ULTIMATE SECUREBOX

DESCRIZIONE TECNICA DEI PRODOTTI E DEI SERVIZI

info@infosecbox.com
www.infosecbox.com

Sommario

1 Introduzione alla soluzione ULTIMATE SECUREBOX 3
2 Come funziona la soluzione ULTIMATE SECUREBOX 4
3 Funzionalità della soluzione ULTIMATE SECUREBOX 6
3.1 Analisi del traffico di rete 6
3.2 Honeypot 7
3.3 URL reputation 7
3.4 Vulnerability assessment interno ed esterno 8
3.5 Dark web Monitoring 9
3.6 Cyber Security Awareness 10
4 Descrizione dei servizi SOC H24 10
5 Come si attiva la soluzione ULTIMATE SECUREBOX 12
5.1 Modalità di Collegamento del dispositivo SECUREBOX 13
5.1.1 Configurazione In Line 13
5.1.2 Configurazione in Mirroring 13
5.1.3 Reti in Alta Affidabilità (High Availability – HA) 14
5.1.4 Configurazione di dispositivi multipli 14
5.1.5 Altre tipologie di configurazione 14
5.2 On-boarding 14
5.2.1 IP Statici / Dinamici 15
5.2.2 Utilizzo di VLAN 15
6 Servizio di manutenzione del Dispositivo SECUREBOX 16
7 Tempi di delivery 17

1 Introduzione alla soluzione ULTIMATE SECUREBOX

ULTIMATE SECUREBOX è la soluzione di Cybersecurity sviluppata e distribuita da Infosecbox per portare alle micro e piccole realtà una protezione completa, integrata, efficace e semplice da gestire.

Le soluzioni presentate sinora sul mercato si esauriscono nell'acquisto di singoli prodotti, che vanno a coprire solo ambiti settoriali di protezione, resi spesso inefficaci da mancanza di manutenzione e soggetti ad obsolescenza. ULTIMATE SECUREBOX si pone al contrario come una soluzione viva e dinamica, costantemente monitorata e gestita da un Security Operation Center (SOC) operativo H24.

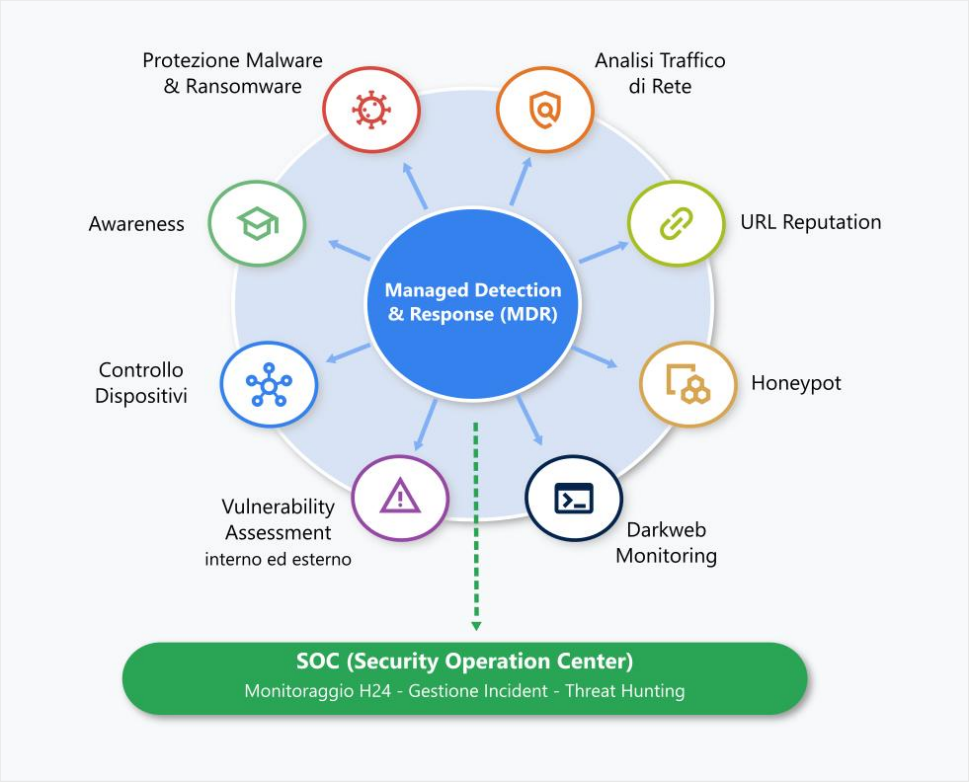

Figura 1 – Soluzione ULTIMATE SECUREBOX

La soluzione nel suo complesso, oltre a consentire di difendersi dal furto dei dati riducendo al minimo i rischi legati a comportamenti non sicuri, offre protezione contro malware, ransomware ed attacchi avanzati (anche effettuati con IA).,. Grazie alla soluzione ULTIMATE SECUREBOX l'organizzazione non rimane mai sola a fronteggiare le minacce informatiche: ogni situazione rilevata viene analizzata in tempo reale da piattaforme informatiche innovative, coadiuvate da esperti di sicurezza qualificati.

