

Darktrace Immune System: 제품 및 서비스

인간의 면역 체계와 마찬가지로 Darktrace의 클라우드 네이티브 AI는 정상적인 행동 패턴을 학습하여 예측할 수 없는 사이버 위협을 차단합니다. Darktrace Immune System은 다양한 시스템과 분산된 사용자 간 직원 행동을 통합하여, 이메일, 클라우드, 협업 플랫폼, 엔드포인트, IoT 및 기업 네트워크에 이르는 기업 전반에서 탐지 및 대응 시간을 대폭 줄입니다. 전 세계 4,000 개 이상의 조직에서 Darktrace를 사용해 자사의 고유한 디지털 환경 정보를 파악하고 초기 단계에서 새로운 공격 및 내부자 위협에 자율적으로 대응하고 있습니다.

The Darktrace Immune System

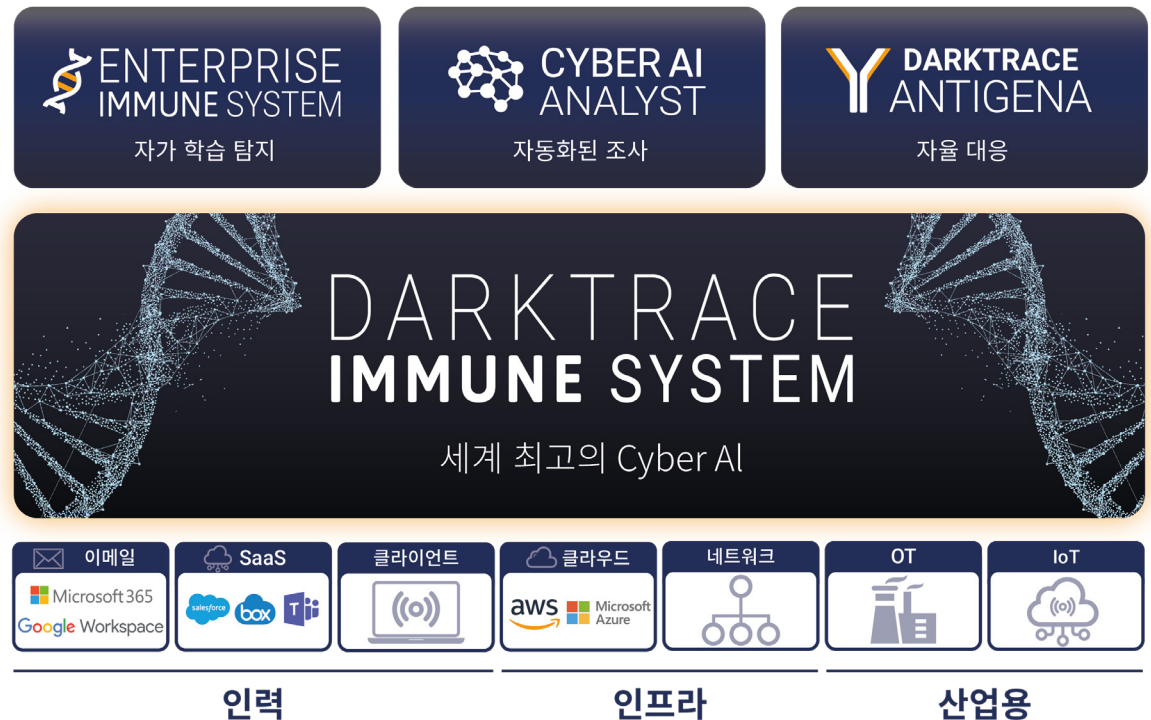
Darktrace Immune System은 통합 플랫폼에서 지도 및 비지도 머신 러닝을 함께 활용하는 핵심 AI 기술로서, 자율적인 사이버 위협 탐지, 조사 및 대응을 지원합니다.

Darktrace의 사이버 인공지능은 자가 학습 기술을 기반으로 합니다. 다시 말해, 정적 규칙이나 과거 공격 데이터를 사용하는 대신, 지속적으로 변화하는 역동적 업무 환경 및 다양한 디지털 인프라의 '정상' 상태를 파악합니다. 이를 통해 클라우드, SaaS 및 이메일 플랫폼을 비롯해 IoT, 엔드포인트, 사이버-물리 시스템 전반을 통합적으로 보호합니다.

Darktrace는 인간의 면역 체계와 마찬가지로 사전 지식 없이도 악성 행동과 무해한 행동을 구별할 수 있으므로, 다른 방식으로는 탐지하지 못하고 지나칠 수 있는 사이버 공격을 식별합니다.

자율 대응 (Autonomous Response) 기술을 기반으로 한 Darktrace AI는 맞춤형 인텔리전스를 사용하여 빠르게 확산되는 공격을 정밀하게 차단합니다. Darktrace는 행동 패턴을 파악하고 있으므로, 기본적으로 '정상' 패턴을 실행하고 일상적인 운영을 유지하여 즉시 위협을 억제할 수 있습니다.

