




## PILLOLE PER L'ACCESSO ALLA PIATTAFORMA LAZARUS

Grazie alla sottoscrizione del prodotto assicurativo Protezione Cyber puoi accedere alla **Piattaforma Lazarus** e **usufruire di servizi di sorveglianza e monitoraggio continuo** - 24 ore su 24 e 7 giorni su 7 - **volti a prevenire e mitigare i rischi derivanti da eventuale attacco cyber.**

Di seguito si riportano gli step per accedere alla Piattaforma Lazarus...

<p style="text-align: center;"><b>1</b></p> <p style="text-align: center;"><b>...COME ACCEDERE ALLA PIATTAFORMA</b></p>  <p>A seguito della sottoscrizione di Protezione Cyber riceverai <u>al tuo indirizzo e-mail personale fornito al momento della sottoscrizione della polizza</u>, il link di accesso alla Piattaforma Lazarus:</p> <p style="text-align: center;"><a href="http://helvetia.cyberscp.it/">http://helvetia.cyberscp.it/</a></p>	<p style="text-align: center;"><b>2</b></p> <p style="text-align: center;"><b>...DA CHI ARRIVA IL LINK DI ACCESSO ALLA PIATTAFORMA</b></p>  <p>Il link di accesso alla Piattaforma arriva da <b>Helvetia Assicurazioni</b>, dal seguente indirizzo e-mail:</p> <p style="text-align: center;">no-reply@helvetia.cyberscp.it</p> <p>Controlla la casella di posta elettronica per monitorare l'avvenuta ricezione del link, <u>avendo cura di verificare anche la cartella spam.</u></p>	<p style="text-align: center;"><b>3</b></p> <p style="text-align: center;"><b>...COSA FARE IN CASO DI PROBLEMI</b></p>  <p>Nel caso in cui <b>non dovessi ricevere il link di accesso alla Piattaforma e/o riscontrassi difficoltà nella registrazione</b></p> <p style="text-align: center;">chiama il numero verde <b>039 888 0025</b></p> <p style="text-align: center;">oppure</p> <p style="text-align: center;">scrivi all'indirizzo e-mail <b>helpdesk@helvetia.cyberscp.it</b></p>
<p style="text-align: center;"><b>Assicurati di aver fornito l'indirizzo e-mail corretto al momento della sottoscrizione!!!</b></p>	<p style="text-align: center;"><b>Aspetta i tempi tecnici utili (circa 10 giorni) alla trasmissione del link e controlla sempre anche la cartella spam!!!</b></p>	<p style="text-align: center;"><b>Ricordati che per qualsiasi necessità il numero verde è sempre attivo e disponibile per te!!!</b></p>

Per ulteriori dettagli sui servizi offerti dalla Piattaforma Lazarus si rimanda all'allegato Manuale Utente

## MANUALE UTENTE

### Obiettivo

Il presente documento è volto a descrivere:

- gli step che il titolare della polizza, a seguito della sottoscrizione del contratto assicurativo, deve seguire per accedere alla Piattaforma di servizi cyber offerti dalla presente polizza;
- le principali funzionalità della Piattaforma di servizi cyber.

### Legenda

Di seguito si riporta la leggenda per una corretta lettura del documento:



I box evidenziano i servizi / le funzionalità della Piattaforma che vengono spiegati in dettaglio nella colonna dedicata.




La lente di ingrandimento evidenzia che per il servizio / funzionalità in oggetto è presente un focus dedicato nelle sezioni successive del documento.

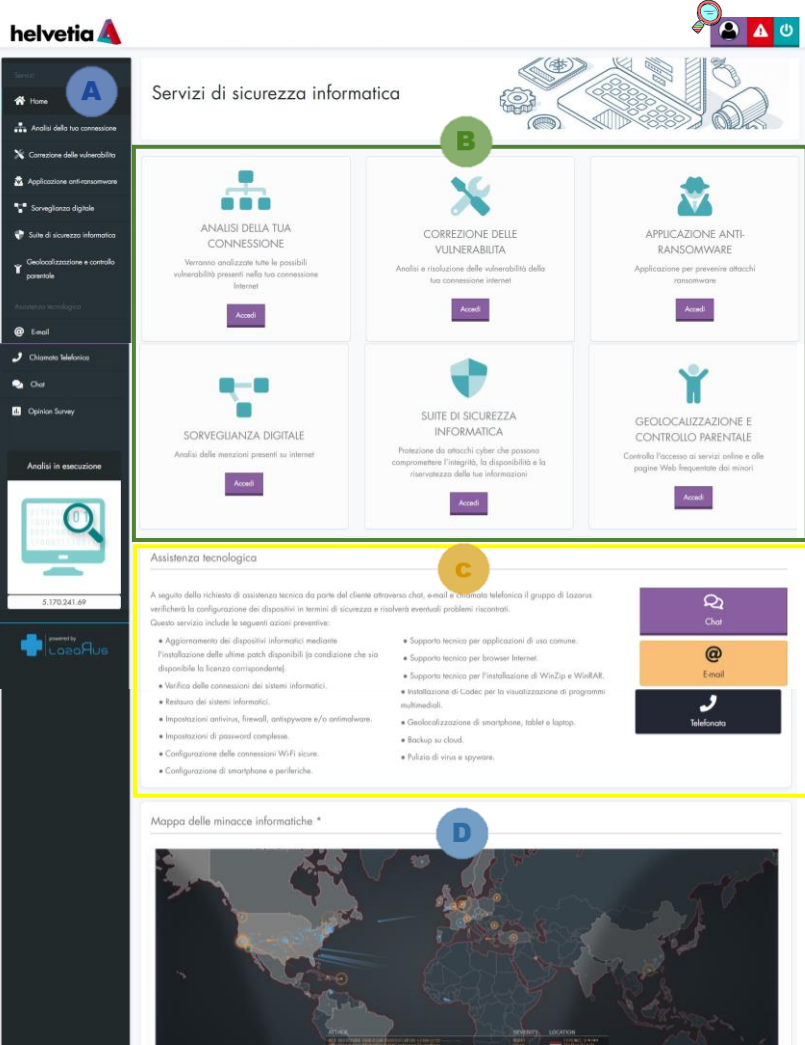
## Funzionamento della Piattaforma di Lazarus

