DARKTRACE

SAMSUNG SDS
Strategic Partner & Master Distributor

Cyber Security for Industrial Immune Systems (IIS)

Continuous Threat Monitoring

Product Overview

Darktrace의 Industrial Immune System(IIS)은 베이지안 확률과 같은 고급 수학 기법과 최첨단 AI 알고리즘을 탑재한 머신 러닝 기술을 이용하여 Industrial Control System(ICS)의 네트워크 상에서 알려져 있는 공격뿐만 아니라 알려져 있지 않은 새로운 유형의 공격까지도 실시간으로 탐지하여 조치를 취하게 해주는 ICS 전용 네트워크 보안솔루션 입니다. IIS는 작업자, 설비 장치 및 자동화 시스템 등 ICS의 모든 구성요소들의 정상행위를 비지도학습 기반 머신 러닝을 통해 스스로 학습하고 학습된 정상행위를 기반으로 이상행위를 탐지해 내는 혁신적인 솔루션입니다.

ICS and SCADA

ICS는 현대적인 용어로써 전통적으로 사용했던 SCADA(Supervisory Control and Data Acquisition)와 DCS(Distributed Control Systems) 등 여러 종류의 control system을 포괄하고 있지만, 언론이나 출판물 등에서는 SCADA와 ICS를 혼용하여 사용하고 있습니다. 또한, 일반적인 IT 시스템/네트워크와 구별하기 위해 ICS를 OT(Operation Technology) 시스템/네트워크라 부르기도 합니다.

IT 시스템과 OT시스템은 같은 조직 내에서 운영되고 있어도 두 시스템은 서로 다른 프로토콜을 사용하고 있었지만, 최근 추세는 유사 기술을 활용한 비용 효율화와 운영 편리성 등의 이점으로 인해 IT 시스템과 OT 시스템의 접점이 증가하고 있습니다.

ICS Cyber Security Issues

ICS는 수많은 종류의 사이버 보안 위협, 예를 들어 작게는 규정위반이나 잠재적 손실을 초래할 수 있는 공격에서부터 크게는 운영 중단, 설비 파괴, 그리고 인간의 삶을 위태롭게 할 수도 있는 위협에 직면해 있습니다.

전통적으로 OT 네트워크는 IT 네트워크와 물리적으로 격리되어 있었지만, 발전소, 공항, 철도 등 기간시설을 파괴할 목적으로 제작된 웜바이러스, Stuxnet이나 미군 정보망에 침투해 군사작전계획을 탈취해간 악성코드, agent.btz와 같은 사이버 공격은 이동식 저장매체 또는 인간의 실수를 이용해 보안상 허점을 노려 침투한 것으로 알려져 있습니다.

Real Vulnerability

독일의 제철소

2014년말 해커들이 독일의 어느 제철소에 대해 APT (Advanced Persistent Threat) 공격 수법을 이용하여 처음에는 제철소 사무용 네트워크에 접속할 수 있는 접근 경로를 알아 냈습니다. 이후, 사무용 네트워크 탐색을 통해 설비제어 네트워크로 침투하여 개별 제어 시스템을 마비시켜 결국 용광로를 제어할 수 없게 되어 제철소 설비에 막대한 피해를 입혔습니다.

하벡스 (Havex)

ICS를 타깃으로 만들어진 악성코드 하벡스는 '워터링 홀 (watering-hole) 수법을 사용합니다. 워터링 홀이란, 사자가 마치 먹이를 습격하기 위해 물웅덩이(watering-hole) 근처에서 매복하고 있는 형상을 빗댄 것으로 공격 대상이 방문할 가능성이 가장 높거나 가장 많이 쓰는 웹사이트를 감염시킨 후 잠복하면서 공격 대상 시스템에 악성코드를 추가로 설치하는 공격입니다. 즉 하벡스는 공격자가 ICS 벤더 웹사이트에 존재하는 소프트웨어 업데이트 파일을 악성코드가 포함된 버전으로 교체해 놓는 것입니다. 이는 전통적인 네트워크 보안 장비로는 방어하기 어렵습니다.

A New Approach: Darktrace and the Immune System

Darktrace의 IIS는 ICS에 대해 실시간 "면역 시스템"을 구현해 줄 수 있는 혁신적인 솔루션입니다.
IIS는 베이지안 확률과 같은 고급 수학에 기반을 두고 머신 러닝 및 AI 알고리즘을 탑재하여 네트워크의 모든 사용자 및 장치에 대한 정상행위를 스스로 학습하고, 이러한 정상행위에서 벗어나는 변화, 즉 이상행위를 감지해 냅니다. 이는 위협적인 침입 인자들을 스스로 감지하고 이를 극복하고자 하는 인간의 면역체계와 같은 원리라고 할 수 있습니다.

Darktrace Technology

최근 사이버보안 동향을 살펴보면, 알려져 있지 않은 취약점을 악용하여 공격하는 사례가 빈번히 발생하기 때문에 알려져 있는 공격 유형 기반의 보안장비로 방어하는 방법은 새로운 공격유형에 중요 시스템들을 그대로 노출하는 결과를 초래합니다. Darktrace는 시스템 환경이나 위협에 대해 rule이나 signature 를 필요로 하지 않으므로 알려져 있지 않은 미확인 위협도 탐지할 수 있습니다. 그 이유는 ICS 환경 내에서 비정상적인 행동 변화가 일어날 때마다 IIS는 스스로 학습한 정상행위를 기반으로 변화를 식별하고 이에 대한 경보를 발생합니다. Darktrace에 내재된 진보된 수학 개념은 수많은 잠재적인 위협요소를 간과하지 않도록 설계되어 있고, 네트워크 트래픽에 대한 규칙뿐만 아니라 위치나 시간대 별로 구분된 수많은 정밀한 지표들을 위협 요소 식별에 활용하기 때문에 오탐을 방지할 수 있습니다.

