CYBERQUAKE

# BROCHURE SERVIZI

# /index/

/philosophy/

# PREVENZIONE, PROTEZIONE E CONFORMITA’

Siamo convinti che la chiave per una sicurezza informatica efficace sia la prevenzione. Offriamo soluzioni personalizzate e una consulenza strategica che combina tecnologie di cybersecurity all’avanguardia e un’approfondita conoscenza delle normative. I nostri esperti in cybersecurity, insieme agli avvocati specializzati in protezione dei dati, lavorano fianco a fianco per offrirvi una protezione totale.

Con l’integrazione dell’Intelligenza Artificiale, CyberQuake potenzia ulteriormente i suoi servizi, garantendo una protezione ancora più avanzata ed efficace. Utilizziamo strumenti basati sull’IA per migliorare l’identificazione delle minacce, l’analisi dei rischi e la risposta agli incidenti, offrendo ai nostri clienti un livello di sicurezza all’avanguardia.



**268 attacchi giornalieri**
**per ogni azienda nel mondo.**

## 84%
### Attacchi Ransomware
Aumento degli attacchi ransomware nel mondo negli ultimi anni.

## 62%
### Aziende Colpite
Organizzazioni vulnerabili attive senza un piano di sicurezza.

Le ricerche indicano che molte imprese, specialmente le piccole e medie imprese, non adottano misure di sicurezza informatica adeguate.
Non parliamo del "**se mi accadrà**" ma del "**quando mi accadrà**".

La nostra filosofia è semplice: prevenzione, protezione e conformità. Siamo convinti che la chiave per una sicurezza informatica efficace sia la prevenzione. Offriamo soluzioni personalizzate e una consulenza strategica che combina tecnologie di cybersecurity all'avanguardia e un'approfondita conoscenza delle normative. I nostri esperti in cybersecurity, insieme agli avvocati specializzati in protezione dei dati, lavorano fianco a fianco per offrirvi una protezione totale.

/about-us/

# Proteggi il Tuo Business con la Sinergia tra CyberSecurity e Consulenza Legale

**CyberQuake** è una società specializzata nella cybersecurity e nella consulenza legale, progettata per offrire soluzioni complete e integrate alle aziende che desiderano proteggere i propri dati e garantire la piena conformità normativa. Il nostro obiettivo è garantire la sicurezza del vostro business in un mondo digitale in costante evoluzione, prevenendo minacce informatiche sempre più sofisticate e assicurando il rispetto delle normative vigenti. **Siamo qui per essere il vostro partner di fiducia nella protezione del patrimonio digitale, offrendo competenza, personalizzazione e un approccio proattivo.**

**Perché CyberQuake?** Negli ultimi anni, gli attacchi informatici sono aumentati in modo significativo, con un incremento del 67% delle violazioni di sicurezza dal 2021 al 2023. Gli attacchi ransomware sono tra i più devastanti, rappresentando il 30% delle minacce totali, con richieste di riscatto che superano spesso milioni di euro. Inoltre, il phishing rimane una delle tecniche più diffuse, responsabile di circa il 90% delle violazioni dei dati. Le PMI sono particolarmente vulnerabili: quasi il 43% degli attacchi informatici nel 2023 ha preso di mira aziende di piccole e medie dimensioni, spesso sfruttando la mancanza di consapevolezza del personale e difese tecnologiche insufficienti. Le PMI sono spesso il bersaglio principale, a causa delle loro difese informatiche meno strutturate rispetto a quelle delle grandi imprese. La nostra missione è proteggere anche le aziende più piccole, garantendo loro un supporto completo nella gestione della sicurezza informatica e nella conformità normativa, per consentirvi di concentrarvi sul vostro core business senza preoccupazioni.

La differenza di CyberQuake sta nella nostra capacità di combinare l'eccellenza tecnica con la conoscenza legale. Non ci limitiamo a implementare soluzioni tecnologiche avanzate, ma assicuriamo anche che tutte le vostre attività siano conformi alle normative sulla protezione dei dati, come il GDPR. Collaboriamo in modo stretto con lo **Studio BLI**, leader nella consulenza legale, per garantire una protezione completa e a 360 gradi.

Con l'integrazione dell'Intelligenza Artificiale (IA), CyberQuake potenzia ulteriormente i suoi servizi, garantendo una protezione ancora più avanzata ed efficace. **Utilizziamo strumenti basati sull'IA per migliorare l'identificazione delle minacce, l'analisi dei rischi e la risposta agli incidenti, offrendo ai nostri clienti un livello di sicurezza all'avanguardia.**

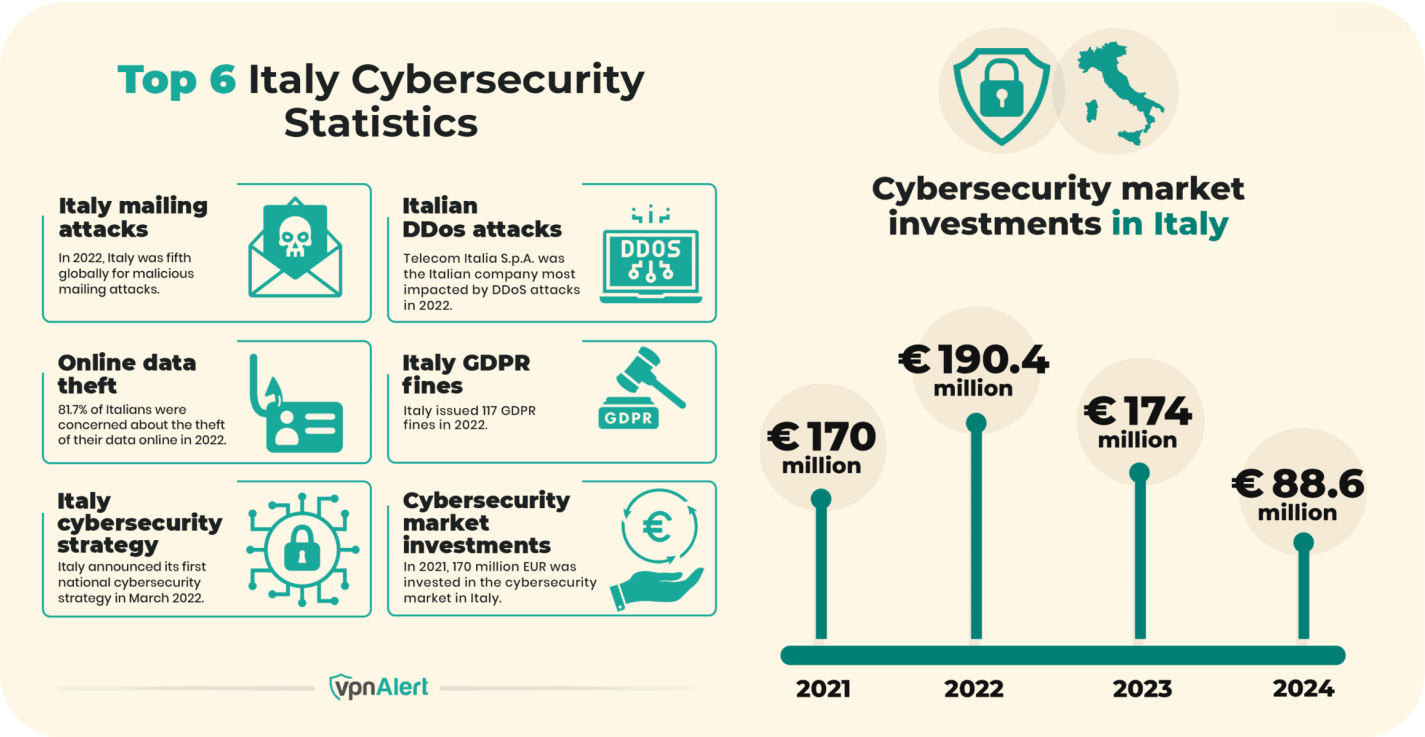
/why-us/

# Perché scegliere CyberQuake?

- **Competenza Multidisciplinare**: Uniamo competenze tecniche, legali e avanzate capacità di IA per offrire soluzioni che rispondono sia alle necessità di sicurezza informatica sia alle esigenze di conformità normativa.
- **Soluzioni Personalizzate**: Ogni azienda è diversa. Per questo sviluppiamo soluzioni su misura, adattandoci alle specifiche necessità della vostra realtà aziendale.
- **Protezione Continuativa**: Il nostro monitoraggio e supporto 24/7 vi garantisce la tranquillità di sapere che il vostro business è sempre protetto.
- **Approccio Proattivo**: Non ci limitiamo a reagire agli attacchi, ma adottiamo un approccio proattivo per prevenire minacce future e migliorare continuamente il livello di sicurezza della vostra azienda, utilizzando l'IA per anticipare possibili scenari di rischio e ottimizzare le difese in modo dinamico.

In un contesto dove le minacce informatiche sono sempre più frequenti e sofisticate, non basta avere difese tecnologiche: è fondamentale anche garantire la conformità legale. Con CyberQuake, vi offriamo la sicurezza di avere al vostro fianco un partner che combina entrambe le competenze, per proteggere il vostro business in ogni aspetto.

**I numeri parlano chiaro**: il 60% delle PMI che subisce un attacco informatico non riesce a riprendersi e chiude entro sei mesi. Gli attacchi ransomware, che crittografano i dati aziendali e richiedono un riscatto, sono aumentati del 150% negli ultimi due anni, con il 40% delle PMI che non riesce a pagare il riscatto e finisce per perdere dati cruciali. Inoltre, attacchi di phishing hanno colpito il 75% delle PMI, sfruttando la mancanza di formazione del personale per rubare credenziali e informazioni sensibili. Questi attacchi causano danni non solo economici ma anche reputazionali, che possono essere fatali per aziende di dimensioni ridotte. Non lasciate che questo accada alla vostra azienda. Con CyberQuake, potete contare su un partner affidabile che vi aiuterà a costruire un sistema di sicurezza solido e resiliente, proteggendo i vostri dati, la vostra reputazione e il vostro futuro. Implementiamo soluzioni tecnologiche avanzate, combinate con un monitoraggio costante e una formazione mirata del personale, per assicurarci che siate sempre un passo avanti rispetto ai cybercriminali.



/services/

# [ PENETRATION TESTING ]

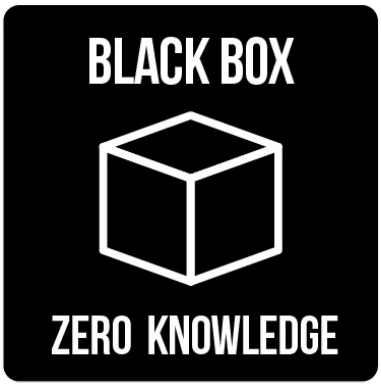
**IN COSA CONSISTE IL SERVIZIO:**

Test di intrusione simulati per valutare le difese aziendali e rilevare vulnerabilità sfruttabili da potenziali attaccanti.

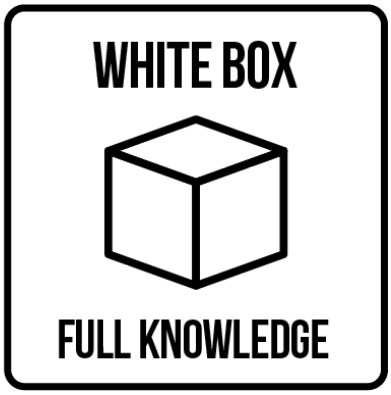
Il nostro servizio di **Penetration Testing** è studiato per testare le difese della tua azienda con simulazioni realistiche di attacchi informatici, mettendo alla prova l'efficacia delle tue misure di sicurezza e identificando le vulnerabilità sfruttabili dai cybercriminali. Questa attività proattiva consente di anticipare le minacce, scoprendo potenziali punti deboli prima che possano causare danni reali. La nostra metodologia combina tecniche avanzate e un approccio completo che permette di testare ogni livello della tua infrastruttura, assicurando una copertura a 360° per tutte le aree critiche della tua sicurezza.

Comprendiamo che ogni azienda ha una struttura unica e esigenze specifiche di sicurezza. Pertanto, i nostri test sono altamente personalizzabili e basati su una fase iniziale di assessment per comprendere i tuoi obiettivi e le aree che necessitano una particolare attenzione. I nostri esperti in cybersecurity lavorano insieme al team IT della tua azienda per pianificare un test mirato che rispecchi le condizioni reali di minaccia e consenta di sviluppare soluzioni di protezione su misura.

**TIPOLOGIE DI PENETRATION TESTING: "WHITE BOX", "GREY BOX" E "BLACK BOX":**








## 01 White Box Testing

- **Descrizione**: Nel White Box Testing, il tester ha pieno accesso alle informazioni sui sistemi e le infrastrutture aziendali, comprese le configurazioni, il codice sorgente, le credenziali e la struttura interna della rete.
- **Approccio e Obiettivi**: Questo approccio mira a individuare vulnerabilità nascoste, comprese quelle difficili da rilevare senza conoscenze approfondite dell'architettura. Il White Box Testing consente un'analisi esaustiva dei sistemi, perché permette di esaminare ogni aspetto interno e di simulare scenari di attacco avanzati.
- **Vantaggi**: Poiché il tester ha una visione completa del sistema, questa tipologia di pentest è ideale per identificare tutte le vulnerabilità presenti, comprese quelle di configurazione e di codice. È particolarmente utile per aziende che vogliono test approfonditi su sistemi critici e applicazioni sviluppate internamente.
- **Limiti**: Non rispecchia scenari realistici di attacchi esterni, poiché un vero attaccante non avrebbe accesso a queste informazioni. Inoltre, richiede più tempo e risorse per essere eseguito.

