Conformità al regolamento generale sulla protezione dei dati in AWS

Dicembre 2020

Note

I clienti sono responsabili della valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS, che potrebbero essere soggette a modifiche senza preavviso e (c) non rappresenta alcun impegno o garanzia da parte di AWS e dai suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non è né parte né modifica di alcun accordo tra AWS e i suoi clienti.

Sommario

Sintesi

Questo documento fornisce informazioni su servizi e risorse che Amazon Web Services (AWS) offre ai suoi clienti, per aiutarli ad allinearsi con i requisiti del Regolamento generale sulla protezione dei dati (GDPR) che potrebbero applicarsi alle loro attività. Tra questi, la conformità agli standard di sicurezza IT, l'attestato C5 (Cloud Computing Compliance Controls Catalog) di AWS, il rispetto del Codice di Condotta del Cloud Infrastructure Services Providers in Europe (CISPE), controlli di accesso ai dati, strumenti di monitoraggio e logging, cifratura e gestione delle chiavi.

Panoramica del Regolamento generale sulla protezione dei dati

Il Regolamento generale sulla protezione dei dati (GDPR) è una legge europea sulla privacy[1] (Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016[2]), entrata in vigore il 25 maggio 2018. Il GDPR sostituisce la Direttiva europea sulla protezione dei dati (Direttiva 95/46/EC) e si prefigge l'obiettivo di armonizzare le leggi relative alla protezione dei dati in tutta l'Unione Europea (UE) con l'adozione di un'unica normativa vincolante in ciascuno Stato membro.

Il GDPR si applica a tutte le organizzazioni stabilite nell'UE e alle organizzazioni, stabilite o meno nell'UE, che trattano i dati personali di soggetti interessati che si trovano nell'UE in relazione all'offerta di beni o servizi rivolti a questi ultimi o in relazione al monitoraggio del comportamento all'interno dell'UE. Per dati personali si intende qualsiasi informazione relativa a una persona identificata o identificabile.

Modifiche che il GDPR introduce per le entità che operano nell'UE

Uno degli aspetti chiave del GDPR è la creazione di coerenza tra gli Stati membri dell'UE sulle modalità con le quali i dati personali possono essere trattati, utilizzati e scambiati in modo sicuro. Le aziende dovranno essere in grado di dimostrare su base continuativa la sicurezza cibernetica dei dati che trattano e la loro conformità al GDPR, implementando e riesaminando regolarmente le misure tecniche e organizzative, oltre a opportune policy di conformità applicabili al trattamento dei dati personali. In caso di violazione del GDPR, le autorità europee di controllo potranno emettere ammende fino a 20 milioni di euro o pari al 4% del fatturato annuo in tutto il mondo, se maggiore.

Preparazione di AWS per il GDPR

Gli esperti di conformità, protezione dei dati e sicurezza cibernetica AWS collaborano con clienti di tutto il mondo per rispondere alle loro domande e aiutarli a prepararsi all'esecuzione di carichi di lavoro nel cloud ai sensi del GDPR. Questi team si occupano anche di riesaminare la preparazione di AWS alla luce dei requisiti del GDPR.

> *Siamo in grado di confermare che tutti i servizi AWS possono essere utilizzati in conformità con il GDPR.*

Addendum sul trattamento dei dati (DPA) di AWS

AWS offre un Addendum sul trattamento dei dati conforme al GDPR (GDPR DPA). Il GDPR DPA di AWS è integrato nei Termini del servizio AWS e viene applicato automaticamente a tutti i clienti che, in tutto il mondo, lo necessitano per essere conformi al GDPR.

Il 16 luglio 2020 la Corte di giustizia dell'Unione europea (CGUE) ha emesso una sentenza relativa allo scudo UE-USA per la privacy e alle clausole contrattuali standard (CSC), note anche come "clausole modello". La CGUE ha stabilito che lo scudo UE-USA per la privacy non ha più validità per il trasferimento di dati personali dall'Unione Europea (UE) agli Stati Uniti (USA). Tuttavia, nella stessa sentenza, la CGUE ha confermato che le imprese possono continuare a utilizzare le CSC come meccanismo per il trasferimento dei dati al di fuori dell'UE.