ULTIMATE SECUREBOX è una soluzione di sicurezza che integra una serie di funzionalità e di servizi di sicurezza indispensabili in un unico ecosistema, che si pone come una piattaforma completa, capace di organizzare e presidiare la sicurezza del cliente in modo organico e

continuativo, garantendo copertura su tutte le aree di rischio. Questa caratteristica porta con sé una serie di vantaggi, tra cui:

1. **Copertura completa delle aree di rischio**

   Ogni servizio affronta un aspetto specifico della sicurezza:
   - SERVIZIO MDR → protezione H24 contro le minacce informatiche,
   - HONEYPOT → intercettazione attaccanti attivi,
   - VULNERABILITY ASSESSMENT → vulnerabilità presenti nell'infrastruttura,
   - DARK WEB MONITORING → esposizione di credenziali e dati sensibili,
   - SECURITY AWARENESS → fattore umano.

2. **Riduzione della complessità gestionale**

   Il cliente non si trova più a coordinare strumenti diversi, con dashboard separate e dati frammentati: un'unica soluzione semplifica la gestione, fornisce una visione centralizzata, favorisce le correlazioni e riduce il carico di lavoro relativo alle operazioni di sicurezza.

3. **Ottimizzazione dei costi**

   Un'unica piattaforma integrata è in grado di ridurre costi di licenze, formazione e gestione, migliorando al contempo la qualità e l'efficacia dei servizi.

2 Come funziona la soluzione ULTIMATE SECUREBOX

L'architettura su cui si basa la soluzione ULTIMATE SECUREBOX, le funzionalità integrate ed i servizi correlati, sono uno sviluppo proprietario della società Infosecbox.

La soluzione consiste in un dispositivo fisico installato presso l'infrastruttura da proteggere, che lavora simultaneamente su diversi aspetti della cybersecurity:

analizza il traffico di rete ed è in grado di individuare, segnalare e, ove possibile, bloccare tentativi di intrusione ed attività anomale; incorpora funzioni di URL reputation che permettono di impedire l'accesso a categorie web considerate a rischio;

integra tecnologie di Honeypot, che simulano asset sensibili e vengono utilizzati per identificare potenziali aggressori;

include servizi di Dark Web Monitoring, capaci di rilevare se dati o credenziali aziendali sono esposti nel Dark Web.

Si aggiungono le **attività di Vulnerability Assessment** sia sulla infrastruttura interna che sul perimetro esterno, strutturate per identificare e permettere di correggere le vulnerabilità prima che possano essere sfruttate dagli attaccanti e dai bot che setacciano il web.

Tutte queste funzionalità abilitano il servizio di Sicurezza Gestita (MDR) erogato dal **SOC** (Security Operation Center) operativo **H24** che monitora costantemente l'infrastruttura. Il SOC

è in grado di intercettare in qualunque momento se sta accadendo qualcosa di anomalo ed intervenire prontamente in modalità attiva, ove possibile, o attraverso segnalazioni chiare, semplici e puntuali, corredate da indicazioni per attuare la risposta corretta alla minaccia.

Tramite il Portale Servizi, è reso disponibile anche un programma completo di Security Awareness, volto a sensibilizzare e formare gli utenti sulle buone pratiche di sicurezza informatica.

La soluzione ULTIMATE SECUREBOX non offre quindi solo strumenti, ma un ecosistema di sicurezza interconnesso, che organizza la difesa dell'azienda in modo organico, proattivo e continuativo.

A livello logico, il funzionamento della soluzione e la comunicazione con il SOC possono essere schematizzati come segue:

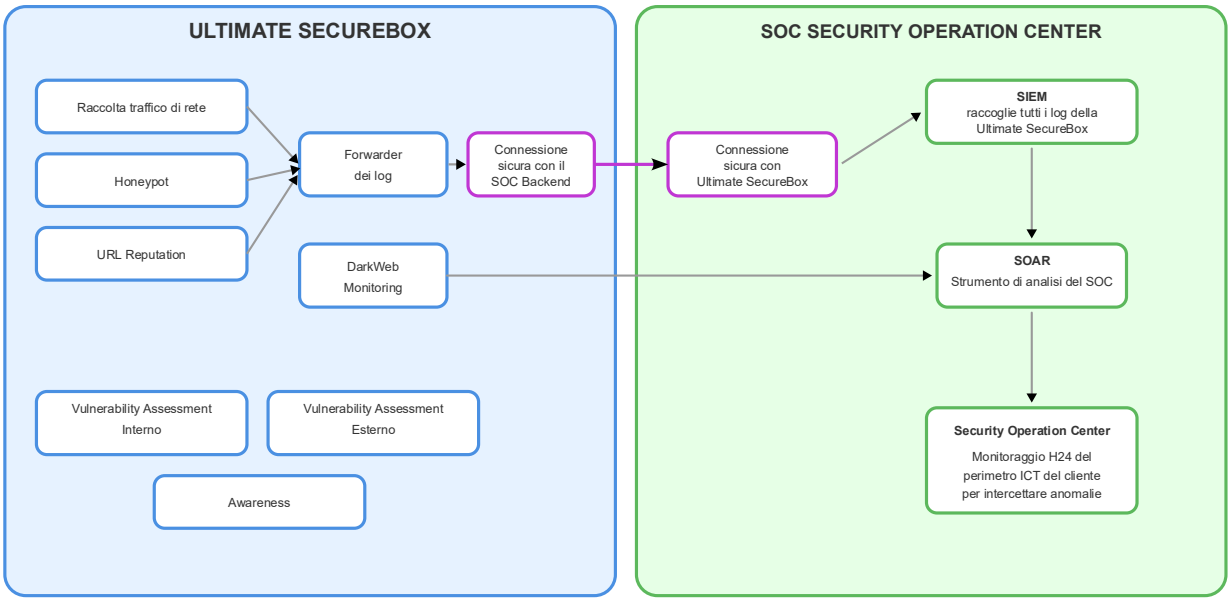

Figura 2 – Architettura di alto livello

All'interno del Portale Servizi di ULTIMATE SECUREBOX, accessibile dal rivenditore e dal cliente, sono mostrate tutte le informazioni relative a tutti i moduli / servizi disponibili e attivati. Per ognuno di questi vengono mostrate a video KPI, grafici, informazioni utili e suggerimenti di remediation per migliorare la Security Posture dell'azienda. Per alcuni moduli è stata anche prevista la possibilità di eseguire facilmente e velocemente il download di report (per esempio per l'estrazione di statistiche o per presentare agevolmente delle informazioni al Management e ad eventuali auditor).

Nei paragrafi di seguito vengono presentati nel dettaglio i servizi offerti ed integrati nella soluzione ULTIMATE SECUREBOX.

Importante: qualora siano presenti conflitti o ridondanze con servizi preesistenti è possibile disattivare i servizi della soluzione ULTIMATE SECUREBOX che sono in sovrapposizione.

3 Funzionalità della soluzione ULTIMATE SECUREBOX

Il dispositivo di ULTIMATE SECUREBOX viene istallato on-site ed esso opera direttamente all'interno dell'infrastruttura da proteggere. Svolge le funzionalità di Cyber Security abilitate, crea una connessione VPN sicura tra l'infrastruttura del cliente ed il back-end del SOC, trasmettendo i log raccolti ed i risultati delle analisi svolte in loco.

3.1 Analisi del traffico di rete

Il dispositivo ULTIMATE SECUREBOX, grazie al modulo di analisi del traffico di rete, è in grado di rilevare attacchi informatici sulla stessa. Questo modulo si basa sul monitoraggio continuo dei dati grezzi di rete (log, pacchetti, flussi) necessario per poter avere visibilità sugli eventi di sicurezza ed è in grado di riconoscere attacchi informatici, comportamenti ed eventi malevoli.

Per poter identificare elementi o attività sospette è stato integrato all'interno della soluzione una componente IDS (Intrusion Detection System), ovvero un sistema di rilevamento delle intrusioni. Grazie a questa componente, la soluzione ULTIMATE SECUREBOX monitora il traffico di rete e genera degli allarmi quando vengono rilevati comportamenti sospetti o malevoli. Nello specifico, i dati di rete raccolti dall'IDS vengono confrontati con regole, firme o modelli di comportamento definiti da specialisti di settore, al fine di identificare elementi sospetti secondo le tecniche di:

- **Signature-based**: confronta ciò che vede con un database di firme note di attacco (es. sequenze di byte tipiche di un exploit).
- **Anomaly-based**: costruisce un modello di "comportamento normale" e segnala deviazioni (es. un PC che improvvisamente invia migliaia di pacchetti verso l'esterno).
- **Heuristic / Behavioral**: combina euristiche e pattern sospetti (es. scansioni di porte, tentativi ripetuti di login falliti...).

In aggiunta, l'IDS integrato nella soluzione ULTIMATE SECUREBOX utilizza tecniche di Deep Packet Inspection (DPI), mediante il quale è in grado di scavare a fondo nei pacchetti di rete analizzandone anche il payload, ovvero il contenuto reale della comunicazione. Questo permette all'IDS di riconoscere applicazioni che utilizzano porte standard per mascherarsi, cercare firme di attacco all'interno del flusso di dati di rete (es. stringhe di exploit SQL injection), identificare anomalie nei protocolli (es. pacchetti malformati, tipici dei tentativi di exploit). Da questa configurazione ne derivano meno falsi positivi e una maggiore capacità di identificare attacchi sofisticati.

Una volta rilevata un'attività sospetta, il SOC è in grado di eseguire analisi approfondite per comprendere meglio la situazione e, laddove necessario, segnalare il contesto, in modo da attuare azioni di remediation e di contenimento.

3.2 Honeypot

All'interno della soluzione ULTIMATE SECUREBOX è stata integrata una componente Honeypot, ovvero un sistema progettato per ingannare eventuali attaccanti. Per questo motivo un Honeypot può essere definito un finto obiettivo, poiché è progettato proprio per sembrare un bersaglio interessante per un attaccante: può imitare un server, un'applicazione, un database, ma è in realtà un sistema fittizio che serve a:

- **Rilevare precocemente le intrusioni**:
  Funge da trappola per identificare attività sospette in corso all'interno della rete. Per fare ciò registra attentamente tutte le attività che avvengono al suo interno: questo include i tentativi di accesso e altre interazioni con il sistema stesso. Dato che si tratta di una trappola, qualsiasi interazione con l'Honeypot è indicativa di un possibile attacco in corso.

