semplice. chiaro. helvetia
La tua Assicurazione svizzera

PILLOLE PER L'ACCESSO ALLA PIATTAFORMA DI 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 di Lazarus…

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

Per ulteriori dettagli sui servizi offerti dalla Piattaforma di 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 dal presente prodotto;
- 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 un 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:

Login Piattaforma di Lazarus

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.

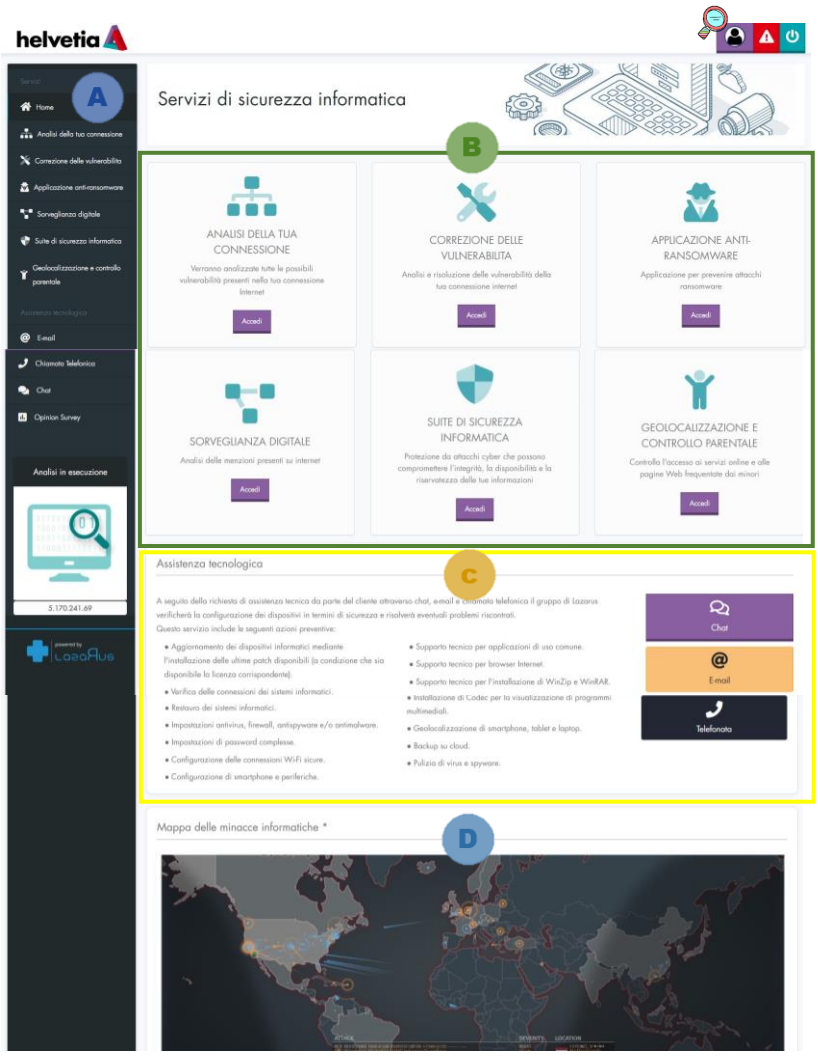
È necessario:

⚠ Aspettare i tempi tecnici utili per la ricezione del link (circa 10 giorni)

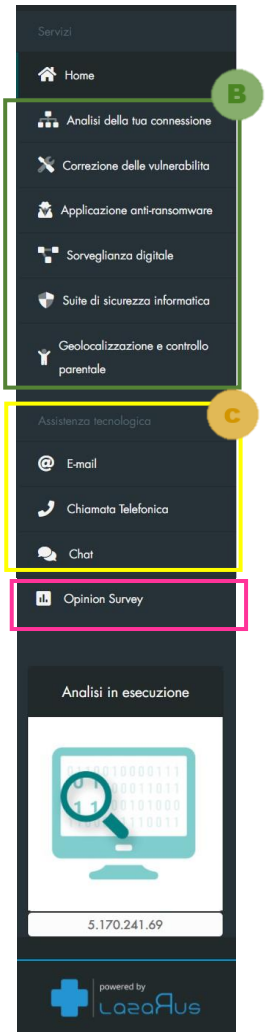
⚠ Controllare la posta elettronica per monitorare la ricezione del link da "no-reply@helvetia.cyberscp.it" utile per l'accesso alla Piattaforma, avendo cura di verificare anche la cartella spam.