A seguito di questa sentenza, i clienti e i partner AWS possono continuare a utilizzare AWS per trasferire i propri contenuti dall'Europa agli Stati Uniti e in altri paesi, in conformità alle leggi UE sulla protezione dei dati, incluso il Regolamento generale sulla protezione dei dati (GDPR). I clienti AWS possono fare affidamento sulle CSC incluse nell'Addendum sul trattamento dei dati (DPA) di AWS nel caso in cui scelgano di trasferire i propri dati al di fuori dell'Unione Europea in conformità con il GDPR. Man mano che il panorama normativo e legislativo si evolve, ci impegneremo per garantire che i nostri clienti e partner possano continuare a godere dei vantaggi di AWS ovunque operino. Per ulteriori informazioni, consulta le FAQ sullo scudo UE-USA per la privacy.

Il ruolo di AWS nell'ambito del GDPR

AWS agisce come titolare e come responsabile del trattamento di dati nell'ambito del GDPR.

Ai sensi dell'articolo 32, i titolari e i responsabili del trattamento sono tenuti a "[mettere in] atto misure tecniche e organizzative adeguate [...] tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche". Il GDPR comprende suggerimenti specifici sui tipi di azioni di sicurezza che possono essere richiesti, ad esempio:

- La pseudonimizzazione e la cifratura dei dati personali.
- La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

AWS come responsabile del trattamento di dati

Quando clienti e partner di AWS Partner Network (APN) utilizzano i servizi AWS per elaborare dati personali nei loro contenuti, AWS funge da responsabile del trattamento dei dati. I clienti e i partner APN possono utilizzare i controlli disponibili nei servizi AWS, inclusi i controlli di configurazione della sicurezza cibernetica, per la gestione delle informazioni personali. In questi casi, il cliente o partner APN può agire come titolare o responsabile del trattamento dei dati, mentre AWS agisce come responsabile principale o secondario del trattamento dei dati. L'Addendum di AWS sul trattamento dei dati conforme al GDPR (DPA) include gli impegni di AWS come responsabile del trattamento dei dati.

AWS come titolare del trattamento dei dati

AWS funge da titolare del trattamento dei dati quando raccoglie dati personali e ne determina gli obiettivi e la modalità di trattamento. Ad esempio, AWS agisce come titolare del trattamento dei dati quando elabora le informazioni dell'account per la registrazione, l'amministrazione, l'accesso ai servizi o le informazioni di contatto per l'account AWS in modo da fornire assistenza attraverso le attività di supporto clienti.

Modello di responsabilità condivisa della sicurezza cibernetica

La responsabilità in materia di sicurezza cibernetica e conformità è condivisa tra AWS e il cliente. Quando un cliente trasferisce sistemi informatici e dati nel cloud, le responsabilità di sicurezza cibernetica vengono condivise tra il cliente e il fornitore di servizi cloud. Quando un cliente passa ad AWS Cloud, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i servizi offerti all'interno di AWS Cloud. Per servizi astratti come Amazon S3 e Amazon DynamoDB, AWS è anche responsabile della sicurezza cibernetica del sistema operativo e della piattaforma.
I clienti e i partner APN, che agiscono in qualità di titolari o responsabili del trattamento, hanno la responsabilità su tutto ciò che inseriscono nel cloud o connettono al cloud. La suddivisione delle responsabilità è generalmente indicata come sicurezza cibernetica *del* cloud versus sicurezza cibernetica *nel* cloud. Il modello condiviso può aiutare a ridurre l'onere operativo a carico del cliente, fornendogli la flessibilità e il controllo necessari allo sviluppo delle infrastrutture all'interno di AWS Cloud. Per ulteriori informazioni, consulta il Modello di responsabilità condivisa AWS.

Il GDPR non modifica il modello di responsabilità condivisa di AWS, che continua ad essere rilevante per i clienti e i partner APN focalizzati sull'utilizzo dei servizi di cloud computing. Il modello di responsabilità condivisa è un approccio utile per illustrare le diverse responsabilità di AWS (in qualità di responsabile principale o secondario del trattamento dei dati) e dei clienti o partner APN (come titolari o responsabili del trattamento) nell'ambito del GDPR.

