mediatech
MEET NEXT TECHNOLOGY

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

Sesto S. Giovanni (MI), 11//02/2025 Nr. Prot.: RG_B11022025_2

Spett.le

Consiglio delle Autonomie Locali della Sardegna

Piazza Palazzo 2

09100 Cagliari (CA)

OGGETTO: Fornitura del servizio Cyber Security MDR Pro

Con riferimento ai colloqui intercorsi, sottoponiamo alla Vostra attenzione la nostra migliore offerta per la fornitura dei servizi di cui all'oggetto.

Restiamo a Vostra disposizione per qualsiasi ulteriore chiarimento e cogliamo l'occasione per inviarvi i nostri cordiali saluti.

Renato Gaudimonte
Mediatech s.r.l.
+39 3312485106
renato.gaudimonte@relatech.com

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

1 Introduzione

La presente proposta configura una soluzione di servizio che sarà erogata da nostro personale altamente specializzato

1.1 Scopo ed Obiettivo del Documento

L'obiettivo della presente offerta è definire gli aspetti tecnici ed economici relativi ad un servizio di Cyber Security erogato attraverso prodotti e servizi specializzati e dal nostro SOC, Security Operation Center, per Consiglio delle Autonomie Locali della Sardegna di seguito identificato come Cliente.

1.2 Presentazione divisione Cyber Security

Mediatech S.r.l. è una realtà che raggruppa competenze, esperienze ed eccellenze in ambito ICT. Nella divisione cyber security il focus sono le prestazioni centrate sui seguenti temi, strettamente legati all'esperienza ed alle competenze maturate:

- IT Strategy
- Information Security
- Risk & Compliance
- Enterprise Architecture IT
- Service Management

La missione di Mediatech S.r.l. è quella di aiutare le Aziende a governare, gestire e proteggere le proprie informazioni.

Le tipologie di intervento sono:

- Vulnerability Assessment
- Penetration Testing
- Ethical Hacking
- Cyber & Security Audit
- ICT Security Architecture
- Certified Cyber Security Training
- Cyber Security Defence
- Social Media and Domain reputation Assessment

Mediatech S.r.l. impronta la propria attività al rigoroso rispetto dei principi espressi nei codici etici internazionali di riferimento per il personale certificato.

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

1.3 Scenario di riferimento

In questi ultimi anni, si è creata una maggiore consapevolezza sui rischi sulla sicurezza delle informazioni aziendali. Ne consegue che la sicurezza delle informazioni è divenuta oggi una delle maggiori preoccupazioni per la maggior parte delle aziende (il 78% dei dirigenti aziendali si dichiara preoccupato per la sicurezza informatica).

Molte aziende stanno investendo ed aumentando la spesa per la sicurezza, spesso anche in modo significativo, ma nonostante questo maggiore sforzo, molti dirigenti aziendali hanno dubbi circa l'efficacia dei loro programmi di sicurezza delle informazioni o dei controlli di sicurezza che sono stati messi in atto.

La società nella quale viviamo sta vedendo un aumento esponenziale del cyber crime, si è passati dall'hacking come forma di sfida ideologica ad attività organizzate di stampo malavitoso. In questo contesto va rimarcato che la maggior parte di minacce alla sicurezza delle informazioni arrivano dall'interno, da dipendenti infedeli, da personale di terze parti che opera all'interno della banca (es: consulenti, progettisti, gestori di servizi vari), a presenze occasionali (es: visitatori).

Anche per questi motivi le autorità europee hanno emanato la Direttiva NIS 2 che prevede misure per un livello elevato di cybersicurezza in tutta l'UE. Questa nuova direttiva di legge intende migliorare la resilienza e le capacità di risposta agli incidenti attraverso misure di gestione del rischio e obblighi di segnalazione in evoluzione della direttiva NIS del 2016.

In questo contesto risulta necessario anche effettuare periodicamente dei controlli per verificare la presenza di vulnerabilità sfruttabili da un attaccante (esterno od interno) al fine di guadagnare accesso ad informazioni riservate. Le attività di Web Vulnerability Assessment, Penetration test e Social Media Assessment sono parte integrante di un processo di Risk Assessment. Fare una verifica del livello di sicurezza delle applicazioni web presenti sui propri siti web, consente di acquisire la consapevolezza di eventuali problematiche, e questo è condizione indispensabile per individuare ed implementare azioni e soluzioni correttive.