La Piattaforma di Lazarus (di seguito Piattaforma), disponibile per i Clienti che hanno acquistato il prodotto Protezione Cyber di Helvetia Italia Assicurazioni S.p.A., offre servizi di sorveglianza e monitoraggio continuo - 24 ore su 24 e 7 giorni su 7 - volta a prevenire e mitigare i rischi derivanti da eventuale attacco cyber.

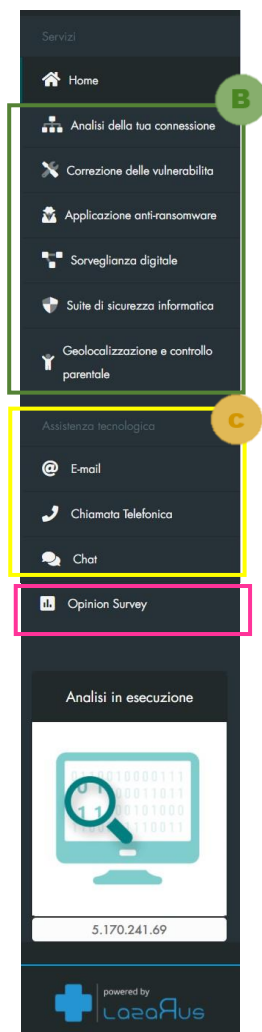
L'accesso alla Piattaforma può essere effettuato utilizzando qualsiasi device a disposizione del Cliente (mobile, pc, tablet, ...), accedendo al link fornito successivamente alla sottoscrizione del contratto.

Di seguito sono descritte le modalità di accesso e le funzionalità della Piattaforma:

 <p>helvetia</p> <p>Piattaforma per la fornitura di servizi di prevenzione e monitoraggio dei rischi informatici, in collaborazione con Lazarus Technology.</p> <p>La Piattaforma permette di accedere ai servizi di analisi della connessione, account online e siti web, nonché al servizio di HelpDesk per la risoluzione di problematiche legate all'assistenza tecnologica, all'installazione o fornitura di servizi e per la riparazione delle vulnerabilità.</p> <p>powered by Lazarus</p> <p>Se non hai mai utilizzato i nostri servizi, clicca qui:</p> <p>1 Nuovo utente</p> <p>Se hai utilizzato i nostri servizi, clicca qui:</p> <p>2 Accesso agli utenti registrati</p>	<h3>Login Piattaforma di Lazarus</h3> <p>A seguito dell'acquisto di Protezione Cyber, il contraente riceve all'indirizzo e-mail fornito in sede di sottoscrizione, il link di accesso alla Piattaforma per potere procedere con la registrazione.</p> <p>È necessario:</p> <ul style="list-style-type: none"><li>⚠️ Aspettare i tempi tecnici utili (circa 10 giorni) per la ricezione del link</li><li>⚠️ Controllare la posta elettronica per monitorare la ricezione del link da "no-reply@helvetia.cyberscp.it" utile per l'accesso alla Piattaforma, avendo cura di verificare anche la cartella spam.</li><li>➊ In caso di nuovi Clienti è necessario accettare i termini e le condizioni previste dal Fornitore e registrarsi creando un proprio ID.</li><li>➋ In caso di Clienti già registrati, è necessario inserire l'indirizzo e-mail fornito in sede di</li></ul>
--	--

