



Adora ICT
CyberSecurity Linking Humans



Darktrace Immune System

Prodotti e servizi

Offerta tecnica

Indice

1. Darktrace Prodotti & Servizi	3
1.1 Darktrace Immune System	3
1.2 Suite Prodotti Darktrace	5
1.3 Servizi Professionali	6
1.4 Vantaggi	7



1. Darktrace

Prodotti & Servizi

Grazie all'AI "self-learning", Immune System di Darktrace è in grado di apprendere i normali "pattern of life" per rilevare e bloccare minacce informatiche sconosciute e imprevedibili.

Comprendendo il DNA digitale di un'organizzazione nella sua evoluzione, questa tecnologia adotta un approccio flessibile per quanto riguarda l'analisi e pervasivo per quanto riguarda l'ambito in cui agisce, ed è in grado di operare all'interno di e-mail, Cloud e piattaforme di collaborazione, nonché all'interno degli endpoint, degli ambienti IoT e delle reti. Più di 5000 organizzazioni in tutto il mondo si affidano a Darktrace per individuare e bloccare qualsiasi tipo di minaccia informatica, da attacchi completamente nuovi o minacce interne.

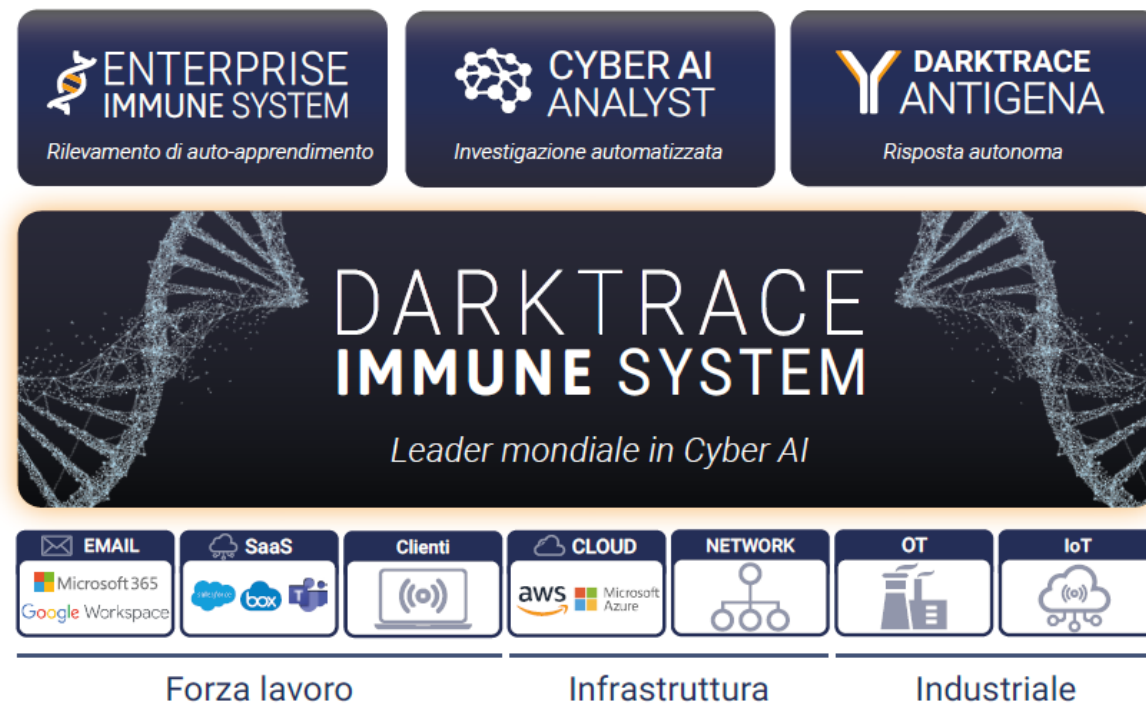
1. Darktrace

Immune System

L'Immune System di Darktrace è la tecnologia fondamentale basata sull'AI in grado di sfruttare una combinazione di machine learning supervisionato e non supervisionato all'interno della stessa piattaforma e di gestire autonomamente rilevamento, indagine e risposta alle minacce informatiche.

La Cyber AI di Darktrace si basa sul "self-learning", cioè non fa affidamento su regole statiche o dati relativi ad attacchi precedenti ma, al contrario, sviluppa una comprensione in continua evoluzione di ciò che è "normale" per la forza lavoro dinamica e le differenti strutture digitali. Questo comporta una protezione unificata all'interno di ambienti diversi come piattaforme Cloud, SaaS e di posta elettronica, nonché IoT, endpoint e sistemi cyberfisici.