Framework rigorosi di conformità e standard di sicurezza cibernetica

Ai sensi del GDPR, può essere necessario includere nelle misure tecniche e organizzative appropriate "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento", nonché l'affidabilità dei processi di ripristino, test e di gestione generale del rischio.

Programma per la conformità di AWS

AWS mantiene costantemente uno standard elevato di sicurezza cibernetica e conformità in tutte le operazioni globali. La sicurezza è sempre stata la nostra massima priorità. AWS viene sottoposto a regolari audit di attestazione di terze parti indipendenti per garantire che le attività di controllo stiano operando come previsto. Più specificamente, AWS è sottoposto a audit in base a una varietà di framework di sicurezza cibernetica globali e regionali dipendenti dalla regione e dal settore. Attualmente, AWS partecipa a oltre 50 diversi programmi di audit.

I risultati di questi audit sono documentati dall'organismo di valutazione e resi disponibili per tutti i clienti AWS tramite AWS Artifact. AWS Artifact è un portale self-service gratuito per l'accesso on-demand ai report di conformità AWS. I nuovi report rilasciati vengono resi disponibili su AWS Artifact, consentendo ai clienti di monitorare costantemente la sicurezza cibernetica e la conformità di AWS con accesso immediato a nuovi report.

I clienti possono usufruire di certificazioni e accreditamenti riconosciuti a livello internazionale, che dimostrano la conformità a rigorosi standard internazionali, come ISO 27017 per la sicurezza cibernetica nel cloud, ISO 27018 per la privacy del cloud, SOC 1, SOC 2 e SOC 3, PCI DSS Livello 1 e altri. AWS aiuta inoltre i clienti a soddisfare gli standard di sicurezza cibernetica locali come il Common Cloud Computing Controls Catalogue (C5) di BSI, un'attestazione riconosciuta dal governo tedesco.

Per informazioni più dettagliate sui programmi di certificazione AWS, i report e le attestazioni di terze parti, consulta Programmi per la conformità di AWS. Per informazioni specifiche sul servizio, consulta Servizi AWS coperti dal programma di compliance.

Cloud Computing Compliance Controls Catalog

Il Cloud Computing Compliance Controls Catalog (C5) è uno schema tedesco di attestazione riconosciuto dal governo e introdotto in Germania dal Federal Office for Information Security (BSI). È stato creato per aiutare le organizzazioni a dimostrare la sicurezza cibernetica a livello operativo rispetto agli attacchi informatici comuni nell'ambito delle *Security Recommendations for Cloud Providers* del governo tedesco.

Le misure tecniche e organizzative della protezione dei dati e le misure per la sicurezza cibernetica delle informazioni si concentrano sulla sicurezza dei dati per garantire riservatezza, integrità e disponibilità. C5 definisce i requisiti di sicurezza cibernetica importanti anche per la protezione dei dati. L'attestazione C5 può essere utilizzata dai clienti AWS e dai rispettivi consulenti sulla conformità come risorsa per comprendere la gamma di servizi di assicurazione per la sicurezza IT offerti da AWS durante il trasferimento dei carichi di lavoro nel cloud. C5 aggiunge il livello di sicurezza IT definito a livello normativo equivalente allo standard IT-Grundschutz, con l'aggiunta di controlli specifici per il cloud.

C5 prevede controlli aggiuntivi che forniscono informazioni riguardo a dove risiedono i dati, al provisioning dei servizi, alla sede di giurisdizione di riferimento, a eventuali certificazioni esistenti, agli obblighi di non divulgazione delle informazioni e una descrizione completa del servizio. Utilizzando queste informazioni, i clienti possono valutare in che modo le normative legali (ad esempio quelle riguardanti la privacy dei dati), le proprie politiche o l'ambito delle minacce sono connessi all'utilizzo dei servizi di cloud computing.