	<p>sottoscrizione e la password creata in precedenza.</p>
 <p>The screenshot shows the Helvetia Home Page with a dark sidebar on the left containing navigation icons for Home, connection analysis, vulnerability, anti-ransomware, digital surveillance, parental control, technical assistance, email, phone, chat, and surveys. The main content area is titled 'Servizi di sicurezza informatica' and features six service cards: 'ANALISI DELLA TUA CONNESSIONE', 'CORREZIONE DELLE VULNERABILITÀ', 'APPLICAZIONE ANTI-RANSOMWARE', 'SORVEGLIANZA DIGITALE', 'SUITE DI SICUREZZA INFORMATICA', and 'GEOLOCALIZZAZIONE E CONTROLLO PARENTALE'. Below these is a 'Assistenza tecnologica' section with a list of services and contact buttons for Chat, Email, and Telefonata. At the bottom is a 'Mappa delle minacce informatiche' showing a world map with threat indicators.</p>	<p><b>Home Page</b></p> <p>Dopo aver effettuato l'accesso alla pagina iniziale è possibile visualizzare:</p> <ul style="list-style-type: none"><li>A. La barra di navigazione</li><li>B. I servizi offerti dalla Piattaforma</li><li>C. Le modalità previste per richiedere assistenza tecnologica</li><li>D. La mappa delle minacce informatiche</li></ul> <p>Di seguito è riportato il dettaglio di ogni sezione.</p>

## Sezione **A**



Cliccando sulle funzionalità presenti nella banda di sinistra della Home Page, è possibile:


- accedere direttamente al servizio desiderato (dettaglio riportato in seguito: focus sezione B);
- richiedere assistenza attraverso le modalità disponibili (dettaglio riportato in seguito: focus sezione C);
- partecipare al sondaggio per esprimere il proprio grado di soddisfazione sui servizi offerti dalla Piattaforma.





## Sezione **B**










## Servizi di sicurezza informatica

In questa sezione sono riportati i servizi disponibili attraverso l'utilizzo della Piattaforma.




 Di seguito si riporta il dettaglio dei singoli servizi.

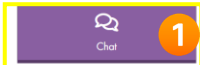
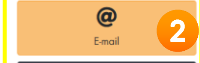
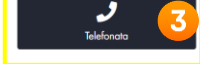
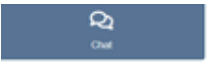





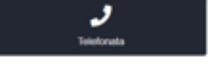


<h2>Analisi della tua connessione <sup>1</sup></h2>  <p>ANALISI DELLA TUA CONNESSIONE</p>	<p>Servizio "<b>analisi della tua connessione</b>": cliccando su <b>ACCEDI</b></p> <p>è possibile accedere alle opzioni disponibili nella presente sezione.</p>
<h2>Analisi della tua connessione</h2>  <p>In cosa consiste il servizio?</p> <p>Servizio di analisi della connessione Internet effettuata tramite dispositivo mobile o computer.</p> <p>Durante l'analisi viene simulato un attacco cyber e vengono effettuati una serie di test sul tuo indirizzo IP per conoscerne il grado di sicurezza informatica.</p> <p>Durante l'analisi della vulnerabilità è possibile continuare a lavorare utilizzando altre applicazioni, tuttavia è necessario non disconnettere il dispositivo da Internet.</p> <p>Quando si avvia il controllo di vulnerabilità, non disconnettere il dispositivo da Internet, ma è possibile continuare a lavorare in altre applicazioni.</p> <p>In caso di domande, fai clic su "Inizia chat" in modo che i nostri esperti possano aiutarti.</p> 	<p>Cliccando su <b>INIZIA</b></p> <p>è possibile analizzare la propria connessione internet e conoscerne il reale grado di sicurezza (cosiddetta vulnerabilità).</p> <p>Cliccando su <b>VEDI ULTIMA ANALISI</b></p> <p>è possibile verificare, attraverso report dedicati, le precedenti analisi di vulnerabilità effettuate.</p> <p>Cliccando su <b>INIZIA CHAT</b></p> <p>è possibile parlare con i tecnici specializzati.</p>
<h2>Correzione delle vulnerabilità <sup>2</sup></h2>  <p>CORREZIONE DELLE VULNERABILITÀ</p>	<p>Servizio "<b>correzione delle vulnerabilità</b>": cliccando su <b>ACCEDI</b></p> <p>è possibile accedere alle opzioni disponibili nella presente sezione.</p>

