IBM Resilient Security Orchestration, Automation and Response on Cloud

Nella presente Descrizione dei Servizi viene illustrato il Servizio Cloud. I documenti d'ordine applicabili riportano prezzi e dettagli aggiuntivi sull'ordine del Cliente.

1. Servizio in Cloud

La piattaforma su Cloud IBM Resilient Security Orchestration, Automation, and Response (SOAR) consente alle organizzazioni di orchestrare ed automatizzare persone, processi e tecnologie associati alla risposta agli incidenti.

La piattaforma su Cloud IBM Resilient SOAR snellisce il processo di risposta agli incidenti e la gestione della risposta in ambito data privacy per consentire alle organizzazioni di reagire agli eventi ed agli incidenti in modo automatico, più veloce e più flessibile. La piattaforma su Cloud Resilient SOAR rappresenta una base per una solida sicurezza informatica che consenta alle organizzazioni di:

- creare piani di risposta in base agli standard e alle best practice di settore;
- Integrare più semplicemente i tool di sicurezza e IT ed organizzare delle risposte ad eventi ed incidenti.
- Collaborare in modo centralizzato in tutta l'organizzazione, fornendo ai diversi 'stakeholder' gli strumenti per adempiere ai compiti legati ai relativi ruoli ed attività, come parte dell'impegno di risposta agli incidenti.

La piattaforma IBM Resilient SOAR è progettata per organizzazioni di varie dimensioni e complessità e può essere acquistata con diversi componenti aggiuntivi opzionali. Il Cliente non è autorizzato ad utilizzare le funzionalità se non specificato nell'offerta o nel componente aggiuntivo acquistato.

1.1 Offerte

Il Cliente può selezionare le seguenti offerte disponibili:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration offre una base solida per la sicurezza informatica. I Clienti potranno creare piani di risposta basati su standard di settore e best practice, integrarsi facilmente con strumenti di sicurezza e IT e organizzare le risposte a eventi e incidenti. Il Servizio Cloud facilita la collaborazione in tutta l'organizzazione, consentendo ai diversi 'stakeholder' di assumere i relativi ruoli e compiti come parte dell'impegno di risposta agli incidenti.

I team di sicurezza possono collaborare su eventi e incidenti relativi alla sicurezza informatica, utilizzando le funzionalità di gestione dei casi appositamente sviluppate della piattaforma. I playbook dinamici si adattano agli attacchi, che sono sempre in rapida evoluzione, ed i team potranno interagire rapidamente con i processi per migliorarne l'efficacia attraverso la personalizzazione dei playbook, dei campi di dati e dei layout di visualizzazione. Le simulazioni aiutano ulteriormente a perfezionare i processi di risposta. Le integrazioni incorporate ed installabili assicurano l'arricchimento dei dati per consentire la raccolta del contesto per il processo decisionale di un team di sicurezza e permettere la gestione delle azioni di correzione, in base alla quantità di Azioni per Mese acquistate. L'inserimento e l'analisi delle e-mail rappresentano un metodo efficace per l'escalation da altri strumenti. L'accesso può essere protetto tramite l'autenticazione SAML. La trasparenza e l'analisi del rischio sono aiutati da dati analitici e dal reporting. La presente offerta è richiesta per tutti i seguenti componenti aggiuntivi.

1.2 Servizi Opzionali

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions abilita le funzioni di orchestrazione della piattaforma. Le integrazioni incorporate ed installabili, comprese le integrazioni con diversi feed di intelligence delle minacce, consentono la raccolta del contesto per il processo decisionale di un team di sicurezza e permettere la gestione delle azioni di correzione.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy consente ai Clienti di valutare e rispondere alle violazioni dei dati sulla privacy. I piani di risposta generati da questa offerta si adattano ai tipi di dati, alle quantità di record ed alle giurisdizioni normative applicabili. I Clienti possono inoltre consultare una base di conoscenze di normative globali riguardanti le normative sulla notifica di violazioni della tutela dei dati personali che contribuisce a personalizzare ulteriormente i propri piani di risposta agli incidenti.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams consente la gestione degli utenti e l'isolamento dei dati tra più team. Le informazioni sensibili vengono gestite in base all'esigenza di accesso, limitando così la consultazione con spazi di lavoro ed un controllo degli accessi basato sui ruoli e personalizzabile. La gestione di utenti e gruppi può essere semplificata utilizzando Active Directory per l'autorizzazione dell'utente. È inoltre possibile configurare i gruppi in modo che ciascuno abbia la propria Organizzazione.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP fornisce funzionalità di gestione dei casi, dei processi, della personalizzazione e dei playbook tra diverse Organizzazioni. Gli eventi e gli incidenti provenienti da diverse Organizzazioni possono essere visualizzati in un'unica coda, fornendo ai managed security service provider (MSSP) una visione completa dei propri clienti. I playbook con una configurazione basata sull'Organizzazione forniscono una gestione semplice dei processi standardizzati e personalizzati.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production è un'istanza separata della piattaforma IBM Resilient SOAR che il Cliente può utilizzare solo come parte delle attività di non produzione del Cliente, incluse, a titolo esemplificativo ma non esaustivo, attività di test, ottimizzazione delle prestazioni, diagnosi dell'errore, verifica delle prestazioni interne, definizione delle attività di 'quality assurance' e/o sviluppo interno di implementazioni addizionali o estensioni del Servizio Cloud, utilizzando le API pubblicate.

