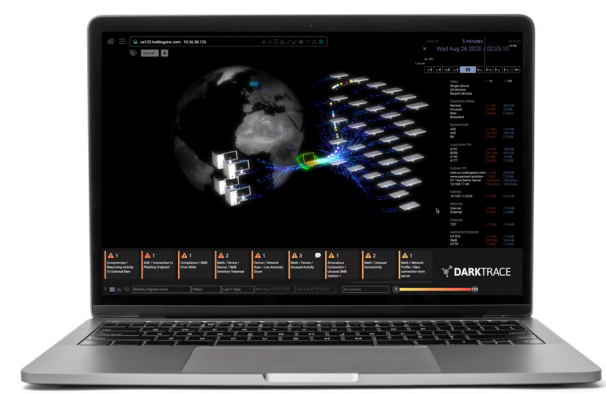
숫자로 보는 위협 현황

보건의료 데이터 침해에 따른 비용은 평균 713 만 달러에 달합니다 .

4,000+

랜섬웨어 일일 공격 건수 4,000+ (2016~2020 년)

2025 년 사이버 범죄비용은 10 조 5 천억 달러로전망됩니다 .



자율적으로 위협을 무력화해 악의적인 활동을 정확히 차단하는 Darktrace Antigena