Cogne Acciai Speciali

335 TB
di traffico di rete analizzati

17.558
indagini automatizzate dall'AI

1.712
ore di analisi umana risparmiate

Cogne Acciai Speciali è un produttore globale di acciai inossidabili e leghe ad alte prestazioni, al servizio di settori critici tra cui energia, aerospazio, automotive e nucleare.

Ottenere una visibilità unificata tra ambienti IT e OT

Cogne Acciai Speciali è un'azienda che opera in contesti altamente regolamentati e mission-critical. I suoi materiali vengono infatti utilizzati in componenti chiave come motori e carrelli di aeromobili, dove affidabilità e continuità operativa sono essenziali.

L'articolata infrastruttura aziendale, con il sito produttivo principale ad Aosta e una presenza industriale e commerciale internazionale, richiede la gestione di un ecosistema tecnologico complesso che integra infrastrutture IT tradizionali e ambienti di controllo industriale interconnessi.

"Ora capiamo meglio come comunicano i nostri impianti, quali protocolli sono in esecuzione e dove possono esserci punti ciechi."

Network & Cyber Security Specialist
Cogne Acciai Speciali

Visibilità limitata tra sistemi IT e OT sempre più convergenti

Con la crescente interconnessione tra sistemi industriali, piattaforme ERP e ambienti di monitoraggio, la visibilità e il controllo sono diventati aspetti sempre più centrali.

"Oggi un impianto industriale non è più soltanto un insieme di macchine", spiega Andrea Gasperin, IT Manager. "È parte di un ecosistema connesso a sistemi ERP e piattaforme di monitoraggio. Questa integrazione è essenziale per il business, ma richiede anche una maggiore consapevolezza di ciò che accade sulla rete".

Prima dell'adozione di Darktrace, il team di sicurezza si affidava principalmente ad antivirus basati su firme, firewall perimetrali e strumenti di filtraggio email basati su regole. Sebbene efficaci contro le minacce note, queste soluzioni offrivano una visibilità limitata sul traffico laterale, sui protocolli industriali e sulle anomalie comportamentali tra ambienti IT e OT.

In pratica, questo significava che pur controllando i principali punti di accesso alla rete, l'azienda aveva una visibilità limitata sulle comunicazioni macchina-macchina, sulle interazioni tra PLC e sui possibili movimenti laterali all'interno delle reti industriali.

Anche la sicurezza della posta elettronica presentava criticità. I falsi positivi rallentavano negoziazioni commerciali, gestione delle fatture e comunicazioni urgenti con clienti e partner. Inoltre, tentativi di impersonificazione sofisticati – spesso privi di link o allegati malevoli – avevano richiesto indagini manuali del team IT.

Con la crescente convergenza tra IT e OT, Cogne Acciai Speciali ha deciso di rafforzare il proprio approccio alla cybersecurity, passando da una visione separata delle infrastrutture IT e OT a una visibilità unificata sull'intero ecosistema digitale e industriale.

Maggiore visibilità tra IT e OT grazie alla Self-Learning AI

La trasformazione è iniziata con l'implementazione di Darktrace / NETWORK e Darktrace / OT, che hanno introdotto visibilità sia sui sistemi IT aziendali sia sugli ambienti di controllo industriale.

Invece di basarsi su regole o firme predefinite, la Self-Learning AI di Darktrace analizza continuamente il comportamento della rete per comprendere il normale "pattern of life" dell'organizzazione, inclusi i protocolli industriali e le comunicazioni tra macchine.

Principali indicatori di visibilità e analisi

Nel corso di un recente periodo di riferimento analizzato nell'ambiente di Cogne Acciai Speciali, Darktrace ha elaborato oltre 335 TB di traffico di rete e analizzato l'attività di quasi 3.000 indirizzi IP interni. Nello stesso periodo, Cyber AI Analyst ha condotto 17.558 indagini autonome, equivalenti a 1.712 ore di analisi umana.

Per il team IT, è stato un cambiamento trasformativo.