- **Ritardare o distrarre gli attaccanti**:
  Spinge un threat actor (attore della minaccia) a perdere tempo su un obiettivo fasullo, proteggendo così i sistemi realmente sensibili.

- **Fornire informazioni preziose**:
  Gli Honeypot forniscono preziose informazioni per l'identificazione degli attaccanti e sulle azioni di mitigazione da applicare. Inoltre, si ottengono informazioni anche sulle tattiche, tecniche e procedure (TTP) utilizzate degli attaccanti. Questi dati possono essere utilizzati per migliorare le difese e rafforzare la sicurezza complessiva. Analizzando le interazioni con l'Honeypot, infatti, gli analisti del SOC ottengono una comprensione più approfondita del comportamento degli attaccanti, consentendo una migliore preparazione contro minacce simili future, estendendo istantaneamente la conoscenza anche a tutti gli altri clienti di Infosecbox.

A seguito di una qualsiasi interazione con l'Honeypot, verrà generato un allarme di sicurezza che, grazie a questo modulo, verrà preso immediatamente in gestione dal SOC, eliminando ritardi e aumentando la capacità di reazione tempestiva. Questo rende possibile intervenire prima che l'attacco raggiunga i sistemi sensibili.

L'Honeypot è uno strumento prezioso e, secondo Infosecbox, fondamentale per la sicurezza informatica, in quanto fornisce un modo strategico per studiare, rilevare e mitigare minacce attraverso l'analisi e l'intercettazione attiva degli attacchi informatici.

3.3 URL Reputation

La URL Reputation o URL Filtering è una funzionalità di sicurezza che mira a controllare e limitare l'accesso degli utenti a determinati siti web, sulla base di regole predefinite. Nello specifico, quando un utente cerca di accedere ad un sito Internet, il sistema confronta l'indirizzo richiesto (URL) con un database di categorie e reputazioni. Se la URL è considerata sicura e appartiene ad una categoria consentita, la navigazione viene permessa. Se invece la URL rientra in una categoria rischiosa (ad esempio phishing, malware, pornografia, gioco

d'azzardo, social network ecc.) oppure ha una reputazione negativa, l'accesso viene bloccato o segnalato.

Gli obiettivi principali di questa funzionalità sono:

- **Protezione dalle minacce**: bloccare siti dannosi che distribuiscono malware, ransomware o phishing.
- **Riduzione del rischio umano**: evitare che gli utenti cadano in trappole digitali senza rendersene conto.
- **Conformità e policy aziendali**: impedire l'accesso a siti non pertinenti o in contrasto con le regole aziendali.

Il dispositivo ULTIMATE SECUREBOX integra questa funzionalità e, tramite servizi di Cyber Threat Intelligence, viene costantemente aggiornato con elenchi di URL dannose, così da limitare il più possibile la navigazione verso sorgenti pericolose. L'integrazione con i servizi di Threat Intelligence assicura la protezione più avanzata, in quanto le informazioni sulle minacce vengono costantemente aggiornate da fonti di tutto il mondo, consentendo una risposta rapida anche alle nuove minacce emergenti.

In sintesi, questi servizi sono fondamentali per mantenere un ambiente sicuro e proteggere da potenziali rischi per la sicurezza informatica.

3.4 Vulnerability Assessment interno ed esterno

Il servizio di Vulnerability Assessment (VA), gestito dagli analisti del SOC di Infosecbox, è uno dei valori aggiunti della soluzione ULTIMATE SECUREBOX. Il VA, infatti, permette di scoprire e sviluppare dei piani per correggere le vulnerabilità del cliente prima che esse possano venire sfruttate da attaccanti malevoli e bot automatici di scansione del web, riducendo così il rischio di compromissione. Il VA continuo è uno strumento essenziale, poiché le minacce evolvono nel tempo e nuove vulnerabilità possono emergere anche con il puntuale aggiornamento dei software e dei sistemi. Inoltre, questo servizio fornisce una visione chiara dello stato di sicurezza generale dell'ambiente informatico, consentendo agli amministratori di sistema e ai responsabili della sicurezza di prendere decisioni informate sulla protezione dei sistemi.

Il servizio di Vulnerability Assessment consiste in due moduli:

- **Vulnerability Assessment Interno**, eseguito tramite un agente installato nel dispositivo SECUREBOX
- **Vulnerability Assessment Esterno**, eseguito tramite un servizio esterno, posizionato nel web

Il Vulnerability Assessment interno ha l'obiettivo di analizzare i sistemi e i dispositivi presenti all'interno della rete aziendale, quindi dietro al firewall. In questo caso si va ad effettuare una scansione per identificare configurazioni deboli o errori di sicurezza. L'analisi si concentra su server, workstation, apparati di rete e applicazioni interne, verificando la presenza di

configurazioni errate o altri punti che potrebbero facilitare azioni malevole, quali un movimento laterale o un'escalation di privilegi. In sintesi, questo modulo serve a valutare il livello di sicurezza "dall'interno", per ridurre i rischi connessi a minacce interne o a compromissioni già avvenute.