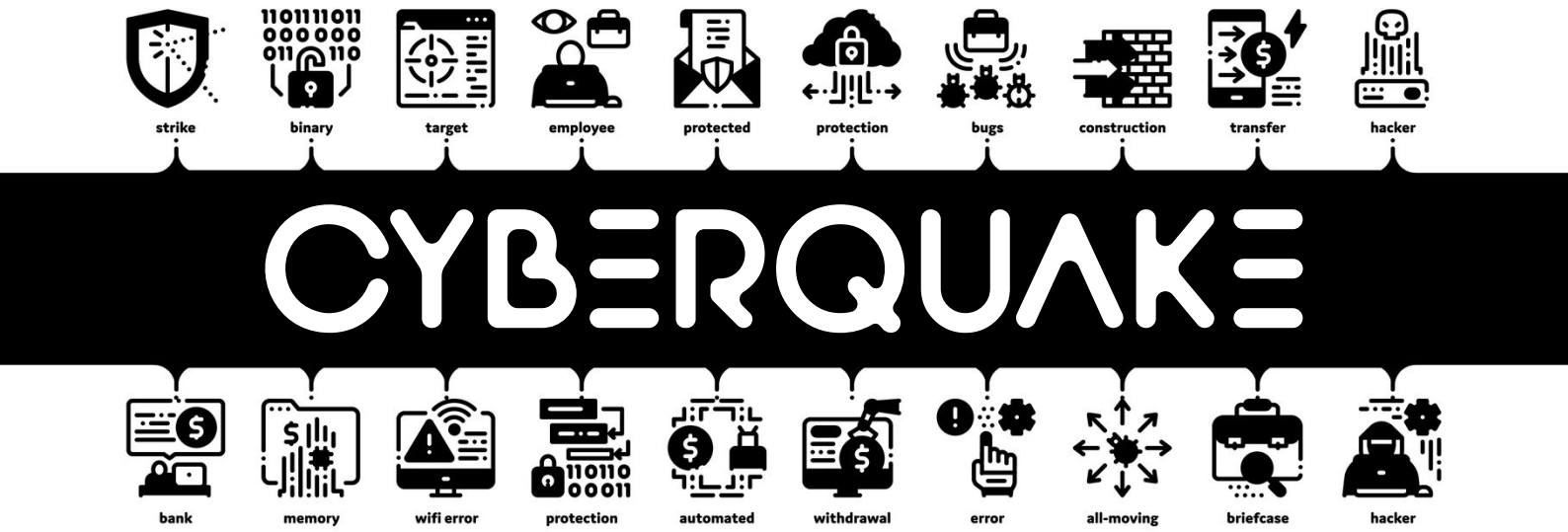
/services/

## 02 Grey Box Testing

- **Descrizione**: Nel Grey Box Testing, al tester viene fornito un accesso limitato alle informazioni, come credenziali di basso livello o dettagli parziali sulla rete e i sistemi. Questo approccio rappresenta uno scenario in cui un attaccante ha già ottenuto alcune informazioni aziendali, ad esempio, tramite ingegneria sociale o accesso non autorizzato a parti della rete.
- **Approccio e Obiettivi**: Il Grey Box Testing cerca di simulare un attacco interno o parzialmente informato, valutando quali danni potrebbero derivare se un intruso ottenesse un accesso limitato. Questo tipo di pentest si concentra sulla capacità dei sistemi di contenere una potenziale intrusione interna e sulla solidità delle autorizzazioni e delle segmentazioni di rete.
- **Vantaggi**: Offre un equilibrio tra realismo e approfondimento, permettendo al tester di verificare le misure di sicurezza senza accedere a tutte le informazioni, ma con sufficienti dettagli per simulare un attacco realistico. È più rapido del White Box Testing e fornisce una visione credibile delle vulnerabilità accessibili a utenti interni.
- **Limiti**: Non fornisce la visione completa di un White Box Testing e potrebbe non identificare tutte le vulnerabilità interne e di configurazione, poiché il tester non ha accesso completo.

## 03 Black Box Testing

- **Descrizione**: Nel Black Box Testing, il tester parte da zero, senza alcuna informazione preliminare sui sistemi, la rete o l'infrastruttura aziendale. Questo approccio imita un attacco esterno in cui l'attaccante non dispone di alcun accesso privilegiato e deve scoprire ogni dettaglio autonomamente.
- **Approccio e Obiettivi**: Il tester cerca di ottenere informazioni sugli obiettivi, individuando superfici di attacco e cercando punti di accesso pubblicamente esposti. Questo test valuta le difese esterne dell'azienda, misurando quanto sia difficile per un attaccante senza conoscenze interne penetrare nei sistemi.
- **Vantaggi**: È molto realistico e rappresenta lo scenario tipico di un attacco informatico esterno. Consente di testare la resistenza alle minacce esterne e le configurazioni di sicurezza esposte su internet.
- **Limiti**: Poiché il tester non ha accesso alle informazioni interne, questo tipo di test può identificare solo le vulnerabilità più visibili e accessibili esternamente. Non rileva le debolezze interne o quelle nascoste all'interno della rete.



/services/

## Quali soluzioni include il servizio

### 01 External PenTesting

- **Descrizione**: Con l'external pentesting, simuliamo attacchi provenienti da una posizione esterna alla rete aziendale, identificando vulnerabilità che potrebbero essere sfruttate tramite internet.
- **Obiettivi principali:** Firewall, server esposti pubblicamente, siti web aziendali, VPN, e-mail.
- **Risultati:** Il test evidenzia vulnerabilità come configurazioni errate del firewall, patch non applicate e possibilità di attacchi brute force su account esposti. Le informazioni raccolte permettono di correggere rapidamente le falle visibili esternamente, aumentando la sicurezza dei sistemi pubblicamente accessibili.

### 02 Internal PenTesting

- **Descrizione**: Questo test simula un attacco che parte dall'interno della rete aziendale, come se un attaccante avesse già ottenuto l'accesso alla rete. È particolarmente utile per rilevare vulnerabilità interne e valutare l'efficacia delle misure di contenimento.
- **Obiettivi principali:** Rete interna, server, workstation, dispositivi connessi.
- **Risultati:** Identificazione di problematiche come configurazioni di rete non sicure, privilegi eccessivi per gli utenti e policy di segmentazione di rete inadeguate. Questo test aiuta a limitare l'espansione di attacchi interni e a migliorare la resilienza della rete aziendale.

### 03 Wireless PenTesting

- **Descrizione**: Con il wireless pentesting, valutiamo la sicurezza delle reti Wi-Fi aziendali, analizzando access point e comunicazioni tra dispositivi, per prevenire accessi non autorizzati o attacchi tramite reti wireless.
- **Obiettivi principali:** Reti Wi-Fi aziendali, autenticazione, crittografia, rogue access points.
- **Risultati:** Identificazione di reti Wi-Fi non protette adeguatamente, vulnerabilità a attacchi di man-in-the-middle e accessi non autorizzati. È un test fondamentale per proteggere le reti wireless, spesso bersaglio di attacchi mirati.

### 04 IoT PenTesting

- **Descrizione**: Simuliamo attacchi contro dispositivi IoT connessi alla rete aziendale, come sensori intelligenti, telecamere di sicurezza e altri dispositivi smart. Questo pentesting è essenziale per aziende che utilizzano tecnologia IoT nella loro infrastruttura.
- **Obiettivi principali:** Dispositivi IoT, smart sensors, telecamere, dispositivi connessi.
- **Risultati:** Individuazione di vulnerabilità come protocolli di comunicazione non sicuri, firmware obsoleti o gestione inadeguata degli accessi, offrendo soluzioni per rafforzare la sicurezza di tutti i dispositivi IoT in rete.

/services/

## 05 Cloud PenTesting

- **Descrizione**: Valutiamo la sicurezza delle infrastrutture e dei servizi ospitati in ambienti cloud, un componente ormai cruciale per molte aziende. Questo test consente di identificare e mitigare vulnerabilità specifiche del cloud.
- **Obiettivi principali:** Configurazioni cloud, gestione delle identità e degli accessi, vulnerabilità delle applicazioni su cloud.
- **Risultati:** Individuazione di errori di configurazione, policy di sicurezza mancanti o inefficaci e altri rischi del cloud. Questo test aiuta le aziende a massimizzare i vantaggi del cloud senza compromettere la sicurezza.

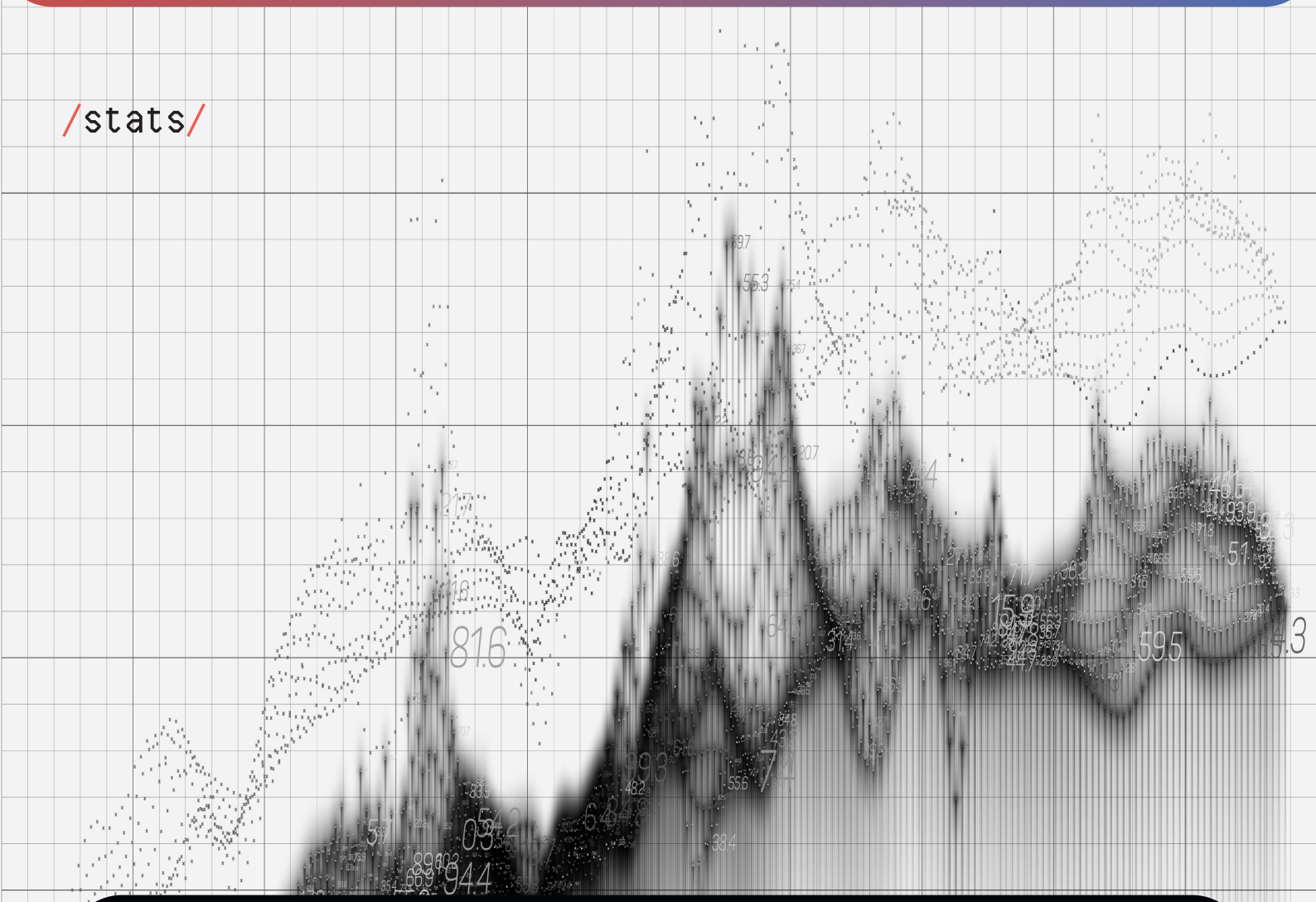
## 06 Social Engineering

- **Descrizione**: Simuliamo attacchi basati sull'ingegneria sociale per testare la capacità del personale di difendersi da tentativi di manipolazione psicologica, come phishing e pretexting.
- **Obiettivi principali:** Phishing, pretexting, spear-phishing, impersonation.
- **Risultati:** Valutazione della prontezza del personale contro minacce basate sulla manipolazione psicologica. Questo test è fondamentale per formare i dipendenti e prevenire le brecce di sicurezza causate da errori umani.

## 07 Red Teaming

- **Descrizione**: Red Teaming rappresenta la simulazione più completa e avanzata di un attacco, in cui un team di esperti lavora in modo prolungato per testare la resilienza aziendale su tutti i fronti: fisico, digitale e organizzativo.
- **Obiettivi principali:** Valutare l'efficacia complessiva delle difese, inclusa la capacità di monitoraggio e di risposta agli incidenti.
- **Risultati:** Identificazione di lacune nelle misure di sicurezza fisica, logica e nelle risposte agli incidenti. Questo approccio fornisce una visione globale e realistica della capacità di resistenza dell'azienda a minacce sofisticate.

/stats/



## Analisi Statistica

I Penetration Testing è uno strumento essenziale per le aziende che desiderano proteggere i propri asset digitali. Ecco alcune statistiche che evidenziano l'importanza di questo servizio:

- **Aumento degli attacchi informatici in Italia**: Nel primo semestre del 2023, l'Italia ha registrato un incremento del 40% negli attacchi informatici rispetto allo stesso periodo dell'anno precedente, con 132 attacchi gravi documentati.
- **Costi elevati delle violazioni**: Il costo medio di una violazione dei dati in Italia è di 3,46 milioni di euro, evidenziando l'impatto finanziario significativo che un attacco può avere su un'azienda.
- **Vulnerabilità delle PMI**: Oltre il 35% delle piccole e medie imprese italiane ha subito almeno un incidente legato al cybercrime, indicando una preparazione spesso insufficiente nel fronteggiare le minacce informatiche.
- **Diffusione del malware**: Nel primo semestre del 2022, l'Italia è stata il paese europeo più colpito da attacchi malware, con 82 milioni di attacchi intercettati.
- **Importanza del Penetration Testing**: La Direttiva NIS2 dell'Unione Europea sottolinea l'obbligo per le organizzazioni essenziali di effettuare regolari attività di Penetration Testing per garantire la conformità e la sicurezza delle infrastrutture critiche.

Queste statistiche evidenziano la necessità per le aziende di adottare misure proattive, come il Penetration Testing, per identificare e mitigare le vulnerabilità prima che possano essere sfruttate da attori malevoli.

/services/

# [ PROTEZIONE DELLA RETE E DELLE INFRASTRUTTURE ]

**IN COSA CONSISTE IL SERVIZIO:**

**Fornisce soluzioni per proteggere l'infrastruttura IT da minacce interne ed esterne.**

La sicurezza delle reti e delle infrastrutture aziendali rappresenta uno degli elementi chiave per assicurare la stabilità e la crescita di un'organizzazione. **Proteggere le reti e le infrastrutture IT** non significa solo prevenire attacchi, ma anche garantire la continuità operativa e la fiducia dei clienti, partner e stakeholder. Le minacce informatiche sono in costante evoluzione e diventano ogni giorno più sofisticate; è fondamentale per le aziende adottare misure proattive e tecnologie all'avanguardia che sappiano difendere ogni aspetto della rete.