 <p><b>Correzione</b></p> <p>Una volta effettuata l'analisi della tua connessione, un esperto potrà analizzare i risultati ottenuti e se ci sono vulnerabilità può aiutarti a risolverle.</p> <p><a href="#">INIZIA CHAT</a></p>	<p>Cliccando su</p> <p><a href="#">INIZIA CHAT</a></p> <p>è possibile analizzare, con il supporto di un esperto, i risultati ottenuti dall'analisi della vulnerabilità della connessione e risolvere eventuali criticità emerse.</p>
<p><b>Applicazione Anti-Ransomware</b> <span style="background-color: #2e7d32; color: white; border-radius: 50%; padding: 2px 5px;">3</span></p> <div style="text-align: center;">  <p>APPLICAZIONE ANTI-RANSOMWARE</p> </div>	<p>Servizio "<b>applicazione anti-ransomware</b>": cliccando su</p> <p><a href="#">ACCEDI</a></p> <p>è possibile accedere alle opzioni disponibili nella presente sezione.</p>
<p><b>Applicazione anti-ransomware</b></p>  <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  <div style="border: 1px solid #ccc; padding: 5px; width: fit-content; margin-top: 10px;">MS Windows x64</div> <div style="background-color: #f96; padding: 5px; width: fit-content; margin-top: 5px;">Richiedi licenza</div> </div> <div> <p><b>Installazione dell'applicazione Anti-Ransomware</b></p> <p>L'applicazione bloccherà in modo proattivo l'installazione di ransomware sul tuo computer in modo che sia sempre al sicuro.</p> <p>Dopo aver scaricato l'applicazione, sarà necessario fare "doppio clic" sul file scaricato per avviare l'installazione.</p> <p>Una volta scaricata l'applicazione, fare clic su "Richiedi licenza" per richiedere il numero di licenza al tecnico.</p> </div> </div>	<p>Cliccando su</p> <div style="border: 1px solid #ccc; padding: 5px; width: fit-content; margin: 10px auto;">MS Windows x64</div> <p>il cliente può scaricare sul proprio device l'applicazione anti-ransomware.</p> <p>Cliccando su</p> <div style="background-color: #f96; padding: 5px; width: fit-content; margin: 10px auto;">Richiedi licenza</div> <p>il cliente può richiedere eventualmente il numero di licenza al tecnico specializzato.</p>
<p><b>Sorveglianza digitale</b> <span style="background-color: #2e7d32; color: white; border-radius: 50%; padding: 2px 5px;">4</span></p> <div style="text-align: center;">  <p>SORVEGLIANZA DIGITALE</p> </div>	<p>Servizio "<b>sorveglianza digitale</b>": cliccando su</p> <p><a href="#">ACCEDI</a></p> <p>è possibile accedere alle opzioni disponibili nella presente sezione.</p>
<p><b>Sorveglianza digitale</b></p>  <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  <div style="background-color: #444; color: white; padding: 5px; width: fit-content; margin-top: 10px;">Accedi</div> <div style="background-color: #2e7d32; color: white; padding: 5px; width: fit-content; margin-top: 5px;">INIZIA CHAT</div> </div> <div> <p><b>In cosa consiste il Servizio?</b></p> <p>Il Cliente potrà effettuare ricerche sul web relative a possibili furti d'identità attraverso il supporto di tecnici specializzati e visualizzare il report con le evidenze dell'analisi.</p> <p>Se hai domande, fai clic su "Inizia Chat" in modo che i nostri esperti possano aiutarti.</p> </div> </div>	<p>Cliccando su</p> <div style="background-color: #444; color: white; padding: 5px; width: fit-content; margin: 10px auto;">Accedi</div> <p>il cliente può effettuare ricerche sul web relative a possibili furti di identità e generare report dedicati</p> <p>Cliccando sul tasto</p> <div style="background-color: #2e7d32; color: white; padding: 5px; width: fit-content; margin: 10px auto;">INIZIA CHAT</div>

	<p>è possibile parlare con un tecnico specializzato.</p>
<p>Suite di sicurezza informatica <b>5</b></p> 	<p>Servizio <b>"suite di sicurezza informatica"</b>: cliccando su <b>ACCEDI</b></p> <p>è possibile accedere alle opzioni disponibili dalla presente sezione.</p>
 <p>Suite di sicurezza informatica</p> <p>Installazione di BitDefender (disponibile solo per Windows)</p> <p>Come assicurato puoi installare un'applicazione di sicurezza informatica (licenza disponibile fino a 5 dispositivi) che offre protezione per salvaguardare i tuoi dati, i pagamenti effettuati sul web e la tua privacy online, in aggiunta ad una copertura contro eventi esterni che possono compromettere l'integrità, la disponibilità e la riservatezza delle tue informazioni.</p> <p>BitDefender ti offre:</p> <ul style="list-style-type: none"> <li>● Protezione da ransomware: blocco del ransomware al fine di evitare che i file personali possano essere criptati, rubati e soggetti a riscatto.</li> <li>● Sicurezza bancaria online: possibilità di effettuare transazioni online in un browser sicuro che protegge i tuoi account da possibili frodi.</li> <li>● Anti phishing: individua e blocca i siti web non attendibili e propensi a rubare dati personali e finanziari (password, numeri di carte di credito, ecc.).</li> <li>● Navigazione sicura: permette di conoscere l'affidabilità degli indirizzi IP delle ricerche effettuate sul web bloccando l'accesso ai collegamenti non sicuri. L'applicazione bloccherà inoltre l'installazione di ransomware o il furto di informazioni, in modo tale che il computer sia protetto contro questa tipologia di attacco.</li> </ul> <p>Clicca sul pulsante scarica per avviare il download dell'applicazione e successivamente fai doppio clic sul file scaricato per avviare l'installazione. Completata l'installazione clicca su Richiedi licenza per richiedere il numero di licenza al tecnico.</p>	<p>Cliccando su <b>Scarica</b></p> <p>il Cliente può scaricare sul proprio device l'applicazione di sicurezza (antivirus) denominato Bit Defender. L'installazione e la registrazione a BitDefender deve essere effettuata utilizzando un sistema operativo Windows mentre, gli accessi successivi, sono possibili anche da altri dispositivi (es. iOS) effettuando il download dallo store (es. Apple Store).</p> <p>Cliccando su <b>Richiedi licenza</b></p> <p>il Cliente può richiedere il numero di licenza al tecnico specializzato per poter attivare l'applicazione di sicurezza installata sul proprio device.</p> <p><b>!</b> In occasione della scadenza annuale dell'antivirus Bit Defender, annualità che decorre dalla data di attivazione dell'abbonamento, al Cliente comparirà, in Piattaforma, un pop-up contenente l'indicazione di procedere al rinnovo. Per poter procedere al rinnovo, il Cliente dovrà</p>