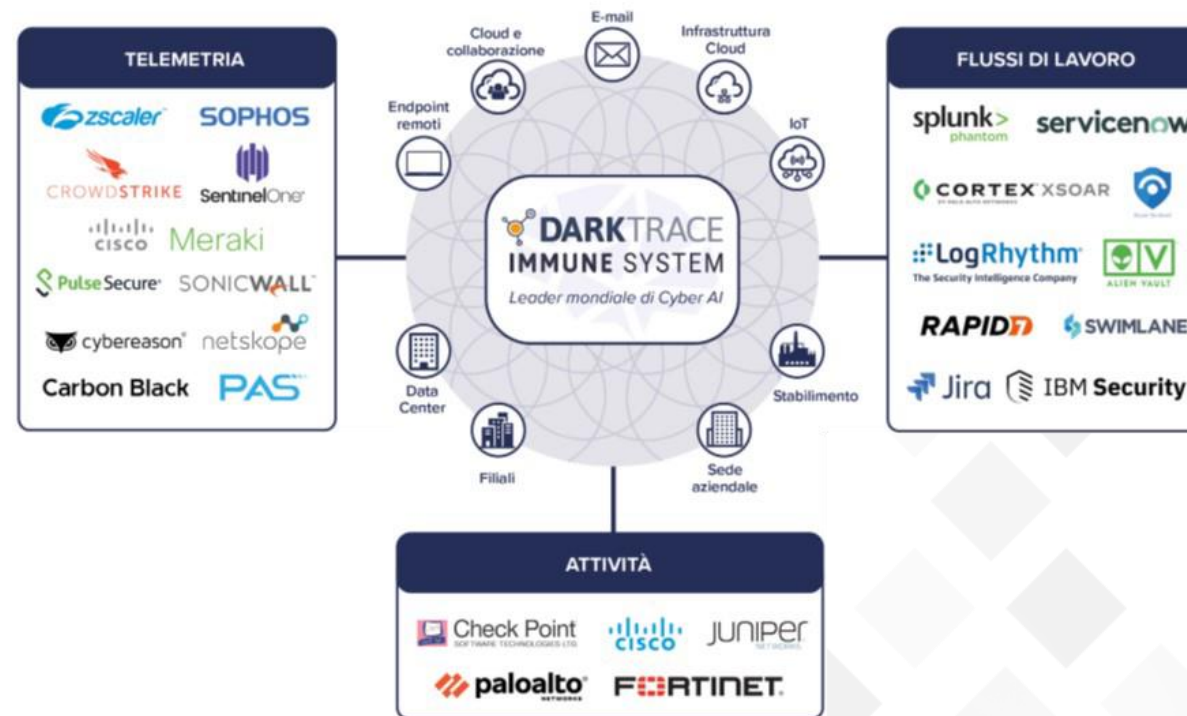
Proprio come il sistema immunitario dell'uomo, la capacità di Darktrace di distinguere comportamenti pericolosi da quelli sicuri, senza una conoscenza pregressa, consente di identificare le minacce informatiche che altri strumenti non sono in grado di individuare e analizzare.



Grazie alle sue funzioni di Autonomous Response, Darktrace Antigena sfrutta la sua intelligenza personalizzata per bloccare con precisione chirurgica anche gli attacchi in rapido movimento. Inoltre, il Cyber AI Analyst gestisce indagini automatizzate basate sull'AI per analizzare, interpretare e segnalare tutti i dati relativo agli incidenti di sicurezza.

Integrazioni Immune System

L'Immune System di Darktrace sfrutta un'architettura aperta e ampliabile per integrarsi facilmente nei diversi ecosistemi mentre si evolvono. Grazie ad integrazioni con un semplice clic, la piattaforma è in grado di elaborare istantaneamente nuove forme di telemetria, condividere informazioni AI personalizzate all'interno di flussi di lavoro definiti e interagire con un'ampia gamma di tecnologie per fornire la tecnologia di Autonomous Response all'interno di sistemi di posta elettronica, difese in linea e piattaforme di collaborazione.



1.2 Suite prodotti Darktrace



Enterprise Immune System: rilevamento delle minacce basato su "self-learning"

- Apprende "in corso d'opera" ciò che è normale per rilevare minacce sconosciute e imprevedibili
- Protegge la forza lavoro dinamica da attacchi zero-day, ransomware e minacce interne
- Protezione dell'intero DNA digitale di un'organizzazione all'interno di ambienti Cloud, endpoint, IoT e rete
- Sinergia con Cyber AI Analyst per l'attivazione di indagini e creazione di report automatizzati



Industrial Immune System: rilevamento delle minacce ICS

- Apprende "in corso d'opera" ciò che è normale per rilevare malware conosciuto e sconosciuto, minacce interne e rischi operativi
- Visualizzazione completa all'interno di ambienti OT, IT e IoT, si adatta a qualsiasi evoluzione
- Sinergia con Cyber AI Analyst per attivazione di indagini e creazione di report automatizzati
- Gestione di risorse di "self-learning" relative a qualsiasi fornitore e tecnologia



