DARKTRACE

SAMSUNG SDS
Strategic Partner & Master Distributor

# Enterprise Immune System (EIS) and Threat Visualizer

## Product Overview

엔터프라이즈 면역 시스템(Enterprise Immune System, EIS)은 네트워크 접점이나 사용자 PC에 설치되어 있는 기존 방어 수단들을 회피하여 침입을 시도하는 사이버 위협을 탐지하고 그에 대한 조치를 취할 수 있게 해 주는 솔루션입니다.
EIS는 고도화된 수학적 기법을 솔루션에 내재하여 네트워크와 시스템 상의 모든 행위를 인지하고 모니터링하여 정상행위에서 벗어나는 이상행위를 감지해 냅니다. 기존의 탐지장비들은 rule 이나 signature에 기반하여 알려져 있는 공격만을 탐지해 낼 수 있는 반면, EIS의 고도화된 수학적 접근방식의 머신러닝 기능은 rule-set이나 signature를 사용하지 않기 때문에 지금까지 알려져 있지 않았던 새로운 공격 형태도 탐지해 낼 수 있습니다.

EIS는 appliance 장비 형태로 실시간 네트워크 흐름을 복제하여 연결할 수 있습니다. 네트워크에 연결이 되면 머신러닝 기능을 통해 개인 사용자뿐만 아니라 네트워크 상의 모든 시스템을 대상으로 사용 패턴을 스스로 학습(non-supervisory machine learning) 하게 되고, 이렇게 솔루션 스스로 터득한 정상 패턴을 기반으로 네트워크 상의 이상행위를 탐지하게 됩니다. EIS는 설치된 이후부터 지속적으로 학습을 수행하기 때문에 조직에 변화가 생겨도 이에 따른 네트워크 및 시스템 사용 패턴을 자동으로 업데이트 합니다.

EIS는 정상 패턴을 기반으로 사용 패턴의 작은 변화도 감지해 낼 수 있습니다. 따라서, 외부 침입에 의한 정보 탈취나 악성코드 감염은 물론, 불만을 품은 직원이나 근무 태만으로 발생할 수 있는 내부위협 까지도 감지해 낼 수 있습니다.

EIS를 통해 탐지해 낼 수 있는 대표적인 예시로, 평소 접속하지 않던 인터넷 도메인에서 다운로드, 인트라넷 또는 파일 시스템 복제, 등록되지 않은 장치 또는 위치에서 데이터에 접근, 비정상적인 응용 프로그램 또는 프로토콜의 실행, 업로드 패턴의 변화 등이 있으며, 이러한 현상들은 정상적인 행동과는 확연한 차이가 있기 때문에 탐지 후 즉시 조사 및 조치를 취해야만 합니다.

## Threat Visualizer

EIS는 탐지된 위협 정보를 visualizer를 통해 시각화 하여 보여 줍니다. Visualizer는 3차원 그래픽 도구로서 보안 분석가나 전문적인 수학 지식 없이도 네트워크 상의 이상행위를 직관적으로 인지하고 분석할 수 있게 도와 줍니다.

## *Key Features!*

- 머신 러닝과 정교한 수학적 기법 적용
- 알려지지 않은 새로운 공격 기법에 의한 위협 탐지
- rule-set이나 signature 없이 이상행위, 악성코드 등 탐지
- 탐지와 동시에 실시간으로 경보 발행
- 직관적으로 위협을 조사하고 분석할 수 있는 3차원 위협정보 시각화 화면 제공
- 네트워크 복제를 통한 간편한 설치

또한 Visualizer는 접속 로그에 남아 있는 어느 지점이든 상관없이 네트워크 상의 데이터 흐름과 상호 연관성에 대한 고도의 통찰력을 실시간으로 사용자에게 제공합니다. 일단 이상행위가 발견되면 visualizer는 이상행위를 일으킨 이벤트의 발단 지점과 진행과정을 보여 주고 이벤트가 남긴 의심 행위들을 추적할 수 있도록 해 줍니다.