	<p>accedere alla Sezione "Suite di Sicurezza informatica" presente in Piattaforma e cliccare sul tasto "ATTIVARE". Sarà poi sufficiente seguire i successivi semplici passi per poter procedere con il completamento dell'operazione di rinnovo.</p>
<p>Geolocalizzazione e controllo parentale <span style="background-color: #4CAF50; color: white; border-radius: 50%; padding: 2px 6px;">6</span></p> <div style="text-align: center; margin: 20px 0;">  <p>GEOLOCALIZZAZIONE E CONTROLLO PARENTALE</p> </div>	<p>Servizio "<b>Geolocalizzazione e controllo parentale</b>": cliccando su</p> <div style="text-align: center; margin: 10px 0;"> <span style="background-color: #9C27B0; color: white; border-radius: 10px; padding: 5px 15px;">ACCEDI</span> </div> <p>è possibile accedere alle opzioni disponibili nella presente sezione.</p>
<div style="text-align: center; margin-bottom: 20px;">  <p>Geolocalizzazione e controllo parentale</p> </div> <div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; align-items: center; margin-bottom: 10px;">  <div> <p><b>BitDefender Parental Control</b></p> <p>Perché ti consigliamo BitDefender Total Security?</p> <ul style="list-style-type: none"> <li>🔑 Funzionalità di Parental Control</li> <li>🔑 Protezione per dispositivi mobili e PC</li> <li>🔑 Monitoraggio dei social media</li> <li>🔑 Geolocalizzazione</li> </ul> </div> </div> <div style="display: flex; align-items: center; margin-bottom: 10px;"> <div style="background-color: #4CAF50; color: white; border-radius: 10px; padding: 5px 10px; margin-right: 10px;">chat</div> <div> <p>BitDefender offre i servizi essenziali di controllo parentale quali: monitoraggio del web, accesso limitato ai siti internet e/o applicazioni e funzionalità avanzate come i controlli di contatto e geolocalizzazione.</p> <p>BitDefender è specializzato nel monitoraggio delle principali piattaforme di social media garantendo un'esperienza sicura per i tuoi bambini.</p> <p>Per usufruire dei servizi sopracitati è necessario installare BitDefender sui dispositivi utilizzati dai tuoi figli e configurare i loro profili. Da questo momento tutte le attività del dispositivo verranno monitorate.</p> </div> </div> <div> <p><b>Caratteristiche del Parental Control:</b></p> <ul style="list-style-type: none"> <li>🔑 Controllo dei contenuti e delle applicazioni: definizione del perimetro delle attività consentite e non consentite sul web ai tuoi figli.</li> <li>🔑 Report dettagliato di tutte le attività svolte dai tuoi figli sul web e relativa cronologia.</li> <li>🔑 Monitoraggio delle attività svolte sui social media dai tuoi figli (richieste di amicizia, fotografie, video, commenti e impostazioni sulla privacy).</li> </ul> </div> </div>	<p>Cliccando su</p> <div style="text-align: center; margin: 10px 0;"> <span style="background-color: #8BC34A; color: white; border-radius: 10px; padding: 5px 15px;">chat</span> </div> <p>è possibile parlare con un tecnico specializzato.</p> <p>Cliccando su</p> <div style="text-align: center; margin: 10px 0;"> <span style="background-color: #333; color: white; border-radius: 10px; padding: 5px 15px;">Accedi alla suite di Sicurezza Informatica</span> </div> <p>il Cliente può accedere alla suite di sicurezza informatica e attivare specifiche funzionalità offerte dall'applicazione di sicurezza Bit Defender. In particolare, tra queste si segnala: controllo parentale; monitoraggio dei social media; ricerche sul web in grado di rilevare l'eventuale grado di vulnerabilità dei propri indirizzi e-mail verificandone la presenza in rete.</p>