Cyber AI Analyst: indagine guidata dall'AI

- Aumenta le capacità dei team della sicurezza indagando automaticamente l'intero ambito degli incidenti di sicurezza
- Creazione di report che consentono ai team una risposta immediata
- Abbina l'intuito e la flessibilità dell'esperienza umana alla velocità e alla scalabilità dell'AI
- Possibilità di attivare le indagini anche on demand o tramite allarmi di terze parti
- Risparmio di tempo, fino al 92% di riduzione del tempo di analisi



Antigena Network: Autonomous Response

- Agisce in modo chirurgico per interrompere in pochi secondi attacchi imprevedibili e in rapido movimento
- Opera in modo dinamico, reagendo alla minaccia non appena si verifica
- Mantiene la normale operatività durante gli incidenti applicando ciò che è "normale"
- Risponde tramite azioni auto-gestite o integrazioni con terze parti utilizzando difese esistenti



Antigena Email: Autonomous Response

- Sfrutta l'AI per "comprendere la persona" alla base di un indirizzo e-mail
- Neutralizza e-mail pericolose che altri strumenti non rilevano
- Blocca gli attacchi di spear phishing e impersonificazione
- Mette a disposizione resoconti AI che dettagliano tutto ciò che riguarda le campagne di attacco neutralizzate
- Distribuzione basata su Cloud, installazione completata in pochi minuti



Antigena SaaS: Autonomous Response

- Neutralizza attacchi imprevedibili che colpiscono Cloud e tool di collaborazione
- Decisioni basate su self-learning AI che "comprendono le persone" alla base di account Cloud dinamici
- Reagisce più rapidamente di qualsiasi persona, prima che possa verificarsi qualsiasi danno
- Mette in pratica azioni precise mentre consente la normale operatività aziendale

1.3 Servizi Professionali

Una gamma di servizi per l'analisi delle minacce e la cyber intelligence disponibili per tutti i clienti, forniti dai Cyber Analyst di Darktrace o dai Partner certificati Darktrace. I Servizi di Darktrace sono progettati per soddisfare le necessità di organizzazioni di qualsiasi dimensione e settore industriale, fornendo ad ogni azienda un servizio personalizzato.

Proactive Threat Notification 24 ore su 24, 7 giorni su 7

- Servizio di notifica sulle minacce completo e proattivo, disponibile 24 ore su 24
- Contatto immediato del cliente in caso di attacco
- Più di 1.000 clienti, in aziende sia di grandi che di piccole dimensioni
- Servizio fornito dai Security Operations Centers (SOC) Darktrace di Cambridge, Regno Unito, San Francisco e Singapore

Ask the Expert

- Consente di ricevere rapidamente feedback e consigli competenti per la risoluzione dei problemi dai Cyber Analyst di Darktrace
- Funzione di chat facile da usare
- Assistenza 24 ore su 24, 7 giorni su 7

Servizi Adora

Il Team Sec Adora può erogare servizi di 1° livello, analizzando in tempo reale i log prodotti dall'Appliance ed evidenziare anomalie sui flussi di dati ed erogare le seguenti attività:

- **Log Management & Security Monitoring and Alerting**
Raccolta, monitoraggio ed analisi dei dati tracciati nei messaggi di log;
- **Security Incident Management**
Supporto operativo nel trovare risposte in caso di un incidente di sicurezza informatica.

Considerazioni generali

La raccolta, l'analisi ed il monitoraggio dei dati relativi ad un determinato tipo di Incidente, sono da considerarsi attività di supporto al 2° livello composta da Security Analyst.

Gli analisti IR (Incident Response) sono preposti a confrontare i dati forniti dall'analisi di 1° livello con i dati in loro possesso riguardanti gli asset IT (Configurazioni, Processi gestiti, ecc.) coinvolti nell'incidente. Una volta raccolte tutte le informazioni necessarie, gli specialisti IR definiscono l'attività di risanamento, avvalendosi dei responsabili del sistema IT del cliente.

In base a quanto precedentemente affermato, si ritiene che la tipologia di attività gestita dal Team Sec di Adora, possa essere considerata al più di supporto nel processo di gestione di un Incidente, fornendo ulteriore analisi ai dati relativi alla Infrastruttura IT oggetto di indagine.

1.4 Vantaggi

- **Risponde alle minacce più velocemente** di un qualsiasi team di sicurezza, grazie al suo sistema di AI

- Libera risorse e persone
Risparmio di tempo e di denaro

- Non interrompe l'operatività
Continuità del servizio

I nostri partner



Le nostre certificazioni





Via Mosca 10, 00142 Roma
Mac4 – Via Benigno Crespi 19 – 20159 Milano
Viale Magna Grecia 51 – 70126 Bari

Info Line:
Tel 0643400115
Fax 064340018

info@adora-ict.com

© Adora ICT - 2019 P.IVA 08590111004 / REA 1104976