Codice di condotta CISPE

Il GDPR permette l'adozione di alcuni codici di condotta per aiutare i titolari e i responsabili del trattamento dati a dimostrare la conformità alle norme vigenti. Uno di questi codici in attesa di approvazione ufficiale dalle autorità dell'UE per la protezione dei dati è il *Codice di condotta CISPE per i fornitori di servizi di infrastrutture cloud* (il *Codice*).[3] Il Codice di condotta CISPE aiuta i clienti del cloud a garantire che gli standard di protezione dei dati utilizzati dal fornitore di infrastrutture cloud siano appropriati alla protezione dei dati e in linea con il GDPR. Alcuni dei vantaggi del Codice:

- **Distribuzione delle responsabilità per ciascun aspetto della protezione dei dati:** il Codice spiega il ruolo del fornitore e del cliente del cloud nell'ambito del GDPR, in particolare per quanto riguarda i servizi di infrastrutture cloud.
- **Descrizione dei principi a cui i fornitori si devono attenere:** il Codice sviluppa i principi fondamentali del GDPR che individuano le attività che i fornitori devono svolgere e gli impegni che si devono assumere per dimostrare la propria conformità al GDPR e aiutare i clienti a garantirla a loro volta. I clienti possono sfruttare questi vantaggi concreti nelle loro strategie di conformità e protezione dei dati.
- **Disponibilità di informazioni relative alla sicurezza cibernetica, necessarie ad aiutare i clienti a raggiungere i loro goal di conformità:** il Codice richiede che i fornitori siano trasparenti in merito alle fasi intraprese per rispettare i loro impegni nell'ambito della sicurezza e della privacy. Alcune di tali fasi includono l'implementazione di strumenti per la protezione della privacy e della sicurezza cibernetica, notifiche in caso di violazione di dati, eliminazione di dati e trasparenza in caso di trattamento dei dati a un livello inferiore da parte di terze parti. Tutti questi impegni sono soggetti a verifica da parte di entità di controllo esterne e indipendenti. I clienti possono utilizzare queste informazioni per acquisire una conoscenza approfondita degli elevati livelli di sicurezza cibernetica forniti.

Per ulteriori informazioni, consulta il registro pubblico CISPE, che fornisce ai clienti AWS garanzie aggiuntive sul fatto che i loro dati vengano controllati in un ambiente sicuro e conforme alle norme durante l'utilizzo di AWS. La conformità di AWS al Codice si aggiunge alla lista di certificazioni e accreditamenti riconosciuti a livello internazionale che AWS ha ottenuto. Tra questi figurano: ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS Livello 1, ecc.

Controllo dell'accesso ai dati

L'articolo 25 del GDPR stabilisce che il titolare del trattamento "mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento." I seguenti meccanismi AWS per il controllo dell'accesso possono aiutare i clienti a soddisfare questo requisito, concedendo l'accesso alle risorse AWS e ai dati dei clienti esclusivamente alle applicazioni, agli amministratori e agli utenti autorizzati.

AWS Identity and Access Management

Al momento della creazione di un account AWS, a questo viene automaticamente associato un utente *root*. Tale account gode di accesso completo a tutti i servizi e risorse AWS disponibili per quell'account AWS. Invece di usare questo account per le attività di routine, è consigliabile utilizzarlo in una prima fase per creare ruoli e utenti aggiuntivi e per compiere attività amministrative per le quali sono necessari privilegi di root. AWS consiglia di applicare fin da subito il principio del privilegio minimo. Tale principio consiste nel definire diversi account di utenti e ruoli per diverse attività e nello specificare l'insieme minimo di permessi necessari per completare ciascuna attività. Tale approccio è un meccanismo che consente di applicare un concetto cardine del GDPR: introdurre processi per la protezione dei dati fin dalla progettazione (data protection by design). AWS Identity and Access Management (IAM) è un servizio web che è possibile usare per controllare in modo sicuro l'accesso alle tue risorse AWS.

Utenti e ruoli definiscono identità IAM con permessi specifici. Un utente autorizzato può assumere un ruolo IAM per eseguire attività specifiche. Le credenziali temporanee vengono create quando viene assunto il ruolo. Ad esempio, è possibile utilizzare i ruoli IAM per fornire in modo sicuro le applicazioni che vengono eseguite in Amazon Elastic Compute Cloud (Amazon EC2) con credenziali temporanee necessarie per accedere ad altre risorse AWS, come i bucket Amazon S3 e i database Amazon Relational Database Service (Amazon RDS) o Amazon DynamoDB. Allo stesso modo, i ruoli di esecuzione forniscono alle funzioni AWS Lambda le autorizzazioni necessarie per accedere ad altri servizi e risorse AWS, come Amazon CloudWatch Logs per il log streaming o la lettura di messaggi da Amazon Simple Queue Service (Amazon SQS). Quando si crea un ruolo, si aggiungono le policy per definire le autorizzazioni.