Il nostro servizio di **Protezione della Rete e delle Infrastrutture** offre una gamma completa di soluzioni progettate per rispondere a sfide specifiche e per adattarsi alle esigenze in continua trasformazione. L'approccio che adottiamo è personalizzato, basato su un'analisi approfondita dell'architettura esistente e delle specifiche vulnerabilità di ogni cliente. Questo ci permette di creare un piano di difesa su misura, che protegge non solo contro le minacce attuali ma anche contro quelle emergenti.

**CARATTERISTICHE DEL SERVIZIO:**

- **Prevenzione Proattiva delle Minacce** La nostra strategia si basa su una visione proattiva della sicurezza, volta non solo a rispondere agli attacchi ma a prevenirli. Utilizzando strumenti avanzati di monitoraggio e analisi, possiamo identificare comportamenti sospetti e potenziali minacce prima che diventino incidenti di sicurezza reali. Questo approccio consente alle aziende di affrontare i rischi informatici con maggiore consapevolezza, garantendo una difesa proattiva e riducendo l'esposizione alle minacce.

- **Soluzioni Scalabili e Flessibili** Le esigenze di sicurezza possono cambiare rapidamente in base alle dinamiche del mercato, alla crescita aziendale e all'evoluzione tecnologica. Le nostre soluzioni sono pensate per essere scalabili e flessibili, permettendo all'azienda di espandere le difese in modo agile e senza soluzione di continuità. Che si tratti di proteggere una rete locale o una rete globale con infrastrutture complesse, le nostre soluzioni sono progettate per adattarsi al cambiamento.

- **Integrazione con Architetture Esistenti** Ogni azienda ha una struttura di rete unica, con tecnologie, processi e policy specifiche. La nostra metodologia prevede una piena integrazione delle soluzioni di sicurezza con le architetture esistenti, minimizzando i tempi di implementazione e i costi associati. Le nostre soluzioni lavorano in sinergia con le risorse IT già presenti, migliorando la resilienza senza interruzioni delle operazioni.

- **Protezione Contro le Minacce Interne ed Esterne** Mentre molte soluzioni di sicurezza sono orientate esclusivamente a difendere da attacchi esterni, il nostro servizio protegge anche contro minacce interne, spesso sottovalutate ma potenzialmente dannose. Attacchi interni, errori umani o accessi non autorizzati da parte di dipendenti rappresentano un rischio concreto. Le nostre soluzioni comprendono sistemi di monitoraggio degli accessi e dei comportamenti anomali, per garantire una protezione completa.

/services/

**I VANTAGGI DELLA PROTEZIONE AVANZATA:**

- Miglioramento della Resilienza Operativa La continuità operativa è essenziale per ogni azienda, indipendentemente dal settore. Grazie a una protezione continua e a un monitoraggio costante, le nostre soluzioni garantiscono la massima resilienza, minimizzando i tempi di inattività e assicurando la protezione degli asset critici anche in caso di tentativi di intrusione.

- Conformità alle Normative e Standard di Sicurezza Sempre più normative richiedono alle aziende di adottare misure di sicurezza rigorose per la protezione dei dati. Le nostre soluzioni sono conformi agli standard internazionali di sicurezza, come il GDPR e il NIST, e aiutano le aziende a mantenere la conformità, riducendo il rischio di sanzioni e danni alla reputazione.

- Pianificazione Strategica della Sicurezza La protezione della rete e delle infrastrutture richiede una pianificazione strategica che includa l'analisi dei rischi, la definizione di policy e la valutazione costante delle difese. Il nostro team di esperti collabora con l'azienda per sviluppare una roadmap di sicurezza a lungo termine, capace di evolvere con il panorama delle minacce e di rispondere efficacemente a nuove sfide.

## Quali soluzioni include il servizio

### 01 Firewall Avanzati

- **Descrizione**: Implementiamo e gestiamo firewall di nuova generazione (NGFW), strumenti che vanno oltre la semplice analisi del traffico, fornendo controlli di sicurezza granulari basati su utenti, applicazioni e contenuti. Questi firewall sono in grado di bloccare accessi non autorizzati e mitigare attacchi complessi, inclusi i tentativi di intrusione e i comportamenti anomali.

- **Vantaggi:** Implementiamo e gestiamo firewall di nuova generazione (NGFW), strumenti che vanno oltre la semplice analisi del traffico, fornendo controlli di sicurezza granulari basati su utenti, applicazioni e contenuti. Questi firewall sono in grado di bloccare accessi non autorizzati e mitigare attacchi complessi, inclusi i tentativi di intrusione e i comportamenti anomali.

### 02 IDS/IPS (Sistemi di rilevamento e prevenzione delle intrusioni)

- **Descrizione**: Integrare sistemi di rilevamento (IDS) e di prevenzione (IPS) delle intrusioni è essenziale per monitorare il traffico in tempo reale e identificare qualsiasi attività sospetta. Questi sistemi analizzano costantemente i pacchetti di dati in entrata e uscita, rilevando e bloccando potenziali minacce come attacchi DoS, tentativi di exploit e anomalie di rete.

- **Vantaggi:** Gli IDS/IPS riducono il rischio di accessi non autorizzati e attacchi dannosi, migliorando la capacità dell'azienda di individuare e rispondere rapidamente a incidenti di sicurezza.

### 03 Sicurezza degli endpoint

- **Descrizione**: Proteggere i dispositivi aziendali (computer, server, smartphone e tablet) è essenziale per una strategia di sicurezza completa. La nostra soluzione per la sicurezza degli endpoint include l'implementazione di software di protezione avanzati, che difendono gli endpoint da malware, ransomware e attacchi mirati.

- **Vantaggi**: Questa protezione permette di mitigare il rischio associato a dispositivi spesso utilizzati da remoto o fuori dalla rete aziendale, migliorando la resilienza contro minacce come il phishing, il malware e gli attacchi mirati.

# /services/

## 04 Zero Trust Architecture

- **Descrizione**: Implementiamo un'architettura Zero Trust, che si basa sul principio di "non fidarsi mai, verificare sempre". Questo modello richiede la verifica continua e rigorosa di ogni utente, dispositivo e applicazione, indipendentemente dalla loro posizione, sia che si trovino dentro che fuori dalla rete aziendale.

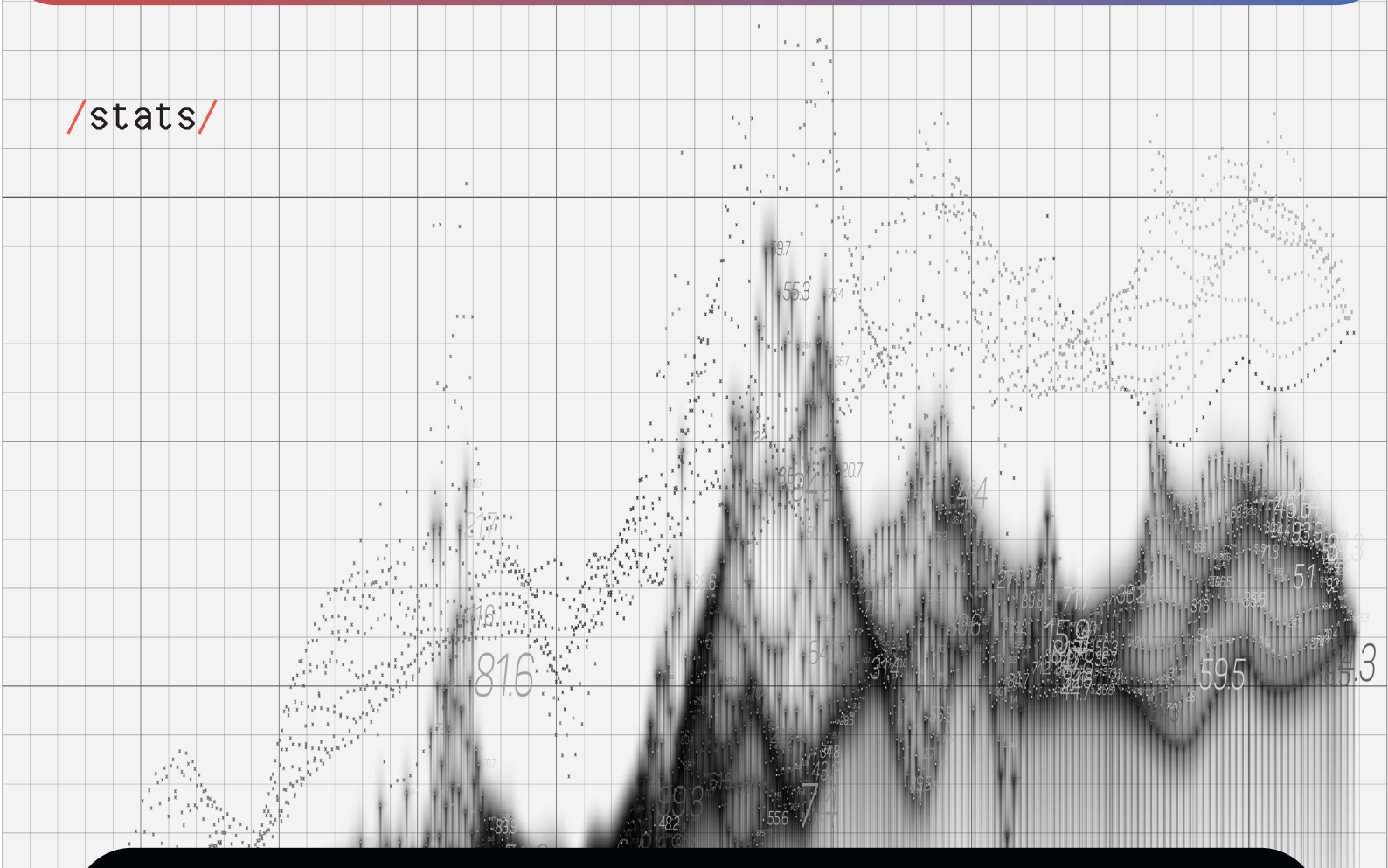
- **Vantaggi:** L'approccio Zero Trust limita l'accesso ai dati solo a utenti autorizzati e dispositivi sicuri, riducendo il rischio di accessi non autorizzati e garantendo un livello elevato di protezione contro minacce interne ed esterne.

## 05 Network segmentation

- **Descrizione**: La segmentazione della rete consiste nel dividere la rete aziendale in diverse sottoreti isolate, limitando così l'accesso tra le diverse aree. In questo modo, eventuali compromissioni restano confinate a una specifica porzione della rete, riducendo l'impatto di attacchi e minimizzando la superficie d'attacco.

- **Vantaggi:** La segmentazione della rete migliora la sicurezza complessiva, limitando l'accesso a dati e risorse critiche solo ai dispositivi e agli utenti autorizzati. In caso di compromissione di una sottorete, questa pratica riduce il rischio di propagazione dell'attacco all'intera infrastruttura.

/stats/



## Analisi Statistica

La protezione delle reti e delle infrastrutture aziendali è fondamentale per salvaguardare i dati sensibili e garantire la continuità operativa. Ecco alcune statistiche che evidenziano l'importanza di implementare soluzioni avanzate di sicurezza:

- **Aumento degli attacchi informatici in Italia**: Nel terzo trimestre del 2024, l'Italia ha registrato un incremento del 115% negli attacchi informatici rispetto allo stesso periodo dell'anno precedente, evidenziando una crescente esposizione alle minacce cibernetiche.
- **Costi elevati delle violazioni dei dati**: Secondo il report annuale di IBM, il costo medio di una violazione dei dati in Italia ha raggiunto i 4,37 milioni di euro nel 2024, con un aumento del 23% rispetto al 2023.
- **Vulnerabilità delle PMI**: Le PMI italiane sono particolarmente esposte, con oltre il 35% che ha subito almeno un incidente legato al cybercrime, spesso a causa di misure di sicurezza insufficienti.
- **Diffusione del malware**: Nel primo semestre del 2024, l'Italia è stata il paese europeo più colpito da attacchi malware, con 82 milioni di attacchi intercettati, sottolineando la necessità di proteggere adeguatamente le infrastrutture IT.
- **Importanza della segmentazione della rete**: La segmentazione della rete è una pratica efficace per limitare l'impatto di eventuali compromissioni, riducendo la superficie d'attacco e impedendo la propagazione delle minacce all'interno dell'organizzazione.

Queste statistiche evidenziano la necessità per le aziende di adottare misure proattive, come l'implementazione di firewall avanzati, sistemi IDS/IPS e architetture Zero Trust, per proteggere le proprie reti e infrastrutture da minacce sempre più sofisticate.

/services/

# [ PROTEZIONE DEI DATI E DELLA PRIVACY ]

**IN COSA CONSISTE IL SERVIZIO:**

**Assicura la protezione e la riservatezza dei dati aziendali, riducendo i rischi legati a violazioni dei dati.**

La protezione dei dati e della privacy è un pilastro fondamentale per qualsiasi organizzazione che desideri tutelare la riservatezza delle proprie informazioni, salvaguardare la fiducia dei clienti e mantenere la conformità a normative sempre più stringenti. In un contesto in cui la quantità e la sensibilità dei dati raccolti sono in costante aumento, le minacce alla sicurezza diventano sempre più sofisticate. La nostra soluzione di **Protezione dei Dati e della Privacy** offre un approccio completo per difendere i dati da violazioni, accessi non autorizzati e perdite, supportando le aziende nella gestione di un ambiente digitale sicuro e conforme.

Adottiamo le tecnologie più avanzate e le best practice di settore per garantire una protezione a più livelli, capace di rispondere alle necessità moderne della cybersecurity. Ogni componente della nostra soluzione è pensato per integrarsi perfettamente con l'ecosistema IT aziendale, creando una rete di difesa che si adatta al tuo business e cresce con esso. Dalla crittografia avanzata all'access control rigoroso, ci assicuriamo che ogni aspetto della protezione dati sia gestito con il massimo livello di sicurezza.

**Una Protezione Completa e Adattabile**

La protezione dei dati non è una soluzione unica, ma un sistema integrato che si adatta alle particolari esigenze e alla struttura di ciascuna azienda. Ecco come la nostra soluzione offre una protezione completa:

- **Sicurezza dei dati sensibili ovunque si trovino** Proteggere i dati significa assicurare la loro riservatezza e integrità non solo quando vengono conservati, ma anche quando vengono trasmessi o processati. Offriamo crittografia end-to-end per garantire che le informazioni rimangano sicure in ogni fase del loro ciclo di vita, indipendentemente dal luogo o dal dispositivo su cui vengono utilizzate.

