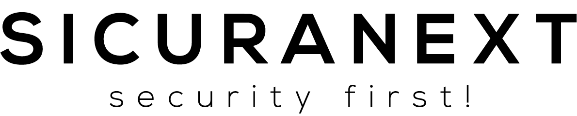


­

**MY SOC**

**New Generation Security Operations Center**

******Proposta Commerciale**

**Dati anagrafici delle parti**

**Fornitore**

|  |  |
| --- | --- |
| **Ragione Sociale** | SicuraNext S.r.l |
| **Indirizzo** | Corso Galileo Ferraris, 110, 10129 |
| **Località** | Torino |
| **Telefono** | 0121 213040 |

**Partner**

|  |  |
| --- | --- |
| **Ragione Sociale** | My Web Tech S.r.l |
| **Indirizzo** | Foro Buonaparte 59, 20121 |
| **Località** | Milano |
| **Telefono** | 02 82196637 |

**Cliente**

|  |  |
| --- | --- |
| **Ragione Sociale** |  |
| **Indirizzo** |  |
| **Località** |  |
| **Telefono** |  |

# 

# **Premessa**

Il documento rappresenta la proposta commerciale per l’erogazione di servizi da parte di SicuraNext (di seguito anche Fornitore) a favore di [NOME CLIENTE] (di seguito anche Cliente).

# **Servizi**

I servizi illustrati nella proposta sono “Octo Security” e “Octo Intelligence”, entrambi hanno lo scopo di incrementare il livello di sicurezza del CLIENTE rilevando, analizzando e bloccando preventivamente le minacce di natura informatica rivolte verso i sistemi interni ed esterni e i dati confidenziali del Cliente.

I servizi sono completamente gestiti dal FORNITORE per il CLIENTE, in formula 24/7/365.

# **Servizio Octo – Security**

## **Introduzione**

Il servizio si pone l’obiettivo di raccogliere dati ed eventi legati alla sicurezza di un sistema informatico e correlare tali dati per individuare potenziali minacce, vulnerabilità e usi non autorizzati sul sistema stesso.

Tale raccolta di informazioni avviene tramite l’installazione di un software proprietario definito “Agent”, che raccoglie costantemente dal dispositivo su cui è installato ogni tipo di informazione legata agli eventi di sicurezza dello stesso, e li invia al sistema centrale che li raccoglie, li cataloga e li analizza.

Oltre alla suddetta raccolta dati, il servizio utilizza le informazioni inerenti agli incidenti di sicurezza che accadono costantemente in tutto il mondo, recepite dalle più affidabili e aggiornate fonti di Cyber Threat Intelligence esistenti, per incrementare la capacità di rilevazione e precisione di correlazione degli eventi di sicurezza del Cliente.

La ricezione di queste informazioni, unite alle più moderne tecnologie di “Machine Learning”, permette alla soluzione di migliorare costantemente la propria capacità di rilevazione, iminuendo drasticamente la presenza di falsi positivi, riducendo considerevolmente il tempo di risposta degli analisti di SicuraNext.

Le informazioni raccolte saranno secretate e disponibili solo agli utenti e ai sistemi autorizzati alla gestione di queste.

Per garantire la massima affidabilità e resilienza, il servizio SOC è implementato in Cloud, ed utilizza una infrastruttura ridondata. Ciò ci permette di non avere interruzioni di servizio o malfunzionamenti del sistema di controllo del SOC e tutela ambo le parti da una possibile perdita di dati. *Le informazioni raccolte saranno secretate e disponibili solo agli utenti e ai sistemi autorizzati alla gestione di queste.*

Il servizio si suddivide nelle seguenti macro area:

* **Presa in carico**

Per la presa in carico si intendono tutte le attività necessarie condotte in fase di avvio del servizio per poter dare l'avvio alla progettualità nel suo completo. Le attività si suddividono in:

* + Vulnerability Assessment
  + Cyber Threat Analysis;
  + Audit & Gap Analysis;
  + Setup delle connessioni tra i sistemi del CLIENTE e la centrale operativa del SOC;
* **Servizi di Security Monitoring** - attività di monitoraggio e protezione del perimetro informatico interno ed esterno del Cliente condotto dagli analisti del Security Operation Center mediante l'utilizzo delle più avanzate tecnologie per la sicurezza difensiva e mediante l'uso di tecnologie proprietarie. Il servizio è erogato in forma H24.
* **Servizio di notifica** – Il SOC, tramite gli analisti, notificherà al cliente ogni minaccia o vulnerabilità rilevato dai sistemi di analisi al Cliente, mettendo a disposizione la conoscenza e le risorse per favorire una messa in sicurezza del perimetro informatico prima che la vulnerabilità possa essere utilizzata per compromettere l’infrastruttura del Cliente.

