>_Code blue
by Dussmann

# SUPPLY CHAIN
## DAL CONTROLLO ALLA RESILIENZA

### >_ Third Party Cyber Risk Management e resilienza digitale

Il quadro normativo europeo in materia di cybersecurity e protezione dei dati ha innalzato in modo significativo le aspettative sulla gestione del rischio cyber di terze parti (TPCRM).

Le organizzazioni sono chiamate ad adottare **processi chiari e strutturati** per la gestione e la segnalazione degli incidenti che coinvolgono i fornitori.

Devono inoltre verificare in modo continuativo **l'efficacia delle misure di sicurezza** e integrare nei rapporti contrattuali **requisiti di cybersecurity espliciti, misurabili e verificabili**.

La gestione della supply chain, quindi, non può più essere improvvisata o affrontata solo quando emerge un problema.

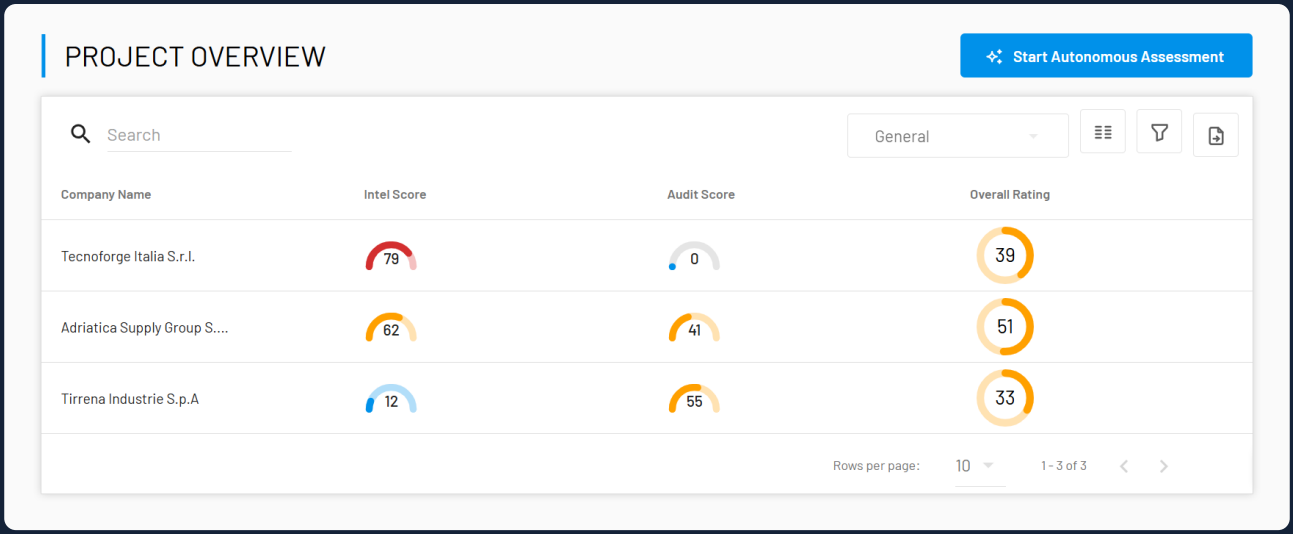
Per rispondere a queste esigenze, diventa essenziale implementare un approccio strutturato e completo, in grado di accompagnare il fornitore lungo tutto il suo ciclo di vita - dall'onboarding fino alla chiusura del rapporto.

Questo significa monitorare il rischio in modo continuativo, analizzando le minacce attraverso fonti pubbliche e private, e osservando i dati che emergono da ambienti underground e dark web, al fine di individuare tempestivamente potenziali segnali di compromissione.

# La soluzione di Code Blue

La piattaforma TPCRM di Code Blue consente una gestione strutturata, scalabile e conforme del rischio di terze parti, attraverso un'architettura integrata che combina automazione avanzata e Intelligenza Artificiale.
Il sistema mette a disposizione un **registro centrale dei fornitori**, con classificazione automatica basata su **livello di rischio, settore e conformità normativa**, garantendo una **tracciabilità end to end della supply chain**.
Le valutazioni del rischio sono automatizzate tramite **questionari standardizzati** - allineati a normative quali **NIS2, DORA, ISO/IEC 27001, SOC 2 e GDPR**.

Il monitoraggio continuo si basa sull'analisi di database di violazioni note, repository di vulnerabilità e fonti di intelligence sul dark web.
La **gestione contrattuale centralizzata** consente di monitorare il rispetto degli **SLA**, evidenziare eventuali carenze contrattuali (come, ad esempio, l'assenza di clausole di audit) e definire livelli minimi di sicurezza.
Ogni attività viene registrata e tracciata in modo completo, garantendo piena trasparenza e trattando i dati in piena conformità al GDPR.