<p><b>Sezione</b> <span style="background-color: #f0c000; border-radius: 50%; padding: 2px 6px;">C</span></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Assistenza tecnologica</p> <p>A seguito della richiesta di assistenza tecnica da parte del cliente attraverso chat, e-mail e chiamata telefonica il gruppo di Lazarus verificherà la configurazione dei dispositivi in termini di sicurezza e risolverà eventuali problemi riscontrati. Questo servizio include le seguenti azioni preventive:</p> <ul style="list-style-type: none"> <li>• Aggiornamento dei dispositivi informatici mediante l'installazione delle ultime patch disponibili (a condizione che sia disponibile la licenza corrispondente).</li> <li>• Verifica delle connessioni dei sistemi informatici.</li> <li>• Restaura dei sistemi informatici.</li> <li>• Impostazioni antivirus, firewall, antispymare e/o antimalware.</li> <li>• Impostazioni di password complesse.</li> <li>• Configurazione delle connessioni WiFi sicure.</li> <li>• Configurazione di smartphone e periferiche.</li> <li>• Supporto tecnico per applicazioni di uso comune.</li> <li>• Supporto tecnico per browser Internet.</li> <li>• Supporto tecnico per l'installazione di WinZip e WinRAR.</li> <li>• Installazione di Codec per la visualizzazione di programmi multimediali.</li> <li>• Geolocalizzazione di smartphone, tablet e laptop.</li> <li>• Backup su cloud.</li> <li>• Pulizia di virus e spyware.</li> </ul> </div> <div style="margin-top: 10px;">    </div>	<p><b>Assistenza tecnologica</b></p> <p>In questa sezione vengono illustrate le modalità (chat, e-mail o contatto telefonico) con le quali il Cliente può richiedere assistenza tecnica.</p>
<p><b>Chat</b> <span style="background-color: #f0c000; border-radius: 50%; padding: 2px 6px;">1</span></p> <div style="margin-top: 10px;">   </div>	<p><b>Cliccando su</b></p> <div style="text-align: center; margin-bottom: 10px;">  </div> <p>è possibile parlare con un esperto attraverso una chat dedicata.</p>
<p><b>E-mail</b> <span style="background-color: #f0c000; border-radius: 50%; padding: 2px 6px;">2</span></p> <div style="margin-top: 10px;">   </div>	<p><b>Cliccando su</b></p> <div style="text-align: center; margin-bottom: 10px;">  </div> <p>appare un pop-up mediante il quale è possibile inserire l'indirizzo e-mail per essere contattati dal team di esperti.</p>
<p><b>Contatto telefonico</b> <span style="background-color: #f0c000; border-radius: 50%; padding: 2px 6px;">3</span></p> <div style="margin-top: 10px;">   </div>	<p><b>Cliccando su</b></p> <div style="text-align: center; margin-bottom: 10px;">  </div> <p>appare un pop-up all'interno del quale è possibile trovare il numero di telefono da chiamare.</p>

## Sezione D

Mappa delle minacce informatiche



## Mappa delle minacce informatiche

In questa sezione vengono visualizzati in tempo reale gli attacchi informatici in essere (provenienza/destinazione), il grado di rischio e il luogo in cui si stanno verificando.



Servizi di sicurezza informatica

**ANALISI DELLA TUA CONNESSIONE**

Veniamo analizzate tutte le possibili vulnerabilità presenti nella tua connessione Internet

[Accedi](#)

**CORREZIONE DELLE VULNERABILITÀ**

Analisi e riduzione delle vulnerabilità della tua connessione Internet

[Accedi](#)

**APPLICAZIONE ANTI-RANSOMWARE**

Applicazione per prevenire attacchi ransomware

[Accedi](#)

Utente di Demostración

- [Profilo utente](#)
- [Supporto tecnico](#)
- [Chiudi sessione](#)

**Profilo utente**  
 accedendo a questa sezione il Cliente può modificare i propri dati personali

**Richiesta urgente di supporto**

**Chiudi sessione**

**Richiesta di supporto**

## Manuale Servizi Lazarus

### Tabella riassuntiva servizi di Lazarus

Sezione	Azioni preventive	Azioni di rimedio a seguito di un incidente cyber
1) HOME BANKING	Analisi di vulnerabilità	Analisi forense delle e-mail
	Servizio di sorveglianza digitale: credenziali compromesse e Deep Web	
2) ACQUISTI ON-LINE	Sorveglianza digitale (dati compromessi nel Deep Web e violazioni)	Eliminazione delle menzioni indesiderate dalle pagine web
3) ASSISTENZA MALWARE	Security Suite	Analisi e pulizia dei sistemi
	Analisi di Vulnerabilità	Recupero Dati (se possibile)
	Applicazione AntiRansomware	Reset del Sistema
4) CYBER BULLISMO	Sorveglianza Digitale	Supporto di esperti
		Report di sorveglianza digitale post incidente
		Certificazioni del contenuto
	Parental Protection	Investigazione del caso (analisi forense IT)
Rimozione di segnalazioni indesiderate su internet		
5) FURTO IDENTITA' DIGITALE	Sorveglianza Digitale (segnalazioni, Deep Web e credenziali)	Analisi forense su account personali e falsi
		Rimozione di informazioni su internet non richieste (cancellazione informazioni)
		Recupero Account
6) RESPONSABILITA' DERIVANTE DA VIOLAZIONI DELLA SICUREZZA DELLA RETE	Analisi della vulnerabilità	Indagine forense dell'incidente e certificazione

## Descrizione servizi di Lazarus

I servizi offerti dalla Piattaforma di Lazarus prevedono:

- azioni preventive sempre disponibili per il Cliente volte a monitorare e tenere sotto controllo la propria rete informatica;
- azioni di rimedio per gli incidenti cyber.

