



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

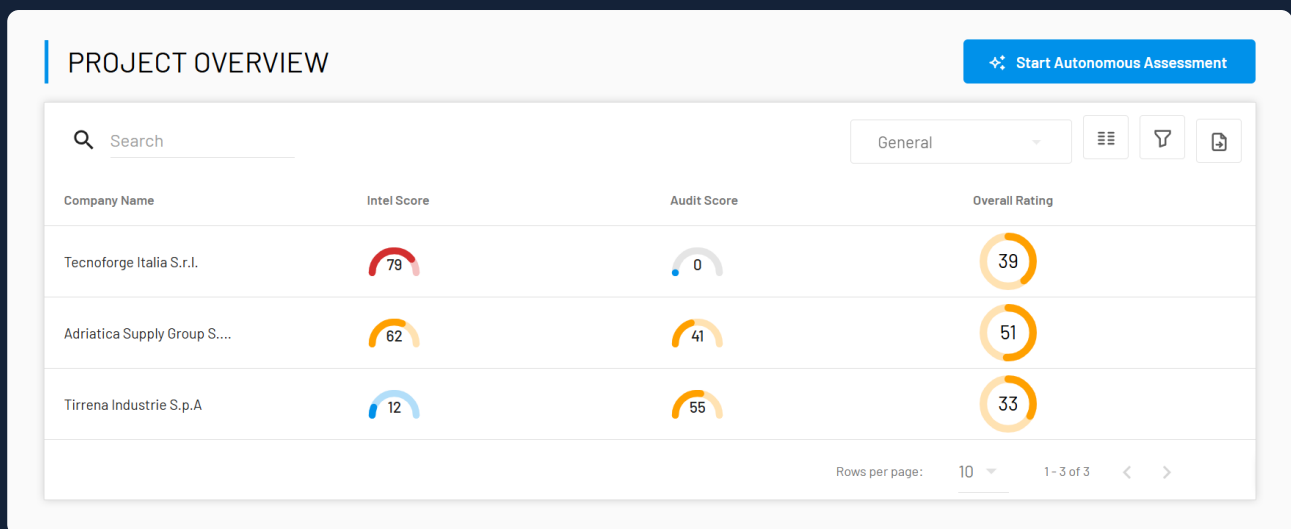
La piattaforma TPCRM di Code Blue consente una gestione strutturata, scalabile e conforme del rischio di terze parti, attraverso un'architettura integrata che combina automazione avanzata e Intelligenza Artificiale. Il sistema mette a disposizione un **registro centrale dei fornitori**, con classificazione 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.



The screenshot displays a 'PROJECT OVERVIEW' dashboard. At the top right, there is a blue button labeled 'Start Autonomous Assessment'. Below the header, there is a search bar and a 'General' filter dropdown. The main content is a table with four columns: 'Company Name', 'Intel Score', 'Audit Score', and 'Overall Rating'. Each score is represented by a semi-circular gauge. At the bottom right, there is a pagination control showing 'Rows per page: 10' and '1 - 3 of 3'.

Company Name	Intel Score	Audit Score	Overall Rating
Tecnoforge Italia S.r.l.	78	0	39
Adriatica Supply Group S...	62	41	51
Tirrena Industrie S.p.A	12	55	33

