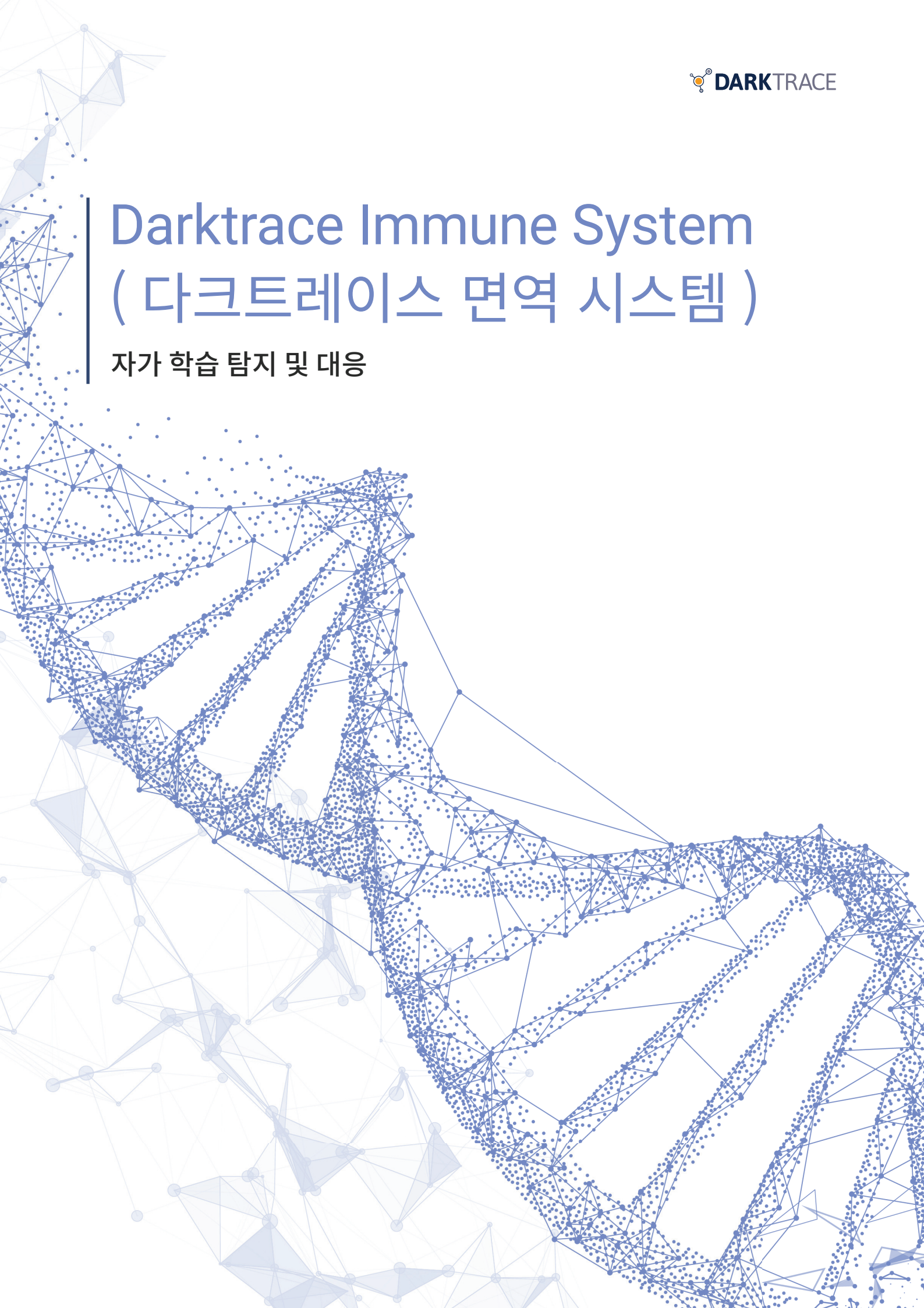
DARKTRACE

Darktrace Immune System
(다크트레이스 면역 시스템)

자가 학습 탐지 및 대응



현재 이메일 위협 환경

목차

디지털 시대의 비즈니스 리더들은 자동화된 사이버 위협이 빠르게 확산되면서 중요 데이터의 도난 및 조작에서 비즈니스 중단으로 인한 막대한 손실에 이르기까지 매우 긴급한 위험 요인에 직면하고 있습니다. 지능형 위협이 점차 늘어나고, 디지털 비즈니스의 복잡성과 다양성, 규모가 확대되면서 이러한 위험이 최근 몇 년 간 급격히 증가했습니다.

과거에는 위협 행위자가 지금처럼 지능적이지 않고 디지털 활동이 예측 가능한 경우가 많아, 기존의 보안 방식으로도 충분히 사이버 위협을 차단하기가 쉬웠습니다. 조직은 정적 규칙들과 과거의 공격 데이터로 보안 툴을 구성하여, 위협이 '무해' 한지 또는 '악성' 인지를 정의해 사전에 탐지하고자 했습니다. 규칙에 따라 이러한 위협이 공격으로 간주되거나, 널리 관측되는 위협을 나중에 탐지할 수 있도록 리버스 엔지니어링 (reverse engineering) 방식으로 발견하는 방식이었습니다.

그러나 새로운 외부 공격과 내부자 위협의 발생 빈도가 점점 증가하고 디지털 자산의 복잡성이 기하급수적으로 높아지면서, 기존 제어 방식에만 의지하던 보안 팀은 점점 보안 위협에 취약해지게 되었습니다. 이처럼 경직된 방어 체계가 정교한 사이버 범죄자들의 새로운 공격 전술과 기법을 탐지하지 못하면서, 위협이 단 몇 초만에 네트워크 트래픽 사이에 섞여 대규모의 복잡한 인프라 전반에 침투할 수 있게 되었습니다.

보안 팀은 기업 IT 네트워크 외에도 SaaS 애플리케이션과 클라우드 워크로드, 산업 장비 및 이메일 플랫폼 등 각종 단편화된 구성 요소를 보호해야 하는 데다가, 이 모든 요소에는 복잡하고 호환되지 않는 자체 제어 기능이 있는 상황입니다. 이처럼 다양한 환경 전반에서 직원 행동이 밀접하게 연관되면서 포인트 솔루션이 동작할 수 없게 되었습니다. 조직 전체에서 전개되는 위협을 포착하는 데 필요한 통합 보안 범위가 제한적이기 때문입니다.

표적 공격이 침투할 수밖에 없는 환경에서, 방어자가 이미 기업 내에 침투한 새로운 위협을 탐지하고 대응해 위기로 확산되기 전에 이를 차단하려면 어떻게 대비해야 하는가의 문제로 업계의 관심이 옮겨갔습니다. 디지털 복잡성으로 어려움을 겪는 다른 수많은 분야와 마찬가지로 비즈니스 리더와 보안 팀은 결국 인공 지능을 활용해 새로운 환경에 대응하게 되었습니다.

Darktrace Immune System (다크트레이스 면역 시스템)

자가 학습 방식

기존 방어 체계가 위협을 사전에 정의하는 데 반해 Darktrace 는 개별 기업의 정상적인 '행동 패턴' 을 학습하고 위협의 징후를 나타내는 미세한 이상 행동을 탐지하는 데 집중합니다 . 이러한 기술은 인간의 면역 체계와 마찬가지로 원래 위치에서 데이터 및 활동을 관찰하여 '자가 학습' 을 수행합니다 . 이는 새로운 정보를 반영하여 수십억 회에 달하는 확률 기반 계산을 수행하고 비즈니스의 변화에 맞춰 지속적으로 학습한다는 의미입니다 .

조직에 침투하는 위협은 기존의 공격이라기보다는 기존 방어 체계를 우회한 새로운 위협이거나 부적절하게 행동하는 직원 및 제 3 자인 경우가 일반적입니다 . Darktrace 의 면역 시스템은 조직 전체의 '고유 상태' 에 대한 감각을 학습함으로써 이전에 관찰된 적 없는 미세한 위협을 새롭게 발견하는데 , 이는 다른 방식으로는 탐지하기 어렵습니다 .

Darktrace 의 핵심 탐지 엔진은 비지도 머신 러닝을 사용해 보호 중인 각 조직의 '정상' 상태를 동적으로 파악합니다 . 면역 시스템은 규칙이나 시그니처 , 정해진 기준 , 학습 데이터 등을 사용하기 보다는 끊임없이 변화하는 디지털 환경을 학습하여 , 모든 사용자와 디바이스 및 이들 간 모든 복잡한 관계의 고유한 특징을 다차원적으로 파악합니다 .

이처럼 독보적인 자가 학습 방식을 통해 Darktrace 는 새로운 유형의 랜섬웨어 또는 내부자 공격을 비롯해 조직적인 스피어 피싱 캠페인이나 중대한 클라우드 구성 오류 등 지능형 공격이 위기로 확산되기 전에 이를 초기 단계에서 탐지합니다 .

Threat Visualizer

Darktrace 의 Threat Visualizer 는 이메일 , 클라우드 및 기업 네트워크 전반에서 단일 창에 인사이트를 표시하여 전체 디지털 인프라에 대한 실시간 가시성을 제공합니다 . 이처럼 직관적이고 사용하기 쉬운 그래픽 인터페이스를 통해 사이버 위협을 시각화하고 조사 정보를 간단히 제시합니다 . Threat Visualizer 를 사용하면 회귀 분석을 통해 사고 발생 시점으로 돌아가 실시간으로 이벤트 전개 상황을 확인할 수 있습니다 . 가장 관련성이 높은 위협만 제시되므로 사고의 우선순위를 설정할 수 있으며 , 모든 단일 이벤트의 세부 상황을 보다 심층적으로 파악할 수 있습니다 .