## **Presa in carico**

Per la ottimale presa in carico e attivazione del Servizio SOC è necessario condurre preliminarmente attività una tantum descritte in dettaglio nei capitoli successivi:

|  |
| --- |
| 1. Audit / Gap Analisys |
| 1. Vulnerability Assessment |
| 1. Cyber Threat Analysis |
| 1. Setup delle connessioni tra sistemi del CLIENTE e centrale operativa |
| 1. Installazione |

Le attività di analisi eseguite nella fase di presa in carico hanno lo scopo di fornire al Cliente e agli analisti di SicuraNext una osservazione puntuale dello stato di fatto e delle configurazioni relative all'implementazione dei presidi di sicurezza IT prima dell’avvio dei servizi.

Alla conclusione della fase di presa in carico verrà redatto da Sicuranext il Verbale di Avvio del Servizio SOC contenente le informazioni primarie definite o ricevute durante l’attività di assesstment. Il verbale verrà discusso e firmato congiuntamente e diventerà parte integrante del contratto di servizio.

## **Real-Time Security Monitoring**

Conclusa la fase di presa in carico entra in esercizio il servizio di real-time security monitoring, organizzato con un gruppo di analisti e specialisti operanti su turni per garantire la copertura della finestra prevista dal contratto.

Il servizio ha lo scopo di rilevare eventuali minacce per i sistemi informativi del Cliente, agendo nel più breve tempo possibile, raccogliendo il massimo delle informazioni disponibili e fornendo contestualmente supporto per rispondere alle minacce.

Per svolgere l'attività il team del SOC esegue in modo continuativo per l'intera finestra oraria del servizio il monitoraggio real-time della sicurezza osservando e analizzando le informazioni raccolte dai sistemi integrati dal SOC all'interno del perimetro del Cliente.

A fronte di allarmi per la sicurezza dei sistemi informativi gli analisti prendono in carico la segnalazione e la processano contestualizzandola in funzione delle caratteristiche dell’ambiente del Cliente, in funzione degli altri dati raccolti (correlazione) e di dati storici relativi ad eventi simili registrati nell'ambiente del Cliente o in contesti esterni tramite un sistema di mappatura degli attacchi informatici già eseguiti in tutto il mondo fino ad oggi.

Le fasi operative si possono sintetizzare come segue:

|  |
| --- |
| Ricezione segnalazione: il SOC invia una segnalazione di una potenziale minaccia afferente alla realtà del Cliente. É possibile attivare il processo di ricezione anche da parte del Cliente mediante segnalazione. |
| Triage: In questa fase l’analista valorizza la segnalazione ricevuta dalla suite allo scopo di identificare se questa rappresenta in effetti un incidente di sicurezza o un falso positivo. |
| Identificazione della mitigazione: Il SOC a seguito del triage avvia le valutazioni per la scelta delle azioni utili per mitigare l’incidente. |
| Apertura Ticket: Comunicazione al Cliente dell’apertura di un ticket e presa in carico della segnalazione |
| Gestione Ticket: Identificazione dell’attività di mitigazione e comunicazione al Cliente. |
| Chiusura Ticket: A fronte della ricezione da parte del Cliente dell’avvenuta applicazione delle attività mitigative suggerite, il SOC raccoglierà tutte le informazioni in merito all’evento e procederà alla chiusura del ticket. |

## **Report di servizio**

Nel contesto dei servizi SOC sono prodotti periodicamente i seguenti report:

* Report riepilogativo del servizio con cadenza trimestrale contenente:
  + sintesi degli incidenti di sicurezza gestiti;
  + elenco dei ticket gestiti;
  + cruscotto executive, con i primari indicatori quantitativi e qualitativi del servizio.

# **Servizio Octo – Intelligence**

## **Introduzione**

SicuraNext mette a disposizione del Cliente un servizio di cyber intelligence attivo che consiste nella raccolta e nell’analisi di dati provenienti dal deep e dal dark, oltre che dalle principali fonti di Intelligence utilizzate dal SOC al fine di proteggere la postura di sicurezza del Cliente e fornire una visione esterna delle minacce cyber che insistono sulla realtà del Cliente stesso.

Nello specifico le macro attività comprese nel servizio sono le seguenti:

* + Brand Reputation Monitoring;
  + VIP Monitoring;
  + Data Leakage Monitoring;
  + Notifica nuove minacce;
  + Controllo domini clone.

Le informazioni che raccolte permettono:

* L’Identificazione in *“near real time”* dei data breach a servizi non direttamente controllati dal CLIENTE che permettono accesso ad informazioni che riguardano il Cliente stesso, come ad esempio database compromessi con credenziali in chiaro, documenti, e informazioni riservate;
* Verifica presenza di domini clone, per evitare che vengano usati per frodare gli utenti utilizzando impropriamente l’immagine del Cliente;
* Verifica della reputazione degli IP del Cliente, per comprendere se stanno avvenendo operazioni malevole dagli stessi, causando l’inserimento dell’IP in una black-list globale comprometterebbe la reputazione del Cliente stesso;
* Monitoraggio della reputazione del Cliente;
* Verifica sui Social, sul Clear, Deep e Dark Web di tutto ciò in cui viene menzionato il Cliente, per trovare potenziali comunicazioni malevole che lo coinvolgano;
* Verifica di documenti legati al Cliente che sono esposti sulla rete involontariamente, a causa di errata configurazione di bucket S3