Il Vulnerability Assessment esterno, invece, guarda la rete aziendale dall'esterno, come farebbe un attaccante o un bot automatico, simulando l'approccio di un attaccante che analizza le eventuali vulnerabilità nei servizi esposti del cliente su Internet. L'attenzione è rivolta ai domini dell'azienda, agli IP pubblici dell'azienda, a siti web, VPN, portali di posta elettronica esposti e, più in generale, a tutte quelle risorse che rappresentano la superficie di attacco visibile pubblicamente. L'obiettivo è individuare porte e servizi non necessari lasciati aperti, applicazioni web vulnerabili, certificati SSL non correttamente configurati o qualsiasi altra falla che possa consentire un accesso non autorizzato alla rete interna.

Combinando questi due moduli, ULTIMATE SECUREBOX offre al cliente una visione completa e realistica del proprio livello di esposizione: da un lato fotografa i rischi derivanti dall'esterno, ossia da Internet, e dall'altro quelli che possono manifestarsi all'interno della rete aziendale.

Per entrambi i moduli l'obiettivo è quello di avere un processo strutturato di identificazione, valutazione e mitigazione delle vulnerabilità presenti nell'infrastruttura. Le scansioni, con cadenza mensile automatica, identificano vulnerabilità che vengono poi classificate in base al loro livello di rischio e all'urgenza di mitigazione, consentendo agli operatori di sicurezza di concentrarsi sulle minacce più critiche, riducendo sensibilmente le opportunità di attacco e le capacità offensive di un potenziale aggressore.

È importante precisare che non si tratta di un'attività puntuale *una tantum*, ma di un processo continuo che tiene traccia delle nuove vulnerabilità che possono emergere nel tempo o aggiornamenti e modifiche infrastrutturali del cliente.

3.5 Dark web Monitoring

Il servizio di "Dark Web Monitoring" è stato progettato ed integrato in ULTIMATE SECUREBOX per aiutare le aziende ad identificare e reagire alla presenza di credenziali di accesso compromesse o rubate che vengono esposti o venduti nel dark web. I vantaggi associati a questo servizio sono:

- **Prevenzione di Danni**: Riduzione del rischio di danni finanziari e di reputazione limitando l'esposizione di dati sensibili.
- **Conformità Regolamentare**: Aiuta a mantenere la conformità con le normative sulla protezione dei dati vigenti notificando le violazioni in tempo utile.

Il monitoraggio inizia con l'identificazione dei domini aziendali del cliente come chiave per tracciare eventuali fughe di dati. Qualsiasi riferimento ai domini aziendali, ai suoi sottodomini o ad indirizzi e-mail associati viene segnalato per ulteriori indagini. Il servizio utilizza software avanzati che scandagliano il dark web, inclusi forum nascosti, mercati di beni illeciti, chat-rooms e altre piattaforme digitali, utilizzando anche algoritmi di machine learning per rilevare

pattern particolari di dati rubati correlati al cliente. Ciò include il riconoscimento di schemi nei dati trafugati e la loro origine presumibile. Nel momento in cui vengono identificate nel dark web informazioni che coinvolgono il dominio del cliente viene generato un report di sicurezza, che può essere analizzato dal cliente e dal suo partner tecnico per prendere i provvedimenti necessari.

I clienti ricevono l'evidenza di quanto raccolto nel Portale Servizi sopra citato (da cui è possibile accedere a tutti i servizi della soluzione ULTIMATE SECUREBOX), che mostrerà in modo semplice la natura delle informazioni trovate, la loro ubicazione nel dark web e le raccomandazioni per mitigare eventuali danni.

Utilizzando il servizio di Dark Web Monitoring, le aziende possono adottare un approccio proattivo nella protezione delle loro informazioni sensibili, anticipando le possibili minacce prima che possano esercitare un impatto significativo sull'organizzazione. Questo tipo di servizio è essenziale per le aziende che desiderano mantenere un alto livello di sicurezza informatica e gestire efficacemente i rischi legati alla presenza di dati aziendali nel dark web.

3.6 Cyber Security Awareness

Il servizio di "Cyber Security Awareness" integrato nella soluzione ULTIMATE SECUREBOX consiste in una piattaforma online dedicata all'educazione e alla formazione continua del personale in materia di sicurezza informatica. Attraverso questo servizio i Clienti possono registrare autonomamente i propri collaboratori e i propri utenti sulla piattaforma, che avranno accesso a brevi lezioni mensili con alcune domande di verifica finali. Ogni lezione, della durata di pochi minuti, copre argomenti cruciali come il phishing, il social engineering, la gestione sicura delle password e altre tematiche pertinenti alla sicurezza delle informazioni, come l'utilizzo ed i rischi associati alle soluzioni di Intelligenza Artificiale.

L'importanza di investire in questi corsi di formazione è molteplice. Innanzitutto, aumenta la consapevolezza e la preparazione degli utenti nel riconoscere e gestire minacce informatiche quotidiane, riducendo significativamente il rischio di incidenti di sicurezza che possono portare a perdite economiche e danni alla reputazione. Inoltre, molte normative relative alla sicurezza informatica ed alla protezione dei dati (es. GDPR, NIS2, etc.), richiedono che le aziende adottino misure adeguate, atte a garantire la sicurezza delle informazioni. Questo include l'obbligo di formare il personale sull'importanza della sicurezza dei dati e sulle pratiche appropriate per proteggerli. Attraverso questa formazione, le aziende non solo migliorano la loro compliance con tali normative, ma instaurano anche una cultura della sicurezza più robusta all'interno della loro organizzazione.