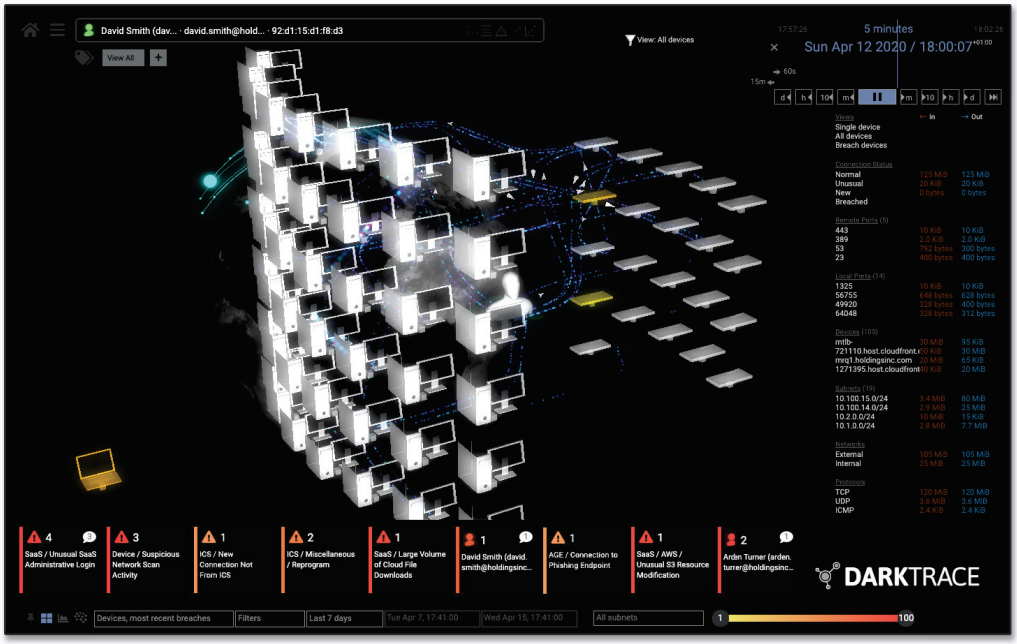


그림 1: Threat Visualizer 맨 아래의 위협 트레이에 디지털 비즈니스 전체에서 식별된

자율 대응

Darktrace 는 Darktrace Antigena 를 비롯해 세계 최초로 검증된 자율 대응 기술을 출시했습니다 .

Darktrace 는 이러한 혁신을 통해 진화하면서 진행 중인 공격을 탐지할 뿐만 아니라 피해가 발생하기 전에 이를 지능적으로 차단했습니다 . Darktrace Antigena 는 전체 디지털 비즈니스에 대한 Enterprise Immune System(기업 면역 시스템) 의 풍부한 정보를 사용하여 신속한 표적 대응을 통해 정밀하게 공격을 차단하며 , 표적형 위협 또는 전혀 알려지지 않은 위협도 무력화합니다 .

Antigena 는 광범위한 검역소 생성으로 추가 운영 중단을 유발하기 보다는 감염된 디바이스나 보안이 침해된 사용자의 정상적인 '행동 패턴'을 정확히 실행하여 몇 초만에 위협을 무력화하고 기본적으로 정상적인 운영을 유지합니다 . 이처럼 자율적으로 수행되는 대응은 세부적인 수준에서 이루어질 뿐만 아니라 위협 진행에 따른 심각도를 파악해 동적으로 환경에 적응합니다 .

Darktrace Antigena 는 이러한 전술적 보호를 넘어 전체 보안 스택의 'AI 두뇌' 역할을 수행하는 전략적 대응을 통해 , 신뢰도 높은 탐지 결과를 활용하므로 대응 메커니즘으로서의 인라인 (inline) 방어를 이전하고 통합할 수 있게 됩니다 . Antigena 는 능동적인 통합 방식으로 원활히 기존 에코시스템에 연결되어 이를 강화함으로써 네트워크에 침입한 공격자의 존재를 방화벽과 네트워크 디바이스에 알릴 수 있습니다 .

Cyber AI 는 자율 대응 기술로 Darktrace 의 핵심적인 Immune System(면역 시스템) 을 활용해 방어자에게 주도권을 다시 넘겨주어 , 가장 복잡하고 취약한 조직도 복원력을 갖춘 자가 방어 디지털 비즈니스로 변화하도록 지원합니다 .

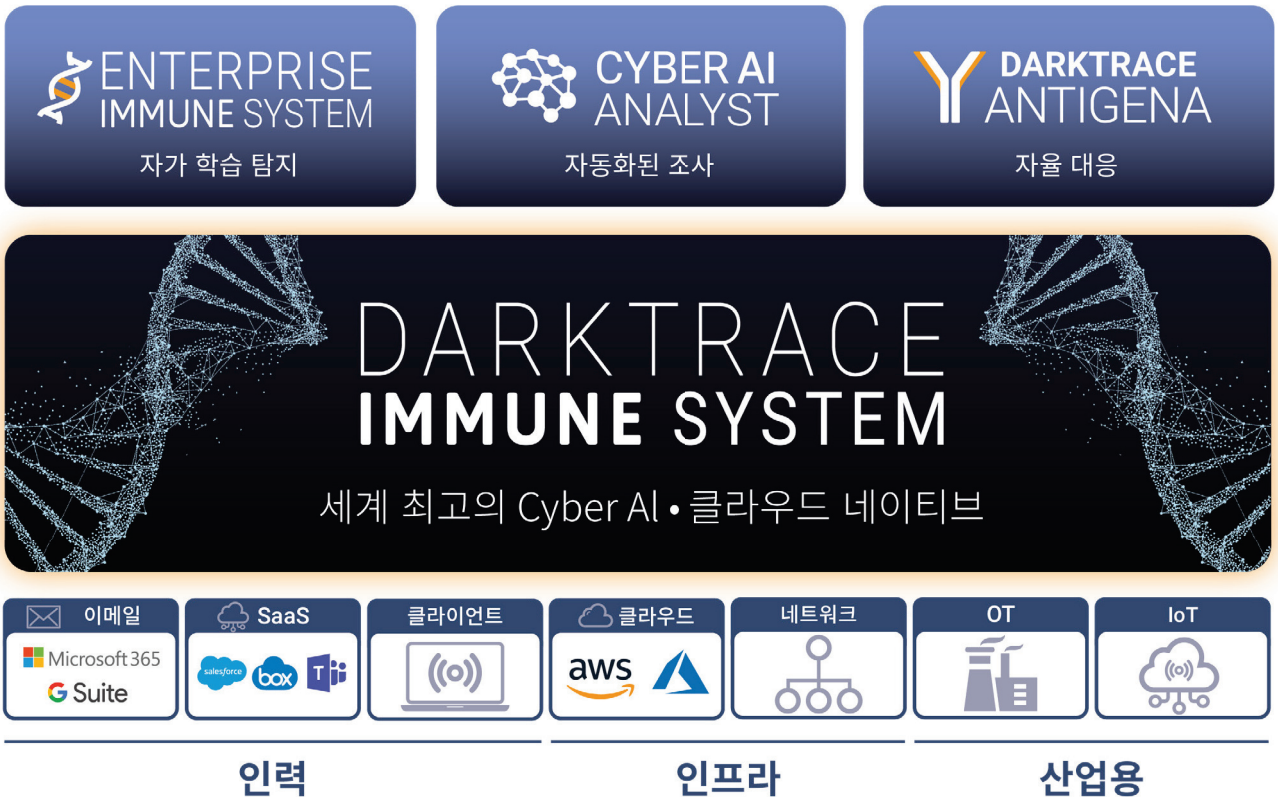


그림 2: Darktrace Immune System(다크트레이스 면역 시스템)

Cyber AI Analyst

Darktrace 의 Immune System(면역 시스템) 과 Antigena 가 탐지 및 대응 시간을 단축하는 데 비해 , Cyber AI Analyst 는 최초로 위협 조사를 완전히 자동화하여 상황 파악에 걸리는 시간을 급격히 줄였습니다 .

보안 팀 내 분석가들은 보통 단서를 추적하고 가설을 수립하고 결론에 도달하면 기업 내 나머지 부서와 조사 결과를 공유하는 식으로 위협을 조사합니다 . 이는 노동 집약적인 단계라 할 수 있습니다 . 시간과 전문성을 요하는 데다가 기계 속도로 빠르게 움직이는 위협에 대응해야 하는 경우가 많지만 , 사람이 대응하는 데에는 기본적으로 한계가 있기 때문에 이를 뛰어 넘기가 쉽지 않기 때문입니다 . Cyber AI Analyst 는 전문 분석가의 직관력을 AI 의 속도 및 확장성과 결합하여 , 이러한 한계를 AI 기반 조사를 통해 극복합니다 . 그 결과 사고 분류 시간이 최대 92% 단축되었습니다 .

Darktrace 의 Immune System(면역 시스템) 이 의심스러운 행동 패턴을 탐지하면 Cyber AI Analyst 는 전사적 조사를 시작하고 다양한 이상 징후를 연계함으로써 광범위한 보안 사고의 속성과 근본 원인에 대한 개략적인 결론을 도출합니다 . AI 는 한 번에 어디서나 동작 가능하므로 동시에 수 천개의 쿼리를 생성하고 수 백개의 병렬 스레드를 팔로우하여 실시간으로 전체 사고 범위를 신속하게 밝힐 수 있습니다 .

무엇보다도 Cyber AI Analyst 는 빠르게 대규모로 분석 워크플로우를 자동화할 뿐만 아니라 사람의 전문성이 가진 기본적인 유연함을 유지합니다 . 이는 사전 정의된 플레이북으로 캡처할 수 없는 혁신적인 공격 기법이 특징인 보안 사고를 시스템이 해석하고 이에 대해 보고할 수 있다는 의미입니다 .

Cyber AI Analyst 는 Darktrace 의 Immune System(면역 시스템) 이 탐지하는 보안 이벤트를 빠짐없이 지속적으로 조사하여 리소스가 부족한 보안 팀이 즉시 대응할 수 있도록 서면 보고서와 동적인 상황 대시보드를 생성합니다 .

제로데이 취약점 공격을 차단하는 Darktrace Cyber AI Analyst

최근 여러 Darktrace 고객사가 Zoho ManageEngine 의 제로데이 취약점인 CVE-2020-10189 를 표적으로 한 공격을 받았을 때 , Cyber AI Analyst 가 결정적인 역할을 한 것으로 나타났습니다 . 나중에 중국의 위협 행위자인 APT41 이 침입을 시도했으며 , 이는 그러한 취약점으로 인한 기회를 틈타 가능한 많은 기업에 처음으로 액세스를 시도하려 한 더 큰 공격의 일부였다는 사실이 밝혀졌습니다 .

Darktrace 는 공격이 시작되자마자 그러한 공격을 자동으로 탐지해 조사했고 , 이를 통해 고객은 위협을 억제하여 피해를 방지할 수 있었습니다 . Cyber AI Analyst 가 생성한 보고서에는 유용한 보안 전략 형태로 사고의 모든 측면에 대한 주요 특징과 설명이 담겨 있었습니다 . 신입 보안 담당자도 이러한 결과를 검토해 5 분 내에 이러한 제로데이 APT 공격에 대응할 수 있을 만한 내용이었습니다 .

