boxxapps
Affidabilità digitale

# Perché scegliere **X-CDS**

**Cyber Defense Solutions** è un ecosistema modulare di piattaforme, sistemi e professionalità progettato per **proteggere le infrastrutture IT** della pubblica amministrazione in modo proattivo, garantendo sicurezza, continuità operativa e sensibilizzazione al rischio informatico.

## Quali vantaggi porta?

La sicurezza informatica è un presupposto essenziale per garantire la continuità operativa e la tutela dei dati negli enti pubblici. Cyber Defense Solutions supporta gli enti nella prevenzione delle minacce digitali, nella mitigazione degli impatti derivanti da eventuali incidenti, nell'adeguamento alle normative vigenti e nella promozione di una maggiore consapevolezza interna, trasformando la gestione della sicurezza in un processo strutturato e affidabile.

- Protezione costante delle infrastrutture IT
- Riduzione dei rischi e dei costi legati agli incidenti
- Conformità a standard e regolamenti vigenti
- Maggiore consapevolezza e responsabilità del personale

# Cosa offre il servizio?

### 1. Audit & Risk Assessment

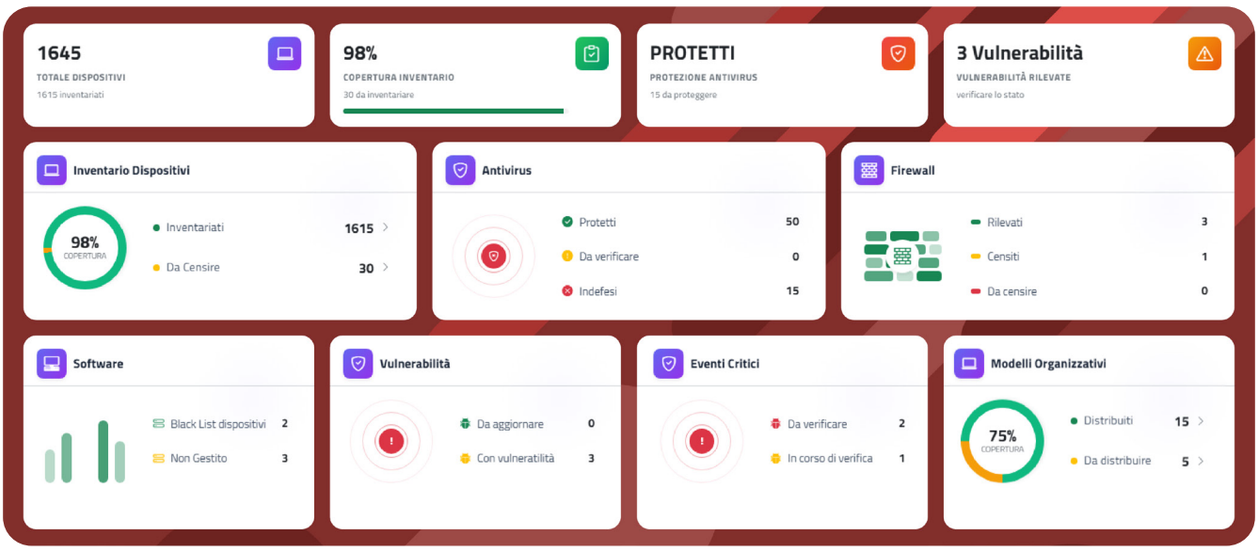
Il servizio Audit & Risk Assessment di CDS offre analisi e monitoraggio IT per garantire sicurezza, conformità AgID e gestione dei rischi. Include dashboard, supporto H24 e aggiornamento continuo dei modelli organizzativi.

**Analisi delle risorse informatiche**
Identifica tutte le risorse IT presenti nell'organizzazione e ne valuta lo stato, garantendo la conformità ai prerequisiti delle misure ICT previste da AgID.

**Dashboard di monitoraggio**
Offre dashboard personalizzabili per mappare l'attuazione delle misure ICT, fornendo una visione chiara e aggiornata dello stato di salute dei sistemi.

**Adeguamento dell'infrastruttura**
Tramite attività sistemistiche, adegua l'infrastruttura alle misure ICT, rilevando asset, software installati e segnalando eventuali criticità e vulnerabilità.

**Evoluzione organizzativa continua**
Aggiorna costantemente i modelli organizzativi per mantenere l'efficienza e l'aderenza a nuove esigenze culturali, tecniche e organizzative all'interno dell'ente.




### 2. Campagna Phishing

Attività di simulazione di attacchi informatici basati su tecniche di phishing, finalizzata a valutare il livello di consapevolezza degli utenti e la capacità di riconoscere tentativi fraudolenti. L'esito delle simulazioni consente di individuare aree di miglioramento e di programmare azioni formative mirate per ridurre il rischio legato al fattore umano.

**Attività mirata in base alle esigenze**
La campagna non è generica, ma progettata in base alle caratteristiche e criticità specifiche dell'ente. Questo approccio aumenta la rilevanza delle simulazioni e rende i risultati più utili per la sicurezza reale.

**Evidenze di efficacia**
A differenza di soluzioni più teoriche, il servizio ha già dimostrato un incremento significativo della consapevolezza tra gli utenti, fornendo un vantaggio competitivo basato su risultati tangibili.

**Formazione basata sui risultati**
Non si tratta di corsi standard: la formazione è costruita sui dati emersi dalle simulazioni, affrontando le aree di vulnerabilità reali. Questo garantisce un impatto diretto e misurabile sulla riduzione del rischio umano.