4 Descrizione dei servizi SOC H24

Il servizio MDR (Managed Detection & Response) erogato dal SOC attivo H24 è il cuore dell'offerta ed il valore aggiunto peculiare della soluzione ULTIMATE SECUREBOX; prevede il

monitoraggio costante dell'infrastruttura, la notifica di eventi di sicurezza e, ove possibile, la risposta in modalità attiva.

Questo servizio è reso disponibile grazie all'utilizzo di una piattaforma appositamente realizzata e basata su uno stack tecnologico innovativo:

- **Correlazione delle informazioni** dei vari moduli presenti all'interno della soluzione ULTIMATE SECUREBOX per analisi di dettaglio e una più accurata visione sull'infrastruttura del cliente e sulla sua postura di sicurezza in generale.
- **Framework proprietario di Infosecbox**, in grado di generare allarmi relativi alle telemetrie dei sistemi/tecnologie del cliente in perimetro.
- **SIEM** per il collezionamento e la gestione dei log provenienti dalla ULTIMATE SECUREBOX.
- **SOAR** per l'orchestrazione e la gestione degli incidenti.

Per migliorare l'efficacia del servizio di protezione, vengono integrate, ad uso interno del team degli analisti SOC, delle automazioni su piattaforma SOAR, oltre ad di una serie di strumenti di Cyber Threat Intelligence e di Feed di Intelligence, atti a migliorare la detection e a rendere più efficace la fase di response.

La qualità del servizio erogato dal Security Operation Center è garantita e regolata dai seguenti SLA (Service Level Agreement):

PRIORITÀ	SLA	AZIONI	ESEMPI
Critical	2h	Notifica Risposta ove possibile	Sistema(i) critico(i) compromesso(i) con possibile esfiltrazione di dati.
High	4h	Notifica Risposta ove possibile	Asset molto probabilmente compromessi. Nessun sistema critico coinvolto.
Medium	8h	Notifica Risposta ove possibile	Nessun sistema critico compromesso.

Gli SLA sono da intendersi in termini di tempi di notifica, ovvero entro quanto tempo il cliente viene avvisato dopo l'individuazione di un incidente qualificato.

Tutti i servizi forniti dal SOC verranno erogati in modalità remota.

5 Come si attiva la soluzione ULTIMATE SECUREBOX

Il Dispositivo ULTIMATE SECUREBOX è stato concepito con caratteristiche “plug&play”, per semplificare il più possibile la fase di installazione. Per un corretto funzionamento della soluzione è importante che siano rispettati i seguenti requisiti tecnici:

- Il numero di utenti (posti di lavoro informatici) massimi consigliati è di circa 50 per la configurazione standard. Valori superiori sono supportati, ma richiedono un approfondimento tecnico con gli specialisti di Infosecbox al fine di effettuare una valutazione sui volumi di traffico di rete.
- La rete su cui è ospitato il dispositivo deve poter comunicare verso Internet.
- Il dispositivo deve avere visibilità su tutto il traffico di rete e gli apparati che si desidera mettere sotto protezione. Generalmente il dispositivo può essere posizionato tra il Firewall e lo Switch (vedi *Figura 3 – Configurazione default*), oppure sono da valutare le ulteriori opzioni di configurazione riportate sotto.
- Il dispositivo deve essere posizionato in un luogo adatto con la possibilità di avere la corretta aerazione.
- Il cablaggio deve essere effettuato con cavetteria idonea (min. cavi rete ethernet Cat.5E RJ45). In caso si utilizzino interfacce di rete non RJ45, sarà necessario dotarsi di un adattatore; in questa situazione è preferibile contattare il supporto di Infosecbox.

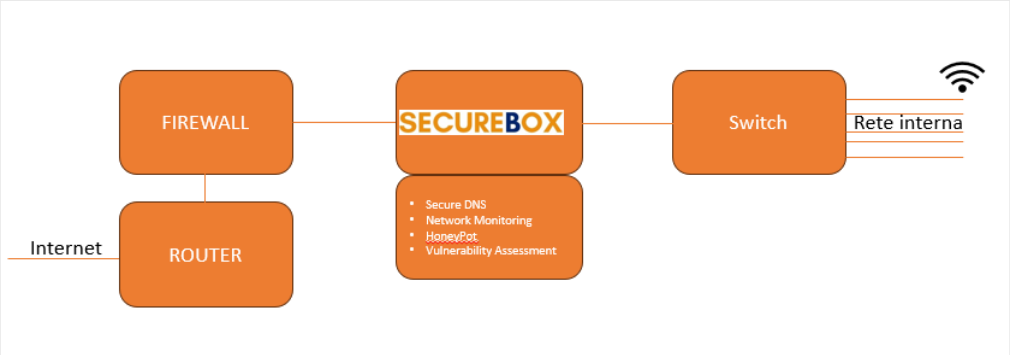

Figura 3 – Configurazione default

Assieme al dispositivo SECUREBOX viene fornita una brochure informativa con poche e chiare istruzioni che guidano passo-passo nel processo di installazione:

Figura 4 – Brochure Informativa

Il dispositivo verrà installato a cura del Rivenditore o dell'Utente Finale, con il supporto remoto fornito da Infosecbox, qualora necessario. Sarà onere del Rivenditore o dell'Utente Finale verificare la funzionalità delle apparecchiature nel tempo.

