

# IVAR

IVAR è un'azienda che produce componenti per impianti termo-idraulici, inclusi modelli di misurazione diretta del calore, collettori di distribuzione e componenti per sistemi geotermici e solari. Operativa dal 1985, IVAR ha 11 filiali in tutto il mondo e produce per i propri clienti più di 10.000 articoli differenti.



## In sintesi

- Visibilità limitata all'interno dell'ecosistema digitale
- Dati estremamente sensibili e proprietà intellettuale presi di mira da attacchi sofisticati
- Scelta della self-learning AI per il rilevamento automatizzato delle minacce
- Fino al 92% di riduzione del tempo di analisi grazie a Cyber AI Analyst

**“Darktrace è in grado di mettere in evidenza eventi potenzialmente critici, indipendentemente dal fatto che siano correlati a minacce già conosciute o a tentativi di attacco mai rilevati prima.”**

Massimo Moimare, CIO, IVAR

## La convergenza OT/IT mette a rischio la sicurezza dei dati

L'essenza di IVAR è la costante innovazione. Con l'obiettivo di ridurre i consumi di energia sia come azienda che da parte dei propri clienti, il team sta ridefinendo nuovi confini nel campo della produzione grazie alle proprie tecnologie all'avanguardia e orientate al risparmio energetico.

Per migliorare l'efficienza operativa, IVAR ha collegato le proprie infrastrutture IT e OT. Ma, mentre la sinergia di questi sistemi cyber-fisici ha favorito l'innovazione e i risultati aziendali, le operazioni fondamentali del team e gli IP sensibili sono diventati nel contempo più vulnerabili agli attacchi. Un problema in particolare era rappresentato dalla crescente prevalenza degli attacchi informatici che prendevano di mira gli ambienti IT per assumere il controllo dei processi ICS.

Anche se la convergenza OT/IT comporta rischi tecnologici nuovi e significativi, fornisce anche un'opportunità per il miglioramento della sicurezza e della resilienza OT, grazie ad un approccio alla cyber defense che coinvolge tutta l'azienda. Per aiutare il team ad adattare e difendere la propria infrastruttura digitale e i dati più importanti, incluse le informazioni relative ai propri clienti e fornitori, IVAR ha scelto la Cyber AI di Darktrace per la rilevazione autonoma delle minacce e la visibilità real-time.

## Autonomous Cyber AI Defense

IVAR era stata presentata a Darktrace da un partner di sicurezza Fasternet, un fornitore di servizi gestiti. Fasternet fornisce servizi di monitoraggio e analisi digitali costanti, report di sicurezza regolari e incontri sulla threat intelligence relativi al continuo miglioramento delle strategie di cyber security di IVAR.

L'offerta tecnologica di Darktrace è apparsa subito interessante per IVAR e Fasternet, grazie alla propria natura AI-native e basata sul self-learning. Ispirata ai principi del sistema immunitario umano, la Cyber AI di Darktrace apprende ciò che è “normale” per ogni utente e dispositivo che appartiene a un'organizzazione e per tutti i collegamenti che li contraddistinguono. Ciò consente all'AI di individuare autonomamente gli impercettibili segnali di una minaccia in tempo reale, indipendentemente da quanto essa sia nuova o sofisticata.



Darktrace ha raggiunto questi obiettivi senza richiedere dati relativi ad attacchi storici, precedenti supposizioni o elenchi di CVE. Al contrario, apprende “in corso d’opera” per evolversi di pari passo con la forza lavoro e con i carichi di lavoro di IVAR in continuo cambiamento. Protocol-agnostic e technology-agnostic, Darktrace fornisce un sistema di difesa olistico e unificato all’interno delle infrastrutture IT, OT e IoT grazie alle sue capacità interamente autonome.

I flussi di lavoro relativi alla sicurezza sono stati drasticamente semplificati grazie a Cyber AI Analyst di Darktrace, che analizza, interpreta e segnala autonomamente l’ambito completo relativo agli incidenti di sicurezza. Generando autonomamente i report sugli incidenti, i team sono in grado di rispondere alle minacce non appena vengono rilevate. Riducendo fino al 92% il tempo di analisi, Cyber AI Analyst aumenta le capacità dei team della sicurezza umani, consentendo a Fasternet e IVAR di concentrare il loro tempo e le loro competenze dove sono più necessari.



## Visibilità in tutto l’ecosistema cyber-fisico

Darktrace è stata fondamentale nel rilevare minacce sofisticate presenti all’interno dell’ecosistema digitale di IVAR e che altri strumenti non avevano rilevato. Secondo Massimo Moimare, CIO di IVAR, “Darktrace è in grado di mettere in evidenza eventi potenzialmente critici, indipendentemente dal fatto che siano correlati a minacce già conosciute o a tentativi di attacco mai rilevati prima”.

Grazie a Darktrace il team ha ottenuto immediatamente risultati di valore. Meno di mezz’ora dopo aver installato il Darktrace Immune System, Fasternet e IVAR hanno ottenuto una visibilità senza uguali grazie a Threat Visualizer, l’interfaccia utente di Darktrace, vincitrice di numerosi riconoscimenti.

Il Threat Visualizer è completo: consente al team della sicurezza di monitorare attività e utenti specifici nel corso del tempo, riproducendo incidenti passati con qualsiasi livello di dettagli. Fornendo sia una panoramica di alto livello sull’ecosistema digitale che una comprensione più granulare a livello di subnet, utenti e dispositivi, il Threat Visualizer ha consentito al team di risolvere minacce e vulnerabilità in modo sempre più mirato e tempestivo. Ciò è stato fondamentale nella protezione di IVAR da exploit zero-day, esfiltrazione di dati e ransomware.

---

**“Darktrace è una soluzione di cyber security proattiva e personalizzabile in base a ogni singola realtà in cui viene installata.”**

Massimo Moimare, CIO, IVAR

---




**“Grazie a Darktrace, IVAR è in grado di proteggere le sue risorse più critiche, i suoi dati sensibili, sia dei clienti che dei fornitori, e la propria reputazione nel modo migliore possibile.”**

Massimo Moimare, CIO, IVAR



**L’intuitiva interfaccia utente di Darktrace individua le minacce all’interno dell’ecosistema digitale in tempo reale**

Per maggiori informazioni

-  Prenota una prova gratuita
-  Leggi il white paper sulla sicurezza
-  Visita il nostro canale YouTube