Per aiutare i clienti a monitorare le policy delle risorse e a identificare le risorse con accesso pubblico o tra più account non intenzionale, è possibile abilitare IAM Access Analyzer per generare risultati completi che identificano le risorse a cui è possibile accedere dall'esterno di un account AWS. IAM Access Analyzer valuta le policy delle risorse utilizzando la logica matematica e l'inferenza per determinare i possibili percorsi di accesso consentiti dalle policy. IAM Access Analyzer monitora costantemente le policy nuove o aggiornate e analizza le autorizzazioni concesse utilizzando le policy per i ruoli IAM, ma anche per le risorse di servizi come i bucket Amazon S3, le chiavi AWS Key Management Service (AWS KMS), le code di Amazon SQS e le funzioni Lambda.

Access Analyzer per S3 avvisa quando i bucket S3 sono configurati per consentire l'accesso a chiunque su Internet o ad altri account AWS, inclusi gli account AWS esterni alla tua organizzazione. Quando si esamina un bucket a rischio all'interno di Access Analyzer per S3, è possibile bloccare tutti gli accessi pubblici al bucket con un solo clic. AWS consiglia di bloccare tutti gli accessi ai bucket a meno che non si richieda l'accesso pubblico per supportare un caso d'uso specifico. Prima di bloccare tutti gli accessi pubblici, assicurati che le applicazioni continuino a funzionare correttamente senza accesso pubblico. Per maggiori informazioni, consulta Blocco dell'accesso pubblico di Amazon S3.

IAM fornisce inoltre le ultime informazioni consultate: ciò consente di identificare le autorizzazioni inutilizzate e rimuoverle dalle entità associate. Utilizzando le ultime informazioni consultate, è possibile perfezionare le policy e consentire l'accesso solo ai servizi e alle azioni necessari. Ciò aiuta ad aderire meglio alla migliore prassi sul privilegio minimo e ad applicarla nel modo migliore. È possibile visualizzare le ultime informazioni consultate per entità o policy esistenti all'interno di IAM o di un intero ambiente di organizzazioni AWS.

Token di accesso temporaneo attraverso AWS STS

AWS Security Token Service (AWS STS) consente di creare credenziali di sicurezza provvisorie e assegnarle a utenti fidati per permettere loro di accedere alle risorse AWS. Le credenziali di sicurezza provvisorie funzionano in modo quasi identico alle credenziali delle chiavi di accesso a lungo termine fornite agli utenti IAM, tranne per le seguenti differenze:

- Le credenziali di sicurezza provvisorie sono a breve termine. È possibile configurarne la durata di validità, a partire da 15 minuti fino a un massimo di 12 ore. Dopo la scadenza delle credenziali provvisorie, AWS non le riconosce più né consente alcun tipo di accesso dalle richieste API che le utilizzano.
- Le credenziali di sicurezza temporanee non vengono salvate insieme all'account dell'utente. Sono invece generate in maniera dinamica e fornite all'utente su richiesta. Una volta scadute le credenziali di sicurezza provvisorie, o prima che ciò avvenga, l'utente può richiederne di nuove, se ha i permessi per farlo.

Queste differenze fanno sì che le credenziali provvisorie presentino i seguenti vantaggi:

- Non occorre distribuire o allegare credenziali di sicurezza AWS a lungo termine con un'applicazione.
- Le credenziali provvisorie sono la base dei ruoli e della federazione delle identità. È possibile concedere agli utenti l'accesso alle tue risorse AWS definendo per loro un'identità AWS provvisoria.
- Le credenziali di sicurezza provvisorie hanno una validità limitata e personalizzabile. Pertanto, non è necessario ruotarle o revocarle in modo esplicito quando non sono più necessarie. Quando le credenziali di sicurezza provvisorie scadono, non possono essere riutilizzate. Il tempo massimo di validità per le credenziali è personalizzabile.