5.1 Modalità di Collegamento del dispositivo SECUREBOX

5.1.1 Configurazione In Line

La configurazione In-Line del dispositivo è ad oggi l'opzione di default. Come riportato nella brochure informativa, questa modalità di integrazione del dispositivo all'interno della rete del cliente prevede il suo inserimento tra il router/firewall di connettività Internet e lo switch interno.
Per l'attivazione dei servizi è quindi sufficiente collegare il cavo dal router/firewall verso il dispositivo, e dal dispositivo verso lo switch.

5.1.2 Configurazione in Mirroring

La configurazione in Mirroring prevede la disponibilità di uno switch di rete interno all'azienda in grado di configurare il traffico in modalità mirroring (TX + RX) su di una specifica porta.
La porta del dispositivo SECUREBOX con la label SWITCH dovrà essere collegata a questa porta.

La porta del dispositivo SECUREBOX con la label MGT dovrà essere collegata ad un'altra porta dello switch o altro dispositivo di rete con raggiungibilità verso Internet.

In questa modalità eventuali disservizi sul dispositivo SECUREBOX non comporteranno disservizi alla connettività dell'azienda.

5.1.3 Reti in Alta Affidabilità (High Availability – HA)

Per i clienti che hanno reti in HA, il dispositivo SECUREBOX deve essere configurato in modalità Mirroring. In questo caso il numero di dispositivi SECUREBOX dovrà coincidere con il numero di switch presenti nel nodo di alta affidabilità.

5.1.4 Configurazione di dispositivi multipli

La soluzione ULTIMATE SECUREBOX è pensata per essere scalabile e garantire i suoi servizi e la sua protezione anche ad aziende con reti complesse. In caso di segregazioni fisiche di rete, multiple sedi di lavoro, necessità di proteggere il traffico sulle reti backend, etc., è possibile configurare più di un dispositivo SECUREBOX all'interno dell'infrastruttura, seguendo le indicazioni di installazione riportate in questa sezione, 5.1, ed in quella di On-boarding, 5.2.

5.1.5 Altre tipologie di configurazione

In caso di reti complesse non incluse negli esempi descritti, o con particolari configurazioni, andrà eseguita un'analisi preventiva dell'infrastruttura e prevedere un intervento congiunto con i tecnici di Infosecbox per operare le corrette configurazioni, definire il posizionamento ideale del Dispositivo SECUREBOX e attivare le funzionalità compatibili con l'infrastruttura di rete del cliente.

5.2 On-boarding

L'attività di **on-boarding** di un nuovo cliente viene gestita in maniera centralizzata ed automatizzata attraverso il Portale Servizi accedendo le credenziali di accesso "Rivenditore".

Dal Portale Servizi si vanno a configurare in modo semplice e controllato tutti i parametri necessari alla gestione logistica, alla attivazione del Dispositivo e all'erogazione dei servizi.

Il flusso operativo prevede i seguenti macro-step:

1. Inserimento **anagrafica** del Cliente Finale.

   Registrazione dei dati identificativi e amministrativi del nuovo Cliente Finale.

2. Raccolta dei **parametri tecnici** per la corretta configurazione della Soluzione SECUREBOX e dei servizi connessi, comprendenti:

- Definizione della modalità di assegnazione della connettività di rete (indirizzo IP statico o dinamico, DHCP – vedi 5.2.1)
- Inserimento dei referenti tecnici del cliente per le comunicazioni operative

- Specifica dei domini da sottoporre a monitoraggio sul dark web
- Definizione di domini e indirizzi IP da sottoporre a Vulnerability Assessment esterno
- In caso di presenza di VLan nella rete del cliente fare riferimento al paragrafo 0

3. Gestione della **logistica** del dispositivo

Inserimento del numero di dispositivi richiesti e dell'indirizzo di spedizione per la consegna del Dispositivo SECUREBOX.

Al termine della fase di inserimento e validazione dei dati, la piattaforma attiva automaticamente il processo di back-end per la preparazione e la spedizione del dispositivo.

Tutte le fasi del processo – dalla configurazione iniziale fino alla consegna – risultano costantemente tracciabili e monitorabili dal Rivenditore tramite il Portale Servizi, che fornisce piena visibilità sullo stato di avanzamento.

Nel momento del corretto collegamento del dispositivo SECUREBOX, secondo le modalità desiderate, verrà inviata una mail automatica di conferma.

Tuttavia, saranno necessarie dalle 24 alle 48 ore per l'attivazione di tutti i servizi di sicurezza della Soluzione ULTIMATE SECUREBOX.

5.2.1 IP Statici / Dinamici

In caso in cui il cliente abbia una configurazione di rete basata su IP Statici, è necessario che un IP libero venga riservato per l'utilizzo del dispositivo SECUREBOX e che le informazion di rete (IP, Netmask, Default Gateway) vengano comunicate durante il processo di on-boarding. In questo modo il dispositivo SECUREBOX verrà configurato con le informazioni fornite prima della spedizione.