- **Conformità alle normative internazionali** Con normative come il GDPR e il CCPA che impongono standard di protezione dei dati sempre più rigidi, le aziende devono assicurarsi di essere pienamente conformi per evitare pesanti sanzioni. Le nostre soluzioni sono progettate per rispondere a questi requisiti, rendendo semplice la gestione della conformità e riducendo il rischio legale associato alla protezione dei dati personali e sensibili.

- **Gestione centralizzata della sicurezza e della privacy** Forniamo strumenti avanzati che permettono un monitoraggio centralizzato della sicurezza dei dati, semplificando la gestione della privacy e delle autorizzazioni. La gestione centralizzata consente di mantenere una visione chiara e aggiornata dello stato della sicurezza e delle policy aziendali, ottimizzando l'efficienza e migliorando la capacità di reazione a potenziali minacce.

- **Rafforzamento della fiducia dei clienti e degli stakeholder** La sicurezza dei dati e la trasparenza nella loro gestione sono ormai elementi chiave per la fiducia dei clienti. Dimostrare l'impegno dell'azienda verso la protezione della privacy rafforza la reputazione e la credibilità, migliorando le relazioni con clienti, partner e stakeholder.

**Approccio Proattivo e Personalizzato**

Per ogni cliente, sviluppiamo una soluzione su misura, basata su un'analisi dettagliata dei rischi specifici e delle necessità aziendali. La nostra metodologia di protezione dei dati si fonda su un approccio proattivo che non solo risponde alle minacce esistenti, ma prevede anche potenziali scenari futuri, rendendo le aziende resilienti alle nuove sfide del panorama della sicurezza.

/services/

**I BENEFICI DELLA NOSTRA SOLUZIONE:**

1. **Protezione dei dati sensibili**: I dati aziendali sono tra gli asset più preziosi di un'organizzazione, e il nostro sistema di protezione aiuta a salvaguardarli da accessi e utilizzi non autorizzati.
2. **Miglioramento continuo della sicurezza**: Attraverso un monitoraggio costante e aggiornamenti periodici, la nostra soluzione assicura che la protezione dei dati evolva insieme alla crescita dell'azienda e alle nuove minacce.
3. **Mitigazione dei rischi e riduzione dei costi legati a incidenti di sicurezza**: Prevenire violazioni dei dati è molto più economico che affrontarne le conseguenze. La nostra soluzione riduce il rischio di incidenti costosi e di impatti negativi sulla reputazione.

## Quali soluzioni include il servizio

### 01 Crittografia avanzata

- **Descrizione**: Proteggiamo i dati aziendali con crittografia end-to-end, che ne garantisce la sicurezza sia quando sono in transito sia quando sono a riposo. Utilizziamo algoritmi crittografici avanzati, come AES-256 e RSA, che rappresentano gli standard più elevati nel settore.

- **Vantaggi:** La crittografia avanzata rende i dati illeggibili a chiunque non sia autorizzato, anche in caso di accesso non autorizzato o di violazione. Questo livello di protezione è essenziale per difendere le informazioni sensibili da tentativi di furto e per rispettare normative come il GDPR.

### 02 Data Loss Prevention (DLP)

- **Descrizione**: Implementiamo soluzioni di Data Loss Prevention (DLP) che permettono di monitorare e controllare i flussi di dati in uscita, impedendo la perdita di informazioni sensibili. I sistemi DLP rilevano e bloccano automaticamente i tentativi di trasferimento di dati critici senza autorizzazione, applicando policy personalizzate per l'azienda.

- **Vantaggi:** Il DLP riduce il rischio di perdita accidentale o intenzionale di dati preziosi e aiuta a prevenire situazioni di non conformità. È uno strumento essenziale per mantenere il controllo sui dati e proteggere le informazioni aziendali da trasferimenti non autorizzati.

### 03 Access control

- **Descrizione**: La gestione rigorosa degli accessi ai dati è cruciale per prevenire accessi non autorizzati. Implementiamo policy di autenticazione multi-fattore (MFA) e di accesso basato sui ruoli (RBAC), che limitano l'accesso ai soli utenti autorizzati in base alla loro funzione aziendale. Ogni tentativo di accesso viene monitorato e registrato per garantire un controllo completo.

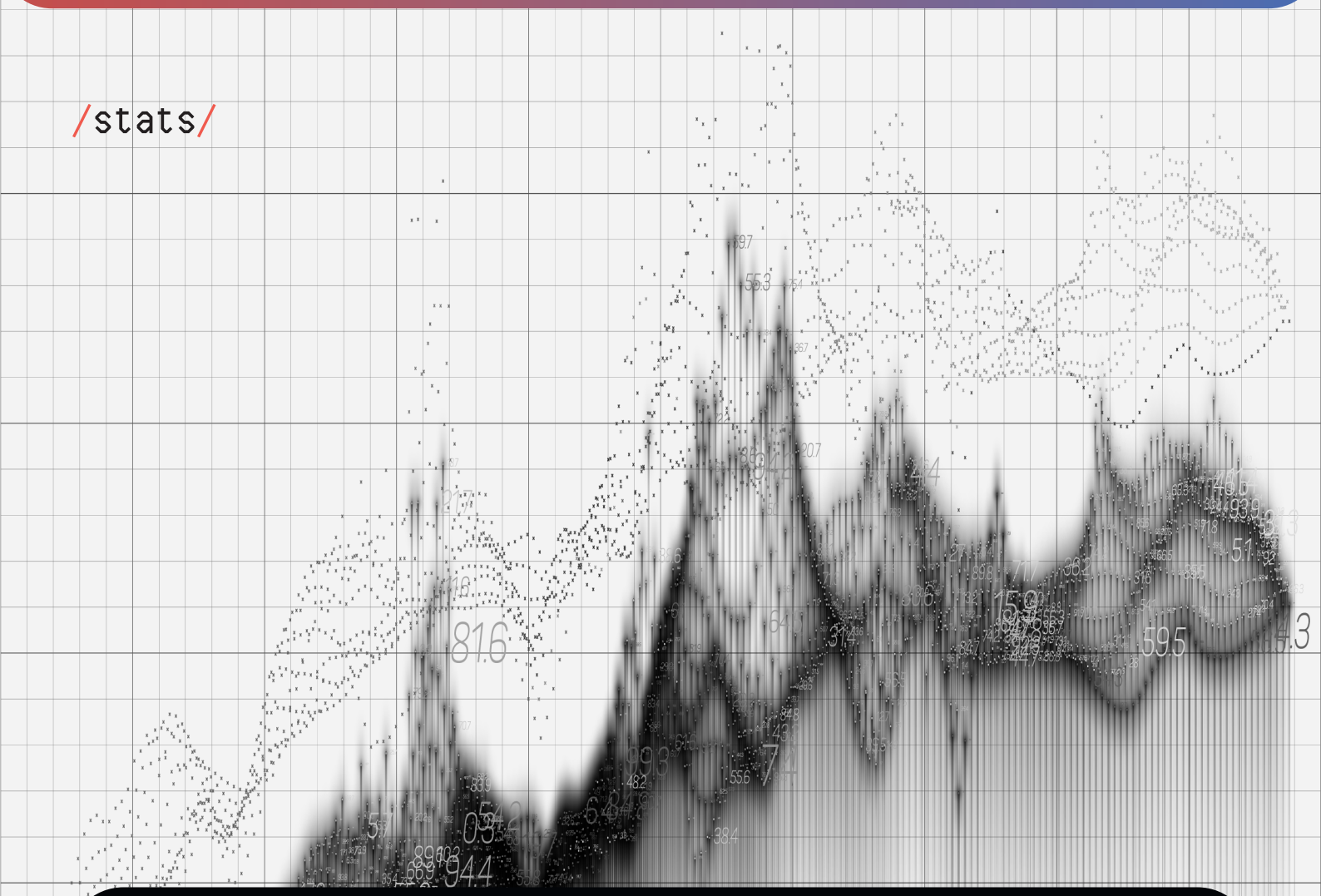
- **Vantaggi**: L'accesso basato sui ruoli riduce il rischio di accessi non autorizzati e migliora la gestione dei permessi. La multi-fattorialità rende molto più difficile per i malintenzionati ottenere accesso ai dati, migliorando la sicurezza delle informazioni aziendali.

/services/

## 04 Data masking e tokenization

- **Descrizione**: Utilizziamo tecniche di data masking e tokenization per proteggere i dati sensibili durante l'elaborazione e in ambienti di sviluppo o testing. Il data masking oscura i dati originali, sostituendoli con dati fittizi ma utilizzabili per analisi e test, mentre la tokenization converte i dati sensibili in token sicuri che non hanno valore fuori dall'ambito specifico.
- **Vantaggi**: Queste tecniche consentono di gestire e lavorare con i dati senza esporre le informazioni sensibili, riducendo il rischio di violazione della privacy e aumentando la sicurezza in fase di test o di trasferimento dei dati.

/stats/



## Analisi Statistica

La protezione dei dati e della privacy è fondamentale per le aziende moderne, sia per salvaguardare le informazioni sensibili sia per mantenere la fiducia dei clienti. Ecco alcune statistiche che evidenziano l'importanza di implementare soluzioni avanzate in questo ambito:

- **Aumento delle violazioni dei dati: Nel 2024, il costo medio globale di una violazione dei dati ha raggiunto i 4,88 milioni di dollari, con un incremento del 10% rispetto all'anno precedente.**
- **Sanzioni per non conformità al GDPR: In Europa, le sanzioni per violazioni del GDPR hanno totalizzato 1,78 miliardi di euro nel 2023, con un aumento del 14% rispetto all'anno precedente.**
- **Vulnerabilità delle PMI: Le piccole e medie imprese sono particolarmente esposte, con oltre il 35% che ha subito almeno un incidente legato al cybercrime, spesso a causa di misure di sicurezza insufficienti.**
- **Importanza della crittografia: L'adozione di tecniche di crittografia avanzata può ridurre significativamente il rischio di violazioni dei dati, proteggendo le informazioni sia in transito che a riposo.**
- **Implementazione di DLP: Le soluzioni di Data Loss Prevention (DLP) aiutano a prevenire la perdita di dati sensibili, monitorando e controllando i flussi di informazioni all'interno dell'organizzazione.**

Queste statistiche sottolineano la necessità per le aziende di adottare misure proattive, come la crittografia avanzata, il controllo rigoroso degli accessi e le soluzioni DLP, per proteggere efficacemente i dati e la privacy.

/services/

# [ MONITORAGGIO E RISPOSTA ALLE MINACCE ]

**IN COSA CONSISTE IL SEVIZIO:**

**Fornisce una vigilanza continua e una risposta tempestiva agli incidenti di sicurezza.**

Nel mondo odierno, caratterizzato da minacce informatiche sempre più sofisticate e da un ambiente digitale in rapida evoluzione, una protezione statica non è sufficiente. Gli attacchi informatici possono colpire in qualsiasi momento e, spesso, mirano a superare i tradizionali meccanismi di difesa. La nostra soluzione di **Monitoraggio e Risposta alle Minacce** offre una vigilanza continua e una risposta proattiva, costruendo una difesa dinamica e adattabile alle minacce più complesse.

Il nostro approccio è focalizzato su tre aspetti essenziali:

1. **Rilevamento tempestivo delle minacce**: Utilizziamo tecnologie avanzate di intelligenza artificiale e machine learning per analizzare enormi volumi di dati, identificando rapidamente i pattern anomali e le attività sospette che possono essere segni di un attacco imminente. Il nostro sistema di monitoraggio è progettato per rilevare le minacce prima che possano causare danni significativi, permettendo all'azienda di rispondere in modo proattivo.
2. **Risposta coordinata e tempestiva**: Il tempo di reazione è fondamentale durante un incidente di sicurezza. La nostra soluzione garantisce un intervento rapido, grazie a un team di esperti di cybersecurity che lavorano in stretta collaborazione con il Security Operations Center (SOC) per contenere e mitigare l'impatto degli attacchi. Siamo pronti ad attivare le procedure di contenimento e risposta in qualsiasi momento, minimizzando il rischio di perdita di dati e l'interruzione delle operazioni aziendali.
3. **Adattabilità e resilienza**: Il nostro sistema è in grado di adattarsi a nuovi tipi di attacco e di evolversi costantemente. Le minacce cambiano e diventano sempre più complesse, ed è per questo che investiamo costantemente in tecnologie all'avanguardia e nella formazione continua del nostro team. La nostra soluzione non solo risponde, ma impara e si adatta, creando una difesa che diventa ogni giorno più robusta.

**Perché è importante proteggere i dati e la privacy?**

Con la crescente quantità di dati sensibili gestiti dalle aziende, la protezione dei dati non è mai stata così cruciale. Ogni violazione di dati può avere conseguenze devastanti, sia in termini di danni finanziari che di perdita di reputazione e fiducia dei clienti. Inoltre, la conformità a normative sempre più rigorose come il GDPR e il CCPA richiede un'attenzione costante alla sicurezza e alla privacy. Le nostre soluzioni avanzate aiutano le aziende a mantenere un controllo completo sulle informazioni critiche, proteggendo i dati sensibili e assicurando la conformità alle normative in modo sicuro ed efficiente.

**I VANTAGGI DELLA NOSTRA SOLUZIONE DI MONITORAGGIO E RISPOSTA ALLE MINACCE:**

- **Riduzione dei tempi di rilevamento e risposta**: La velocità è tutto nel prevenire e limitare i danni da attacchi. Il nostro SOC 24/7 monitora ogni evento di sicurezza in tempo reale, garantendo che qualsiasi attività sospetta venga identificata e trattata immediatamente.

- **Miglioramento continuo della sicurezza**: Ogni minaccia rilevata e analizzata contribuisce a migliorare l'efficacia delle difese aziendali. I nostri sistemi SIEM e di threat hunting aggiornano costantemente le loro capacità di analisi e rilevamento, creando un ciclo di feedback che rende la protezione sempre più precisa ed efficiente.

- **Piena conformità alle normative di sicurezza**: Con l'adozione di misure avanzate di monitoraggio e risposta, l'azienda assicura la conformità a normative e standard internazionali come GDPR, ISO 27001 e NIST. La conformità non solo riduce il rischio di sanzioni, ma migliora anche la fiducia dei clienti e degli stakeholder, aumentando il valore aziendale.