보안 분석가들은 visualizer를 활용하여 복잡한 상황 하에서도 깊이 있는 분석을 수행할 수 있습니다. 이를 위해 wireshark와 같은 툴로 포렌식 분석을 할 수 있는 네트워크 패킷 다운로드 기능도 제공합니다.

## Complementary Technology

기존 signature 기반 보안 장비들은 새로운 공격 패턴이나 알려지지 않은 공격을 방어하는데 한계가 있지만, EIS의 머신러닝 탐지 방식은 완전히 새로운 공격이나 위협에도 이에 대한 사전 지식 없이 대응할 수 있습니다.

EIS에서 제공하는 데이터는 syslog, SNMP, connectors, file, databases, 또는 API 등 사용자가 원하는 형태로 SIEM이나 보안 dashboard 등에 전송하여 활용할 수 있습니다.

## Mathematical Foundations

Darktrace에 내재된 수학 기법의 핵심적인 역할은 데이터들 간의 상호 연관성을 찾아낼 뿐만 아니라 이 과정에서 발견된 불확실한 부분(uncertainty)에 대해 통계적 기법을 활용하여 정량화 합니다. 이를 위해 베이지안 확률 분석에 기반한 다양한 결과들을 종합하여 불확실한 부분들을 밝혀내게 됩니다.

Darktrace는 베이지안 추정 모델을 포함하여 다양한 수학적 접근 방식을 활용하기 위해 4가지 수학적 분석 엔진을 탑재하고 있습니다. 이들 수학적 분석 엔진 중 3가지는 개별 사용자가 사용하고 있는 각종 디바이스 및 시스템, 그리고 조직 전체적인 행동 모델을 만들어 내는데 사용됩니다. 만일 이 3가지 엔진 중 하나라도 이상행위를 탐지하게 되면 위협 판별기 엔진으로 초기 경보를 전송합니다. 이 위협 판별기가 초기 경보를 전송 받게 되면 이와 관련된 모든 영역, 모든 시간대에 대해 조사를 벌여 오탐 여부를 식별하고, 정탐일 경우 세부적인 조사를 진행할 수 있도록 경보를 발생합니다. 이와 같이 다중 베이지안 접근 방식 및 위협 판별기를 포함한 4가지 엔진의 특수한 조합은 조직 전반에 걸쳐 이상행위를 정확하게 탐지해 낼 수 있는 원동력을 제공합니다.

## Policy and Compliance Module

EIS는 시스템 정책 관리뿐만 아니라 compliance 관련 사항을 모니터링하고 준수할 수 있게 해줍니다. 예를 들어 웹하드 접근 통제, 특정 사이트 차단, 특정 시스템의 외부 접속 금지 등 고객 특성 및 요구사항에 맞춰 보안 정책 및 compliance 이슈사항 등을 반영할 수 있습니다.

## Your data is your data

EIS는 고객이 보유하고 있는 데이터 센터 내에서만 작업을 수행합니다. 따라서 데이터 센터 외부로 고객 데이터가 유출되지 않으며, 사전에 협의가 없는 한 Darktrace의 전문가들 조차도 고객 데이터에 접속 하거나 이를 공유하는 경우는 없습니다.

## Installation and Configuration

EIS는 단일 장비로 raw network traffic 구간에서 스위치의 span 포트 또는 inline tap 장비에 연결하여 사용합니다. 따라서 별도의 추가 장비 없이 간단하게 설치가 가능하며, 모든 UI는 웹 브라우저를 통해 조회할 수 있으며. 한 대의 EIS는 peak traffic volume에 따라 차이는 있을 수 있으나, 통상적으로 수천에서 수만 대(IP 數 기준)의 개별 기기들을 커버할 수 있습니다. 지역적으로 분산되어 있는 네트워크라 할지라도 여러 대의 Darktrace 장비를 cluster로 묶어 줌으로써 대규모 데이터 전송 없이 효율적으로 작업을 수행할 수 있습니다.


제품 문의

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

삼성SDS SAMSUNG


## 다크트레이스 엔터프라이즈 면역 시스템