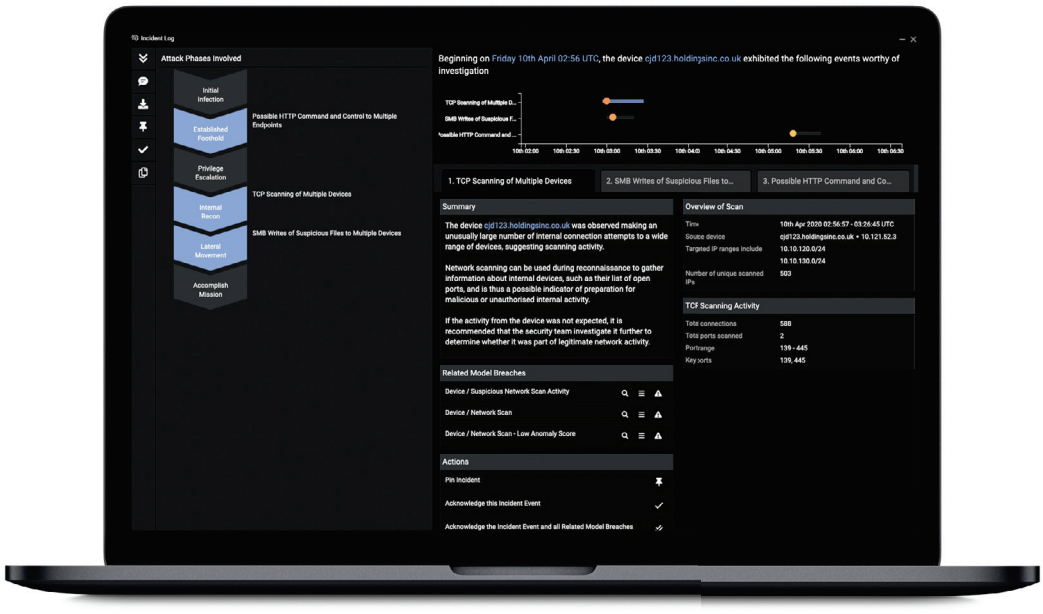


그림 3: Cyber AI Analyst 가 생성한 공격 단계별 사고 개요

전사적 보호

위협 행위자들이 점점 한번에 하나 이상의 기술을 공격에 활용하면서 , 방어자가 전체 디지털 비즈니스를 통합적으로 보호해야 하는 상황이 되었습니다 . 비밀번호 유출처럼 간단한 사고도 한번에 여러 시설에 대한 공격을 유발할 수 있게 된 것입니다 . Darktrace 의 Immune System(면역 시스템) 은 다양한 고립형 시스템에 활용할 수 있도록 설계되어 , 통합 탐지 및 대응을 지원하고 이메일과 클라우드 및 기업 네트워크 전체를 보호할 수 있습니다 .

이처럼 다양한 환경 전반의 인사이트가 동일한 통합 보기로 표시될 뿐만 아니라 배경에서 단일 AI 엔진이 이러한 인사이트를 통합하고 상관성을 분석합니다 . 이러한 설계 원칙은 디바이스 또는 사용자의 정상 패턴의 전체 범위가 조직의 다양한 부분에서 나타나며 , 단일 보안 사고에는 보통 디지털 환경 내 다른 곳에서 발생하는 관련 이벤트와 지표가 포함된다는 사실을 기반으로 합니다 . 기술별 단위 보안을 처리하는 것은 더이상 의미가 없기 때문에 , 실시간으로 이를 확인할 수 있어야 보다 효율적으로 사고를 관리할 수 있습니다 .

Darktrace 는 탐지 및 대응 통합 외에도 완벽한 가시성 지원을 중요하게 생각합니다 . 오늘날 보안 팀은 언제든지 툴링을 통해 보안 경고 생성 외에도 손쉽게 다양한 환경을 살펴보고 이를 파악할 수 있어야 합니다 .

아래의 실제 사례 연구에는 Darktrace 의 Immune System(면역 시스템) 이 클라우드 , SaaS, 이메일 , 산업 및 기업 네트워크 전반에서 '정상' 상태를 통합적으로 파악하여 공격을 식별한 것으로 나타납니다 .

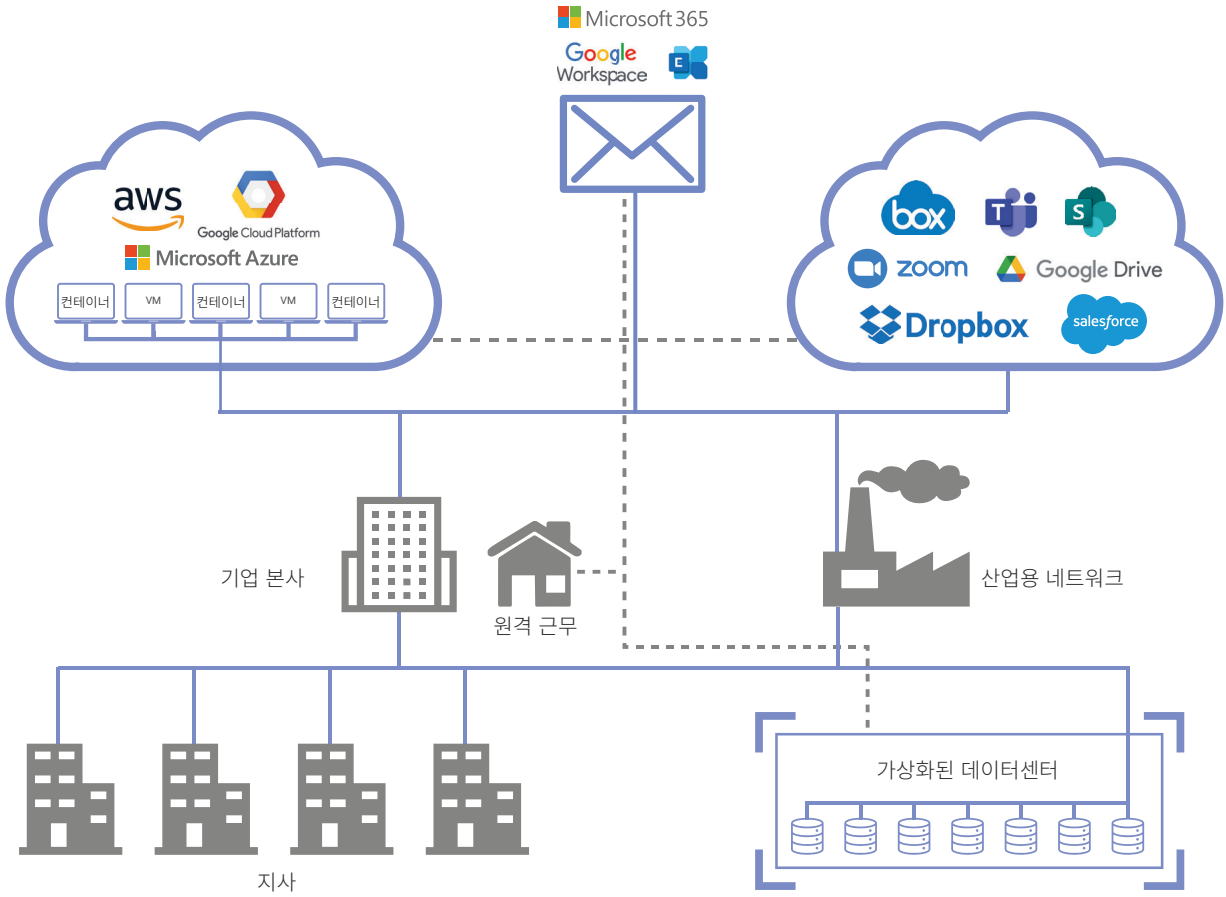
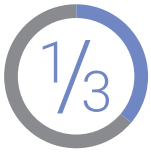


그림 4: 전체 디지털 비즈니스 전반의 Darktrace 개요

클라우드 및 SaaS 를 위한 Cyber AI



클라우드 환경 전반에서 비정상적인 행동을 모니터링하는 기업은 1/3 이채 되지 않습니다

출처: Cybersecurity Insiders

클라우드로의 대규모 이전을 통해 근본적으로 디지털 비즈니스와 네트워크 경계의 기존 패러다임이 재편되었습니다 . 하이브리드 인프라와 분산된 업무 환경에서 일하는 직원들은 이제 점점 다양해지는 디지털 자산의 구성 요소가 되고 멀티클라우드 방식으로 인해 새로운 층위의 복잡성이 더해졌으나 , 대다수의 조직은 이에 대응하기에 역부족입니다 .

보안 팀은 클라우드 내 가시성과 제어 기능 부족으로 어려움을 겪고 있을 뿐만 아니라 호환 불가능한 다양한 방어 체계로 인해 권한 수준이 지나치게 낮아지고 단순 오류가 발생하는 경우가 많습니다 . 이와 같은 기존의 '고립형 (stovepipe)' 방식은 보안 범위가 충분하지 않아 강력한 통합 보안이라고 하기에는 어려우며 , 정적이고 사일로화된 방식으로 인해 보안이 침해된 크리덴셜과 내부자 위협 및 중대한 구성 오류를 탐지하지 못합니다 .

Darktrace 의 Immune System(면역 시스템) 은 이메일 , 클라우드 및 기업 네트워크에 나타나는 분산되고 예측 불가능한 행동을 동적으로 분석하는 등 모든 레이어에서 ' 정상' 상태를 파악하는 자가 학습 AI 를 통해 이러한 격차를 해소합니다 . 이처럼 보안 범위가 통합되면 시스템은 AWS 에서의 비정상적인 리소스 생성 또는 개방형 S3 버킷 , Salesforce 에서의 의심스러운 데이터 이동 , Microsoft 365 에서의 새로운 수신함 규칙 또는 처음 보는 로그인 위치 등 위협의 징후를 나타내는 미세한 이상 행동을 발견할 수 있습니다 .

정책 기반 제어와 달리 면역 체계 방식은 지능형 공격을 나타내는 미약한 신호들의 상관성을 분석할 수 있는 통합 탐지 엔진을 제공하여 , 클라우드에서 모든 신뢰할 수 있는 계정의 사용자를 파악합니다 .

