Cyber AI 平台

Industrial Immune System

工業免疫系統由以 Cyber AI 為基底，是一種自我學習技術，能夠檢測工業環境中的網路威脅和漏洞。該解決方案經由被動學習營運技術、IT 和工業物聯網的「正常行為」而生效，從而使其能夠識別可能會被忽略之新出現攻擊的細微跡象。

主要優點

- 在工作中學習
- 跨營運技術、資訊技術和物聯網的 100%能見度
- 自動適應您所處的環境
- 不受技術環境和網路協定影響
- 即時檢測新出現的威脅或漏洞的細微跡象
- 適應不斷變化的環境

大規模覆蓋

透過監測網路流量，Industrial Immune System 可以直接查看並提供包括從基本流程(Purdue 模型 1 級)到監測功能、業務物流和企業網路（4 級和 5 級）以及雲端網路和 SaaS 服務之外所有內容的自我學習保護。

被動監測

將新設備連接到工業網路一直都不是簡單的例行程序，因為對於許多應用程式來說，即使是最輕微的服務中斷都可能造成破壞。

工業免疫系統被動連接到 ICS 網路，以盡可能接收最多的通信流量副本。該系統使用網路交換機的內置端口鏡像或「跨域」功能，或者使用故障保護分路器，有時透過聚合器將某處的大量連接聚集在一起，來攝取原始網路數據的副本。

自我學習 AI

Industrial Immune System 以 AI 為基底，可保護您的工業環境免於各種類型的威脅和漏洞，並自動適應您的特定網路。該技術不依賴黑名單，而是透過「在職」學習並識別新出現的異常活動而發揮作用。

這種自我學習功能表示 Industrial Immune System 與協定完全無關，並且在包括從 Modbus、BACnet 一直到 CIP 的任何操作環境中都是有效的。Industrial Immune System 可與各種技術無縫接軌，而不影響正常運行。

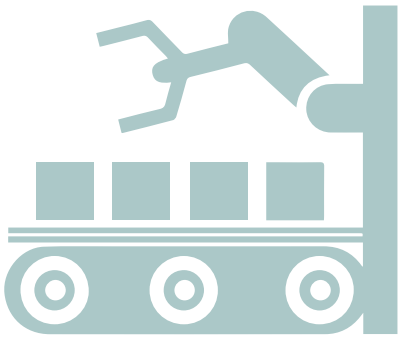
跨營運技術、資訊技術和物聯網的統一視圖

透過其直觀的 Threat Visualizer 介面，Darktrace 為安全團隊提供了他們多樣化數位基礎架構的即時概述，包括網路中的每個用戶、設備和控制器。這讓營運商可以主動調查網路威脅和 ICS 的特定區域。

Threat Visualizer 可以在營運商層級以及資訊技術安全營運中心使用，從而實現營運技術和資訊技術安全團隊之間的合作。

Threat Visualizer 顯示工業環境的圖形化即時概覽，並允許進行深入調查。

實際使用案例：裝配線上被洩密的設備



未知的攻擊者以領導食品製造商在裝配線上的幾台工業物聯網設備作為目標。含裝袋機、切片機和攪拌機等設備正試圖連接到外部目的地並在公司網路內移動。這些設備因為缺乏安全認證，無法連接到核心 IT 基礎架構。

即時聯結這些因素，Darktrace AI 研判異常行為將對公司網路和裝配線完整性造成重大威脅。藉由 Darktrace 的人工智慧技術，包括工業物聯網和 ICS 在內的整個基礎架構都能夠被看見並受到保護。

安全團隊能夠從網路中刪除被洩密的設備，從而保護食品供應商的製造基礎設施受到任何損害，並在攻擊者取得核心 IT 基礎設施的存取權限之前就採取行動。

客戶對我們的評語

> Darktrace Industrial 正在從根本上改變 ICS 防禦的方式。
>
> **- Chief Information Officer, City of Las Vegas**

> 人工智慧對於我們的安全態勢至關重要，因為具備足夠的靈活性來捍衛我們整個 SCADA 環境，包括各種舊有系統。
>
> **- Director of Networking, Utilities Kingston**

> 無可否認 Darktrace 帶來的好處，但這不是關於能夠關上所有門，因為某個人總是會打開一扇門 – 無論是被感染的 USB 隨身碟或是軟體驅動漏洞。重要的是一旦發生違規，您擁有能夠識別的能力。
>
> **- Group Head of Security, Drax**

更多資訊

馬上預約 Demo

雲端白皮書

Darktrace 用戶心得