1 In caso di nuovi Clienti è necessario accettare i termini e le condizioni previste dal Fornitore e registrarsi creando un proprio ID.

2 In caso di Clienti già registrati, è necessario inserire l'indirizzo e-mail fornito in sede di

	sottoscrizione e la password creata in precedenza.
	**Home Page** Dopo aver effettuato l'accesso alla pagina inziale è possibile visualizzare: A. La barra di navigazione B. I servizi offerti dalla Piattaforma C. Le modalità previste per richiedere assistenza tecnologica D. La mappa delle minacce informatiche Di seguito è riportato il dettaglio di ogni sezione.

Sezione A



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

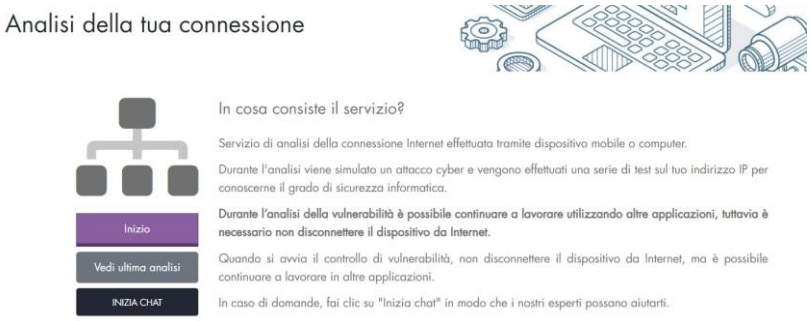
- accedere direttamente al servizio desiderato (dettaglio riportato in seguito: focus sezione B);
- richiedere assistenza attraverso le modalità disponibili (dettaglio riportato in seguito: focus sezione C);
- partecipare al sondaggio per esprimere il proprio grado di soddisfazione sui servizi offerti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

Sezione B

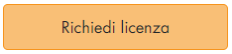
Servizi di sicurezza informatica

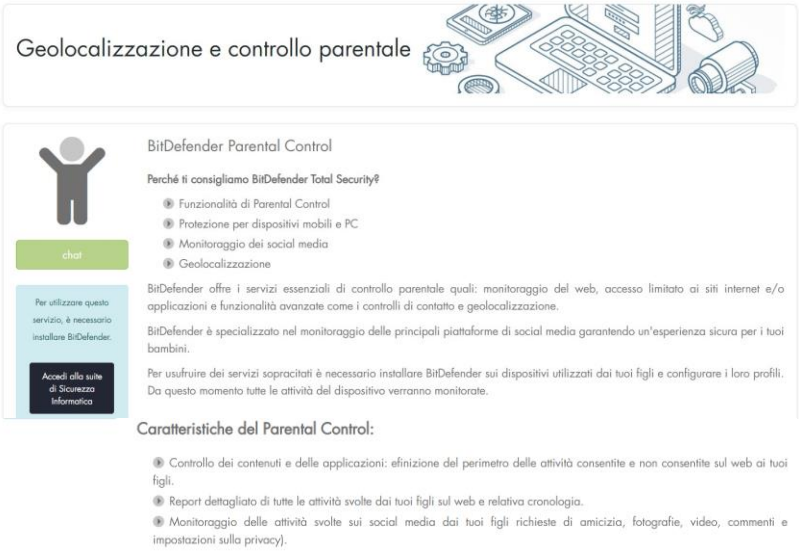
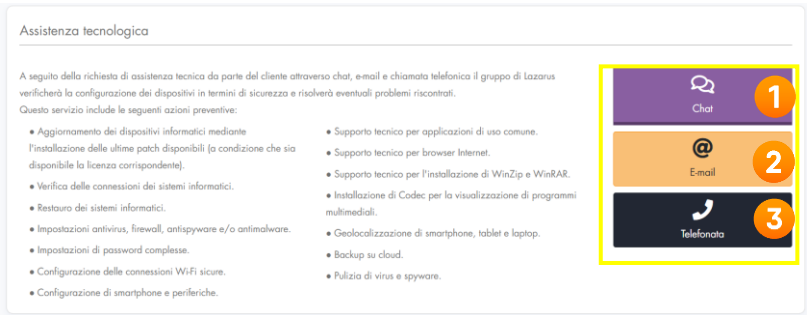
In questa sezione sono riportati i servizi disponibili attraverso l'utilizzo della Piattaforma.