그림 5: Darktrace 의 전용 SaaS 콘솔에는 SaaS 애플리케이션의 비정상적 행동에 대한 개요가 나타나고 활동의 지리적 위치가 표시됨

Microsoft 365 보안 침해 및 SharePoint 침입

Darktrace Cyber AI 는 한 미국 보험사의 SaaS 플랫폼 전반에서 '정상' 상태를 맞춤식으로 파악하고 가시성을 확보하여 보안이 침해된 Microsoft 365 계정에서 시작된 공격을 차단하는 데 핵심 역할을 수행했습니다 .

위협 행위자가 아랍에미리트의 IP 주소에서 고객의 Microsoft 365 계정에 로그인하자 , Cyber AI 는 해당 행동을 비정상이라 판단했습니다 . 다른 Microsoft 365 계정에서는 IP 로 로그인된 적이 없었기 때문입니다 . 4 일 후 보기 드문 다른 아랍에미리트 IP 에서 보안이 침해된 동일 계정에 액세스하는 것이 관찰되었습니다 . 이번에는 위협 행위자가 새로운 이메일 규칙을 설정한 데다가 비정상적인 액세스 권한을 사용해 해당 사용자의 개인 SharePoint 계정에서 파일을 읽고 썼습니다 .

Darktrace Cyber AI 는 이러한 사고에서 확인된 특정 네트워크의 아랍에미리트 IP 와 통신하는 다른 사용자 계정을 이전에 관찰한 적이 없었습니다 . 이는 관찰된 행동이 고객이라 보기에는 매우 비정상적이며 보안 침해의 결과임을 나타냅니다 .

고객의 레거시 툴을 사용하면 보안이 침해된 계정에 변경이 이루어진 경우 위협 탐지만 가능하지만 , Cyber AI 는 비정상적인 행동이 발생하자마자 이를 즉시 탐지해 SaaS 서비스 간 공격자의 움직임을 명확하게 밝혀냅니다 . Darktrace 는 공격 초기 단계에 즉시 보안 팀에게 공격을 알려 , 모든 상세 정보를 명확히 제시하고 해당 위협으로 인해 심각한 피해가 발생하기 전에 이를 무력화시켰습니다 .

클라우드 구성 오류

유럽의 한 유명 제조업체는 Microsoft Azure 서버를 사용하여 제품 상세 정보와 예상 매출액에 관한 내용이 담긴 파일을 저장했습니다 . 서버에 있는 파일과 루트 IP 를 사용자 이름과 비밀번호로 제어하면서도 이처럼 민감한 데이터를 암호화되지 않은 상태로 두었습니다 . 디바이스가 보기 드문 외부 IP 주소에서 ZIP 파일을 다운받았을 때 , Darktrace 는 매우 비정상적이라 판단한 이상 활동을 탐지하게 되었습니다 .

나중에 외부 IP 는 새로 설정된 Microsoft Azure 서버였으며 , URL 을 아는 누구나 ZIP 파일에 액세스할 수 있다는 사실이 밝혀졌습니다 . 내부 또는 외부에서 네트워크 트래픽을 가로채기만 하면 URL 정보를 얻을 수 있었던 것입니다 . 보다 집요한 공격자들은 URL 의 파일 '핵심' 매개 변수에 무차별 대입 공격을 감행했을 수도 있었습니다 .

문제가 된 민감한 파일의 손실 또는 유출로 인해 전체 제품 라인이 위험해질 수도 있었지만 Darktrace 는 이 사고를 탐지 즉시 보고하여 귀중한 지적 재산권 손실을 방지하도록 지원했으며 , 제품 정보 보호를 지속적으로 개선하기 위해 보안 팀이 클라우드 내 데이터 스토리지 관행을 변경하도록 했습니다 .

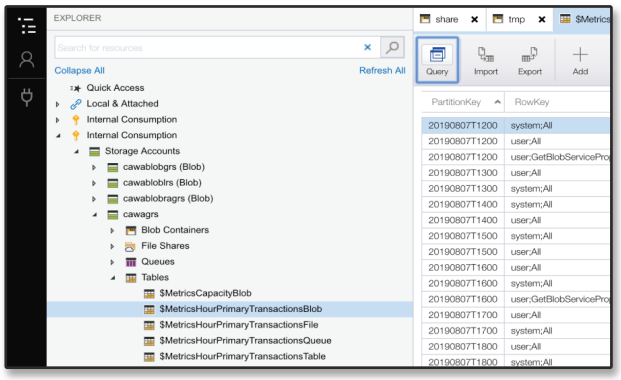


그림 6: Azure 의 민감한 파일

의심스러운 Box 파일 다운로드

한 글로벌 농산물 공급 업체의 Box 플랫폼 내에서 의심스러운 요청이 수 차례 이어졌는데 , 이는 사용자 계정의 보안 침해를 나타내는 것이었습니다 .

해당 계정을 사용한 행위자는 Box 에 성공적으로 로그인한 후 비용 보고서 , 청구서 및 기타 재무 문서를 다운로드했습니다 . 잠재적인 위협 행위자는 민감한 비밀번호 목록이 포함된 파일의 잠금까지 해제했습니다 .

Cyber AI 는 해당 조직의 모든 개별 직원에 대한 '고유 상태' 를 맞춤식으로 파악하여 위협을 즉시 식별할 수 있었습니다 . Darktrace 의 Immune System(면역 시스템) 은 정상적인 사용자가 아주 이례적인 시간에 활동했음을 탐지했으며 , 행위자의 IP 주소 또한 해당 직원이 이 특정 SaaS 서비스를 사용하던 과거 액세스 위치와 비교할 때 매우 비정상적이라는 사실을 파악했습니다 .

다른 문맥에서 보면 해당 직원이 이러한 문서에 액세스하는 것이 정상이라 생각되었겠지만 , Box 내 사용자 행동에 대한 Darktrace Cyber AI 의 심층적인 이해와 세부적인 가시성 덕분에 계정 보안 침해의 미세한 징후를 발견할 수 있었습니다 . Cyber AI Analyst 는 자율적인 조사를 통해 폭넓게 사고 내용을 밝히면서 , 각각의 무단 파일 노출이 연결된 사고의 일부라는 사실을 파악하고 보안 침해를 보안 팀의 주요 우려 사항으로 강조했습니다 .

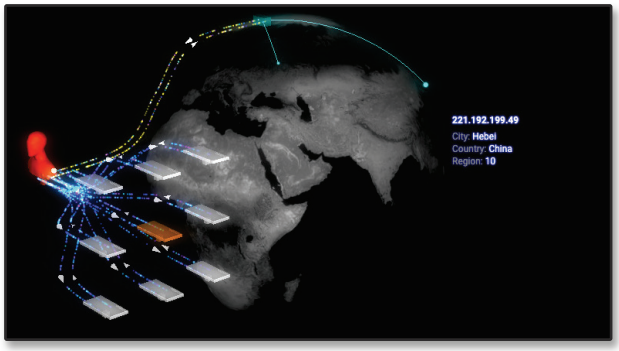


그림 7: 비정상적인 IP 주소 위치를 보여주는 Darktrace

Microsoft 365에서 '불가능한 이동' 규칙을 우회하는 공격

한 국제 비영리 단체에서 Darktrace 는 Azure AD 의 정적인 '불가능한 이동' 규칙을 우회한 Microsoft 365 계정 탈취를 탐지했습니다 . 해당 단체는 전세계에 사무소를 두고 있었는데 , Darktrace 의 자가 학습 AI 가 과거 기록을 바탕으로 해당 사용자와 동료들이 거의 사용하지 않는 한 IP 주소에서 로그인이 발생한 것을 확인하고 보안 팀에 이를 즉시 경고했습니다 .

Darktrace 는 이후 인바운드 및 아웃바운드 이메일을 삭제하는 새로운 이메일 처리 규칙이 해당 계정에 설정됐다는 사실을 알렸습니다 . 이는 보안 침해의 명백한 징후였으며 보안 팀은 공격자가 피해를 주기 전에 계정을 잠금 처리할 수 있었습니다 .

이 새로운 이메일 처리 규칙을 설정하여 공격자는 정상적인 사용자가 모르게 회사 내 다른 직원들과 수차례 연락을 시도했습니다 . 이는 영구적인 액세스 권한을 얻어 조직 내 다양한 거점을 활용하려는 사이버 범죄자들이 흔히 사용하는 수법으로 , 대규모 공격을 준비하는 상황일 수 있습니다 .

Darktrace 는 확실한 사용자의 평소와 다른 행동과 보기 드문 IP 주소를 분석하여 이를 명백한 계정 탈취 사례로 식별함으로써 기업에 심각한 피해를 방지했습니다 .

> **Darktrace 는 Azure AD 의 정적인 '불가능한 이동' 규칙을 우회한 Microsoft 365 계정 탈취를 탐지했습니다 .**

Microsoft 365 및 팀 전반의 보안 침해

최근 미국의 한 공인 회계 법인에서 Microsoft 365 계정의 보안 침해가 발생했습니다 . Darktrace 는 처음에 아웃바운드 이메일 트랙픽 급증과 비정상적인 로그인 위치 등 몇 가지 이상징후를 포착했습니다 . 해당 법인과 거의 모든 사용자들은 미국 위스콘신에 있었는데 , 캔사스에 위치한 IP 주소가 해당 Microsoft 365 계정에 로그인하는 데 사용된 것으로 나타난 것이었습니다 . 비정상적인 로그인 외에도 동일한 캔사스 IP 주소에서 Microsoft Teams 에 로그인한 기록이 탐지되었습니다 .

그림 8: 새로운 이메일 규칙이 생성된 직후 처음 보는 IP 주소에서 Microsoft Teams 에 로그인 발생

'불가능한 이동' 규칙만 적용되었다면 이러한 징후를 놓쳤겠지만 , 다양한 SaaS 애플리케이션 전반의 활동과 행동에 대한 정보를 활용해 Darktrace 의 AI 는 이러한 이벤트를 자격 증명 도난의 전형적인 사례로 인식할 수 있었습니다 . 해당 위협 행위자가 곧이어 새로운 이메일 규칙을 생성하자 Darktrace 는 이 이벤트를 다른 비정상적인 행동과 연관지어 악성일 가능성을 파악할 수 있었습니다 .