>_ 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 **Dusmann**

Tabella Comparativa: Requisiti Normativi vs. Capacità Piattaforma CODE BLUE

Requisito Normativo	Capacità Richieste	Caratteristiche Piattaforma CODE BLUE
MONITORAGGIO CONTINUO NIS2 Art. 21, DORA Art. 28	<ul style="list-style-type: none"> • Scansione dark web • Fonti OSINT • Database vulnerabilità • Registro rischi unificato • Punteggio rischio dinamico 	<input checked="" type="checkbox"/> Valutazioni Passive OSINT Identificazione vulnerabilità senza indagini attive
		<input checked="" type="checkbox"/> Monitoraggio dark web (forum criminali, credential leaks, ecc.)
		<input checked="" type="checkbox"/> Registro centrale rischi con correlazione automatica dati
		<input checked="" type="checkbox"/> Matrice probabilità/impatto per prioritizzazione
REQUISITI CONTRATTUALI GDPR Art. 28, NIS2 Art. 21	<ul style="list-style-type: none"> • Repository centralizzato • Gestione SLA • Clausole diritto alla revisione • Audit trail • Workflow approvazione 	<input checked="" type="checkbox"/> Workflow automatizzati
		<input checked="" type="checkbox"/> Permessi basati su ruoli
GESTIONE CICLO VITA FORNITORE DORA Art. 28, NIS2 Art. 21	<ul style="list-style-type: none"> • Registro centrale • Onboarding automatizzato • Tiering basato su rischio • Procedure offboarding 	<input checked="" type="checkbox"/> Individuazione e Classificazione AI Identificazione fornitori critici end-to-end
		<input checked="" type="checkbox"/> Tiering automatico per rischio, settore, conformità
		<input checked="" type="checkbox"/> Visibilità Supply Chain completa
VALUTAZIONE RISCHI DORA Art. 30, NIS2 Art. 21	<ul style="list-style-type: none"> • Questionari standardizzati • Algoritmi scoring • Rivalutazioni programmate • Modelli compliance 	<input checked="" type="checkbox"/> Valutazioni Automatizzate AI Compilazione assistita questionari
		<input checked="" type="checkbox"/> Modelli predefiniti (NIS2, DORA, ISO 27001, SOC 2, GDPR)
		<input checked="" type="checkbox"/> Monitoraggio continuo con trigger rivalutazione
		<input checked="" type="checkbox"/> Riduzione tempi risposta fornitori
CONFORMITÀ DOCUMENTAZIONE Tutti i framework	<ul style="list-style-type: none"> • Audit trail completo • Archiviazione documenti • Dashboard compliance • Raccolta prove regolatori 	<input checked="" type="checkbox"/> Reportistica di Conformità Report automatizzati per audit readiness
		<input checked="" type="checkbox"/> Audit trail di tutte le valutazioni e accessi
PROTEZIONE DATI GDPR, Schrems II	<ul style="list-style-type: none"> • Residenza dati UE • Trattamento GDPR-compliant • Meccanismi trasferimento • DPA management 	<input checked="" type="checkbox"/> Residenza Dati UE configurabile
		<input checked="" type="checkbox"/> Trattamento GDPR-compliant nativo
		<input checked="" type="checkbox"/> Meccanismi Schrems II implementati
INTEGRAZIONE ECOSISTEMA Requisito operativo	<ul style="list-style-type: none"> • API aperte • Connettori pre-built • Export dati 	<input checked="" type="checkbox"/> API per integrazioni personalizzate
		<input checked="" type="checkbox"/> Connettori pre-assemblati (Slack, Teams, JIRA)
		<input checked="" type="checkbox"/> 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.

Adriatica Supply Group S.p.A.

Overall
Rating



Risk Factors
By Severity



Risk Assessment

Last assessment date: February 25, 2026

Reassess

COMPLETE

Vulnerability Scan

Download Report

62

Intel Score
Medium

High/Critical CVEs: 233
High/Critical data leaks: 0

View all risks >

Audit

Download Report

41

Audit Score
Medium

Progress: 100%

Answered by: AI: 23% • Human: 77%

Audit Analysis >

Send Audit

Visit Audit >

VECTORS SCORES

100

Patching
Weight - 20%



High/Critical CVE's: 233
Medium risk CVE's: 313

100

Emails
Weight - 10%



SPF's not configured: 121
DMARC's not configured: 291

0

Cloud
Weight - 10%



Publicly Exposed Assets: 0
Public Files: 0
Subdomain Takeovers: 0

100

Breaches
Weight - 10%



Emails in breaches: 29
Emails found online: 49

0

Dataleaks
Weight - 10%



Critical/High Dataleaks: 0
Medium/Low risk Dataleaks: 0

100

Blacklists
Weight - 10%



IPs Blacklisted: 171
Domains Blacklisted: 0

0

Suspicious Activities
Weight - 10%



Infected Domains: 0
Total Domains: 0

22

Https
Weight - 10%



Domains without valid SSL: 13
SSL Certificates: 13

100

DDOS Readiness Assessment
Weight - 10%



Assets without DDOS Protection: 603
Assets with DDOS Protection: 526

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