1.3 Servizi di accelerazione

Le offerte IBM Security Expert Labs (SEL) for Resilient Services sono servizi erogati a distanza che offrono l'assistenza di un esperto Resilient per la definizione dell'architettura e per l'implementazione della distribuzione Resilient. L'offerta IBM Resilient Security, Orchestration and Response, sotto forma di Servizio Cloud o software on-premise, rappresenta un prerequisito per tutti questi Servizi.

1.3.1 IBM SEL for Resilient Base Starter Service

Nel corso di un impegno della durata di 5 giorni, IBM fornirà:

- assistenza nella definizione dell'architettura di IBM Security Resilient;
- installazione & configurazione di IBM Security Resilient (ove applicabile);
- formazione per Analisti e Designer sulla configurare e sull'utilizzo degli attuali piani di Risposta agli Incidenti del Cliente, tenendo conto dei requisiti chiave delle organizzazioni del Cliente;
- Playbook configurati di IBM Security Resilient basati sui processi univoci delle organizzazioni del Cliente;
- istruzioni sul monitoraggio dei KPI e delle Metriche in base alle esigenze delle organizzazioni del Cliente ed alle migliori pratiche del settore; e
- individuare opportunità di integrazione per il supporto, l'automazione e l'orchestrazione del processo end-to-end.

1.3.2 IBM SEL for Resilient Premium Starter Service

Nel corso di un impegno della durata di 3 giorni, IBM provvederà a:

- assistere nella definizione dell'architettura di IBM Security Resilient;
- installare IBM Security Resilient (ove applicabile);
- configurare inizialmente IBM Security Resilient nell'ambiente del Cliente; e
- formare Analisti e Designer sulla configurare e sull'utilizzo degli attuali piani di Risposta agli Incidenti del Cliente, tenendo conto dei requisiti chiave delle organizzazioni del Cliente.

1.3.3 IBM SEL for Resilient Additional Day

In aggiunta al servizio Base o Premium Starter, in un impegno della durata di 1 giorno, IBM eseguirà qualsiasi attività correlata a IBM Security Resilient, concordata in anticipo. Ad esempio:

- ulteriore supporto per l'installazione o la configurazione di IBM Security Resilient o delle estensioni (ove applicabile);
- ulteriore formazione o supporto agli Analisti per garantire che IBM Security Resilient sia adeguato e possa rappresentare una soluzione SOAR chiave per il Cliente;
- guidare i Designer nella configurare e l'utilizzo dei propri 'Playbook' che riflettono i requisiti chiave delle organizzazioni dei clienti; o
- effettuare una rapida scansione dell'ambiente IBM Security Resilient per eventualmente suggerire potenziali aree di miglioramento.

2. Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)

Il Supplemento al Trattamento dei Dati Personali (DPA o Data Processing Addendum) di IBM, disponibile alla pagina web http://ibm.com/dpa e le Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Sheet o Appendice DPA) nei seguenti link forniscono ulteriori informazioni sulla protezione dei dati per i Servizi Cloud e per le opzioni relative ai tipi di Contenuto che potrebbe essere trattato, per le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Il DPA si applica ai dati personali presenti nel Contenuto, nella misura in cui si applichino i) il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation, EU/2016/679, GDPR); o ii) altre leggi sulla protezione dei dati riportate alla pagina http://www.ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

3. Livelli di Servizio e Supporto Tecnico

3.1 Service Level Agreement ("SLA")

IBM fornisce al Cliente il seguente Service Level Agreement ("SLA"). IBM applicherà il Rimborso più elevato applicabile sulla base della disponibilità cumulativa del Servizio Cloud raggiunta, come mostrato nella tabella seguente. La percentuale di disponibilità viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti di Inattività del Servizio nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. La definizione di Inattività del Servizio, il processo di reclamo e le modalità per contattare IBM in relazione ai problemi di disponibilità del servizio sono riportati nel manuale di supporto al Servizio Cloud di IBM all'indirizzo https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Inferiore al 99,9%	2%
Inferiore al 99,0%	5%
Inferiore al 95,0%	10%

* La quota di abbonamento rappresenta il prezzo contrattuale per il mese soggetto al reclamo.

