REEVO | GRIMALDI GROUP

CASE STUDY

Come Grimaldi Group protegge logistica e supply chain con ReeVo

SUMMARY

CASE STUDY

REEVO | GRIMALDI GROUP

Come Grimaldi Group protegge logistica e supply chain con ReeVo

Nel settore della logistica internazionale, la continuità operativa non è semplicemente un obiettivo tecnologico: è un requisito strategico. Un cardine del presente e del futuro di una impresa.
Per un gruppo che gestisce flotte, terminal, supply chain e flussi informativi distribuiti in tutto il mondo, la cybersecurity diventa un elemento essenziale per garantire efficienza, affidabilità e competitività.

È esattamente nel cuore di questa centralità, con tutte le conseguenze che comporta, che si inserisce il percorso di trasformazione digitale e di sicurezza intrapreso da **Grimaldi Group** grazie alla collaborazione con ReeVo, un incrocio virtuoso quello tra le due società che, negli anni, ha contribuito a costruire un **modello di difesa evoluto, resiliente e orientato alla prevenzione**.

CASE STUDY

REEVO | GRIMALDI GROUP

Un gigante globale della logistica integrata

Parlare di Grimaldi Group significa parlare di uno dei **principali protagonisti mondiali della logistica integrata**. Un ecosistema complesso che unisce trasporto marittimo, terminal portuali e logistica terrestre in una rete internazionale che movimenta merci e persone ogni giorno.
“Grimaldi è un attore internazionale storico che da tre generazioni affronta logistica integrata, quindi non solo sul mare ma anche nei terminal a terra”, racconta il **Generale Paolo Pelosi, CISO e Direttore SILE del Gruppo**. “Ha un numero di dipendenti prossimo ai 16.000 con un indotto che viaggia intorno alle 100.000 persone, con una flotta che supera le 150 navi, con un fatturato mondiale di oltre 5,5 miliardi”.
Numeri che spiegano bene il livello di complessità da gestire. Ogni nave, ogni terminal, ogni piattaforma digitale e ogni sistema informativo rappresentano nodi critici di una catena globale che deve rimanere sempre operativa.
In questo contesto, la protezione dei dati e delle infrastrutture digitali non riguarda solo l’IT, ma la **capacità stessa dell’azienda di garantire continuità al business e affidabilità al mercato.**

CASE STUDY

REEVO | GRIMALDI GROUP

Innovazione, sostenibilità e sicurezza: un equilibrio strategico

Negli ultimi anni il mondo della logistica ha vissuto una trasformazione radicale. L'automazione dei processi, l'interconnessione tra supply chain e l'adozione di piattaforme digitali hanno aumentato enormemente le opportunità, ma anche la superficie di attacco.
Per Grimaldi Group, **innovazione e sostenibilità devono procedere insieme alla sicurezza**.
"La sostenibilità è diventata un fattore moltiplicatore di propulsione anche del business", spiega Paolo Pelosi. "Accompagnato contemporaneamente con la giusta misura dall'attenzione alla sicurezza e prima di tutto il fattore umano che è quello che poi mette in atto tutte le strategie".
Il fattore umano emerge come elemento centrale della strategia. Non solo tecnologia quindi, ma **cultura della sicurezza** diffusa all'interno dell'organizzazione.
Secondo Pelosi, proprio questo approccio consente di evitare che la sicurezza venga percepita come un limite operativo o un ostacolo alla crescita.
"Il primo elemento che fa sì che l'**implementazione della sicurezza non sia un fatto rigido che possa andare a detrimento del business** è coinvolgere il fattore umano sotto l'aspetto della cultura della sicurezza", sottolinea il manager.
Da qui nasce anche la scelta del Board di rafforzare la governance cyber con una struttura dedicata.
"La proprietà ha fatto sì che all'interno del Sile stesso si creasse un settore dedicato alla cyber sicurezza che possa perseguire la tutela della propria clientela per quanto riguarda i dati e le infrastrutture, posando quindi la propria complessità su delle basi estremamente solide ma molto resilienti".