/services/

- **Protezione contro attacchi sofisticati e minacce persistenti**: L'analisi proattiva delle minacce, integrata da un team di threat hunters specializzati, consente di individuare attacchi di tipo APT (Advanced Persistent Threat) e altre tecniche avanzate di intrusione, che potrebbero altrimenti rimanere non rilevate per mesi o anni.

- **Scalabilità e flessibilità**: La nostra soluzione si adatta alla crescita dell'azienda e può essere personalizzata per coprire nuove aree di rischio man mano che le infrastrutture e le esigenze aziendali cambiano. Che si tratti di aggiungere monitoraggio per nuovi endpoint o di estendere la copertura a nuove sedi o ambienti cloud, il nostro sistema è progettato per essere flessibile e scalabile.

Attraverso tecnologie avanzate e un team di esperti dedicato, assicuriamo una protezione continua contro le minacce informatiche, supportando l'azienda nel mantenere un ambiente sicuro, conforme e pronto a rispondere alle sfide future.

## Quali soluzioni include il servizio

### 01 SOC 24/7 (Security Operations Center)

- **Descrizione**: Il nostro Security Operations Center (SOC) opera 24 ore su 24, 7 giorni su 7, garantendo un monitoraggio continuo delle infrastrutture aziendali. Il SOC utilizza tecnologie avanzate per rilevare e analizzare qualsiasi attività anomala, consentendo di intervenire in tempo reale contro potenziali minacce.

- **Vantaggi:** Un SOC attivo h24 fornisce una risposta immediata a qualsiasi incidente, riducendo drasticamente il tempo di esposizione alle minacce e aumentando la capacità dell'azienda di difendersi da attacchi continui. È una soluzione ideale per le aziende che desiderano un monitoraggio costante senza sovraccaricare il proprio team IT.

### 02 SIEM (Security Information and Event Management)

- **Descrizione**: Implementiamo sistemi SIEM per raccogliere, analizzare e correlare i log di sicurezza provenienti da diverse fonti, come firewall, endpoint, applicazioni e server. I sistemi SIEM permettono di individuare comportamenti anomali e potenziali minacce, trasformando grandi quantità di dati in insight di sicurezza utilizzabili.

- **Vantaggi:** Con un SIEM, l'azienda ottiene una visione completa e centralizzata di tutti gli eventi di sicurezza, migliorando il rilevamento delle minacce e la reattività. Inoltre, la gestione dei log semplifica il processo di audit e di conformità alle normative di sicurezza.

### 03 Threat hunting

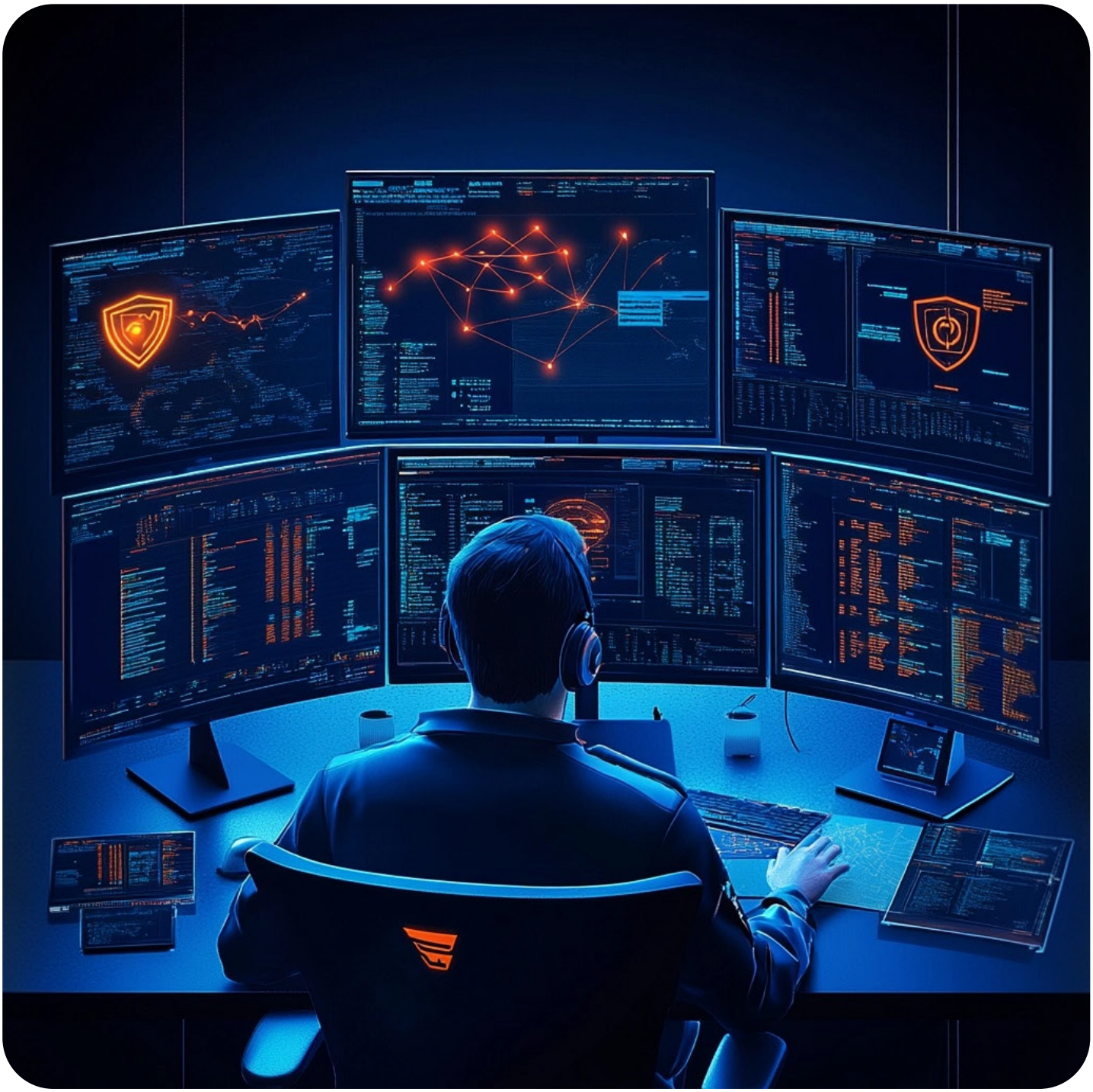
- **Descrizione**: La caccia alle minacce (threat hunting) è una tecnica proattiva che consente di cercare e identificare minacce nascoste o non rilevate dai tradizionali sistemi di sicurezza. I nostri specialisti utilizzano strumenti avanzati e analisi comportamentali per scovare minacce che potrebbero eludere i controlli automatizzati, come attacchi di tipo APT (Advanced Persistent Threat).

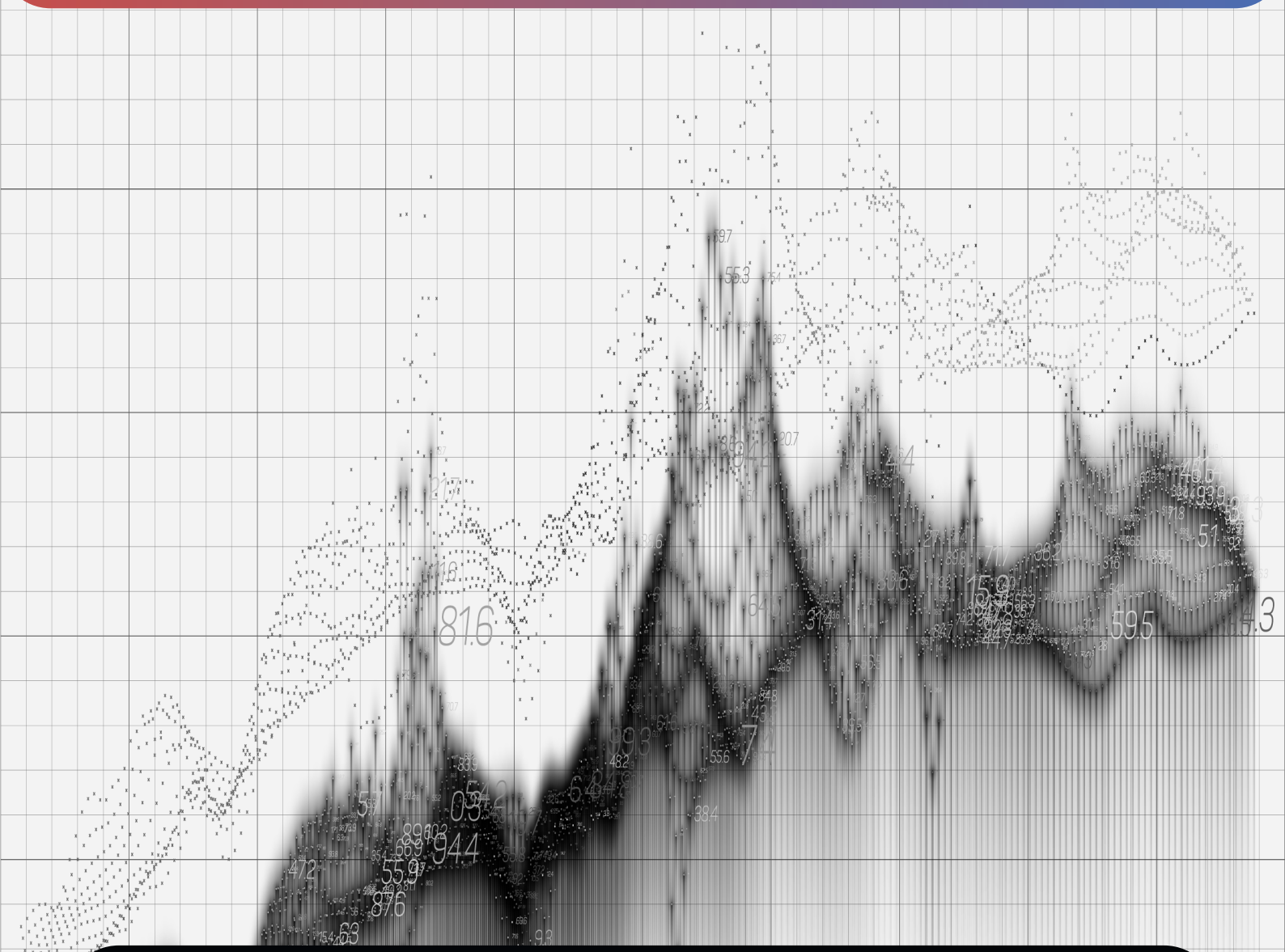
- **Vantaggi**: Il threat hunting riduce il rischio di attacchi nascosti che rimangono attivi per lunghi periodi, identificando e neutralizzando le minacce in fase iniziale. È un approccio ideale per le aziende che desiderano una protezione a un livello avanzato, andando oltre il monitoraggio passivo.

/services/

## 04 Incident response

- **Descrizione**: La nostra soluzione di risposta agli incidenti (incident response) include la creazione di piani dettagliati e procedure per gestire gli incidenti di sicurezza. I nostri esperti collaborano con il team IT aziendale per sviluppare un piano di risposta efficace, che include la gestione dell'incidente, la comunicazione con le parti interessate e la mitigazione dei danni.
- **Vantaggi**: Un piano di incident response efficace aiuta l'azienda a reagire rapidamente e a limitare l'impatto degli incidenti di sicurezza, riducendo i tempi di inattività e i costi associati a una violazione. È un elemento fondamentale per garantire una ripresa rapida e minimizzare il rischio di danni duraturi.





## Analisi Statistica

Il monitoraggio continuo e la risposta tempestiva alle minacce informatiche sono fondamentali per proteggere le aziende dalle crescenti minacce nel panorama digitale. Ecco alcune statistiche che evidenziano l'importanza di implementare soluzioni avanzate in questo ambito:

- **Aumento degli attacchi informatici in Italia**: Nel terzo trimestre del 2024, l'Italia ha registrato un incremento del 115% negli attacchi informatici rispetto allo stesso periodo dell'anno precedente, con una media di 2.301 attacchi settimanali per organizzazione.
- **Costo delle violazioni dei dati**: Secondo il report "Cost of a Data Breach 2024" di IBM, il costo medio di una violazione dei dati in Italia ha raggiunto i 4,37 milioni di euro, segnando un aumento del 23% rispetto al 2023.
- **Tempo di identificazione e contenimento**: Le aziende italiane impiegano in media 218 giorni per identificare e contenere un incidente di sicurezza, 40 giorni in meno rispetto alla media globale di 258 giorni.
- **Efficacia dell'uso di AI e automazione:**: L'adozione di intelligenza artificiale e automazione nella sicurezza ha permesso di ridurre il costo medio delle violazioni di 3,24 milioni di euro.

Queste statistiche sottolineano l'importanza per le aziende di adottare misure proattive, come il monitoraggio continuo e la risposta tempestiva alle minacce, per proteggere efficacemente i propri dati e la propria infrastruttura IT.

/services/

# [ VALUTAZIONE DEL RISCHIO E CONSULENZA ]

**IN COSA CONSISTE IL SERVIZIO:**

**Fornisce un'analisi approfondita dei rischi e delle vulnerabilità di sicurezza, supportando le aziende nel mitigare i rischi con soluzioni personalizzate.**

La nostra offerta di **Valutazione del Rischio e Consulenza** è studiata per supportare le aziende in ogni fase della gestione del rischio, dall'identificazione delle vulnerabilità alla messa in atto di strategie di difesa robuste e mirate. Comprendiamo che ogni organizzazione è unica, con esigenze specifiche in base al settore, alla struttura operativa e agli obiettivi di crescita. Per questo, lavoriamo a stretto contatto con il cliente per fornire una consulenza personalizzata che tenga conto delle sfide attuali e delle dinamiche evolutive del panorama della cybersecurity.

Attraverso un'analisi dettagliata e sistematica delle vulnerabilità e delle potenziali minacce, il nostro obiettivo è non solo identificare e mitigare i rischi immediati, ma anche costruire una resilienza a lungo termine. Siamo convinti che una postura di sicurezza robusta debba essere basata su una strategia chiara e un percorso evolutivo che possa crescere insieme all'azienda. Ogni intervento è finalizzato a proteggere gli asset critici e a salvaguardare il valore aziendale, migliorando al contempo l'efficienza operativa e la fiducia degli stakeholder.