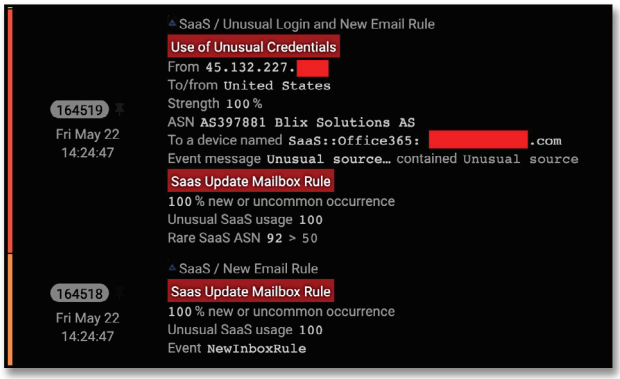


그림 9: Darktrace 의 SaaS 모듈은 다른 사용자들은 접속하지 않고 , 내부 시스템에서 처음 보는 IP 주소에서 사용자의 Microsoft 365 계정에 로그인되어 새로운 수신함 규칙이 생성된 것을 발견 . 모든 요소가 100% 비정상적인 SaaS 활동을 나타냄

5 분 후 Antigena Email 은 흔한 제목에 PDF 파일이 첨부된 대량의 아웃바운드 이메일을 경고하는 알림을 전송했습니다 . 뿐만 아니라 이 사용자의 아웃바운드 이메일 전송량이 급증했음을 탐지하고 이러한 이메일 각각에 "OOC(Out of Character)" 태그로 플래그를 지정했습니다 . 이는 정상적인 행동에서 벗어나 수신자 수가 급증했으며 내부 보안이 침해됐을 가능성을 뜻하는 것이었습니다 .

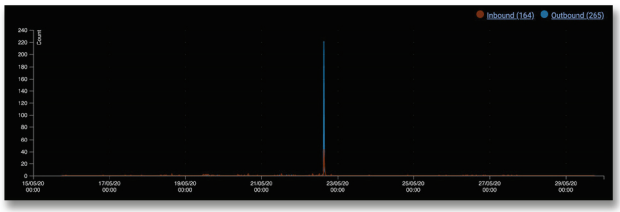


그림 10: Antigena Email 이 사용자의 정상 행동을 심각하게 위반했음을 나타내는 수신자 수 급증 탐지

Darktrace 의 SaaS Module 이 탐지한 이례적인 로그인 행동은 Antigena Email 이 플래그를 지정한 비정상적인 아웃바운드 이메일 행동과 연계됐을 가능성이 있었으므로 , 보안 팀은 공격이 시작되자 공격의 규모를 확인하고 이를 무력화했습니다 . 해당 계정이 악성 활동에 활용되고 있는 것이 분명했습니다 . 220 개 아웃바운드 이메일은 모두 흔한 제목에 의심스러운 첨부 파일이 포함되어 있었기 때문입니다 . 따라서 보안 팀은 즉시 보안이 침해된 계정을 비활성화했습니다 .

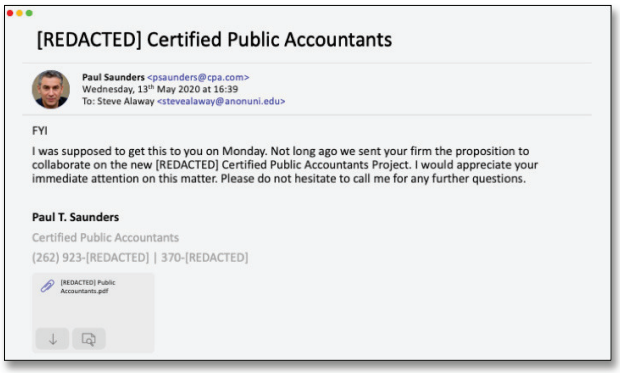


그림 11: 공격자가 전송한 이메일 수정본에포함된 악성 첨부파일

이메일을 위한 Cyber AI

94%

사이버 위협의 94% 는 이메일을 통해 조직에 침투

출처: 데이터 보안 침해 조사 보고서

사이버 범죄자들은 이메일을 스푸핑하거나 신뢰할 수 있는 계정을 해킹해 사용자를 속여 기업 계정에서 거액을 송금하거나 클릭 한 번으로 랜섬웨어 공격을 트리거하도록 합니다 . 기존 이메일 제어는 네이티브 방식이든 타사를 통해서든 단일 시점에서 격리 상태의 이메일을 분석하고 이를 블랙리스트 , 시그니처 및 사전 정의된 '위협' 과 대조하여 상관관계를 파악하는 방식입니다 . 이러한 접근 방식은 기본 스팸 메일 및 이와 유사한 무차별적 '드라이브 바이' 캠페인을 포착할 수 있긴 하지만 , 지능형 소셜 엔지니어링 공격이나 은밀한 스피어 피싱 캠페인의 취약 지표는 대체로 탐지하지 못합니다 .

그러나 Darktrace 의 Antigena Email 은 독보적인 기술을 통해 모든 사용자와 연락처의 정상적인 '행동 패턴' 을 분석하여 이메일 통신 내에서 다양하게 변화하는 '인적 요소' 를 파악할 수 있습니다 . Cyber AI 로 지원되는 이 기술은 다른 기술과는 달리 , 수신자가 정상적인 '행동 패턴' 의 문맥 내에서 특정 이메일과 동료 및 조직 내 다른 부서와 연락하는 것이 비정상적인지를 명확하게 묻습니다 . 이처럼 다차원적으로 상황을 파악하므로 시스템은 매우 정확한 의사결정을 내리고 '정상처럼 보이는' 스푸핑 이메일에서 공급망 계정 탈취에 이르는 전방위적인 지능형 이메일 공격을 무력화할 수 있습니다 .

Antigena Email 은 모든 내외부 사용자의 동적 패턴을 학습함으로써 수평적인 내부 간 통신과 함께 인바운드 및 아웃바운드 이메일을 분석합니다 . 또한 수신자를 동적인 개인 및 피어로 취급하여 정상으로 보이는 이메일이 명백한 악성임을 밝힘으로써 '정상 상태' 에서 벗어난 미묘한 이상 행동을 탐지할 수 있습니다 .

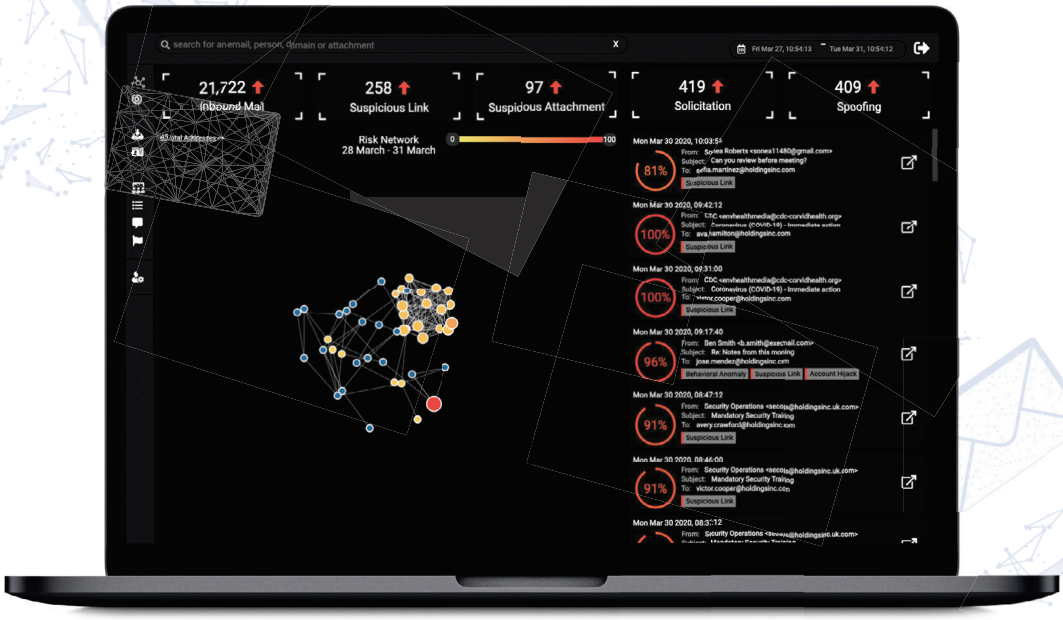


그림 12: 경고를 간략히 표시하는 Antigena Email 인터페이스

조직적인 스푸핑 공격

Darktrace 는 한 미국 기술 기업의 고위 경영진을 사칭하는 고도의 표적 소셜 엔지니어링 공격을 탐지했습니다 . 당시 위협 행위자는 지급 요청에 앞서 신뢰를 얻고 오프라인 통신을 설정하기 위해 다수의 '정상처럼 보이는' 이메일을 전송한 것으로 보입니다 . 정적 분석과 제한된 범위로 인해 레거시 이메일 방어 체계가 공격을 탐지할 수 없었던 데 비해 , Darktrace 는 다음 관찰 결과를 바탕으로 지정된 수신자에게 각 이메일이 전송되지 않도록 보류했습니다 .

1. 비정상적인 제목과 발신자 . 이메일은 제목란에 표적이 된 직원의 이름이 있었고 , 별 관련이 없어 보이는 Gmail 주소에서 전송된 것이었습니다 .

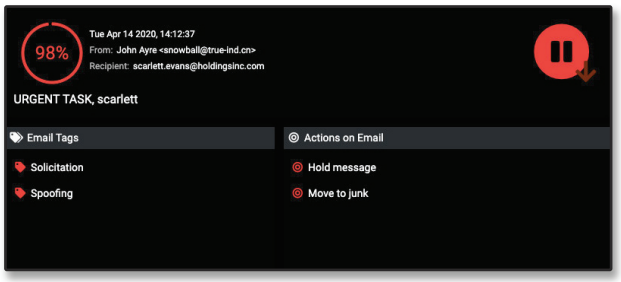


그림 13: 98% 의 이상 징후 점수를 기록한 30 개 이메일 중 하나

2. 연관성 없음 . Darktrace 가 파악한 해당 기업의 이메일 및 네트워크 환경에 대한 전체 정보를 통해 Antigena 는 이 발신자와 조직 간 아무런 관계가 없음을 확인했습니다 .