In particolare, devono essere presi in considerazione i tre aspetti fondamentali per la gestione della sicurezza delle informazioni/servizi informativi, che sono:

- Confidenzialità: solo gli utenti autorizzati possono accedere alle informazioni necessarie
- Integrità: protezione contro alterazioni o danneggiamenti
- Disponibilità: le informazioni devono sempre essere disponibili

I servizi di Vulnerability Assessment , Penetration Test e Social Media Assessment sono finalizzati alla valutazione del grado di sicurezza di reti, sistemi, applicazioni ed informazioni e possono essere effettuati anche per testare la sicurezza di ambienti Wireless e Voip. Le attività vengono svolte con strumenti automatici affiancate da attività mirate di tipo manuale in modalità Ethical Hacking.

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

1.4 CLIENTE – Esigenze Espresse

A seguito dei colloqui intercorsi recentemente si sono evidenziate le seguenti necessità:

1) Messa in sicurezza della struttura informatica fissa costituita da:
   - PC, Server fisici e virtuali on premis e cloud
   - apparati mobili, suddivisi fra telefoni cellulari e tablet

2 La proposta MDR (Managed Detection and Response)

2.1 Descrizione del servizio MDR

MDR (Managed Detection and Response) è un servizio gestito di sicurezza informatica attivo h.24x7 per proteggere l'infrastruttura aziendale dagli attacchi e incidenti informatici più recenti.

Prevede:

- monitoraggio continuo da parte degli operatori del Secutiry Operation Center sito in Via Galileo Galilei 67, Cinisello Balsamo (MI) che avvisano prontamente e collaborano con il cliente per fornire una risposta rapida ed accurata in caso di attacco
- rilevazione avanzata delle minacce «Zero-Day»
- risposta rapida alle violazioni e report periodici-tool di tecnologie sempre aggiornate e delle più avanzate, attentamente selezionate, che includono Intelligenza Artificiale e Machine Learning, per analizzare tutte le attività di rete e identificarne comportamenti anomali e minacce.
- messa in sicurezza dell'organizzazione aziendale dagli attacchi ed incidenti informatici (anche i più recenti e difficili da identificare)
- aggiornamento costante delle tecnologie e supporto di esperti/analisti per l'intervento rapido in caso di allarmi.
- costi predeterminati grazie ad un servizio gestito e all inclusive (con eventuale analisi forense)
- rispetto normative Privacy, sicurezza dei dati e NIS2

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

Il servizio MDR Pro (PC, server fisici e virtuali) include:

- Installazione di un motore EDR gestito dagli operatori del SOC.
- Servizi di correlazione con meccanismi di Ai e ML
- Introduzione di Honeypot e sonde di rete (NTA – Network Traffic Analyzer).
- Installazione di un motore XDR di ultima generazione gestito dagli operatori del SOC.

Il servizio MDR Advanced (apparati mobili) include:

- Installazione di un motore EDR gestito dagli operatori del SOC.
- Servizi di correlazione con meccanismi di Ai e ML
- Introduzione di Honeypot e sonde di rete (NTA – Network Traffic Analyzer).

Caratteristiche distintive e tecnologie

• Security Operation Center (SOC) certificato ISO27001

• Tecnologie più avanzate (AV, EDR, XDR, SIEM, SOAR)

• Competenze dei professionisti certificati del SOC attivo h24/7x7/365g che, grazie agli analisti di 1°,2° e 3° livello, è in grado di gestire minacce ed attacchi complessi.

• Constanti studi fatti dal reparto R&D della società, in collaborazione con varie Università Italiane. (tra cui l'Università della Calabria polo strategico in ambito Cyber Security)

• Viene messa a disposizione del cliente una console dedicata di visualizzazione intuitiva e comprensibile.

• Tra i partner tecnologici: Cynet, Rapid7, Barracuda Networks, Eset, Kaspersky e Stormshield.

• SLA Segnalazione entro 5 minuti dall'allarme; Intervento entro 20 minuti; Incident Response entro un'ora. (possibili SLA personalizzati)

• Utilizzo delle licenze in comodato d'uso per la durata contrattualizzata.