I nostri servizi sono adatti a organizzazioni di tutte le dimensioni, dalle piccole imprese che cercano un supporto per la conformità e la protezione di dati sensibili, fino alle grandi aziende che necessitano di un approccio sofisticato per gestire e mitigare i rischi complessi. La nostra esperienza copre settori come la finanza, la sanità, la logistica, l'industria manifatturiera, e altri, con soluzioni su misura che rispondono alle esigenze di ognuno.

## Quali soluzioni include il servizio

### 01 Valutazione delle vulnerabilità

- Effettuiamo scansioni e audit di sicurezza approfonditi per individuare potenziali punti deboli nei sistemi informatici. L'analisi copre tutti i livelli – software, hardware e processi operativi – fornendo una visione chiara delle criticità e permettendo alle aziende di agire in modo tempestivo.

### 02 Analisi del rischio basata sulle minacce

- Attraverso una mappatura accurata dei rischi, costruiamo scenari di attacco specifici per la vostra attività, considerando le minacce più rilevanti nel panorama attuale della cybersecurity. Questo approccio permette di focalizzare le risorse sui rischi più concreti, ottimizzando le strategie difensive.

### 03 Piani di remediation personalizzati

- Dopo l'analisi delle vulnerabilità, forniamo raccomandazioni concrete e personalizzate per mitigare i rischi individuati. I nostri piani di remediation sono costruiti su misura per il contesto aziendale del cliente, garantendo un miglioramento tangibile delle difese di sicurezza.

### 04 Risk assessment continuo

- La sicurezza è un processo in evoluzione. Eseguiamo valutazioni periodiche per adattare le difese aziendali alle minacce emergenti. Questo servizio assicura che la vostra azienda mantenga sempre un livello di protezione adeguato, anche di fronte a nuove sfide nel panorama della cybersecurity.

# /services/

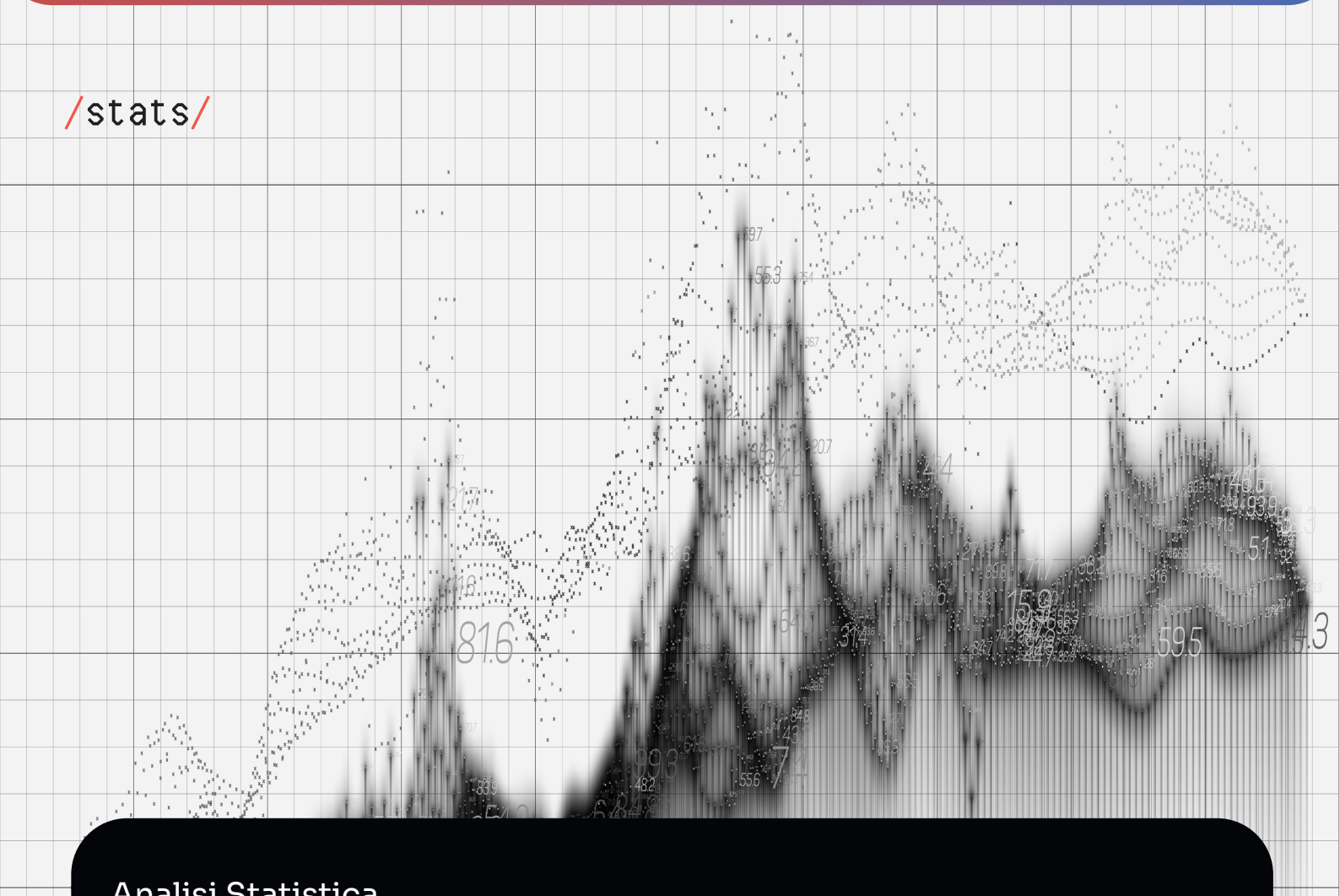
## 05 Cybersecurity maturity model

- Misuriamo il livello di maturità della vostra sicurezza informatica attraverso un framework strutturato, evidenziando punti di forza e aree da migliorare. Questo modello guida le aziende nel percorso di crescita verso una maggiore resilienza di sicurezza.

## 06 Supply chain risk assessment

- Identifichiamo e valutiamo i rischi derivanti dalle relazioni con fornitori e partner terzi, proteggendo la vostra azienda dalle vulnerabilità che potrebbero infiltrarsi lungo la catena di fornitura. Questo processo include la valutazione di policy, protocolli di sicurezza e conformità dei partner, garantendo una difesa omogenea e completa.

/stats/



## Analisi Statistica

La crescente frequenza e complessità degli attacchi informatici evidenzia l'importanza cruciale di una solida strategia di valutazione del rischio e consulenza in cybersecurity. Ecco alcune statistiche rilevanti che sottolineano l'urgenza di tali servizi:

- **Aumento dei costi delle violazioni dei dati**: In Italia, il costo medio di una violazione dei dati ha raggiunto i 4,37 milioni di euro nel 2024, segnando un incremento del 23% rispetto all'anno precedente. Questo rappresenta l'aumento più significativo dai tempi della pandemia.
- **Tempo di identificazione e contenimento**: Le aziende italiane impiegano in media 218 giorni per identificare e contenere una violazione, 40 giorni in meno rispetto alla media globale di 258 giorni. Tuttavia, questo periodo prolungato può comportare danni significativi.
- **Impatto dell'Intelligenza Artificiale e dell'automazione**: Le organizzazioni che integrano estensivamente l'IA e l'automazione nella sicurezza informatica risparmiano in media 3,24 milioni di euro sui costi di una violazione e riducono il tempo di risposta di 114 giorni rispetto a quelle che non adottano queste tecnologie.
- **Settori più colpiti**: In Italia, le aziende del settore tecnologico hanno registrato le violazioni più onerose, con costi medi di 5,46 milioni di euro, seguite dal settore industriale (5,13 milioni di euro) e da quello farmaceutico (5,01 milioni di euro).
- **Vettori di attacco prevalenti**: Il phishing rappresenta il 17% degli attacchi iniziali, con un costo medio di 4,18 milioni di euro per violazione, seguito dal furto o compromissione di credenziali al 13% (4,75 milioni di euro).

Queste statistiche evidenziano l'importanza di una valutazione proattiva dei rischi e di una consulenza specializzata per proteggere le aziende dalle crescenti minacce informatiche.

/services/

# [ FORMAZIONE E SENSIBILIZZAZIONE DEL PERSONALE ]

**IN COSA CONSISTE IL SERVIZIO:**

**Garantisce che il personale sia formato e consapevole delle minacce alla sicurezza informatica.**

La sicurezza informatica non è solo una questione di tecnologia e sistemi, ma coinvolge ogni persona all'interno dell'organizzazione. Anche il più avanzato sistema di difesa informatica può essere compromesso da errori umani o dalla mancanza di consapevolezza. Per questo motivo, la Formazione e Sensibilizzazione del Personale rappresenta un elemento cruciale per costruire una cultura della sicurezza all'interno dell'azienda. Il nostro servizio è progettato per educare e preparare i dipendenti, rendendoli la prima linea di difesa contro le minacce informatiche.

**Perché la Formazione e la Sensibilizzazione del Personale sono fondamentali?**

Secondo studi recenti, più del 90% degli attacchi informatici inizia con un errore umano, spesso dovuto a mancanza di consapevolezza o distrazione. La formazione non solo riduce drasticamente il rischio di incidenti, ma migliora anche la risposta del personale in caso di attacco, riducendo i tempi di reazione e aumentando la resilienza complessiva dell'organizzazione. Le aziende che investono in programmi di formazione e sensibilizzazione vedono una riduzione significativa delle violazioni e un miglioramento della sicurezza complessiva.

**VANTAGGI PER L'AZIENDA:**

- Riduzione del rischio di attacchi riusciti: I dipendenti formati sono meno propensi a cadere vittima di tentativi di phishing o altre minacce di ingegneria sociale, riducendo il rischio di accessi non autorizzati.
- Incremento della conformità alle normative: Molte normative, come il GDPR, richiedono che il personale sia adeguatamente formato in tema di protezione dei dati. I programmi di formazione supportano la conformità alle normative.
- Creazione di una cultura della sicurezza: Quando la sicurezza è parte integrante della cultura aziendale, tutti i membri dell'organizzazione, dal top management ai nuovi dipendenti, si sentono responsabilizzati e parte di una missione comune.
- Maggiore efficienza e risposta agli incidenti: Un personale consapevole e preparato è in grado di rispondere tempestivamente agli incidenti, minimizzando il loro impatto.

## Quali soluzioni include il servizio

### 01 Programmi di formazione continua

- **Descrizione**: Offriamo corsi di formazione regolari e aggiornati su diverse tematiche di sicurezza, personalizzabili in base al livello di conoscenza e al ruolo specifico dei partecipanti. Tra i temi trattati, vi sono la gestione sicura delle password, la protezione delle informazioni sensibili, il riconoscimento di tentativi di phishing e le misure di sicurezza da adottare per il lavoro da remoto.
- **Vantaggi:** Un programma di formazione continua assicura che il personale sia costantemente aggiornato sui rischi e le pratiche di sicurezza. Questa formazione regolare permette ai dipendenti di diventare consapevoli e preparati, riducendo significativamente la possibilità di errori umani e migliorando la resilienza dell'organizzazione.

/services/

## 02 Simulazioni di phishing

- **Descrizione**: Le simulazioni di phishing sono test periodici che riproducono attacchi di phishing realistici per valutare la capacità dei dipendenti di riconoscere tentativi di ingegneria sociale. Durante queste simulazioni, i dipendenti ricevono email simulate di phishing, con report dettagliati sui risultati e feedback personalizzati per migliorare la consapevolezza.

- **Vantaggi:** Le simulazioni di phishing aiutano a identificare i punti deboli nella consapevolezza del personale e a rinforzare la loro capacità di riconoscere e ignorare email fraudolente. Questo tipo di addestramento pratico fornisce feedback immediato e tangibile, consentendo ai dipendenti di apprendere dagli errori in un ambiente sicuro.

## 03 Campagne di sensibilizzazione

- **Descrizione**: Organizziamo campagne di sensibilizzazione che diffondono materiale educativo, linee guida e aggiornamenti su best practice di sicurezza informatica. Attraverso newsletter, poster, infografiche, webinar e video formativi, manteniamo i dipendenti informati e coinvolti sui temi della sicurezza.

- **Vantaggi:** Le campagne di sensibilizzazione creano un ambiente in cui la sicurezza è una priorità condivisa. Questo approccio costante e informale aiuta a rafforzare le nozioni di sicurezza e a promuovere comportamenti sicuri in modo naturale, creando una cultura aziendale orientata alla protezione delle informazioni.

/stats/

## Analisi Statistica

La formazione e la sensibilizzazione del personale in materia di sicurezza informatica sono fondamentali per proteggere le aziende dalle minacce cibernetiche. Ecco alcune statistiche che evidenziano l'importanza di investire in questo ambito:

- **Prevalenza degli attacchi informatici**: Nel 2021, il 40% delle grandi imprese italiane ha registrato un aumento degli attacchi informatici rispetto all'anno precedente, in parte a causa della diffusione dello smart working e dell'uso di dispositivi personali per scopi lavorativi.
- **Carenza di formazione**: Nonostante l'importanza della formazione, il 74% delle aziende non fornisce ai dipendenti alcuna formazione sulla sicurezza informatica, esponendo l'organizzazione a rischi elevati.
- **Efficacia della formazione**: Una ricerca ha rivelato che il 79% degli utenti che hanno ricevuto una formazione sulla sicurezza informatica l'ha trovata utile. Tuttavia, solo il 31% di loro ha smesso di riutilizzare le password, indicando la necessità di programmi formativi più efficaci.
- **Consapevolezza del rischio**: Il 30% delle piccole imprese considera il phishing come la principale minaccia informatica, mentre l'83% delle PMI non è preparato a riprendersi dai danni finanziari di un attacco informatico.

Queste statistiche sottolineano l'importanza di implementare programmi di formazione e sensibilizzazione per il personale, al fine di ridurre il rischio di attacchi informatici e proteggere le risorse aziendali.

/services/

# [ LEGAL CYBERCOMPLIANCE ]

**IN COSA CONSISTE IL SERVIZIO:**

**Assicura che l'azienda aderisca agli standard di sicurezza informatica internazionali e alle normative vigenti.**

In un contesto globale sempre più regolamentato, la sicurezza informatica è sotto la lente di normative e standard internazionali sempre più rigorosi. Il rispetto delle normative non è solo una questione di conformità legale, ma una dimostrazione di affidabilità, integrità e professionalità per le aziende. Essere conformi agli standard di sicurezza non significa solo evitare sanzioni; è un impegno verso la protezione dei dati aziendali, la fiducia dei clienti e la stabilità delle operazioni.