## **Attivazione del servizio**

Il Cliente verrà intervistato tramite documentazione apposita al fine di reperire le informazioni necessarie per effettuare l’attivazione del servizio.

|  |
| --- |
| * Identificazione domini |
| * Identificazione VIP aziendali |
| * Definizione perimetro asset oggetto del servizio |

## **Fase Operativa**

|  |
| --- |
| * Attività di OSINT su deep e dark web |
| * Identificazione Databreach |
| * Identificazione Domini malevoli |
| * Monitoraggio utenti VIP |
| * Notifica nuove minacce |
| * Apertura Ticket |
| * Identificazione e classificazione della minaccia |
| * Segnalazione al CLIENTE |
| * Proposta di attività mitigative per gestire l’incidente individuato |

## **Report di servizio**

Nel contesto dei servizi di Cyber Threat Intelligence sono prodotti periodicamente i seguenti report:

* Report riepilogativo del servizio con cadenza trimestrale contenente:
  + sintesi degli incidenti di sicurezza gestiti;
  + elenco dei ticket gestiti;
  + cruscotto executive, con i primari indicatori quantitativi e qualitativi del servizio.

# **Vocabolario**

| **Termine** | **Definizione** |
| --- | --- |
| SOC | Security Operations Center, inteso come servizio, luogo fisico e team di specialisti. |
| Operatore IT | Figura tecnica specializzata che opera all'interno dei reparti che gestiscono l'infrastruttura e i servizi IT dell'organizzazione. Può essere un dipendente, un consulente o un operatore di un outsourcer che l'organizzazione ha delegato per la gestione di un determinato insieme di servizi IT. |
| Utente interno | Dipendente o collaboratore dell'organizzazione che accede ai servizi IT accessibili all'interno della rete informatica dell'organizzazione stessa. |
| Utente esterno | Persona non appartenente all'organizzazione che accede a servizi IT dell'organizzazione esposti all'esterno della rete informatica. Possono essere consumatori finali, consulenti e professionisti esterni, clienti e fornitori dell'organizzazione. |
| IT Operation Incident  *o per brevità*  Incident | Se non accompagnato dalla parola Security, rappresenta un evento che non fa parte dell’operatività standard di un servizio e che causa, o può causare, un’interruzione o una riduzione della qualità di tale servizio per motivi non dipendenti da attacchi informatici. Alcune cause di questa tipologia di indicenti sono: guasto tecnico, bug nel software, saturazione di risorse di calcolo o di spazio, ecc. |
| Cyber Security Incident  *o per brevità*  Security Incident | Evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza ICT causando un danno per gli asset ICT ovvero per il patrimonio informativo dell’organizzazione e per il quale si rende necessaria l’applicazione di misure di contrasto e/o contenimento da parte delle strutture preposte. |

# **OFFERTA ECONOMICA**

Riportiamo di seguito il dettaglio dell’offerta economica per la realizzazione della soluzione descritta, i prezzi riportati sono senza IVA**.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OPZIONE – OCTO SECURITY - SOC | | | | |
| Descrizione Servizio | Range Host | Costo Attivazione | Canone Mensile | Canone Annuo |
| OCTO SECURITY - SOC |  |  |  |  |
| Sconto multi-pacchetto |  |  | | |
| TOTALE | |  |  |  |
| SCONTO PARTNER | |  | | |
| TOTALE SCONTATO | |  | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OPZIONE – OCTO INTELLIGENCE - CTI | | | | | |
| Descrizione Servizio | Range Host | Numero VIP | Costo Attivazione | Canone Mensile | Canone Annuo |
| OCTO INTELLIGENCE - CTI |  |  |  |  |  |
| CTI – VIP EXTRA |  |  |  |  |  |
| Sconto multi-pacchetto |  |  |  | | |
| TOTALE | | |  |  |  |
| SCONTO PATNER | | |  | | |
| TOTALE SCONTATO | | |  | | |

|  |  |
| --- | --- |
| TOTALE |  |

Per il CLIENTE (Timbro e Firma)

Per PARTNER (Timbro e Firma)

# **CONDIZIONI COMMERCIALI DI VENDITA**

* I prezzi sono da intendersi iva esclusa;
* La modalità di fatturazione è trimestrale ed anticipata;
* La modalità di pagamento è tramite Ri.Ba 30 giorni a fine mese.
* La durata del contratto è di 3 anni.
* La validità della proposta è di 30 giornate lavorative

In caso di modifica del perimetro operativo l’eventuale adeguamento economico del Contratto di Servizio corrispondente sarà valutato di volta in volta.

Qualora l’infrastruttura IT del CLIENTE fosse vittima di un disastro, il servizio non comprende le eventuali attività tecnico-specialistiche atte a svolgere le attività di ripristino (recovery) necessarie.

Per PARTNER (Timbro e Firma)

Per il CLIENTE (Timbro e Firma)

**12**