HWG Sababa

GRUPPO multicedi

Multicedi rafforza la resilienza cyber del proprio ecosistema retail da €2,1 miliardi con HyperSOC™ per IT e OT



Executive Summary

Multicedi, una delle principali aziende del Sud Italia nella grande distribuzione organizzata, gestisce circa **600 supermercati affiliati**, supportati da 5 centri di distribuzione e da un'infrastruttura digitale molto articolata.

Per rafforzare la sicurezza informatica del proprio ambiente IT e OT in continua evoluzione, Multicedi ha scelto di collaborare con **HWG Sababa**. Grazie all'adozione del servizio **HyperSOC™** e all'estensione della visibilità su migliaia di dispositivi connessi, l'azienda ha migliorato le proprie capacità di rilevamento e risposta alle minacce, ridotto il rischio operativo e consolidato il proprio percorso di adeguamento alla Direttiva NIS2.

Risultati principali

- **Monitoraggio continuo della sicurezza su 600 punti vendita e 5 centri di distribuzione**
- **+50% di miglioramento nei tempi di rilevamento e risposta alle minacce (MTTD / MTTR)**
- **Visibilità centralizzata su sistemi IT e migliaia di dispositivi OT connessi**
- **Rafforzamento della governance della sicurezza e maggiore preparazione alla NIS2**

Profilo dell'azienda

Multicedi è uno dei principali operatori della grande distribuzione organizzata nel Sud Italia. L'azienda gestisce una rete di circa 600 supermercati affiliati, operanti sotto diversi brand e supportati da cinque centri logistici distribuiti sul territorio.

L'organizzazione conta oltre 1.300 utenti – tra cui circa 300 dipendenti negli uffici e 1.000 operatori di magazzino e ha generato 2,1 miliardi di euro di fatturato nel 2025.

L'infrastruttura digitale dell'azienda riflette la scala e la complessità delle sue operazioni retail, combinando sistemi IT tradizionali con un numero crescente di dispositivi OT connessi che supportano le operazioni logistiche e le attività dei punti vendita.

Le principali sfide

Multicedi si è trovata ad affrontare diverse sfide di cybersecurity tipiche di ambienti retail di grandi dimensioni e altamente distribuiti.

Superficie di attacco estesa

L'azienda gestisce 5 centri di distribuzione collegati in modo continuativo a circa 600 punti vendita per attività di reporting fiscale, coordinamento logistico e gestione operativa. Ogni negozio, magazzino o sistema remoto rappresenta un potenziale punto di ingresso nella rete aziendale.

Infrastruttura ibrida e multi-cloud

Multicedi utilizza un'architettura ibrida: una parte dell'infrastruttura è on-premise, mentre la maggior parte delle applicazioni è distribuita su quattro diversi ambienti cloud, aumentando la complessità delle attività di monitoraggio e governance.

Visibilità limitata sull'Operational Technology

Migliaia di dispositivi OT – tra cui scanner, sistemi di magazzino, terminali Android, sistemi di refrigerazione e di controllo degli impianti – supportano le operazioni quotidiane. Molti di questi asset non rientrano nel perimetro dei tradizionali sistemi di monitoraggio IT.

Risorse interne dedicate alla sicurezza limitate

Nonostante la portata delle operazioni, il team IT interno è composto da 10 professionisti, responsabili di infrastrutture, applicazioni e sicurezza, con solo 2 figure dedicate alla cybersecurity.

Pressione normativa

In qualità di operatore del settore alimentare su larga scala, Multicedi deve conformarsi a normative europee in evoluzione, come la Direttiva **NIS2**, che richiedono livelli più elevati di governance, monitoraggio e gestione del rischio cyber.

A differenza di molte organizzazioni, Multicedi ha scelto di non attendere un incidente informatico prima di agire.

"Quando si opera su questa scala, la gestione del rischio non è un esercizio teorico. Se le operazioni si fermano anche solo per poco tempo, il costo è immediato."
– Livio De Prisco, CIO di Multicedi

La soluzione: operazioni di sicurezza integrate tra IT e OT

Per affrontare queste sfide e accompagnare il proprio percorso di trasformazione digitale, Multicedi ha avviato una collaborazione con un system integrator specializzato in ambienti IT e OT con 25 anni di esperienza nel supporto di grandi aziende retail in Italia. Insieme hanno definito una roadmap pluriennale per il potenziamento della sicurezza informatica.

Nel 2023, Multicedi ha selezionato **HWG Sababa come provider SOC**, adottando servizi di managed security operations attraverso **HyperSOC™**.

L'iniziativa ha dato vita ad un'architettura di sicurezza coordinata che combina monitoraggio continuo, rilevamento delle minacce, visibilità sugli asset e collaborazione operativa tra il SOC e il team IT interno di Multicedi.