Il nostro servizio di Conformità e Normative è progettato per aiutare le aziende a raggiungere e mantenere la conformità con i principali standard di cybersecurity, adattandosi alle normative locali e internazionali. Grazie a una consulenza approfondita e a una gestione meticolosa della conformità, supportiamo le organizzazioni nella mitigazione dei rischi, nel rispetto delle normative vigenti e nel rafforzamento della loro reputazione.

**Come supportiamo la conformità della tua azienda**

Il nostro approccio alla conformità è completo e personalizzato, basato su un'analisi approfondita delle esigenze aziendali e delle normative applicabili. Offriamo:

- **Audit di Conformità (Compliance Audit)**: L'audit di conformità è un servizio fondamentale per verificare che l'azienda rispetti tutte le normative vigenti in materia di protezione dei dati personali e sicurezza informatica, come il GDPR e la Direttiva NIS II. Questo servizio prevede un'analisi completa delle procedure interne, dei sistemi di sicurezza informatica e delle policy aziendali per identificare eventuali lacune e aree di non conformità. Il nostro approccio inizia con una valutazione preliminare delle attività aziendali, durante la quale conduciamo interviste con i responsabili delle diverse aree operative per comprendere il contesto e identificare i rischi specifici. Successivamente, eseguiamo analisi tecniche dei sistemi informativi per verificare la presenza di vulnerabilità e valutare l'adeguatezza delle misure di sicurezza implementate. Al termine dell'audit, forniamo un rapporto dettagliato che include le aree di miglioramento e raccomandazioni pratiche per garantire la conformità e ridurre al minimo i rischi. Questo audit non è solo una verifica formale, ma rappresenta un'opportunità per sviluppare un percorso di miglioramento continuo in termini di sicurezza e compliance.

- **Redazione e implementazione di Policy Aziendali (Policy Drafting)**: La gestione efficace della sicurezza informatica e dei dati personali richiede policy aziendali ben definite, che siano comprensibili e applicabili da tutti i livelli dell'organizzazione. Offriamo un servizio completo di redazione e implementazione di policy personalizzate, che includono le migliori prassi per la gestione della sicurezza IT, la protezione dei dati personali e la risposta agli incidenti. Identifichiamo le aree aziendali che necessitano di policy specifiche, come la gestione dell'accesso ai dati, l'uso sicuro dei dispositivi aziendali e personali, e la protezione delle informazioni sensibili. Collaboriamo con il management per sviluppare policy adatte alle specifiche esigenze aziendali, fornendo anche formazione al personale per assicurarci che ogni membro dell'organizzazione sia consapevole delle proprie responsabilità. Organizziamo sessioni formative interattive per spiegare le policy e supportare l'implementazione pratica delle stesse, con l'obiettivo di garantire una conformità operativa effettiva.

# /services/

- **Assistenza Contrattuale (Contractual Assistance)**: I contratti con fornitori, partner e clienti possono rappresentare un punto critico per la sicurezza informatica, soprattutto se non affrontano adeguatamente i rischi legati alla cybersecurity. Il nostro servizio di assistenza contrattuale è volto a redigere e revisionare le clausole contrattuali per minimizzare tali rischi e garantire la conformità con le normative. Sviluppiamo clausole contrattuali su misura che affrontano aspetti come la gestione degli incidenti di sicurezza, la responsabilità delle parti e la protezione dei dati personali. Questo include anche la revisione dei contratti con i fornitori di servizi cloud e altri partner tecnologici, assicurandoci che siano in linea con le migliori prassi di sicurezza e che prevedano adeguate garanzie per la protezione dei dati. Offriamo inoltre supporto durante le negoziazioni contrattuali, affinché l'azienda possa difendere efficacemente i propri interessi e mitigare i rischi legati alla collaborazione con terze parti.

- **Incident Response Legale (Legal Incident Response)**: In caso di incidente informatico, una gestione tempestiva e corretta degli aspetti legali è fondamentale per limitare i danni e garantire il rispetto delle normative. Il nostro servizio di incident response legale è progettato per supportare l'azienda in ogni fase della gestione dell'incidente, con particolare attenzione alle implicazioni legali. Aiutiamo le aziende a sviluppare piani di risposta agli incidenti, che includono procedure dettagliate per la gestione degli aspetti legali e per la comunicazione con le autorità competenti, come il Garante per la protezione dei dati personali. In caso di incidente, il nostro team offre supporto immediato per raccogliere prove, identificare le cause, contenere l'impatto e gestire le notifiche obbligatorie verso le autorità e le parti interessate. Lavoriamo in stretta collaborazione con il team IT per garantire che tutte le azioni siano conformi alle normative e per minimizzare i rischi legali. Dopo la risoluzione dell'incidente, conduciamo una valutazione post-evento per identificare le lezioni apprese e sviluppare raccomandazioni per migliorare la resilienza dell'azienda e prevenire futuri incidenti.

- **Formazione e sensibilizzazione del personale**: La conformità non è solo una questione tecnica; è fondamentale che tutto il personale sia informato e consapevole delle proprie responsabilità in tema di sicurezza e privacy. Offriamo programmi di formazione personalizzati per educare i dipendenti sulle normative di sicurezza, sui comportamenti da adottare e sugli errori da evitare.

- **Audit periodici e valutazione della conformità**: Un elemento cruciale per mantenere la conformità è il monitoraggio costante. Eseguiamo audit periodici per valutare l'efficacia delle misure adottate e identificare eventuali carenze. Questi audit possono essere interni o preparativi per certificazioni esterne e sono progettati per mantenere l'azienda sempre aggiornata rispetto ai cambiamenti normativi.

**I BENEFICI DELLA CONFORMITA' PER L'AZIENDA**

- **Protezione contro le sanzioni**: La non conformità alle normative di sicurezza e privacy può portare a sanzioni finanziarie ingenti e danni reputazionali. Il nostro servizio di conformità riduce drasticamente questo rischio, proteggendo l'azienda da multe, restrizioni operative e danni di immagine.

- **Miglioramento della fiducia dei clienti e dei partner**: La trasparenza nella gestione dei dati e la conformità agli standard di sicurezza rappresentano un valore aggiunto per clienti e partner. Dimostrare un impegno concreto nella protezione delle informazioni sensibili rafforza la fiducia e migliora le relazioni commerciali, aumentando il valore competitivo dell'azienda.

- **Ottimizzazione dei processi aziendali**: L'implementazione di standard di sicurezza promuove una gestione dei dati strutturata e coerente, migliorando i processi aziendali. La conformità diventa un'opportunità per l'azienda di riorganizzare i flussi di lavoro, ridurre inefficienze e aumentare l'efficacia operativa.

- **Riduzione del rischio di attacchi informatici**: La conformità non è solo una questione legale; i requisiti normativi includono pratiche di sicurezza che migliorano direttamente la protezione contro attacchi e violazioni dei dati. Il nostro servizio aiuta l'azienda a sviluppare una solida postura di sicurezza, riducendo il rischio di attacchi e di esposizione alle minacce.

# /services/

**CONFORMITA' COME INVESTIMENTO STRATEGICO:**

La conformità alle normative di sicurezza e privacy è sempre più considerata un vantaggio strategico: non solo protegge l'azienda, ma rappresenta un segno di qualità e affidabilità per il mercato. Con l'evoluzione delle normative e l'introduzione di nuovi requisiti, investire nella conformità significa prepararsi al futuro, rafforzando la propria posizione competitiva e anticipando le aspettative di clienti e stakeholder.

Grazie al nostro servizio di **Conformità e Normative**, la tua azienda può operare serenamente e in piena conformità, con la certezza di rispettare gli standard più elevati di cybersecurity.

## Quali soluzioni include il servizio

## 01 GDPR (Regolamento Generale sulla Protezione dei Dati)

- **Descrizione**: Il GDPR è il regolamento dell'Unione Europea che stabilisce le linee guida per la raccolta, la gestione e la protezione dei dati personali. Aiutiamo le aziende ad adattarsi alle normative GDPR, assicurando che siano adottate le misure di sicurezza necessarie per proteggere i dati personali e garantire i diritti degli utenti.
- **Vantaggi:** La conformità al GDPR riduce il rischio di sanzioni finanziarie e di danni reputazionali, proteggendo l'azienda da multe fino al 4% del fatturato annuo globale. Inoltre, il rispetto delle normative GDPR migliora la fiducia dei clienti, dimostrando un impegno verso la trasparenza e la protezione dei dati personali.

## 02 NIS II

- **Descrizione**: La Direttiva NIS II è una normativa dell'Unione Europea che si pone l'obiettivo di rafforzare la sicurezza informatica delle infrastrutture critiche e dei servizi essenziali, quali energia, trasporti, sanità e finanza. La direttiva impone obblighi di sicurezza e segnalazione di incidenti informatici, assicurando che le organizzazioni adottino misure di sicurezza appropriate per mitigare i rischi legati alle minacce cyber e garantire la continuità dei servizi essenziali.
- **Vantaggi:** L'adozione della NIS II migliora la resilienza e la capacità di risposta alle minacce informatiche, riducendo il rischio di interruzioni nei servizi critici. La conformità alla direttiva può aumentare la fiducia di clienti e partner, dimostrando un impegno per la protezione delle infrastrutture sensibili e la continuità operativa. Inoltre, l'implementazione di standard di sicurezza aiuta le aziende a stare al passo con le migliori pratiche di cybersecurity a livello europeo.

## 03 NIST Cybersecurity Framework

- **Descrizione**: Anche se sviluppato negli Stati Uniti, il **NIST Cybersecurity Framework** è utilizzato globalmente e rappresenta uno standard di best practice nella gestione dei rischi. La sua adozione è particolarmente utile per clienti che operano anche sul mercato americano o in settori regolati.
- **Vantaggi**: L'adozione del NIST Cybersecurity Framework permette alle aziende di migliorare la gestione dei rischi informatici secondo standard riconosciuti a livello globale, aumentando la resilienza contro minacce cyber avanzate. Questo framework offre un approccio strutturato e flessibile, adattabile a organizzazioni di diverse dimensioni e settori, rendendolo particolarmente utile per aziende che operano nel mercato americano o in ambiti altamente regolamentati, come finanza e sanità. La conformità al NIST può aumentare la credibilità e la fiducia da parte di clienti e partner internazionali, dimostrando l'adozione di best practice nella protezione dei dati e delle infrastrutture. Inoltre, il framework facilita la comunicazione dei rischi all'interno dell'organizzazione e con le parti esterne, favorendo la collaborazione e la condivisione delle informazioni sulle minacce per una difesa più efficace.

/services/

## 04 ISO/IEC 27001 - 27002

- **Descrizione**: La norma ISO 27001 è uno standard internazionale per la gestione della sicurezza delle informazioni, progettato per aiutare le aziende a proteggere i propri dati attraverso l'implementazione di controlli di sicurezza, policy e processi specifici. Offriamo supporto per la preparazione e l'ottenimento della certificazione ISO 27001, garantendo che l'organizzazione sviluppi un sistema di gestione della sicurezza (ISMS) robusto e conforme ai requisiti. La norma ISO 27002 è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO/IEC 27001 al fine di proteggere le risorse informative; ISO/IEC 27001 è il documento normativo di certificazione al quale l'organizzazione deve fare riferimento per costruire un Sistema di Gestione della Sicurezza delle Informazioni che possa essere certificato da un ente indipendente, mentre la norma ISO/IEC 27002 non è certificabile in quanto è una semplice raccolta di raccomandazioni. La versione corrente è la 2022 (ISO/IEC 27002:2022).

- **Vantaggi:** La conformità alla ISO 27001 - 27002 dimostra l'impegno dell'azienda verso la sicurezza delle informazioni, riducendo il rischio di attacchi informatici e violazioni dei dati. Inoltre, la certificazione può rappresentare un vantaggio competitivo, evidenziando l'affidabilità e la professionalità dell'azienda sul mercato.

## 05 Agenzia per la Cybersicurezza Nazionale (ACN) e Strategie di Cybersecurity

- **Descrizione**: Le linee guida e le disposizioni dell'ACN sono rilevanti per chiunque operi in cybersecurity. La **Strategia Nazionale di Cybersicurezza 2022-2026** rappresenta un quadro di riferimento per la resilienza e la protezione dei dati e delle infrastrutture italiane, elementi centrali nella consulenza che potete offrire ai vostri clienti.

- **Vantaggi:** L'adesione alle linee guida dell'ACN e alla Strategia Nazionale di Cybersecurity rafforza la resilienza delle aziende e delle istituzioni italiane, migliorando la loro capacità di prevenire e rispondere agli attacchi informatici. La conformità a questi standard non solo aumenta la sicurezza delle infrastrutture critiche e dei dati sensibili, ma consente anche alle aziende di dimostrare un impegno concreto verso la protezione della sicurezza nazionale e la continuità operativa. Per i fornitori di servizi di cybersecurity, operare secondo le direttive dell'ACN costituisce un vantaggio competitivo, permettendo loro di attrarre clienti che richiedono un'elevata affidabilità e aderenza agli standard nazionali. Inoltre, la partecipazione attiva alla Strategia Nazionale offre opportunità di collaborazione con enti pubblici e privati, contribuendo a rafforzare l'ecosistema di cybersecurity nazionale e a promuovere la fiducia nell'economia digitale.

## 06 Perimetro di Sicurezza Nazionale Cibernetica (D.L. 105/2019)

- **Descrizione**: Questo decreto è fondamentale per la protezione delle infrastrutture critiche nazionali e impone alle aziende di rispettare requisiti di sicurezza rigorosi. La vostra società, con una competenza in cybersecurity, può supportare le aziende a conformarsi a queste normative, proteggendo i loro sistemi critici.

- **Vantaggi**: L'adeguamento al Perimetro di Sicurezza Nazionale Cibernetica permette alle aziende di migliorare la protezione delle loro infrastrutture critiche, riducendo il rischio di attacchi che potrebbero compromettere la sicurezza nazionale. La conformità a questa normativa assicura inoltre un controllo e monitoraggio costante delle minacce cyber, rendendo le organizzazioni più resilienti contro gli attacchi informatici avanzati. Questo impegno per la sicurezza può aumentare la fiducia dei clienti e partner, dimostrando l'adesione a standard elevati di protezione e la capacità di rispondere efficacemente alle minacce emergenti. Inoltre, le aziende che rispettano il decreto potrebbero beneficiare di agevolazioni o supporto da parte dello Stato per rafforzare le proprie misure di sicurezza, contribuendo a migliorare la sicurezza collettiva del paese.