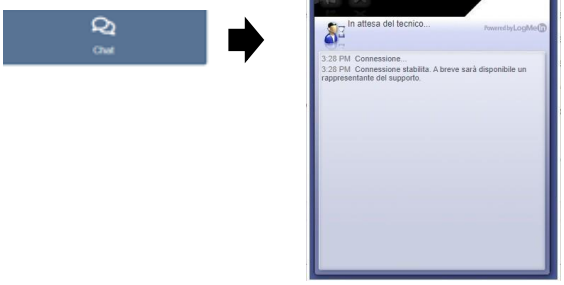
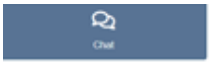
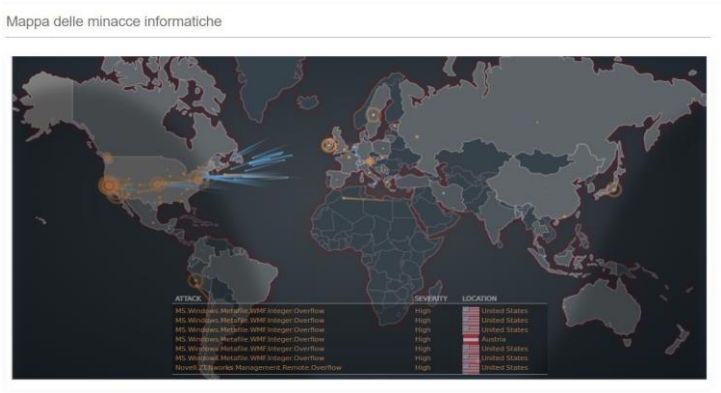
Di seguito si riporta il dettaglio dei singoli servizi.

Analisi della tua connessione 1  	Servizio **"analisi della tua connessione":** cliccando su ACCEDI è possibile accedere alle opzioni disponibili nella presente sezione.
 	Cliccando su INIZIA è possibile analizzare la propria connessione internet e conoscerne il reale grado di sicurezza (cosiddetta vulnerabilità). Cliccando su VEDI ULTIMA ANALISI è possibile verificare, attraverso report dedicati, le precedenti analisi di vulnerabilità effettuate. Cliccando su INIZIA CHAT è possibile parlare con i tecnici specializzati.
Correzione delle vulnerabilità 2  	Servizio "**correzione delle vulnerabilità":** cliccando su ACCEDI è possibile accedere alle opzioni disponibili nella presente sezione.