**Misurazione e miglioramento continuo**
Il servizio non si limita a una singola simulazione: analizza gli esiti, individua le criticità e pianifica azioni correttive. Questo ciclo virtuoso consente di monitorare nel tempo l'evoluzione della consapevolezza degli utenti.

**3. Penetration test**

Verifica tecnica che simula attacchi informatici controllati al fine di individuare vulnerabilità presenti nei sistemi, nelle applicazioni e nelle infrastrutture digitali. I risultati permettono di valutare il livello di esposizione al rischio e di pianificare interventi correttivi mirati per rafforzare la sicurezza complessiva.

**Le 3 fasi per la sicurezza del tuo perimetro informatico**

**AZIONE**

La nostra squadra di esperti mette in atto il piano di attacco precedentemente definito.

**REPORT**

Viene generato un Summary Report con le vulnerabilità riscontrate e le modalità di correzione.

**FOLLOW UP**

Verifica se le azioni correttive adottate sono state efficaci e che il livello di rischio sia mantenuto basso

**4. Security Operation Center ( X - SOC )**

Il gruppo interno alla nostra organizzazione che si occupa della gestione e del monitoraggio della sicurezza informatica, con il compito di rilevare, analizzare e rispondere in tempo reale alle minacce; le sue attività principali comprendono:

- **Monitoraggio della sicurezza**
  SOC monitora costantemente l'ambiente informatico dell'organizzazione, compresi i sistemi, le reti, le applicazioni e i dispositivi, al fine di identificare eventuali anomalie, intrusioni o attività sospette. Questo monitoraggio viene solitamente effettuato utilizzando strumenti di sicurezza come i sistemi di rilevamento delle intrusioni (IDS) e i sistemi di informazioni e gestione degli eventi (SIEM).

- **Analisi delle minacce**
  Una volta rilevate le anomalie o gli eventi di sicurezza, il SOC analizza e valuta le minacce per determinare la loro natura, il livello di rischio e l'impatto potenziale sull'organizzazione. L'analisi delle minacce comprende l'individuazione delle vulnerabilità, la comprensione delle tattiche utilizzate dagli aggressori e l'identificazione dei potenziali obiettivi.

- **Intelligence sulla sicurezza**
  Il SOC si avvale di informazioni e intelligence sulla sicurezza provenienti da fonti interne ed esterne. Queste informazioni consentono di identificare le minacce emergenti, i modelli di attacco e le best practice di sicurezza da attuare. L'intelligence sulla sicurezza aiuta il SOC a prendere decisioni informate e ad adottare misure preventive per proteggere l'organizzazione da futuri attacchi.

- **Rilevamento degli incidenti**
  Con interazione e collaborazione del personale preposto con il Team del CERT per collaborare, quando necessario, con le autorità competenti e attività propedeutica all'indagine forense per comprendere l'origine dell'incidente.

**5. Computer Emergency Response Team (X - CERT)**

Il CERT adotta un approccio proattivo e integrato, orientato alla preparazione e alla resilienza dell'organizzazione, andando oltre la sola risposta agli incidenti.

Con il supporto dell'Incident Response Team (IRT) vengono attivate azioni mirate per rilevare, contenere e risolvere eventi critici secondo priorità definite. Le attività si svolgono in conformità agli standard internazionali ISO 27035, 27037 e 27042, assicurando rigore metodologico nella gestione degli incidenti, nella raccolta delle evidenze e nella produzione di report utili per il miglioramento interno e, se necessario, per indagini forensi.

### 6. X - WASP

X-WASP è la piattaforma SIEM (Security Information and Event Management) progettata per garantire un controllo centralizzato e continuo sugli eventi di sicurezza informatica. Attraverso la raccolta e l'analisi dei log provenienti da firewall, server, dispositivi di rete e sistemi di rilevamento, X-WASP consente di identificare attività anomale o potenzialmente malevole in modo tempestivo.

**Media mensile dei dati raccolti per cliente**

**36.600+**

EVENTI DI SICUREZZA GESTITI SUPERIORI AD L9

**34.200+**

VULNERABILITÀ ANALIZZATE

**1.060.200+**

EVENTI COMPLESSIVI MONITORATI

## Benefici per l'ente

- **Riduzione del rischio Cyber**
  Prevenzione attiva e risposta rapida garantiscono una maggiore resilienza contro minacce e attacchi.
- **Risparmio economico**
  Riducendo i tempi di rilevamento e risposta, si diminuiscono i costi legati ai data breach.
- **Miglioramento della governance**
  Dashboard personalizzate permettono una visione chiara dello stato di sicurezza e delle priorità da affrontare.
- **Supporto continuo**
  Assistenza H24 7/7 tramite ticket, remoto o onsite garantendo interventi tempestivi quando serve.
- **Ottemperanza normativa**
  L'infrastruttura viene allineata costantemente alle misure ICT e agli standard ISO, garantendo compliance continua.
- **Cultura della sicurezza**
  Formazione e simulazioni rafforzano la consapevolezza dei dipendenti, primo scudo contro gli attacchi cyber.

**+1800** Pubbliche Amministrazioni servite

**+ 10** anni di esperienza a fianco della PA

**+ 50k** asset in continuo monitoraggio

**+ 8** servizi qualificati nel marketplace


Seguici su:

Tel: 041 3090915
N. verde: 800 893984

E-mail: info@boxxapps.it
PEC: boxxapps@legalmail.it

Viale della Stazione, 2 -
30020 Marcon (VE)