Cyber AI Platform

Industrial Immune System

Cyber AI 로 지원되는 Industrial Immune System 은 산업용 환경에서 사이버 위협과 취약점을 탐지하는 자가 학습 기술입니다 . 이 솔루션은 OT, IT 및 산업용 IoT 전반에서 ' 정상' 상태를 수동적으로 학습하여 , 다른 방식으로는 탐지하기 어려운 새로운 공격의 미세한 지표를 인식할 수 있습니다 .

주요 이점

- 자가 학습
- OT, IT 및 IoT 전반에서 100% 가시성 확보
- 자동으로 환경에 적응
- 기술 및 프로토콜과 무관
- 새로운 위협 또는 취약점의 미세한 징후를 실시간으로 탐지
- 환경 변화에 적응

규모에 따른 심층 보안

Industrial Immune System 은 네트워크 트래픽을 모니터링하여 , 기본 프로세스 (퍼듀 모델 레벨 1), 관리 감독 기능 , 기업 물류 및 엔터프라이즈 네트워크 (레벨 4 및 5) 을 넘어 클라우드 네트워크와 SaaS 서비스에 이르는 모든 환경에 대한 직접적인 가시성을 제공하고 자가 학습을 통해 이를 보호합니다 .

수동적인 모니터링

아주 약간만 서비스가 중단되더라도 심각한 피해가 발생할 수 있는 어플리케이션이 많기 때문에 새로운 디바이스를 산업용 네트워크에 연결하기란 결코 간단한 일이 아니며 일반적이지도 않습니다 .

Industrial Immune System 은 ICS 네트워크에 수동으로 연결되어 가능한 많은 통신 트래픽의 복사본을 수신합니다 . 기본 제공 포트 미러링 또는

자가 학습 AI

AI 로 지원되는 Industrial Immune System 은 모든 종류의 위협 및 취약점으로부터 산업용 환경을 보호하고 특정 네트워크에 자동으로 적응합니다 . 이 기술은 블랙리스트에 의존하는 대신 '자가 학습' 을 통해 새로운 비정상 활동을 식별합니다 .

이 같은 자가 학습 기능은 Industrial Immune System 이 실제로 프로토콜의 제약을 받지 않으며 Modbus 에서 BACnet, CIP 에 이르는 모든 운영 환경에서 유효함을 의미합니다 . Industrial Immune System 은 일상적인 작업을 중단하지 않고도 모든 종류의 기술과 원활히 연동됩니다 .

네트워크 스위치의 ' 스패닝 (spanning)' 기능을 사용하거나 , 단일 위치에 다양한 연결을 통합하도록 애그리게이터를 통해 오류 보호 (fail-safe) 탭을 사용하여 원시 네트워크 데이터의 복사본을 수집합니다 .

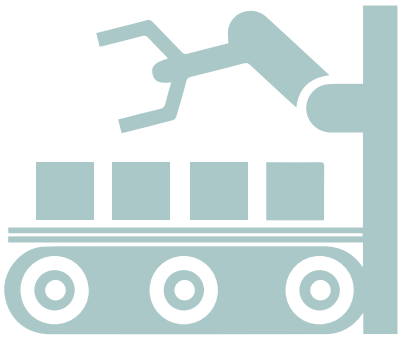
OT, IT 및 IoT 전반에서 통합 보기 제공

Darktrace 는 직관적인 Threat Visualizer 인터페이스를 통해 네트워크 내 모든 사용자 , 디바이스 및 컨트롤러를 포함한 다양한 디지털 인프라의 개요를 보안 팀에 즉시 제공합니다 . 이를 통해 운영자는 사전 대응적으로 사이버 위협 및 ICS 의 특정 영역을 조사할 수 있습니다 .

Threat Visualizer 는 IT Security Operation Center(SOC) 뿐만 아니라 운영자 수준에서 사용할 수 있으므로 OT 및 IT 보안 팀 전체의 협업이 가능합니다 .

Threat Visualizer 는 산업용 환경에 대한 시각적 개요를 실시간으로 표시하며 심층 조사를 지원합니다 .

실제 활용 사례 : 생산 라인의 설비 보안 침해



알려지지 않은 공격자가 주요 식품 제조업체 생산 라인의 여러 산업용 IoT 디바이스를 표적으로 삼았습니다 . 포장 기계와 절단기 , 혼합기 등의 설비가 외부 대상에 연결을 시도하며 기업 네트워크 내에서 이동하려 했습니다 . 이러한 디바이스는 핵심 IT 인프라에 연결하는 데 필요한 보안 승인을 얻지 못한 상태였습니다 .

Darktrace AI 는 이러한 요소들의 상관성을 실시간으로 분석하여 비정상적인 행동을 기업 네트워크 및 생산 라인의 무결성에 대한 심각한 위험이라고 판단했습니다 . Darktrace 의 인공 지능을 사용해 산업용 IoT 및 ICS 를 포함한 전체 인프라를 시각적으로 파악하고 보호할 수 있었습니다 .

보안 팀은 보안이 침해된 디바이스를 네트워크에서 제거하여 공격자가 핵심 IT 인프라에 대한 액세스 권한을 얻기 전에 식품업체의 제조 인프라가 피해를 입지 않도록 보호할 수 있었습니다 .

고객 사례

> Darktrace Industrial 은 ICS 방어 체계를 근본적으로 변화시키고 있습니다

- 라스베이거스 시 , 최고정보관리자 (CIO)

> AI 는 보안 상태 유지에 매우 중요합니다 . 다양한 레거시 시스템을 포함해 우리 회사 전체의 SCADA 환경을 유연하게 보호해주기 때문입니다 .

- Utilities Kingston, 네트워킹 담당 이사

> Darktrace 가 제공하는 이점은 명백합니다 . 감염된 USB 를 통해서든 소프트웨어 드라이브 바이 취약점을 통해서든 언제나 침입 통로가 있게 마련이므로 모든 진입 지점을 차단할 수 있는지가 중요한 중요한 것이 아닙니다 . 그보다는 보안 침해 발생 시 이를 식별할 수 있는지 여부가 관건입니다 .

- Drax, 보안 담당 부서장

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

대한민국: +82 2 6138 4600
아시아 태평양: +65 6804 5010
북미: +1 (415) 229 9100
유럽: +44 (0) 1223 394 100

info@darktrace.com | darktrace.com

@darktrace