Di seguito sono riportati nel dettaglio i singoli servizi offerti:

### 1) Home banking

Azioni preventive	Azioni di rimedio per gli incidenti cyber
Analisi di vulnerabilità	Analisi forense delle e-mail
Servizio di sorveglianza digitale: credenziali compromesse e Deep web	

#### *Azioni preventive*

Il team di esperti, attraverso l'utilizzo di specifici tool, verifica che non vi siano malware<sup>1</sup> sui dispositivi e, contemporaneamente, il servizio di sorveglianza digitale esamina automaticamente le informazioni del Cliente presenti in rete, nel Dark Web<sup>2</sup> e Deep Web<sup>3</sup> e gli indirizzi e-mail dei quali gli hackers hanno preso il controllo.

#### *Azioni di rimedio*

A seguito di una richiesta del Cliente, il team di esperti analizza le e-mail ricevute per identificare eventuali casistiche di phishing<sup>4</sup> e redige un report con i dettagli dell'analisi che può essere utilizzata a supporto di attività legali e/o di recupero delle somme sottratte e, se necessario, in sede di denuncia da parte dell'Assicurato.

<sup>1</sup> Malware: programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.

<sup>2</sup> Dark web: siti internet nascosti e accessibili solo da particolari browser il cui scopo è mantenere l'attività digitale anonima e privata. Vengono spesso utilizzati a sostegno di operazioni fraudolente.

<sup>3</sup> Deep web: insieme delle risorse informative del World wide web (uno dei principali servizi di internet che permette di navigare e di usufruire di un insieme di contenuti amatoriali e professionali collegati tra loro tramite un link) non indicizzate dai normali motori di ricerca.

<sup>4</sup> Phishing: truffa di informazioni personali, dati finanziari o codici di accesso effettuata su internet da parte di un malintenzionato che si finge un ente affidabile.

## 2) Acquisto Online

Azioni preventive	Azioni di rimedio
Sorveglianza digitale (dati compromessi nel Deep Web e violazioni)	Eliminazione delle menzioni indesiderate dalle pagine web

### *Azioni preventive*

Il servizio di sorveglianza digitale monitora le informazioni del Cliente presenti in rete, nel Dark Web, nel Deep Web e gli indirizzi e-mail dei quali gli hackers hanno preso il controllo.

### *Azioni di rimedio*

Tramite il servizio di sorveglianza digitale il Cliente può chiedere:

- l'eliminazione di menzioni indesiderate dalle pagine web;
- consigli tecnici da parte di un team di esperti sulle azioni da intraprendere;
- un'analisi approfondita della propria rete, pc, ecc.

## 3) Assistenza malware

Azioni preventive	Azioni di rimedio
Security Suite	Analisi e pulizia dei sistemi
Analisi di Vulnerabilità	Recupero Dati (se possibile)
Applicazione AntiRansomware	Reset del Sistema

### *Azioni preventive*

La Piattaforma mette a disposizione i seguenti servizi:

- antivirus BitDefender Total Security 2020 (qualora non fosse fruibile, il Fornitore provvederà a rendere disponibile altro antivirus con medesime caratteristiche);
- analisi delle vulnerabilità (da utilizzarsi periodicamente al fine di mantenere i dispositivi elettronici nel miglior stato di sicurezza possibile);
- AntiRansomware volto a ridurre gli impatti di eventuali attacchi informatici (per sistemi operativi MS Windows).

### *Azioni di rimedio*

I tecnici dell'help desk identificano la natura dell'attacco informatico per il recupero, il ripristino e/o la decontaminazione dei dati:

- se è gestibile da remoto, i dati del Cliente, a seguito della decontaminazione del dispositivo, saranno nuovamente archiviati sullo stesso;
- se non è gestibile da remoto, il Fornitore procede al ritiro del dispositivo per consegnarlo ai tecnici informatici dei centri appartenenti al network convenzionato;

- se avviene tramite ransomware<sup>5</sup> con relativa richiesta di riscatto, il team di esperti procede alla raccolta delle prove, verifica la veridicità della minaccia, avvia le azioni necessarie per mitigare il rischio e procede alla consegna del dispositivo ai tecnici informatici dei centri appartenenti al network convenzionato.

#### 4) Cyber bullismo

Azioni preventive	Azioni di rimedio
Sorveglianza digitale	Supporto di esperti
	Report di sorveglianza digitale
	Certificazioni del contenuto per gli incidenti cyber
Parental Protection	Investigazione del caso
	Rimozione di segnalazioni indesiderate su internet

##### *Azioni preventive*

Il servizio di sorveglianza digitale, attivo anche a seguito del verificarsi di un incidente cyber, permette un controllo continuo delle segnalazioni “negative” presenti nel web e la rimozione di quelle indesiderate. Congiuntamente al servizio di sorveglianza digitale, il Parental Protection offre protezione ai minori raccogliendo informazioni ed elementi utili a tutelarli da attacchi di cyber bullismo.