Multi-Factor Authentication

Per una maggiore sicurezza, è possibile aggiungere l'autenticazione a due fasi all'account AWS e agli utenti IAM. Una volta attivata la Multi-Factor Authentication (MFA), l'accesso alla Console di gestione AWS avviene dopo l'inserimento di user name e password (prima fase), insieme a un input per l'autenticazione da parte del tuo dispositivo MFA AWS (seconda fase). La MFA può essere impostata per l'account AWS e per i singoli utenti IAM creati nell'account. La MFA consente anche di controllare gli accessi ai servizi API di AWS.

Ad esempio, è possibile definire una policy che consente un accesso totale a tutte le operazioni che avvengono tramite API AWS all'interno di EC2, negando esplicitamente l'accesso per specifiche operazioni API (ad esempio `StopInstances` e `TerminateInstances`) se l'utente non ha eseguito l'accesso con la MFA.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
         "Sid": "AllowAllActionsForEC2",
         "Effect": "Allow",
         "Action": "ec2:*",
         "Resource": "*"
      },
      {
         "Sid": "DenyStopAndTerminateWhenMFAIsNotPResent",
         "Effect": "Deny",
         "Action": [
             "ec2:StopInstances",
             "ec2:TerminateInstances"
```

```
                ],
                "Resource": "*",
                "Conditions": {
                    "BoolIfExists":
{"aws:MultiFactorAuthPresent":false}
                }
            }
        }
}
```

Per aggiungere un ulteriore livello di sicurezza ai bucket S3, è possibile configurare la cancellazione MFA, che richiede un'autenticazione aggiuntiva per modificare lo stato di versioni multiple di un bucket ed eliminare definitivamente una versione dell'oggetto. La cancellazione MFA fornisce una protezione aggiuntiva nel caso in cui le credenziali di sicurezza siano compromesse.

Per utilizzare la cancellazione MFA, è possibile utilizzare un dispositivo MFA hardware o virtuale per generare un codice di autenticazione. Consulta la pagina Multi-factor Authentication per un elenco dei dispositivi MFA hardware o virtuali supportati

Accesso alle risorse AWS

Per implementare un accesso granulare a risorse AWS, è possibile assegnare autorizzazioni di grado differente a persone diverse per risorse diverse. Ad esempio, puoi consentire solo ad alcuni utenti l'accesso completo a EC2, S3, DynamoDB, Amazon Redshift e altri servizi AWS.

Altri utenti, invece, possono essere autorizzati ad accedere in modalità di sola lettura solo ad alcuni bucket Amazon S3, a gestire solo alcune istanze EC2 o ad accedere solo alle informazioni di fatturazione.

La seguente policy rappresenta un esempio di un metodo utilizzabile per permettere tutte le azioni su un bucket specifico di Amazon S3 e negare esplicitamente l'accesso a ogni servizio AWS che non sia Amazon S3.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
               "Effect": "Allow",
               "Action": "s3:*",
               "Resource": [
                    "arn:aws:s3:::bucket-name",
```

```
                    "arn:aws:s3:::bucket-name/*"
                ],
            },
            {
              "Effect": "Deny",
              "NotAction": "s3:*",
              "NotResource": [
                    "arn:aws:s3:::bucket-name",
                    "arn:aws:s3:::bucket-name/*"
                ]
             }
        ]
}
```

Le policy possono essere associate a un account utente o a un ruolo. Per altri esempi di policy IAM, consulta Esempi di policy basate su identità IAM.

Definizione dei limiti per l'accesso ai servizi regionali

In qualità di cliente, mantieni la responsabilità sui tuoi contenuti e scegli quali servizi AWS possono elaborarli, archiviarli e ospitarli. AWS non accede ai tuoi contenuti e non li utilizza per alcuno scopo senza il tuo consenso. In base al modello di responsabilità condivisa, puoi scegliere le regioni AWS in cui vengono archiviati i contenuti, consentendo di distribuire i servizi AWS dove preferisci, in base ai requisiti geografici specifici. Ad esempio, se vuoi assicurarti che i tuoi contenuti si trovino solo in Europa, puoi scegliere di distribuire i servizi AWS esclusivamente in una delle regioni AWS europee.