In assenza di una configurazione di rete basata su IP Statici, sarà sufficiente indicare nel portale la voce DHCP. Il dispositivo dovrà quindi ricevere l'assegnazione del proprio indirizzo IP secondo le specifiche del protocollo DHCP dalla rete del cliente.

5.2.2 Utilizzo di VLAN

Se la rete del cliente utilizza le VLAN, è necessario che vengano fornite in fase di On-boarding (sempre tramite il portale a disposizione) le informazioni relative alle subnet e tag VLAN utilizzate, in modo da configurare il dispositivo SECUREBOX per avere la corretta visibilità su tutti gli asset desiderati e per la connettività Internet.
Al fine di garantire il corretto funzionamento del modulo di Vulnerability Assessment interno è indispensabile che il cliente garantisca la corretta configurazione delle rotte di rete per assicurare la raggiungibilità di tutti i dispositivi che desidera avere in perimetro.

Importante: In caso di utilizzo di VLAN, configurazione in Mirroring e segregazione delle VLAN per la rete di management rispetto a quella del perimetro di monitoraggio, è necessario indicare subnet e tag VLAN per le due differenti porte del dispositivo SECUREBOX taggate come SWITCH e MTG. In questa situazione è necessario contattare il team tecnico di Infosecbox.

6 Servizio di manutenzione del Dispositivo SECUREBOX

Il dispositivo ULTIMATE SECUREBOX è coperto da un servizio di Manutenzione, erogato dalla società Infosecbox, valido per tutta la durata del contratto per la fornitura dei servizi di Cyber Security denominato ULTIMATE SECUREBOX.

Con tale servizio di Manutenzione Infosecbox si impegna, a seguito della denuncia di vizi e difetti del dispositivo SECUREBOX che venga effettuata nel termine di 8 giorni dalla consegna (oppure entro 8 giorni dalla relativa scoperta di vizi e difetti), a riparare o sostituire a propria cura e spese il dispositivo SECUREBOX che dovesse risultare difettoso o guasto.

A seguito della segnalazione sarà svolto un intervento remoto di analisi del dispositivo da parte di Infosecbox e/o dei suoi subappaltatori; nel caso si renda necessaria la sostituzione, sarà inviato un nuovo dispositivo SECUREBOX e sarà richiesta la restituzione di quello danneggiato.

Sono esclusi dalle garanzie rese con il servizio di Manutenzione i guasti ed i malfunzionamenti dovuti ad un improprio o cattivo utilizzo del dispositivo, come ad esempio:

- modifica e/o interventi sul dispositivo da parte di un terzo non abilitato da Infosecbox;
- danni provocati anche accidentalmente;
- atti dolosi, vandalici e/o di sabotaggio;
- atti di guerra, di insurrezione, di occupazione di fabbricati ed edifici in genere, di sequestri, di occupazione militare, di invasione, confisca; di contaminazione nucleare e/o biologica e/o chimica e/o radioattiva a seguito di atti terroristici di qualsiasi genere;
- esplosione o emanazione di calore o di radiazioni provenienti da trasmutazioni del nucleo dell'atomo, come pure causati da radiazioni provocate dall'accelerazione artificiale di particelle atomiche;
- fenomeni elettrici ed atmosferici (ad es. sovratensioni dovute a fulmini ovvero scariche sulla linea di alimentazione, nubifragi, incendi, devastazioni, inondazioni ed ogni altra calamità naturale, con esclusione di terremoti, maremoti ed eruzioni vulcaniche);
- furto del dispositivo SECUREBOX da parte di terzi;
- danneggiamento degli impianti da parte di animali.

Inoltre, non dovranno essere aggirate le limitazioni tecniche e le misure tecnologiche del dispositivo e del relativo software e l'utilizzo del dispositivo dovrà essere effettuato nella piena osservanza delle leggi, dei regolamenti, delle condizioni del contratto e delle disposizioni in genere concernenti la materia. La violazione di uno o più obblighi e/o divieti previsti nel presente articolo costituisce, ai fini del servizio di Manutenzione, grave inadempimento e Infosecbox avrà altresì la facoltà di sospendere l'esecuzione del servizio ULTIMATE SECUREBOX.

7 Tempi di delivery

Di seguito viene riportata la tabella con i Tempi di Delivery definiti per le attività descritte:

ATTIVITÀ	SLA	CONDIZIONI
Tempo di on-boarding un nuovo Utente Finale	immediato	a seguito della corretta compilazione delle informazioni richieste sul Portale Servizi del Rivenditore
Tempo Spedizione Dispositivo	5gg lavorativi	dalla corretta compilazione delle informazioni richieste sul Portale Servizi del Rivenditore
Tempo di attivazione servizio SOC	immediato	a seguito della corretta installazione del Dispositivo nell'infrastruttura dell'Utente Finale
Manutenzione: Tempo di presa in carico della verifica del malfunzionamento	1gg lavorativo	dalla segnalazione di malfunzionamento (effettuata dal cliente/partner o rilevata dalla soluzione in automatico)
Manutenzione: Tempo Spedizione Sostituzione	5gg lavorativi	dalla verifica dell'esito positivo del malfunzionamento e quindi necessità di sostituzione