	Cliccando su **INIZIA CHAT** è possibile analizzare, con il supporto di un esperto, i risultati ottenuti dall'analisi della vulnerabilità della connessione e risolvere eventuali criticità emerse.
Applicazione Anti-Ransomware 3 	Servizio "**applicazione anti-ransomware":** cliccando su **ACCEDI** è possibile accedere alle opzioni disponibili nella presente sezione.
	Cliccando su MS Windows x64 il cliente può scaricare sul proprio device l'applicazione anti-ransomware. Cliccando su Richiedi licenza il cliente può richiedere eventualmente il numero di licenza al tecnico specializzato.
Sorveglianza digitale 4 	Servizio "**sorveglianza digitale":** cliccando su **ACCEDI** è possibile accedere alle opzioni disponibili nella presente sezione.
	Cliccando su Accedi il cliente può effettuare ricerche sul web relative a possibili furti di identità e generare report dedicati

	Cliccando sul tasto  è possibile parlare con un tecnico specializzato.
Suite di sicurezza informatica 5 	Servizio "**suite di sicurezza informatica":** cliccando su  è possibile accedere alle opzioni disponibili dalla presente sezione.
	Cliccando su il Cliente può scaricare sul proprio device l'applicazione di sicurezza (di seguito antivirus) effettuando il download dallo store (es. Apple Store). Cliccando su  il Cliente può richiedere il numero di licenza al tecnico specializzato per poter attivare l'applicazione di sicurezza installata sul proprio device. ⚠ In occasione della scadenza annuale dell'antivirus, 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 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.
Geolocalizzazione e controllo parentale 6  	Servizio "**Geolocalizzazione e controllo parentale":** cliccando su ACCEDI è possibile accedere alle opzioni disponibili nella presente sezione.
 	Cliccando su chat è possibile parlare con un tecnico specializzato. Cliccando su Accedi alla suite di Sicurezza Informatica il Cliente può accedere alla suite di sicurezza informatica e attivare specifiche funzionalità offerte dall'antivirus. 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.
Sezione C  	**Assistenza tecnologica** In questa sezione vengono illustrate le modalità (chat, e-mail o contatto telefonico) con le quali il Cliente può richiedere assistenza tecnica.

Chat 1 	Cliccando su  è possibile parlare con un esperto attraverso una chat dedicata.
E-mail 2 	Cliccando su  appare un pop-up mediante il quale è possibile inserire l'indirizzo e-mail per essere contattati dal team di esperti.
Contatto telefonico 3 	Cliccando su  appare un pop-up all'interno del quale è possibile trovare il numero di telefono da chiamare per ricevere assistenza dal team di esperti.
Sezione D 	**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.

Cliccando su queste sezioni, il Cliente può:

Profilo utente
modificare i propri dati personali

Richiesta urgente di Supporto
Richiedere supporto al team di esperti

Chiudi sessione
Chiudere la sessione

Manuale Servizi Lazarus

Tabella riassuntiva servizi offerti dalla Piattaforma 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 Control	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 sevizi offerti dalla Piattaforma di Lazarus prevedono:

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

Di seguito sono riportati nel dettaglio i singoli servizi offerti:

1) Home banking

Azioni preventive	Azioni di rimedio
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[1] sui dispositivi e, contemporaneamente, il servizio di sorveglianza digitale esamina automaticamente le informazioni del Cliente presenti in rete, nel Dark Web[2] e Deep Web[3] 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[4] 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.

[1] **Malware:** programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico;
[2] **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;
[3] **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;
[4] **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;
- 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[5] con relativa richiesta di riscatto, il team di esperti procede alla raccolta delle prove, verifica la veridicità della minaccia, avvia le azioni

[5] **Ransomware:** è un tipo di malware che limita l'accesso dei file che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione.

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 Control	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 Control 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.

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[6] 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.

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.

[6] **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.

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 DI LAZARUS

A seguito della sottoscrizione del prodotto Protezione Cyber di Helvetia Italia Assicurazioni S.p.A. riceverai, all'indirizzo e-mail fornito al momento della sottoscrizione, il link di accesso alla Piattaforma di Lazarus.

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

È necessario 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.

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

helvetia
La tua Assicurazione svizzera

Numero di telefono: **039 888 0025**

Indirizzo e-mail: **helpdesk@helvetia.cyberscp.it**

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