CASE STUDY

REEVO | GRIMALDI GROUP

Dal modello perimetrale alla difesa multilivello

L'evoluzione tecnologica del Gruppo ha richiesto anche una trasformazione profonda delle strategie di cybersecurity.
Luigi Cavucci, Deputy CISO di Grimaldi Group spiega come l'azienda sia passata da un approccio tradizionale a un modello di sicurezza molto più avanzato.
"Le nostre strategie sono state allineate a quello che è il contesto digitale, a quello che è stata l'innovazione che Grimaldi ha inserito in quasi tutti i suoi processi".
Il cambio di paradigma è stato netto.
"Siamo partiti da un modello di difesa perimetrale per approdare a un **modello basato sul defense in depth**", racconta Cavucci. "Abbiamo istituito delle sentinelle dei controlli di sicurezza su diversi strati proteggendo dati, applicazioni e identità".
Non più quindi un unico punto di controllo, ma un **sistema distribuito e capace di monitorare continuamente ogni livello dell'infrastruttura**.
Questo approccio permette oggi a Grimaldi di identificare e contrastare le minacce in tempo reale, riducendo drasticamente i tempi di reazione e aumentando la resilienza complessiva.

CASE STUDY

REEVO | GRIMALDI GROUP

La partnership con ReeVo: un percorso costruito nel tempo

La collaborazione con ReeVo nasce da lontano.
“Quelli che allora erano i ragazzi di Security Lab erano una boutique di sicurezza, li abbiamo incrociati dieci anni fa e con loro abbiamo iniziato un percorso”, ricorda Luigi Cavucci.
Nel tempo, la crescita di Grimaldi Group e l’evoluzione delle minacce hanno richiesto una maturazione parallela anche da parte del partner tecnologico.
“Essendo noi una multinazionale in crescita, anche dal punto di vista della consapevolezza in quanto a sicurezza delle informazioni, avevamo bisogno che anche Security Lab facesse questo passaggio insieme a noi”.
L’ingresso nel gruppo ReeVo ha rappresentato un punto di svolta.
“Abbiamo accolto con favore la notizia e dopo un primo periodo di assestamento abbiamo toccato da subito con mano i vantaggi dei nuovi servizi di Security Lab inseriti nel gruppo ReeVo”.

CASE STUDY

REEVO | GRIMALDI LINES

Il SOC come cuore della cyber resilience

Uno degli ambiti in cui il cambiamento è stato più evidente riguarda il Security Operations Center.
“Il servizio che più ha beneficiato di questo cambio è stato sicuramente il **SOC**”, afferma Cavucci. “La capacità di monitoraggio e di prevenzione, anche di classificazione degli eventi che impattano sul nostro patrimonio informativo è aumentata”.
Per un’organizzazione globale come Grimaldi, **il monitoraggio continuo rappresenta una leva strategica fondamentale**. La rapidità con cui una minaccia viene identificata può fare la differenza tra un semplice alert e un blocco operativo con impatti sulla supply chain internazionale.
Il SOC sviluppato insieme a ReeVo si basa su un approccio evoluto di Security Operations che integra monitoraggio continuo H24, **analisi comportamentale, correlazione avanzata degli eventi e capacità di risposta automatizzata**. L’obiettivo non è soltanto identificare un attacco in corso, ma **intercettare anomalie** e indicatori di compromissione **prima che possano trasformarsi in un incidente** capace di impattare l’operatività globale del Gruppo.
Con la “defense in depth” ogni componente infrastrutturale - come ad esempio firewall, endpoint, sistemi di identity management, workload cloud, reti operative e applicazioni critiche - alimenta continuamente il motore di analisi del SOC. Viene quindi monitorata e protetta in modo indipendente, ma coordinato.
“La capacità di identificazione più pronta in real time a fronte di minacce sempre più pericolose” è diventata uno dei pilastri della nuova strategia cyber del Gruppo.
Uno degli aspetti più innovativi introdotti insieme a ReeVo riguarda inoltre l’approccio **CTEM, Continuous Threat Exposure Management**, integrato direttamente nelle attività del SOC. Non ci si limita quindi al monitoraggio passivo dell’infrastruttura: il team simula continuamente scenari di attacco realistici per verificare il reale livello di esposizione alle minacce.
“Sostanzialmente noi simuliamo degli scenari di attacco cercando di anticipare i tempi rispetto a nuove minacce o vulnerabilità critiche che magari una semplice scansione non avrebbe mai rilevato”.
Questo modello consente di **individuare vulnerabilità latenti, validare la resilienza delle infrastrutture e migliorare costantemente le capacità di detection e risposta agli incidenti.**

A rafforzare ulteriormente il SOC entra in gioco anche l'intelligenza artificiale. ReeVo ha integrato **capacità di AI e automazione nei processi di Security Orchestration, accelerando le attività di classificazione, prioritizzazione e remediation degli incidenti.**
"Nello sviluppo di questa soluzione proprietaria si è inserito il gruppo ReeVo con la soluzione di Security Orchestration pilotata anche dall'intelligenza artificiale".
In pratica, il **SOC è oggi in grado di automatizzare numerose attività operative**: correlazione avanzata degli eventi, analisi comportamentale, arricchimento automatico degli alert tramite threat intelligence e attivazione immediata delle prime contromisure.
Un **ruolo centrale** viene sempre svolto anche dalla **cyber threat intelligence**. Attraverso feed informativi aggiornati e bollettini continui sulle minacce emergenti, ReeVo supporta Grimaldi nella protezione non solo dell'infrastruttura interna ma anche dell'intero ecosistema digitale collegato alla supply chain.
"Il gruppo ReeVo ci aiuta a presidiare quelli che sono i punti di contatto digitali con i nostri partner e fornitori, garantendoci anche con il contrasto in real-time di minacce emergenti la resilienza della catena di approvvigionamento".