3. Whale 스푸핑 노출 . Darktrace 는 사칭을 당한 고위 경영진 3 명을 확인하고 공격자가 CEO 의 정상적인 외부 개인 주소를 스푸핑하고 있었음을 알게 되었습니다 . 뿐만 아니라 사칭을 당한 사용자의 노출 점수가 높았는데 , 이는 'Whale Spoof(Whale 스푸핑)' 공격을 당하기 쉬운 눈에 띄는 표적이었음을 나타냅니다 .

Antigena 는 이러한 여러 취약 지표의 상관성을 분석하여 , 이메일을 조직적인 공격의 구성 요소로 인식하고 조직의 보안 전문가들이 검토할 수 있도록 버퍼에 보관했습니다 . 이를 통해 표적이 된 수신자가 이메일 콘텐츠에 접근하여 오프라인 통신을 설정할 수 없도록 한 것입니다 .

공급망 계정 탈취 이메일 공격

Darktrace 는 한 다국적 에너지 기업에서 공급망 공격을 식별하고 , 발신자와 해당 회사가 잘 아는 관계였으며 여러 명의 내부 사용자가 이전에 서로 연락을 주고받은 적이 있다는 사실을 알게 되었습니다 . 일상적인 연락을 주고받은지 2 시간도 채 안되어 피싱 링크가 포함된 각 이메일이 39 명의 사용자에게 신속히 전송되었습니다 . 제목란과 링크는 조금씩 달랐는데 , 이는 철저히 준비한 공격자가 보낸 고도의 표적 이메일이었습니다 . 그러나 Antigena 는 다음의 이상 징후를 토대로 39 개의 이메일 전송을 모두 보류하고 페이로드를 이중으로 잠금처리했습니다 .

1. 비정상적인 로그인 위치 . 지리적 위치를 식별할 수 있는 IP 주소를 추출하여 , 공격자가 원래 로그인 위치인 영국이 아닌 미국 내 IP 에서 로그인하기 시작했음을 밝혀냈습니다 .

2. 링크 불일치 . 해당 링크는 모두 Microsoft Azure 개발자 플랫폼에서 호스팅되었습니다 . 이는 호스트 도메인의 평판 검사를 우회할 가능성이 높았으나 , 이전에 연락을 주고받은 기록과 조직의 네트워크 트래픽을 고려할 때 발신자와는 상당히 달랐습니다 . 다른 이메일 보안 제품은 이러한 컨텍스트 인텔리전스를 활용하지 않기 때문에 이런 결론에 도달하기가 불가능했을 것으로 보입니다 .

3. 비정상적인 수신자 . 이러한 특정 수신자 그룹이 동일한 소스에서 이메일을 수신할 가능성을 평가하기 위해 수신자의 '연관성 이상' 점수가 할당됩니다 . Darktrace 는 시간 경과에 따라 컨텍스트를 조사 결과에 추가하여 , 3 번째 이메일부터는 이러한 수신자 그룹이 100% 비정상이라고 추론했습니다 .

4. 비정상적인 주제 . 이러한 이메일의 제목란은 눈에 띄지 않게 전문가가 쓴 내용처럼 보이도록 한 시도이므로 , 피싱과 연관된 키워드를 찾으려는 시그니처 기반의 모든 대응 방식은 실패했을 것입니다 . 그러나 Darktrace 는 이러한 수신자가 대체로 이런 스타일의 문구를 이용한 사업 제안서 이메일을 받는 것은 아니라는 사실을 파악했습니다 .

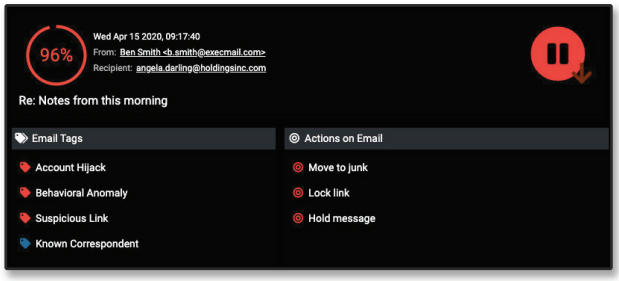
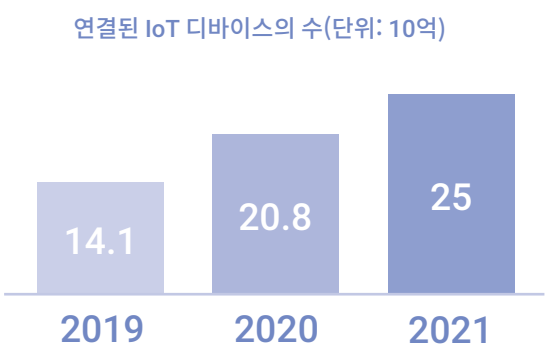


그림 14: 계정 탈취를 탐지하고 이메일 전송을 보류한 Darktrace

사물 인터넷 (IoT) 을 위한 Cyber AI



출처: Gartner

스마트 커피 머신에서 인터넷에 연결된 CCTV 카메라에 이르는 다양한 IoT 가 출현하면서 기업에 완전히 새로운 위협 벡터가 등장하게 되었습니다 . IoT 디바이스는 그 편리함과 매력으로 인기를 끌고 있으나 , 보안을 고려하지 않고 설계된 것이 대부분이라 손쉬운 침입 경로 또는 데이터 유출의 은밀한 수단이 되는 경우가 많습니다 .

보안이 지원되는 디바이스의 경우 기존 엔드포인트 보안은 알려진 위협을 차단하는 데는 유용하지만 , 예측할 수 없는 IoT 환경에 대응하려면 더욱 광범위한 기업 전략이 필요합니다 . 대부분의 경우 보안 팀은 디스크 공간 , CPU 또는 기존 운영 체제가 없는 스마트 디바이스에서 표준 안티바이러스 소프트웨어를 실행할 수 없습니다 . 게다가 스마트 디바이스에 엔드포인트 솔루션을 설치하려면 그러한 솔루션의 존재 자체를 먼저 알아야 합니다 . 그러나 대다수의 조직은 네트워크 가시성 부족으로 인해 IP 기반 IoT 디바이스는 물론 , 핵심 워크스테이션과 서버의 정확한 수를 파악하는 데 어려움이 있습니다 .

IoT 보안을 해결하려면 취약점이나 관리되는 디바이스 뿐만 아니라 디지털 비즈니스 전반에 나타나는 복잡한 행동을 모니터링하는 등 보다 포괄적으로 상황을 파악해야 합니다 . Cyber AI 를 활용하면 네트워크 내 위치에 상관없이 보유 중인 디바이스 전체를 모니터링할 수 있습니다 . Darktrace 는 모든 디바이스의 정상적인 '행동 패턴' 을 학습하여 , 스마트 수조에서 자율 주행 차량에 이르는 사물 인터넷 (IoT) 을 표적으로 하는 전방위 공격을 탐지할 수 있습니다 . Darktrace Antigena 는 이에 실시간으로 대응하며 조직 내 모든 환경에서 위협을 억제하고 위험을 완화합니다 .

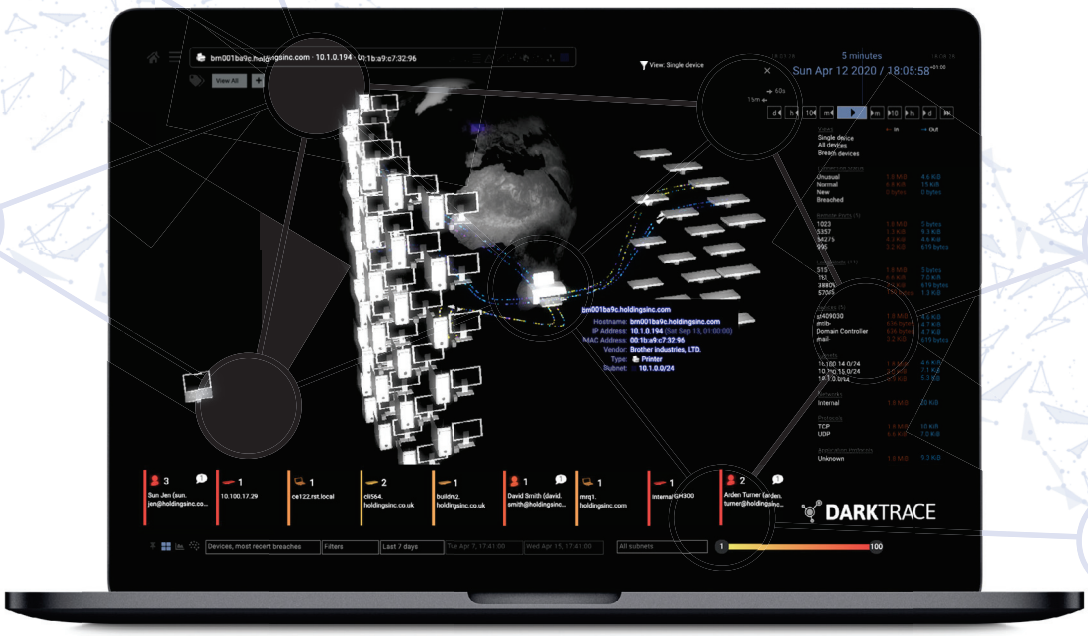


그림 15: 보안이 침해된 스마트 프린터와 비정상적인 연결 (노란색으로 표시)

CCTV 해킹을 통한 산업스파이

일본의 한 투자 자문 회사에서 Darktrace 는 인터넷에 연결된 CCTV 시스템에 알려지지 않은 공격자가 침입했다는 사실을 발견했습니다 . 공격자는 해당 디바이스를 사용해 네트워크에 거점을 확보하여 녹화된 카메라 동영상을 모두 볼 수 있었습니다 . CEO 사무실에서 중역 회의실에 이르는 사무실 전체를 모니터링하기 위해 설치된 카메라가 보안 위험 요소가 된 것입니다 .

Darktrace 의 AI 는 이상 징후를 신속히 탐지했습니다 . 대규모 데이터가 암호화되지 않은 CCTV 서버에서 송수신되는 것이 관찰되었습니다 . 공격자가 민감한 정보를 유출하기 위해 데이터를 수집하고 있었던 것입니다 . 공격자가 데이터 유출을 시도한 시점에 Antigena 는 신속하고 정밀한 방어 활동을 수행했습니다 .