/services/

## 07 Codice dell'Amministrazione Digitale (CAD)

- **Descrizione**: Il CAD stabilisce le linee guida per la digitalizzazione della Pubblica Amministrazione e richiede requisiti di sicurezza informatica. Questo è un riferimento importante per eventuali clienti pubblici o per aziende che forniscono servizi alla PA.

- **Vantaggi:** L'adozione delle linee guida del CAD migliora l'efficienza e la trasparenza della Pubblica Amministrazione, facilitando l'accesso ai servizi digitali per cittadini e imprese. Per le aziende che forniscono servizi alla PA, la conformità al CAD rappresenta un vantaggio competitivo, poiché dimostra la capacità di operare secondo standard di sicurezza e digitalizzazione richiesti dalla normativa italiana. Questo impegno non solo accresce la fiducia della PA, ma può anche aprire opportunità di collaborazione e contratti nel settore pubblico. Inoltre, il rispetto dei requisiti di sicurezza del CAD contribuisce a proteggere i dati e i servizi digitali, riducendo il rischio di attacchi e violazioni che potrebbero danneggiare la reputazione e le operazioni della PA.

## 08 PCI-DSS (Payment Card Industry Data Security Standard)

- **Descrizione**: Il PCI-DSS è uno standard di sicurezza progettato per proteggere le informazioni delle carte di credito e ridurre il rischio di frodi. Offriamo supporto per l'implementazione di pratiche di sicurezza che rispettano i requisiti del PCI-DSS, garantendo che tutte le transazioni e i dati delle carte siano gestiti in modo sicuro e conforme agli standard.

- **Vantaggi:** La conformità al PCI-DSS riduce il rischio di violazioni dei dati e frodi, proteggendo sia l'azienda sia i clienti. La certificazione PCI-DSS è un requisito fondamentale per qualsiasi organizzazione che gestisca pagamenti con carta, garantendo al contempo maggiore sicurezza e protezione delle informazioni sensibili dei clienti.

## 09 Cybersecurity Maturity Model Certification (CMMC)

- **Descrizione**: Per clienti che lavorano con il Dipartimento della Difesa degli Stati Uniti o altre agenzie governative, il CMMC è un requisito fondamentale. La vostra competenza in cybersecurity potrebbe includere supporto nella preparazione a questo standard di conformità.

- **Vantaggi**: La conformità alla CMMC è essenziale per le aziende che collaborano con il Dipartimento della Difesa degli Stati Uniti o altre agenzie governative, poiché garantisce che rispettino elevati standard di sicurezza nella protezione delle informazioni sensibili. L'ottenimento della certificazione CMMC non solo apre l'accesso a contratti governativi e a opportunità nel settore della difesa, ma rafforza anche la reputazione aziendale, dimostrando un impegno concreto verso la sicurezza e l'affidabilità. Per i clienti, il supporto nella preparazione alla CMMC rappresenta un valore aggiunto, poiché facilita l'adozione delle best practice richieste dal governo statunitense, riducendo al contempo il rischio di non conformità. Inoltre, il processo di certificazione promuove una maggiore consapevolezza e maturità nella gestione dei rischi, creando una cultura aziendale orientata alla cybersecurity che può migliorare la resilienza complessiva contro le minacce informatiche.

## 10 Conformità SOX (Sarbanes-Oxley Act)

- **Descrizione**: La legge SOX è un regolamento statunitense che richiede alle aziende quotate in borsa di seguire rigide pratiche di trasparenza e controllo interno. Offriamo supporto per la creazione di un ambiente di controllo e trasparenza in linea con i requisiti della SOX.

- **Vantaggi**: La conformità alla SOX aumenta la fiducia degli investitori e migliora la trasparenza aziendale, riducendo il rischio di frodi e di pratiche contabili non conformi.

/services/

## 11 HIPAA (Health Insurance Portability and Accountability Act)

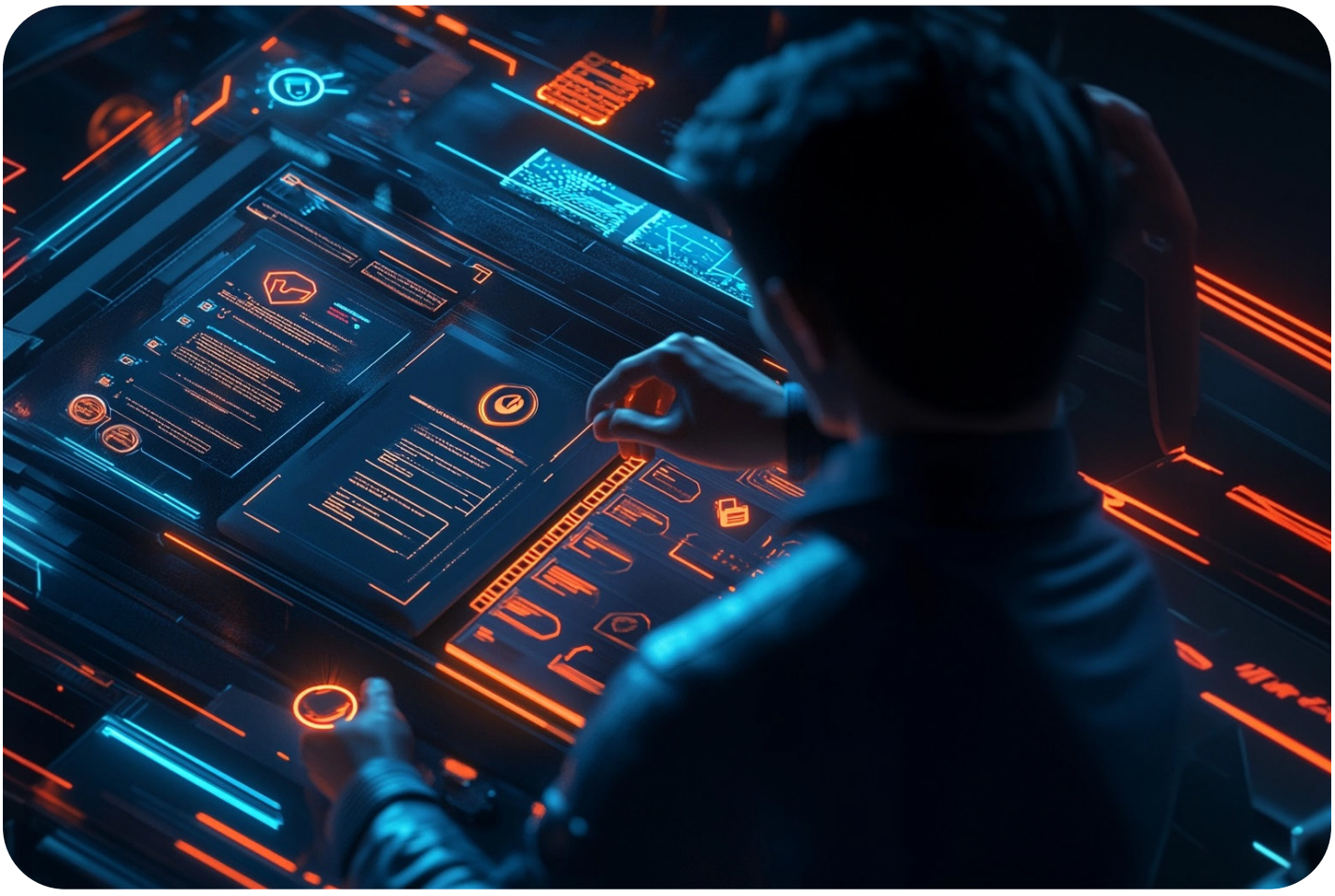
- **Descrizione**: Per le aziende che operano nel settore sanitario e gestiscono informazioni sanitarie protette (PHI), garantiamo la conformità allo standard HIPAA. Questo include la protezione dei dati sensibili dei pazienti e l'implementazione di misure di sicurezza per prevenire accessi non autorizzati.

- **Vantaggi:** La conformità all'HIPAA è fondamentale per evitare sanzioni e assicurare la fiducia dei pazienti, garantendo che le informazioni sanitarie siano sempre protette.

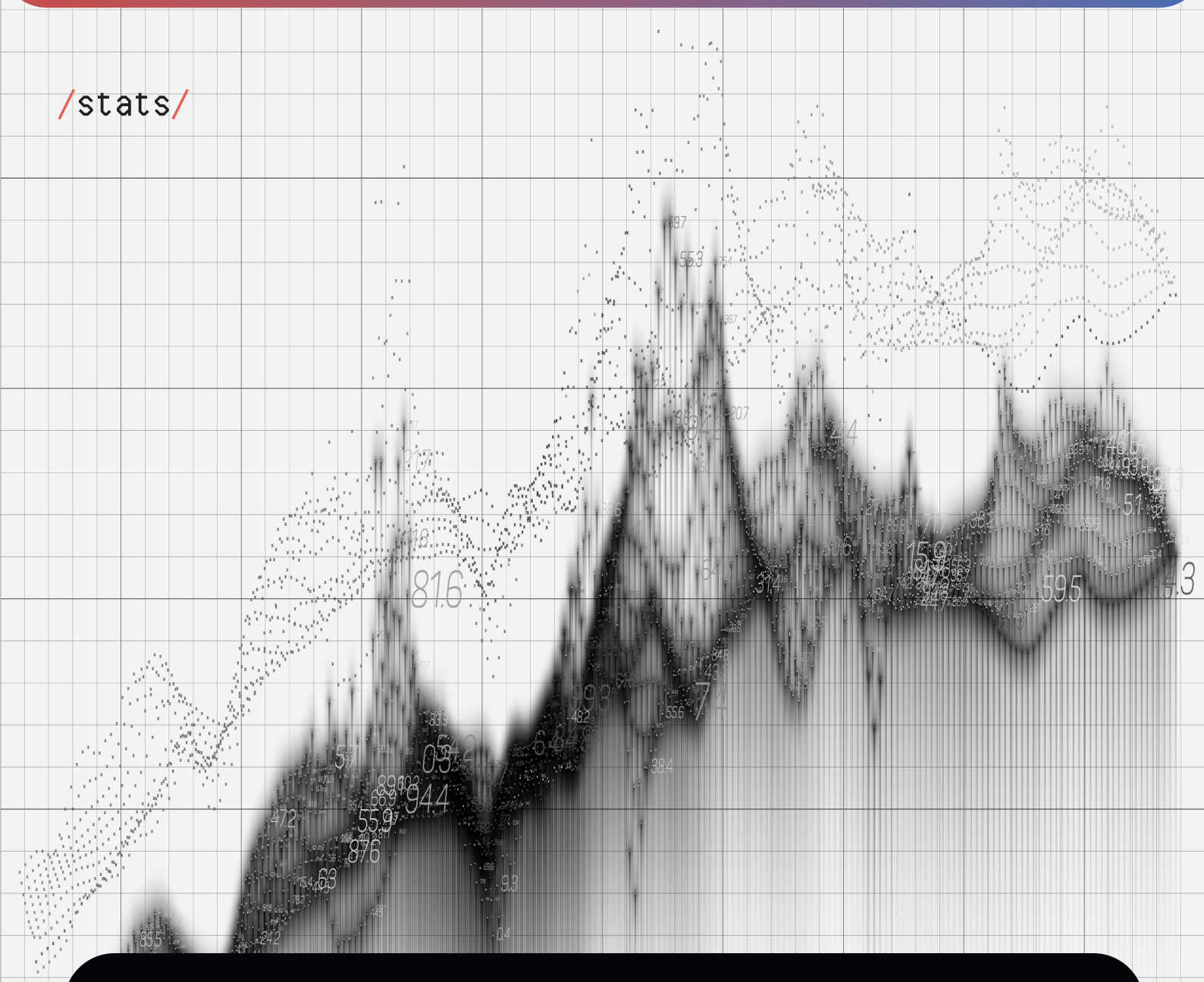
## 12 Leggi settoriali e specifiche per i mercati in cui operano i clienti

- **Descrizione**: Alcuni settori, come il finanziario e il sanitario, hanno regolamentazioni aggiuntive (es. HIPAA per la sanità negli Stati Uniti, regolamenti di Banca d'Italia per il settore finanziario). È utile segnalare che la vostra società è in grado di assistere i clienti nel rispetto di normative specifiche dei settori in cui operano.

- **Vantaggi:** La conformità alle normative settoriali specifiche, come HIPAA per la sanità negli Stati Uniti o i regolamenti della Banca d'Italia per il settore finanziario, garantisce alle aziende la possibilità di operare in modo sicuro e legale nei propri mercati di riferimento. Rispettare queste normative permette alle organizzazioni di evitare sanzioni e di proteggere dati sensibili, dimostrando l'impegno per la sicurezza e la privacy dei propri clienti e pazienti. Inoltre, l'aderenza alle leggi settoriali migliora la fiducia e la credibilità dell'azienda nel mercato, poiché conferma la capacità di gestire dati e sistemi secondo gli standard più elevati del settore. Per le aziende, affidarsi a un partner che comprenda a fondo queste normative rappresenta un vantaggio competitivo, riducendo il rischio di non conformità e aumentando la loro competitività in ambiti altamente regolamentati.



/stats/



## Analisi Statistica

La conformità alle normative di sicurezza informatica è fondamentale per le aziende che desiderano proteggere i propri dati e mantenere la fiducia dei clienti. Ecco alcune statistiche che evidenziano l'importanza di aderire agli standard di sicurezza:

- **Violazioni dei dati e conformità**: Secondo un rapporto del 2024, oltre il 40% delle aziende non ha superato un audit di conformità negli ultimi dodici mesi. Tra queste, il 31% ha subito una violazione dei dati, rispetto al 3% delle aziende che hanno superato gli audit di conformità.
- **Investimenti in sicurezza informatica**: In Italia, le aziende allocano in media l'11,8% del budget IT alla sicurezza informatica, una percentuale superiore alla media europea dell'8,8%. Questo indica una crescente attenzione alla conformità e alla protezione dei dati.
- **Impatto delle normative sulla sicurezza**: L'adozione della direttiva NIS 2 e della norma ISO/IEC 27001 consente alle aziende di rafforzare la loro sicurezza informatica, garantendo una maggiore protezione delle infrastrutture critiche e la conformità alle normative.

Queste statistiche sottolineano l'importanza per le aziende di investire nella conformità alle normative di sicurezza informatica per ridurre il rischio di violazioni e proteggere le informazioni sensibili.

# /contacts/

CYBERQUAKE

**Via Francesco Domenico Guerrazzi, 23**
**50132 - Firenze (ITALY)**

**www.cyberquake.tech**

**info@cyberquake.tech**

**+39 328 66 58 586**