• Set up Verrà organizzato un Kick Off con il cliente da parte dello staff tecnico ReSoc per poi procedere con gli step d'installazione concordati con il cliente

Mediatech S.r.l.
P.iva e C.F. 03164980173
Sede Legale
Via Sofonisba Anguissola 23
Cap 20146 Milano
mnt.it
info@mnt.it
sdi-gif@pcert.it

mediatech
MEET NEXT TECHNOLOGY

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

Gli impegni del SOC

Il SOC è operativo 24h/24h x 365 gg l'anno

Lo staff di ReSoc monitorerà gli avvisi dall'installazione del cliente. Lo staff contatterà i punti di contatto del cliente tramite i canali di comunicazione approvati, in base alla matrice di severità degli avvisi di seguito indicata.

Lo staff sarà a disposizione del cliente per fornire le misure di risoluzione consigliate della minaccia rilevata

Severity	Response	Response Time
Critical	*Call and email the customer	Within 2 hours
High	*Call and email the customer	Within 4 hours
Medium	Email Customer	Within 12 hours
Low	Email Customer	Within 24 hours

*ReSoc contatterà il Cliente al telefono qualora determini che l'incidente di Sicurezza debba essere riportato al più presto al Cliente.

Mediatech S.r.l.
P.iva e C.F. 03164980173

Sede Legale
Via Sofonisba Anguissola 23
Cap 20146 Milano

mnt.it
info@mnt.it
sdi-gif@pcert.it

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

3 Condizioni economiche di fornitura

La tabella che segue riporta sinteticamente i servizi offerti e la relativa valorizzazione economica riservata a TIM Spa.

Tutti i valori indicati devono essere considerati al netto di IVA

3.1 Servizi Offerti

Codice Prodotto	Descrizione	Qtà	Canone annuale per end-point
			12M
MNT-MDRP-0050	ReSOC MDR pro Fascia 1-50	1	189,30 €

3.2 Termini e Modalità di fatturazione e pagamento

La fatturazione avverrà secondo le seguenti modalità:

- 100% alla consegna delle credenziali di accesso della Dashboard e attivazione del servizio di monitoraggio SOC
- Pagamento 30 giorni data fattura.

Mediatech S.r.l.
P.iva e C.F. 03164980173
Sede Legale
Via Sofonisba Anguissola 23
Cap 20146 Milano
mnt.it
info@mnt.it
sdi-gif@pcert.it

Sede di Milano
Viale Ercole Marelli, 165
20099 Sesto San Giovanni (MI)
+39 02.6738.2597
+39 02.6738.2596

Sede di Brescia
Via Roma 107/G
25040 - Corte Franca (BS)
+39 030.9807.51
+39 030.9828.342
+39 030.9884.137

3.3 Validità dell'offerta

L'offerta ha una validità 30 giorni

3.4 Vincoli e prerequisiti

Mediatech S.r.l. declina ogni responsabilità di tipo civile o penale derivante dalla non titolarità del Cliente sui sistemi da questi indicati come di propria competenza.

Mediatech S.r.l. declina ogni responsabilità di tipo civile o penale derivante da informazioni errate o non conformi alla realtà comunicate da Cliente a Mediatech S.r.l.

Per la corretta erogazione del servizio sarà necessario che Cliente identifichi una propria persona quale riferimento per i consulenti di Mediatech S.r.l. durante lo svolgimento delle attività.

3.5 Note di Confidenzialità

Dati gli argomenti trattati, il seguente documento è da considerarsi Confidenziale: nessuna parte di questo documento può essere comunicata a terzi, fotocopiata, riprodotta o tradotto in altra lingua senza il preventivo consenso scritto di Mediatech srl ed il CLIENTE.

4 Accettazione

Per Accettazione in tutte le sue parti:

1. Introduzione
2. Servizio SOC
3. Condizioni economiche

Data

_____

Il cliente

Mediatech S.r.l.
P.iva e C.F. 03164980173

Sede Legale
Via Sofonisba Anguissola 23
Cap 20146 Milano

mnt.it
info@mnt.it
sdi-gif@pcert.it