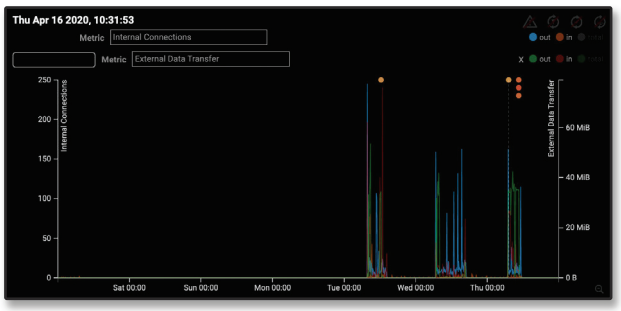


그림 16: IoT 디바이스 통신과 관련된 내외부 연결

시스템은 해당 디바이스에서 외부 서버로의 데이터 이동을 정확하게 차단하면서도 CCTV 가 원래 기능대로 계속 작동되도록 했습니다 . AI 는 기계 속도로 공격을 차단하며 시장에 민감한 정보의 심각한 보안 침해를 방지했습니다 .

Antigena 는 초기 단계에서 공격에 상응하는 대응을 통해 공격을 억제함으로써 , 보안 팀이 위협을 조사하고 문제를 해결할 수 있는 골든 타임을 확보해 피해를 방지하도록 했습니다 .

스마트 사물함을 통한 민감 데이터 유출

북미의 한 놀이 공원이 공격받는 사건이 발생했습니다 . 위협 행위자가 인터넷이 연결된 취약한 스마트 사물함을 통해 민감한 고객 정보 탈취를 시도했던 것입니다 .

기본 설정에 따라 스마트 사물함은 주기적으로 공급 업체의 타사 온라인 플랫폼에 연결되었는데 , 위협 행위자는 이처럼 자동화된 프로세스의 출처를 식별하고 이를 탈취하여 해당 디바이스의 보안을 침해했습니다 .

Darktrace 의 AI 는 사물함이 비정상적으로 많은 양의 암호화되지 않은 데이터를 희귀한 외부 사이트로 전송하기 시작하자마자 공격을 탐지했습니다 . 디바이스와 공급 업체의 플랫폼 간 주기적인 통신이 이루어지자 이에 맞춰 연결 시간이 측정되었는데 , 이는 규칙 기반의 보안 방어 체계를 우회하기 위해 설계된 '로우 앤 슬로우 (low and slow)' 공격을 나타내는 것이었습니다 .

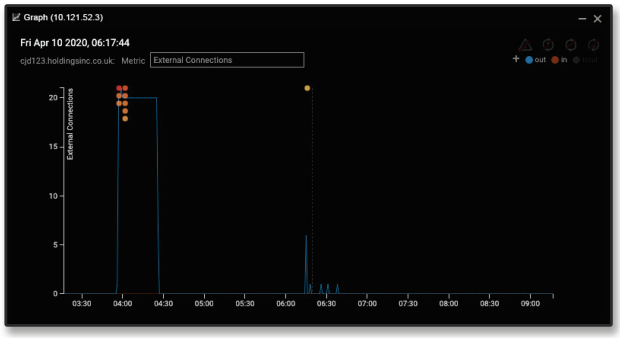


그림 17: 스마트 로커에 대한 비정상적인 수의 연결

Darktrace 의 AI 는 사물함의 이전 행동 및 피어의 행동과 관련된 통신을 지속적으로 분석하여 , AI 의 사이버 대응이 필요하다고 판단했습니다 . Darktrace Antigena 는 몇 초만에 대응을 시작하며 , 보안이 침해된 디바이스의 모든 발신 연결을 지능적으로 차단하고 , 보안 팀이 대응 시간을 확보해 위협을 해결하고 모든 데이터 유출을 방지하도록 지원했습니다 .

Darktrace Immune System(면역 시스템) 은 '자가 학습' 을 기반으로 새로운 정보를 반영해 지속적인 업데이트를 수행하여 , 다른 툴이 놓치는 은밀한 위협을 탐지하고 위협이 진행됨에 따라 맞춤형 자율 대응을 수행합니다 .

산업용 네트워크를 위한 Cyber AI

90% OT 보안 팀의 90% 는 2 년 간 한 번 이상의 치명적인 사이버 공격을 겪습니다

출처: 포네몬(Ponemon)

원래 인터넷에 연결되지 않았던 산업 제어 시스템 (ICS) 은 새로운 비즈니스 목표와 효율 정책을 실현하기 위해 기업 IT 네트워크와 점차 융합되어 왔습니다 . 안타깝게도 보안 관점에서 이러한 상황으로 인해 운영 기술을 보호하는데 장애가 되는 다양한 과제가 생겨났습니다 .

보안을 고려하지 않고 설계된 오래된 디바이스는 이제 취약점을 찾아 조직의 경계를 살펴보는 사이버 범죄자들에게 노출되어 있습니다 . 취약점이 노출된 장비는 보다 치명적인 네트워크 공격의 게이트웨이로 사용되는 경우가 많으며 , IT 네트워크에서 시작되는 공격으로 인해 물리적인 작업에 부수적인 피해가 생기면서 생산에 심각한 차질이 빚어질 수 있습니다 .

산업 환경의 규모와 범위가 커지면서 조직들은 보다 심층적이고 효과적으로 이러한 사이버 - 물리적 공격에 대응하기 위해 AI 로 눈을 돌리고 있습니다 . OT 및 IT 전반에 대한 Darktrace 의 통합 인사이트와 분석을 통해 AI 는 위협 진입 지점에 상관없이 위협이 조직에 침입하자마자 이를 탐지합니다 . 다른 경우와 마찬가지로 이 경우에도 고객들은 Cyber AI Analyst 의 인사이트가 신속히 생성된 개략적인 사고 개요와 기술적 변환 작업에 매우 중요하다고 생각하는 것으로 나타났습니다 .

그림 18: IT 및 OT 를 표적으로 하는 Triton 스타일의 공격에서 모든 원격 데스크톱 '홉' 을 표시하는 Cyber AI Analyst

Shamoon 바이러스 탐지

Shamoon 악성코드는 손상된 하드 드라이브를 초기화하고 주요 시스템 프로세스를 덮어쓰기하여 감염된 장비를 사용할 수 없게 만듭니다. Darktrace는 한 글로벌 에너지 회사에서 평가판을 사용하던 중 산업 제어 시스템 (ICS)을 직접 표적으로 한 이 악명높은 사이버 공격을 탐지했습니다.

Darktrace가 Shamoon 기반의 사이버 공격을 발견했을 당시 중동의 몇몇 기업들은 새로운 유형의 악성코드로 피해를 입은 상황이었습니다.

Darktrace Cyber AI는 원격 포트 445에서 수십 개의 감염된 디바이스가 동시에 수행하는 비정상적인 네트워크 스캔과 비정상적인 Remote PowerShell 사용을 탐지했습니다. Remote PowerShell은 내부 이동 중 침입에 상당히 자주 악용됩니다. 해당 디바이스는 기존의 관리 디바이스로 분류되지 않아, WinRM 사용이 더욱 의심스러운 상황이었습니다.

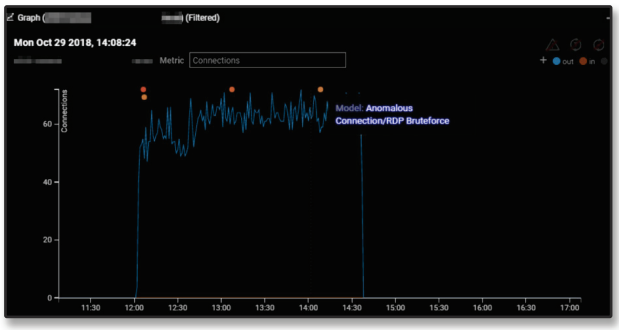


그림 19: 뚜렷한 증가세를 보이는 내부 연결 색칠된 모든 점은 RDP 무차별 대입 공격 탐지를 나타냄

Darktrace는 이후 비정상적인 크리덴셜 사용으로 보이는 또다른 활동 클러스터를 식별했습니다. Darktrace는 특정 프로토콜의 비정상적인 사용과 이러한 인사이트의 상관성을 분석하여, 해당 조직 환경 전반에서는 매우 보기 드문 다수의 관련 이상 징후를 식별하고 공격자가 네트워크 내부로 이동하는 것을 확인했습니다.

ICS를 표적으로 하는 스캔 툴

ICS 시스템으로 인해 조직의 기존 사이버 보안 방어 체계에 사각 지대가 생기는 경우가 많습니다. 한 공공설비 회사는 Darktrace 평가판을 사용하는 동안 사각지대를 해소할 수 있었습니다. 당시 공조제어시스템에서 비정상적인 통신 채널을 통해 네트워크 밖의 여러 디바이스로부터 대규모 연결을 수신하는 것이 관찰되었는데, 이는 사실 네트워크가 있는 국내가 아닌 해외에서 연결 요청이 온 것이었습니다.

면밀한 조사를 통해 Darktrace는 정찰 툴을 사용한 취약점 스캔과 관련된 연결 요청을 탐지했는데, 이는 해당 디바이스에 불법적으로 액세스하려는 시도였습니다. 뿐만 아니라 외부 디바이스는 제어 장치에서 데이터를 읽어들이라는 요청을 보냈는데, 외부 당사자가 민감한 ICS 정보에 액세스하려는 시도였을 가능성이 있었습니다. 이 사고에서 Darktrace는 IT 및 OT 네트워크에 폭넓은 가시성을 제공하고, 네트워크 외부에서 내부 디바이스에 연결하려는 비정상적인 시도를 면밀히 조사함으로써 독보적인 기술력을 입증할 수 있었습니다.