"La differenza principale è stata la visibilità", afferma Gasperin. "Ora capiamo meglio come comunicano i nostri impianti, quali protocolli sono in esecuzione e dove possono esserci punti ciechi." Questo livello di visibilità consente di individuare più rapidamente anomalie, movimenti laterali sospetti e configurazioni errate sia negli ambienti IT sia in quelli OT. Con Darktrace, la visibilità è ora condivisa tra il team IT interno, gli ingegneri di impianto responsabili dei sistemi industriali e il SOC esterno di Cogne Acciai Speciali. Ne sono derivati processi di escalation più chiari e flussi di lavoro più strutturati tra questi gruppi, migliorando il coordinamento e accelerando la risposta agli incidenti.

"Lavoriamo a stretto contatto con il SOC", spiega Gasperin. "Avere una visione condivisa delle reti IT e industriali ci permette di intervenire più rapidamente e con più sicurezza."

Sicurezza email più intelligente con minore carico operativo

Cogne Acciai Speciali ha implementato Darktrace / EMAIL™ per le criticità persistenti di sicurezza della posta elettronica.

Gli strumenti di filtraggio tradizionali faticavano a distinguere tra linguaggio tecnico legittimo e contenuti malevoli, causando interruzioni delle attività. Allo stesso tempo, i tentativi di impersonificazione mirati richiedevano indagini manuali lunghe e complesse.

Con l'analisi comportamentale delle email basata su AI di Darktrace, i messaggi sospetti vengono analizzati automaticamente in base al contesto comportamentale e non solo a indicatori statici. Cyber AI Analyst classifica e indaga automaticamente tutti gli alert rilevanti, riducendo le verifiche manuali richieste al team IT.

Questo cambiamento ha migliorato l'efficienza rafforzando la fiducia degli utenti. I dipendenti ricevono informazioni contestuali più chiare sulle potenziali minacce, e possono prendere decisioni più consapevoli senza compromettere la continuità operativa.

Perché Darktrace?

Per Cogne Acciai Speciali, il fattore distintivo non è stato semplicemente aggiungere un ulteriore livello di sicurezza, ma ottenere una visibilità unificata tra ambienti IT e OT convergenti, abilitando al tempo stesso operazioni di sicurezza sempre più autonome.

La Self-Learning AI di Darktrace analizza di continuo il comportamento della rete in ambienti aziendali e industriali, apprendendo i normali modelli operativi dell'organizzazione. Questo diverso approccio comportamentale di Darktrace consente di individuare anomalie sottili e minacce emergenti che spesso sfuggono agli strumenti tradizionali basati su regole.

Allo stesso tempo, Cyber AI Analyst indaga automaticamente gli alert e correla i segnali rilevanti all'interno dell'infrastruttura, riducendo in modo significativo il carico investigativo manuale per i team di sicurezza

Combinando Darktrace / NETWORK, Darktrace / OT e Darktrace / EMAIL, Cogne Acciai Speciali ha costruito un modello di sicurezza proattivo che rafforza la protezione delle infrastrutture digitali e industriali e supporta al contempo le esigenze operative di un ambiente manifatturiero attivo 24 ore su 24.

Verso una cyber governance integrata

Con l'evoluzione dei requisiti normativi, inclusi gli sviluppi legati alla direttiva NIS2, la convergenza tra sicurezza IT e OT sta diventando sempre più strategica.

Con una visibilità misurabile sull'infrastruttura digitale e industriale, Cogne Acciai Speciali può oggi formalizzare ulteriormente i propri modelli di governance e rafforzare la collaborazione tra team IT, ingegneri di impianto e partner di sicurezza esterni.

Per l'organizzazione, rafforzare la cybersecurity non ha significato rallentare le operazioni, ma aumentare la consapevolezza, ridurre il carico investigativo e costruire una base più resiliente per una crescita industriale sicura e sostenibile.

"Avere una visione condivisa delle reti IT e industriali ci permette di intervenire più rapidamente e con più sicurezza."

Network & Cyber Security Specialist
Cogne Acciai Speciali