3.2 Supporto tecnico

Il supporto tecnico per il Servizio Cloud, inclusi i dettagli di contatto di assistenza, i livelli di gravità, le ore di disponibilità del supporto, i tempi di risposta e altre informazioni e processi relativi al supporto, possono essere consultati selezionando il Servizio Cloud nella guida di supporto IBM disponibile alla pagina https://www.ibm.com/support/home/pages/support-guide/.

4. Corrispettivi

4.1 Calcolo dei Corrispettivi

Le metriche dei corrispettivi per il Servizio Cloud sono specificate nel Documento d'Ordine.

Al presente Servizio Cloud si applica il seguente calcolo dei corrispettivi:

- Un Utente Autorizzato è una persona specifica cui è stato fornito l'accesso ai Servizi Cloud in qualsiasi modo, direttamente o indirettamente (ad esempio, tramite un programma multiplexing, dispositivo o server applicativo) con qualsiasi mezzo.
- "Utente simultaneo" è un utente che accede simultaneamente al Servizio Cloud in qualsiasi modo, direttamente o indirettamente (ad esempio, tramite un programma multiplexing, un dispositivo o un server delle applicazioni) in qualsiasi momento specifico. Una persona che accede simultaneamente al Servizio Cloud più volte viene conteggiata solo come singolo Utente simultaneo.
- Per Impegno si intende un servizio professionale o di formazione correlato ai Servizi Cloud.
- Un Elemento è la ricorrenza di un elemento specifico che viene elaborato, gestito o che è relativo all'uso del Servizio Cloud. Per gli scopi di questo Servizio Cloud, un Elemento è considerato un'Azione. Un'azione è una richiesta di orchestrazione o automazione effettuata dal Servizio Cloud ad un altro programma software.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), stipulati prima del 1 gennaio 2019, si applicano le condizioni riportate alla pagina web https://www.ibm.com/acs.

5.1 Verifica

Il Cliente provvederà a i) mantenere e fornire su richiesta le registrazioni e l'output degli strumenti di sistema, come ragionevolmente richiesto da IBM e dai suoi revisori esterni, per verificare la conformità del Cliente alle condizioni del presente Accordo, e ii) richiedere tempestivamente a IBM, tramite un nuovo ordine, gli eventuali ulteriori diritti di utilizzo, pagare i corrispettivi aggiuntivi in base alle tariffe applicate da IBM al momento, assumendosi tutte le responsabilità determinate in seguito a tali controlli, come specificato da IBM nella fattura. Questi obblighi di verifica della conformità restano validi per la durata del Servizio Cloud e per i due anni successivi.

5.2 Requisiti di titolarità per gli Add-On

Il Cliente deve acquisire un numero ed un tipo uguale di titolarità sia per la base che per qualsiasi Servizio Cloud aggiuntivo.

5.3 Limitazioni sull'Utilizzo

Ciascun Cliente ha diritto ad effettuare un massimo di centomila (100.000) query al mese per il Servizio Minacce. Il Cliente crea una query per il Servizio Minacce aggiungendo una risorsa ad un incidente quando il proprio Servizio Minacce è stato attivato. Da quel momento in poi, se l'incidente rimane aperto e attivo, ogni due (2) giorni sarà generata automaticamente una nuova query del Servizio Minacce.

Ciascun Cliente ha diritto a generare un massimo di cento (100) email di notifica al giorno per ciascun Utente Autorizzato/Simultaneo. Le email di notifica vengono generate dalla piattaforma Resilient in base alla configurazione controllata dal Cliente.

5.4 Ulteriori informazioni su Elaborazione e Protezione dei Dati

A scanso di equivoci, IBM Resilient SOAR Platform on Cloud:

- non effettua la crittografia dei Contenuti a riposo;
- non è progettato per elaborare alcuna Categoria Particolare di Dati Personali; e
- non devono essere inseriti dati personali nei campi di testo libero se non richiesti.

È possibile trovare informazioni dettagliate sulla crittografia e sui tipi di Dati Personali trattati all'URL delle Specifiche Tecniche a cui si fa riferimento nell'Articolo 2 riportato in precedenza.

6. Condizioni derogative

6.1 Uso dei Dati

IBM non utilizzerà o divulgherà i risultati derivanti dall'utilizzo da parte del Cliente del Servizio Cloud che sono specifici del Contenuto del Cliente (Approfondimenti) o che altrimenti identifichino il Cliente. IBM tuttavia utilizzerà il Contenuto e altre informazioni derivanti dal Contenuto (ad eccezione degli Approfondimenti), come parte del Servizio Cloud, allo scopo di migliorare il Servizio Cloud. Allo scopo di migliorare il processo di rilevamento delle minacce e la conseguente protezione dalle stesse, IBM potrà decidere di condividere gli identificatori di minacce ed altre informazioni di sicurezza presenti nel Contenuto.

Accettato da:

_____

Firma e timbro del Cliente

Data: .....

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: "Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)", "Service Level Agreement ("SLA")".

Accettato da:

_____

Firma e timbro del Cliente

Data: .....