##### *Azioni di rimedio*

Il team di esperti esegue le seguenti azioni:

- raccoglie tutte le informazioni digitali presenti sia su internet che nei principali social media (Facebook, Twitter, Instagram, Snapchat, ecc.);
- a seguito della raccolta delle prove e del materiale, effettua delle verifiche per identificare l'origine e/o i responsabili;
- elabora un report dedicato che viene messo a disposizione del team legale o utilizzato a supporto di eventuali denunce alla polizia postale;
- constatato l'evento di cyber bullismo, se necessario, avvia il processo di ritiro delle informazioni e delle segnalazioni da internet e dai social media.

Tutte le operazioni sono coordinate da un team di esperti certificati.

---

<sup>5</sup> Ransomware: è un tipo di malware che limita l'accesso dei file che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione.

## 5) Furto identità digitale

Azioni preventive	Azioni di rimedio per gli incidenti cyber
Sorveglianza Digitale (segnalazioni, Deep Web e credenziali)	Analisi forense su account falsi
	Rimozione di informazioni indesiderate da internet (cancellazione informazioni)
	Recupero Account

### *Azioni preventive*

Il servizio di sorveglianza digitale raccoglie tutte le segnalazioni presenti sul web relative alle credenziali digitali (Deep Infusion si occupa di monitorare continuamente i dati digitali del Cliente).

### *Azioni di rimedio*

Il team di esperti provvede a:

- raccogliere i dati dell'incidente (lo spoofing<sup>6</sup> del profilo e/o dei dati bancari, tentativi di estorsione monetaria, la verifica delle credenziali d'accesso, profili sostituiti o ecc...);
- verificare che non ci siano malware nel device;
- esaminare i profili social e gli account e-mail per identificare eventuali accessi fraudolenti; gli esperti, in caso di impossibilità di accesso, provvedono al ripristino e/o al recupero degli stessi.

Nel caso in cui il furto d'identità comporti la diffamazione o la perdita di reputazione, attraverso la Deep Infusion sono monitorate le segnalazioni che hanno un impatto sull'immagine del Cliente e, se necessario, si procede alla loro rimozione dal web.

Vengono inoltre redatte:

- una relazione forense a supporto di eventuali azioni legali;
- specifica documentazione al fine di ripristinare il profilo/account del Cliente.

## 6) Responsabilità derivante da violazioni della sicurezza della Rete

Azioni preventive	Azioni di rimedio
Analisi della vulnerabilità	Indagine forense dell'incidente e certificazione

### *Azioni preventive*

Il servizio di analisi della vulnerabilità offerto dalla Piattaforma rileva la presenza nel dispositivo del Cliente di eventuali malware che possono essere diffusi a terzi con il rischio di contaminare siti, reti e/o device.

<sup>6</sup> Spoofing: manipolazione dei dati trasmessi in una rete telematica tramite la falsificazione del proprio indirizzo IP o mediante l'utilizzo illecito di user name e password di altri utenti.



*Azioni di rimedio*

Il team di esperti provvede a:

- raccogliere tutte le informazioni contenute nel reclamo effettuato da terze parti al fine di verificare l'esistenza di possibili malware, prevenirne la diffusione e di individuare eventuali strumenti coinvolti (browser, e-mail, rete, ecc...);
- effettuare l'analisi forense dell'incidente cyber ed elaborare il conseguente report che permette di valutare se la richiesta di risarcimento di terzi è legittima.

Sulla base delle risultanze ottenute, in coordinamento con il team legale, vengono intraprese le azioni più appropriate.

*Il Fornitore Lazarus è responsabile del trattamento dei dati personali: al primo accesso, il Cliente dovrà accettare i termini e le condizioni della Piattaforma, esprimendo il proprio consenso tramite una casella di spunta. Qualora il Cliente si avvalga di uno qualsiasi dei servizi di analisi di vulnerabilità offerti, dovrà acconsentire ai termini e alle condizioni specifici, che devono essere accettati a mezzo dell'apposita sezione della Piattaforma.*

## LOGIN PIATTAFORMA LAZARUS

A seguito della sottoscrizione del prodotto Protezione Cyber di Helvetia riceverai, all'indirizzo email fornito al momento della sottoscrizione, il link di accesso alla Piattaforma Lazarus.

Accedendo all'indirizzo web <http://helvetia.cyberscp.it/> potrai procedere con la relativa registrazione.



È necessario controllare la posta elettronica per monitorare la ricezione del link da "helvetia.cyberscp.it" utile per l'accesso alla Piattaforma, avendo cura di verificare anche la cartella spam.



Di seguito si riportano i riferimenti da contattare nel caso in cui non dovessi ricevere il link di accesso alla Piattaforma e/o riscontrassi difficoltà nella registrazione.



### Protezione Cyber



Numero di telefono: **039 888 0025**



Indirizzo e-mail: **[helpdesk@helvetia.cyberscp.it](mailto:helpdesk@helvetia.cyberscp.it)**

Per ulteriori informazioni si rimanda al Set Informativo del prodotto Protezione Cyber