# Intelligenza Artificiale al servizio del TPCRM

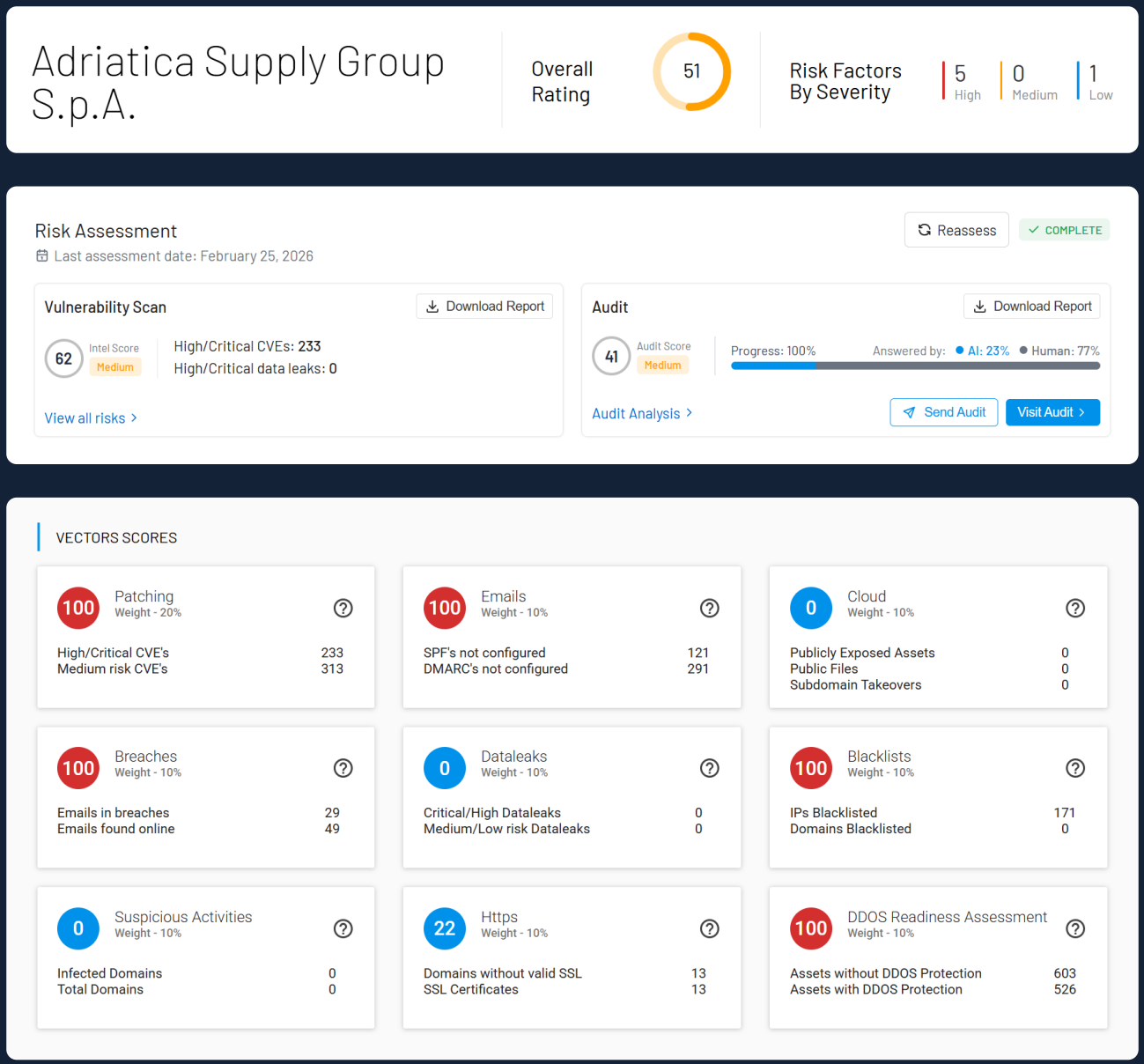
La piattaforma integra Intelligenza Artificiale per rendere la gestione del rischio fornitori più rapida, coerente e affidabile, operando in ambienti isolati e regionalizzati, senza alcun utilizzo dei dati dei clienti per l'addestramento dei modelli.
L'AI elabora esclusivamente le informazioni strettamente necessarie, protegge le PII secondo principi di minimizzazione e sicurezza, non trasferisce mai credenziali o dati sensibili ed è progettata con controlli multilivello (crittografia, accessi basati su ruoli, API isolate e logging protetto).
Opera entro regole e controlli ben definiti e supporta attività come la sintesi dei documenti, la classificazione dei fornitori, l'analisi della threat intelligence e il supporto alla remediation - mantenendo sempre il ruolo centrale del giudizio umano.