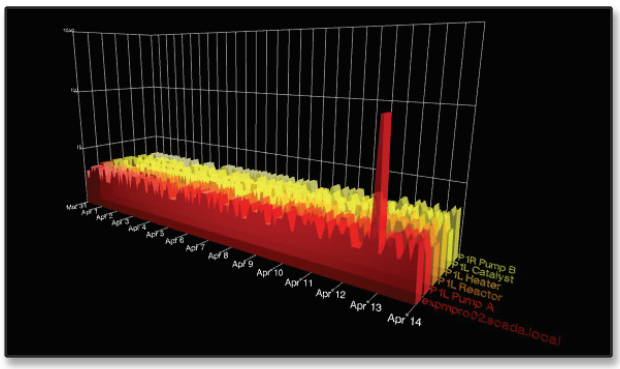


그림 20: SCADA 디바이스에서 두드러지게 보이는 비정상적인 연결

네트워크를 위한 Cyber AI

69% 조직의 69% 는 AI 를 사이버 공격 대응의 필수 요소로 생각합니다

: Capgemini Research Institute

Darktrace 의 자가 학습 AI 는 작업 위치나 애플리케이션의 속성에 상관없이 조직 내 동적인 시스템과 직원을 보호하도록 설계되었습니다 . 레거시 온프레미스 방어 체계와는 달리 , Darktrace 는 네트워크에서 정상 행동을 파악하고 클라우드 , SaaS 및 이메일 서비스 내 행동으로 그 범위를 확장하여 정보를 업데이트합니다 . Darktrace 는 이와 같은 추가 컨텍스트를 통해 네트워크 상의 '로우 앤 슬로우' 데이터 도난 및 크리덴셜 손상을 비롯해 기계 속도로 빠르게 이동하는 랜섬웨어에 이르는 전방위적인 사이버 위협을 탐지합니다 .

그런 다음 Darktrace Antigena 가 신속히 네트워크 내 새로운 위협을 정확히 차단하므로 , 보안 팀은 중요 데이터가 도난당하거나 암호화되기 전에 대응 시간을 확보할 수 있게 됩니다 . 이처럼 동적인 보호는 지능적이고 정확할 뿐만 아니라 광범위한 영역을 포괄하며 , 자율적인 대응과 인라인 (inline) 방어와의 능동적인 통합을 통해 랜섬웨어 , 암호화폐 채굴 작업 , 내부자 위협 등을 자동으로 무력화합니다 .

마찬가지로 기업 네트워크에서 얻은 실시간 인사이트는 비즈니스의 다른 영역에 있는 데이터 포인트에 대한 Immune System(면역 시스템) 의 의사 결정을 알리기도 합니다 . 예를 들어 직원이 이메일 내 악성 링크를 클릭한 후 디바이스가 감염되는 경우 , Darktrace 는 네트워크 내 감염을 차단하고 동일한 캠페인에 속한 다른 모든 이메일을 자동으로 식별해 무력화할 수 있습니다 .

어떤 경우든 네트워크에서 탐지가 이루어지면 비로소 Darktrace 의 Cyber AI Analyst 가 빠르게 대규모로 사고의 전체 범위를 조사하기 시작합니다 . Darktrace 는 몇 분 내에 사용하고 실행할 수 있는 자세한 사고 보고서를 자동으로 생성합니다 . 이를 통해 인공 지능을 최대한 활용하여 몇 초만에 위협을 차단하고 보안 팀이 보다 전략적인 업무에 집중하도록 지원할 수 있습니다 .

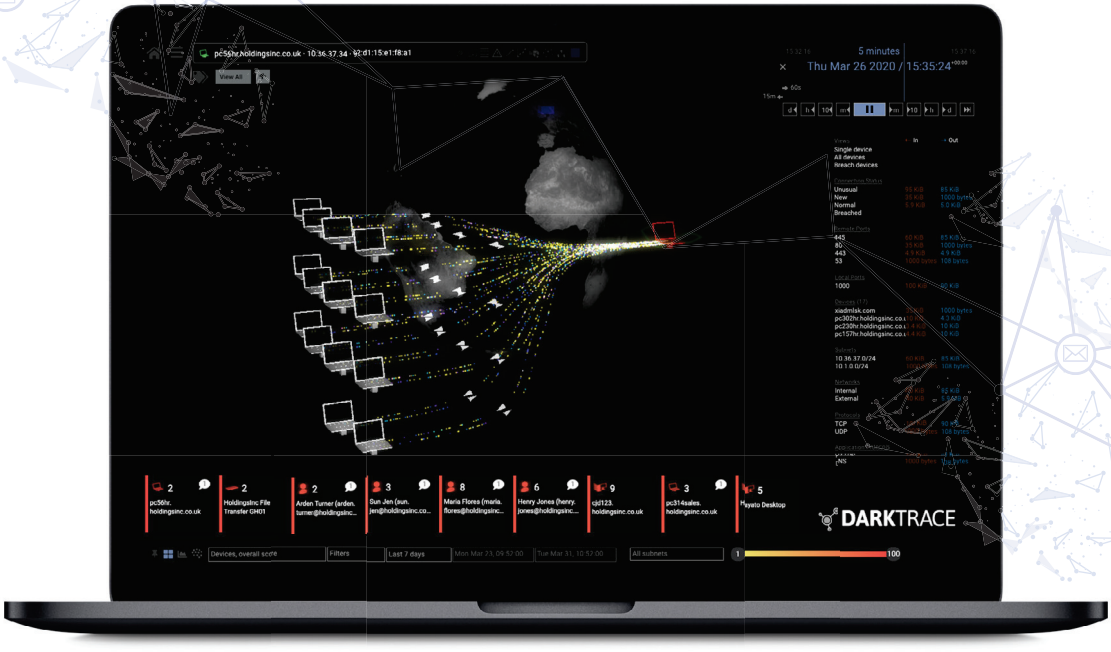


그림 21: 네트워크 스캔을 실행 중인 노트북을 탐지하는 Darktrace

Sodinokibi 랜섬웨어에 감염된 금융사

Darktrace 는 미국의 한 중견 서비스 기업을 표적으로 한 Sodinokibi 랜섬웨어 공격을 탐지했습니다 . 이러한 ' 이중 위협' 은 랜섬웨어를 사용해 표적 공격을 실행하면서 동시에 피해 기업의 데이터 유출을 시도하며 , 몸값을 지불하지 않으면 공격자는 데이터를 공개하겠다고 협박합니다 .

외부 연결 RDP 서버가 우크라이나의 보기 드문 외부 IP 주소로 비정상적인 연결을 시작하자 Darktrace 는 최초의 보안 침해 징후를 식별했습니다 . 그런 다음 AI 는 파일 공유 플랫폼인 Megaupload 에서 300MB 의 데이터가 다운로드되는 것을 탐지하고 , 조직 내에서 이러한 서비스를 사용하는 사람이 없음을 확인한 후 이에 대해 즉시 비정상 활동이라는 경고를 표시했습니다 .

Darktrace 가 3 분 후 네트워크 스캔과 지속적인 명령 및 제어 (C&C) 트래픽을 탐지하자 , 감염된 RDP 서버가 외부 대상으로 매우 비정상적인 연결을 하기 시작했습니다 . 마침내 AI 는 업로드 중인 40GB 의 데이터와 내부 SMB 공유에 액세스 중인 비정상적인 파일 (랜섬노트로 추정) 을 탐지했습니다 .

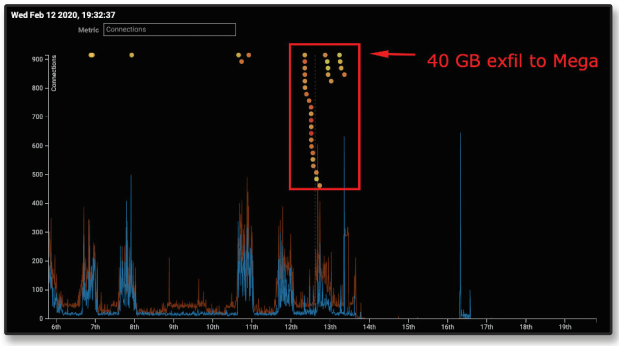


그림 22: 도메인 컨트롤러 연결

공격의 최종 단계에서만 20 개 이상의 Darktrace 모델이 트리거되었습니다 . Darktrace Antigena 가 활성화되었더라면 몇 초만에 대응해 위협을 무력화했을 것입니다 .

은밀히 진행 중인 비트코인 채굴

직원 수가 500 명에 달하며 높은 평판을 자랑하던 한 법률 회사는 알려진 위협을 스캔하는 보안 제어 기능을 갖추고 있었으나 , 5 개월 간 자사 네트워크 내에서 비트코인 채굴이 진행중이었던 사실을 모르고 있었습니다 .

Darktrace 솔루션을 설치한 후 이 회사는 여름 인턴 한 명이 회사 인프라에 비트코인 채굴 악성코드를 설치해 75 대가 넘는 컴퓨터를 이용하고 있었음을 알게 되었습니다 . 네트워크 속도 저하는 물론 회사의 생산성까지 악화되면서 , 암호화폐 채굴 작업으로 인해 해당 회사는 중대한 평판 위험에 노출되었습니다 .

AI 가 이처럼 비정상적인 행동을 발견하지 못했더라면 인턴십이 끝난 후에도 채굴 작업이 수 개월 간 지속되었을 것입니다 .

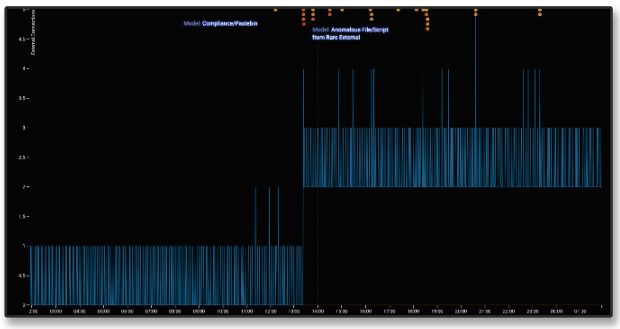


그림 23: 외부 연결 및 관련 모델 브리치가 갑자기 늘어난 상황을 보여주는 그림

원하는 환경에서 직접 Cyber AI 를 경험해보세요 .

여기를 클릭해 무료 평가판 신청하기

다크트레이스에 대해서

Darktrace 는 세계를 선도하는 사이버 인공지능 기업이자 자율 대응 기술 (Autonomous Response technology) 을 세계 최초로 개발한 기업이다. Darktrace 의 자율학습 기반 인공지능은 인체의 면역체계에서 영감을 얻어 개발된 기술로, 현재 4,000 개가 넘는 기업과 조직을 클라우드, 이메일, 사물인터넷 (IoT), 네트워크 및 산업시스템 등을 노리는 사이버 위협으로부터 보호하고 있다 .

Darktrace 는 1,300 명이 넘는 직원을 두고 있으며 본사는 샌프란시스코와 영국 케임브리지에 위치하고 있다. Darktrace 인공지능은 매 3 초마다 새로운 사이버 위협에 대처했으며 피해가 초래하기 전에 고객을 보호하고 있습니다.

연락처

소프트플로우㈜
070-7724-2752
info@softflow.io