Cyber AI Analyst는 추가로 AI 조사를 수행하여 보안 사고의 전체 범위를 자동으로 분류, 해석 및 보고합니다. Cyber AI Analyst는 보안 전문가의 전문성과 AI의 속도 및 확장성을 결합하여 사고의 우선순위를 지정하고 보고서를 작성하여 보안 팀이 즉시 대응할 수 있도록 지원합니다.



The graphic features three main components at the top: 'ENTERPRISE IMMUNE SYSTEM' (자가 학습 탐지), 'CYBER AI ANALYST' (자동화된 조사), and 'DARKTRACE ANTIGENA' (자율 대응). Below these is a large central banner with the text 'DARKTRACE IMMUNE SYSTEM' and '세계 최고의 Cyber AI'. At the bottom, there are three columns representing different domains: '인력' (Human Resources) with icons for Email (이메일), SaaS (SaaS), and Client (클라이언트); '인프라' (Infrastructure) with icons for Cloud (클라우드), Network (네트워크), and OT (OT); and '산업용' (Industrial) with an IoT (IoT) icon. Each icon includes logos for associated services like Microsoft 365, Google Workspace, Salesforce, Box, Teams, AWS, and Azure.

Darktrace 제품군



Enterprise Immune System - 자가 학습 방식의 위협 탐지

- 역동적 업무 환경 전반에서 예측하기 어려운 사이버 위협을 발견
- 클라우드, SaaS, 엔드포인트, IoT 및 네트워크 전반의 통합 보기
- 제로데이 공격, 랜섬웨어 및 내부자 위협 등 위협의 전체 범위 탐지
- 원활한 배포를 통해 자가 학습을 수행하여 몇 시간 내에 결과 도출



Industrial Immune System - 자가 학습 방식의 ICS 위협 탐지

- 새로운 공격, 내부자 위협 및 운영 위험을 탐지
- 정해진 기준이나 조정 불필요
- ICS 프로토콜 및 기술과 무관
- OT, IT 및 IIoT 전체 시각화



Cyber AI Analyst - AI 조사

- Darktrace 가 탐지하는 모든 위협을 자동으로 조사
- 분석 전문가의 행동을 모방하여 사고의 우선순위 지정
- 보고서를 작성하여 보안 팀이 즉시 대응할 수 있도록 지원
- 분류 시간을 최대 92% 단축



Antigena Network - 자율 대응

- 정밀한 대응을 수행하여 몇 초만에 위협 차단
- 사고 발생 중에도 '정상' 패턴을 실행하여 정상적인 운영 유지
- 보안 팀이 대응 시간을 확보하고 전략적 업무를 우선하도록 지원
- 클라우드, SaaS 및 기존 네트워크 전반에서 동작
- Darktrace Mobile App 을 통해 언제 어디서나 제어



Antigena Email - 자율 대응

- AI 를 활용해 이메일 '발신자 파악'
- 다른 툴이 놓치는 악성 이메일 무력화
- 스피어 피싱 및 위장 공격 포착
- 클라우드 네이티브 방식으로 몇 분만에 설치 가능



Antigena SaaS - 자율 대응

- 클라우드 및 협업 도구에서 예측할 수 없는 공격 무력화
- 동적 클라우드 계정 사용에 대한 '인간을 이해하는' 자가학습 인공지능 기반의 의사 결정
- 악성 행위가 종결되기 이전, 인간의 조치보다 빠른 반응
- 정상 비즈니스 허용 간의 정확한 조치

Darktrace 전문가 서비스

고객들은 Darktrace Cyber Analyst 또는 Darktrace Certified Partner가 제공하는 다양한 위협 분석 및 사이버 인텔리전스 서비스를 이용할 수 있습니다. Darktrace 서비스는 다양한 업종에 걸친 모든 규모의 조직이 고유 환경에 맞는 최적의 솔루션을 사용할 수 있도록 설계되었습니다.

Ask the Expert(전문가 지원)

- Darktrace Cyber Analyst가 제공하는 신속한 피드백 및 전문가의 문제 해결 조언
- 사용하기 쉬운 채팅 기능
- 연중무휴 24 시간 지원

연중무휴 24 시간 지원되는 사전 예방적 위협 알림

- 24시간 지원되는 포괄적 사전 예방적 위협 알림 서비스
- 공격 발생 즉시 고객에게 연락
- 중소기업 및 대기업에 이르는 1,000 개 이상 고객사 보호
- 영국 케임브리지, 샌프란시스코 및 싱가포르에 위치한 Darktrace Security Operations Center(보안 운영 센터, SOC)에서 지원

Immune System 통합

Darktrace Immune System은 확장 가능한 개방형 아키텍처를 사용하여 고객의 다양한 에코시스템에 원활히 연결되며, 에코시스템의 변화에 따라 진화합니다. 원클릭 통합 방식으로 이러한 플랫폼은 새로운 형태의 텔레메트리를 즉시 수집하고, 설정된 워크플로우 전반에서 맞춤형 AI 인사이트를 공유하고, 다양한 기술과 호환될 수 있습니다. 이를 통해 이메일 시스템과 인라인 (inline) 방어 체계 및 협업 플랫폼 전체에 자율 대응 (Autonomous Response) 기술이 구현됩니다.