>_Code blue
by Dussmann

## Tabella Comparativa: Requisiti Normativi vs. Capacità Piattaforma CODE BLUE

| Requisito Normativo | Capacità Richieste | Caratteristiche Piattaforma CODE BLUE |
|---|---|---|
| **MONITORAGGIO CONTINUO**<br>NIS2 Art. 21, DORA Art. 28 | • Scansione dark web<br>• Fonti OSINT<br>• Database vulnerabilità<br>• Registro rischi unificato<br>• Punteggio rischio dinamico | ☑ **Valutazioni Passive OSINT**<br>Identificazione vulnerabilità senza indagini attive |
| | | ☑ **Monitoraggio dark web**<br>(forum criminali, credential leaks, ecc.) |
| | | ☑ **Registro centrale rischi**<br>con correlazione automatica dati |
| | | ☑ **Matrice probabilità/impatto**<br>per prioritizzazione |
| **REQUISITI CONTRATTUALI**<br>GDPR Art. 28, NIS2 Art. 21 | • Repository centralizzato<br>• Gestione SLA<br>• Clausole diritto alla revisione<br>• Audit trail<br>• Workflow approvazione | ☑ **Workflow automatizzati** |
| | | ☑ **Permessi basati su ruoli** |
| **GESTIONE CICLO VITA FORNITORE**<br>DORA Art. 28, NIS2 Art. 21 | • Registro centrale<br>• Onboarding automatizzato<br>• Tiering basato su rischio<br>• Procedure offboarding | ☑ **Individuazione e Classificazione AI**<br>Identificazione fornitori critici end-to-end |
| | | ☑ **Tiering automatico**<br>per rischio, settore, conformità |
| | | ☑ **Visibilità Supply Chain** completa |
| **VALUTAZIONE RISCHI**<br>DORA Art. 30, NIS2 Art. 21 | • Questionari standardizzati<br>• Algoritmi scoring<br>• Rivalutazioni programmate<br>• Modelli compliance | ☑ **Valutazioni Automatizzate AI**<br>Compilazione assistita questionari |
| | | ☑ **Modelli predefiniti**<br>(NIS2, DORA, ISO 27001, SOC 2, GDPR) |
| | | ☑ **Monitoraggio continuo** con trigger rivalutazione |
| | | ☑ **Riduzione tempi risposta** fornitori |
| **CONFORMITÀ DOCUMENTAZIONE**<br>Tutti i framework | • Audit trail completo<br>• Archiviazione documenti<br>• Dashboard compliance<br>• Raccolta prove regolatori | ☑ **Reportistica di Conformità**<br>Report automatizzati per audit readiness |
| | | ☑ **Audit trail** di tutte le valutazioni e accessi |
| **PROTEZIONE DATI**<br>GDPR, Schrems II | • Residenza dati UE<br>• Trattamento GDPR-compliant<br>• Meccanismi trasferimento<br>• DPA management | ☑ **Residenza Dati UE** configurabile |
| | | ☑ **Trattamento GDPR-compliant** nativo |
| | | ☑ **Meccanismi Schrems II** implementati |
| **INTEGRAZIONE ECOSISTEMA**<br>Requisito operativo | • API aperte<br>• Connettori pre-built<br>• Export dati | ☑ **API per integrazioni** personalizzate |
| | | ☑ **Connettori pre-assemblati** (Slack, Teams, JIRA) |
| | | ☑ **Capacità esportazione** multi-formato |

**La piattaforma di CODE BLUE trasforma la compliance da obbligo normativo a vantaggio competitivo, riducendo lo sforzo manuale considerevolmente e accorciando i tempi di risposta dei fornitori grazie all'intelligenza artificiale.**




Code Blue Italy nasce come joint venture tra Dussmann Service Italia e Code Blue Ltd, leader internazionale nella gestione delle crisi cyber.

È il partner strategico per le organizzazioni che vogliono affrontare il rischio informatico in modo strutturato e orientato alla resilienza, preparandosi prima che l'attacco avvenga, intervenendo con efficacia durante l'emergenza e guidando il recupero dopo l'incidente.

Nel solo 2025 Code Blue ha gestito oltre 100 crisi cyber complesse a livello internazionale, trasformando l'esperienza sul campo in metodologie concrete di preparazione, risposta e ripartenza.

Formazione, processi collaudati e supporto decisionale permettono alle aziende di ridurre l'impatto operativo, economico e reputazionale e tornare rapidamente alla continuità.

>_Code blue
by Dussmann

info@codebluecyber.it
www.codebluecyber.it