A differenza di altre proposte focalizzate sull'implementazione autonoma di singole tecnologie, Multicedi ha scelto un approccio basato su un **ecosistema integrato**. Il partner ha guidato la progettazione dell'infrastruttura e l'integrazione della sicurezza endpoint, mentre HWG Sababa ha fornito servizi di managed detection and response tramite HyperSOC™, garantendo monitoraggio continuo e supporto operativo.

" Con un'infrastruttura così distribuita, il vero valore non è aggiungere strumenti ma costruire un framework coerente che permetta di avere controllo sull'intero ecosistema."
– Livio De Prisco, CIO of Multicedi

Capacità implementate

Managed Security Operations con HyperSOC™
Implementazione di un monitoraggio SOC 24/7 con correlazione SIEM sull'intero perimetro IT e gestione centralizzata dei log. HyperSOC™ funge da piattaforma centrale per monitoraggio, rilevamento e risposta, costituendo il fulcro operativo delle tecnologie di sicurezza distribuite nell'ambiente. Gli analisti SOC collaborano direttamente con il team IT di Multicedi, garantendo supervisione continua ed expertise specializzata.

Endpoint Threat Detection and Response
Implementazione di funzionalità di managed detection and response sugli endpoint tramite SentinelOne, consentendo l'identificazione e il contenimento rapido di attività sospette.

Visibilità e mappatura degli asset OT
Implementazione di Armis Centrix™ per l'Asset Management e la sicurezza, una piattaforma avanzata di cyber exposure management per ambienti OT, che ha permesso a Multicedi di ottenere visibilità in tempo reale su migliaia di dispositivi connessi nella propria infrastruttura distribuita. La piattaforma ha identificato e classificato automaticamente un'ampia gamma di asset, tra cui scanner barcode, sistemi di gestione del magazzino, terminali Android, unità di refrigerazione e sistemi di controllo edifici, eliminando i punti ciechi e portando alla luce dispositivi precedentemente non gestiti.

Monitoraggio della supply chain e degli accessi di terze parti
Monitoraggio continuo delle connessioni dei fornitori e dei punti di accesso di terze parti, rafforzando il controllo sull'ecosistema dei partner. Le misure includono limiti automatici alle sessioni VPN, il blocco degli account dopo tentativi di accesso falliti e il monitoraggio di attività anomale.

Hyperautomation nel SOC
Introduzione graduale di meccanismi di automazione all'interno di HyperSOC™ per accelerare i processi di investigazione e risposta agli incidenti, riducendo le attività manuali e migliorando i tempi di intervento.

I risultati: stabilità operativa e resilienza misurabile

Grazie all'implementazione di HyperSOC™, Multicedi ha rafforzato la propria postura di sicurezza mantenendo al tempo stesso continuità operativa sull'intera rete retail.

Il monitoraggio continuo e il coordinamento delle operazioni SOC hanno migliorato le capacità di rilevamento e risposta alle minacce, aumentando al contempo la visibilità sull'infrastruttura IT e OT dell'organizzazione.

Risultati operativi

Il progetto ha portato miglioramenti concreti nelle operazioni di sicurezza:

- **Riduzione del rischio operativo** su 600 punti vendita e 5 centri di distribuzione
- **Riduzione del 50% nei tempi di rilevamento e risposta** alle minacce (MTTD e MTTR)
- **Visibilità centralizzata sugli asset IT e OT**, inclusi migliaia di dispositivi operativi
- **Maggiore controllo sugli accessi di fornitori e terze parti**, con rilevamento e prevenzione più rapide di attività non autorizzate
- **Maggiore allineamento ai requisiti della Direttiva NIS2**, grazie a capacità di governance e monitoraggio rafforzate

Il supporto continuo del SOC ha inoltre **aumentato l'efficacia del team IT interno**, permettendo alle risorse di concentrarsi sull'evoluzione dell'infrastruttura e su iniziative strategiche anziché sulla gestione reattiva degli incidenti.

Impatto strategico

Oltre ai miglioramenti operativi, l'iniziativa ha rafforzato la cybersecurity governance all'interno dell'organizzazione.

Il rischio cyber è oggi considerato un rischio di business, discusso regolarmente a livello di executive e board. La partecipazione del management ai programmi di sensibilizzazione sulla sicurezza, in linea con i requisiti della Direttiva NIS2, ha ulteriormente rafforzato la capacità dell'organizzazione di governare e gestire i rischi informatici .

Grazie alla combinazione tra l'expertise architetturale del partner e il servizio HyperSOC™ di HWG Sababa, Multicedi ha sviluppato un modello di sicurezza centralizzato in grado di supportare la scala e la complessità della propria infrastruttura retail distribuita.

Le prossime fasi della roadmap prevedono attività di penetration testing su tutti i punti vendita affiliati, con l'obiettivo di potenziare la sicurezza dell'intero ecosistema retail.

"Nessuna organizzazione è intoccabile. La lezione principale è non tentare di gestire la cybersecurity da soli. I team IT interni raramente sono specialisti della difesa cyber. Senza partner esperti si rischia di spendere di più ottenendo meno protezione."

– Livio De Prisco, CIO di Multicedi