Darktrace의 Threat Visualizer(3D 사용자 인터페이스)를 사용하면 실시간 모니터링 및 탐지 내역 확인, 분석도 가능하지만, SIEM과 연계하여 기존 프로세스 및 절차와 통합 할 수도 있습니다.

또한 Darktrace는 IT 및 OT 환경에서 모든 사용자 및 장치의 연결 상태를 Threat Visualizer로 보여줌으로써 네트워크에 대한 가시성을 제공하면서 사이버 위협 발생시 피해를 입히기 전에 이를 무력화 시키기 위한 실시간 방어 조치를 취합니다.

Passive Observation

IIS는 네트워크 스위치의 span 기능 또는 내장 미러 포트를 사용하거나 미러링 탭 또는 집성탭을 사용하여 연결되기 때문에 ICS 네트워크에 어떠한 영향도 미치지 않습니다.

Darktrace는 Level 2 (감시 제어), Level 3 (데이터 서버) 및 Level 4 (IT 네트워크)에 연결하여 심층 방어를 제공 할 수 있습니다. 또한 사이버 보안 범위를 Level 1 (필드 장치)까지 확장할 수 있습니다. 이렇게 유연한 분산 아키텍처 덕분에 Darktrace는 여러 계층과 다양한 네트워크 토폴로지를 안전하게 보호 할 수 있습니다.

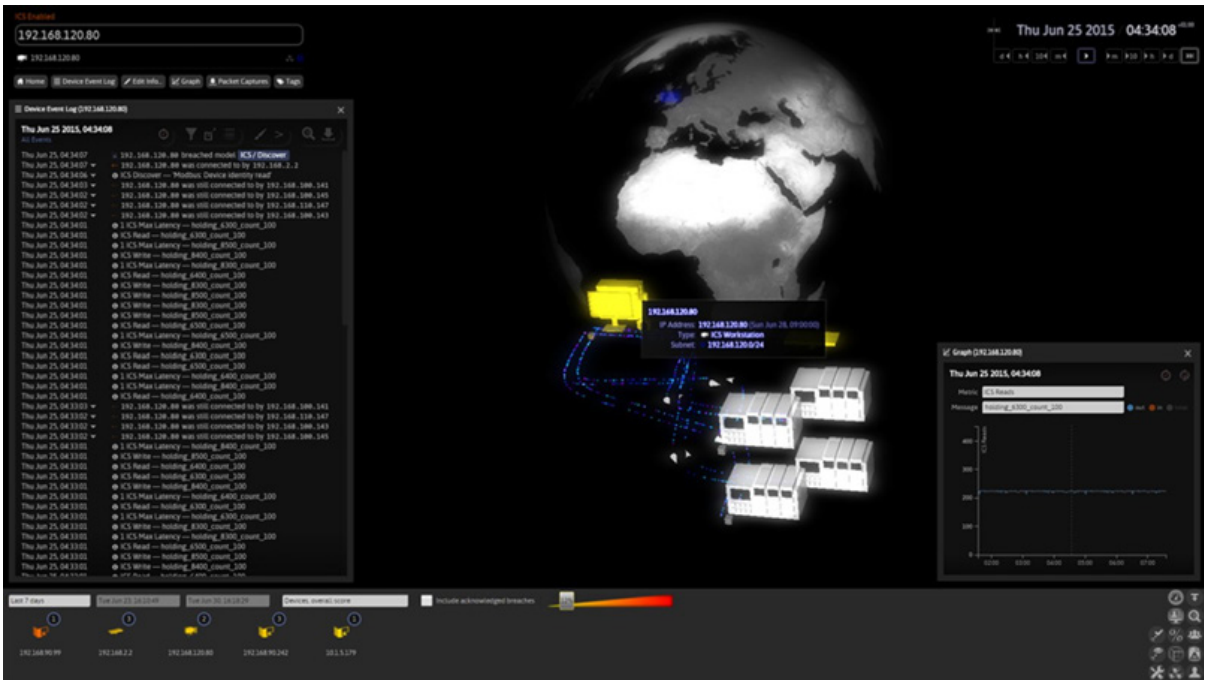
Darktrace Proof of Value

Darktrace의 POV (Proof of Value)를 통해 고객의 ICS 환경 내에서 IIS의 기능을 직접 경험할 수 있습니다. 만일 운영환경에 어떠한 영향도 주지 않고 안전한 POV를 원한다면 OT 네트워크에 설치하기 전에 IT 네트워크에 설치하여 Darktrace의 안전성을 검증할 수도 있습니다.

Darktrace는 외부 위협뿐만 아니라 단순한 실수 또는 특정한 목적을 가진 내부 위협 등 네트워크 상의 이상행위를 탐지해 낼 수 있는 비지도 학습 기반 머신 러닝 보안솔루션입니다.

제품 문의
다크트레이스 홈페이지 : www.darktrace.com
다크트레이스 한국지사 : korea@darktrace.com
다크트레이스 한국총판 : darktrace@samsung.com

삼성SDS SAMSUNG



Drax Power(영국 최대 발전회사)의 SCADA 네트워크에 설치된 Darktrace IIS의 Threat Visualizer