CTEM e simulazione degli attacchi: la sicurezza diventa predittiva

L'adozione del CTEM è un passaggio fondamentale: la **sicurezza non è più solamente reazione agli incidenti**, ma capacità di prevedere e testare continuamente i possibili scenari di rischio.
In un ecosistema globale interconnesso, questo approccio consente di aumentare la resilienza operativa e **ridurre drasticamente l'esposizione alle vulnerabilità**.

CASE STUDY

REEVO | GRIMALDI GROUP

L’intelligenza artificiale come pilastro operativo

All’interno della strategia cyber di Grimaldi, l’intelligenza artificiale è già oggi un elemento concreto e operativo. “Per noi l'intelligenza artificiale è già un pilastro operativo”, spiega Cavucci.
Uno dei primi esempi è rappresentato dal sistema GSBot (Grimaldi Security Bot), sviluppato per contrastare il phishing. “Siamo partiti con una soluzione automatica di identificazione e contrasto di minacce che vengono dal phishing”, racconta il Deputy CISO. “Oggi GSBot, basato sull'intelligenza artificiale, è in grado anche di fornire risposte agli utenti”.
Il valore aggiunto non è solo tecnologico ma anche culturale.
“Oltre a fare prevenzione e contrasto, fa anche formazione, quindi innalza il grado di consapevolezza dei nostri utenti”.
L’AI viene utilizzata anche nell’orchestrazione della sicurezza e nella gestione delle minacce emergenti grazie alle soluzioni sviluppate insieme a ReeVo.

Proteggere la supply chain significa proteggere il business

Per Grimaldi Group la resilienza non riguarda soltanto l’azienda, ma l’intero ecosistema di partner, fornitori e clienti.
“Abbiamo capito che la nostra **resilienza passa anche per quella dei nostri fornitori e dei nostri partner”, afferma Cavucci.**
È qui che la collaborazione con ReeVo assume un ruolo strategico.
“Il gruppo ReeVo ci aiuta a presidiare quelli che sono i punti di contatto digitali con i nostri partner e i nostri fornitori, e ci garantisce anche, con il contrasto in real-time di minacce emergenti, la resilienza della catena di approvvigionamento”.
La **protezione della supply chain diventa quindi parte integrante della strategia di business continuity**.

Un modello maturo, flessibile e tecnologicamente agnostico

Uno degli aspetti più interessanti del modello costruito da Grimaldi insieme a ReeVo è la sua capacità di evolvere nel tempo senza dipendere da una singola tecnologia.
“Il modello sviluppato con ReeVo oggi è un modello molto maturo”, conclude Luigi Cavucci. “Credo che uno dei pilastri di questo **modello** sia il fatto che è **agnostico dal punto di vista tecnologico**”.
Questa caratteristica permette al Gruppo di integrare continuamente nuove tecnologie e nuove capacità senza dover ripensare l’intera architettura di sicurezza.
“ReeVo è in grado di suggerirci tecnologie sempre più all'avanguardia, nelle migliori condizioni possibili, soprattutto dal punto di vista della threat intelligence, così come della risposta agli attacchi informati”.

Il futuro di Grimaldi Group tra crescita globale e centralità delle persone

Guardando al futuro, Grimaldi Group punta a rafforzare ulteriormente la propria presenza internazionale **mantenendo però saldi i valori che hanno guidato la crescita dell’azienda.**
“Grimaldi nel futuro continuerà a mantenere la propria identità e personalità in una dimensione molto più globale a livello mondiale”, conclude Paolo Pelosi. “Senza mai tradire il concetto di sostenibilità, di operatività, di etica e senza che venga mai trascurato quello che è il fattore umano”.
Ed è proprio questo **equilibrio tra innovazione, sicurezza, sostenibilità e cultura aziendale che rende il caso Grimaldi-ReeVo un esempio concreto di come la cybersecurity possa diventare un abilitatore strategico della trasformazione digitale.**

REEVO

#ReeVolutionaryStory