Le politiche IAM forniscono un meccanismo semplice per limitare l'accesso ai servizi in regioni specifiche. È possibile aggiungere una condizione globale (*aws:RequestedRegion*) alle policy IAM collegate alle entità IAM per applicare questa condizione a tutti i servizi AWS. Ad esempio, la policy seguente utilizza l'elemento `NotAction` con effect `Deny`, che nega esplicitamente l'accesso a tutte le azioni non elencate nella dichiarazione se l'area richiesta non è europea. Le azioni svolte nei servizi CloudFront, IAM, Amazon Route 53 e AWS Support non dovrebbero essere negate perché si tratta di servizi globali AWS comuni.

```
{
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Sid": "DenyAllOutsideRequestedRegions",
```

```
                "Effect": "Deny",
                "NotAction": [
                     "cloudfront:*",
                     "iam:*",
                     "route53:*",
                     "support:*"
                 ],
                 "Resource": "*",
                 "Condition": {
                    "StringNotLike": {
                        "aws:RequestedRegion": [
                              "eu-*"
                        ]
                    }
                 }
            }
        ]
}
```

Questa policy IAM di esempio può essere implementata anche come policy di controllo dei servizi (SCP) in organizzazioni AWS. Tale policy definisce i limiti di autorizzazione applicati a specifici account AWS o unità organizzative (UO) all'interno di un'organizzazione. Ciò consente di controllare l'accesso degli utenti ai servizi regionali in ambienti complessi con più account.

Esistono funzionalità di limitazione geografica per le regioni lanciate di recente. Le regioni introdotte dopo il 20 marzo 2019 sono disabilitate per impostazione predefinita. Queste regioni devono essere abilitate per poterle selezionare. Se una regione AWS è disabilitata per impostazione predefinita, è possibile utilizzare la Console di gestione di AWS per abilitarla e disabilitarla. Abilitare e disabilitare una regione AWS permette di verificare che gli utenti dell'account AWS possano accedere alle risorse di quella regione.[4]

Controllo accessi ad applicazioni web e applicazioni mobile

AWS offre un servizio per gestire l'accesso ai dati all'interno delle applicazioni dei clienti. Per aggiungere una funzione di controllo del login utente o dell'accesso a un'applicazione web e ad applicazioni mobile, è possibile usare Amazon Cognito. I pool di utenti di Amazon Cognito forniscono una directory utente sicura e in grado di ricalibrare le risorse per centinaia di milioni di utenti. Per proteggere l'identità degli utenti, è possibile aggiungere la multi-factor authentication (MFA) ai pool di utenti.

L'autenticazione adattiva sfrutta un modello basato sul rischio per prevedere quando potrebbe essere necessario inserire la seconda fase di autenticazione.

Con i pool di identità di Amazon Cognito (identità federate), puoi vedere chi ha effettuato l'accesso alle tue risorse e l'origine dell'accesso (app mobile o applicazione web). Queste informazioni possono essere utili per creare ruoli IAM e policy di sicurezza cibernetica che accordano e vietano l'accesso alle risorse a seconda del tipo di origine dell'accesso (da applicazioni mobile o applicazioni web) e a seconda del fornitore di identità.

Monitoraggio e logging

L'articolo 30 del GDPR afferma che "ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità". Questo articolo include anche dettagli su quali informazioni debbano essere registrate durante il controllo del trattamento di tutti i dati personali. Il titolare e il rappresentante del trattamento devono anche inviare tempestivamente notifiche in caso di incidenti di sicurezza cibernetica, quindi è fondamentale che questi siano tempestivamente rilevati. Per aiutare i clienti a garantire la conformità a tali obblighi, AWS offre i seguenti servizi relativi a monitoraggio e logging.

Gestione e configurazione di asset con AWS Config

AWS Config fornisce una visualizzazione dettagliata della configurazione di vari tipi di risorse AWS di un account AWS. Ciò include il modo in cui le risorse sono correlate tra loro e in cui sono state configurate in passato, al fine di permettere di evidenziare come questi due elementi cambiano nel tempo.

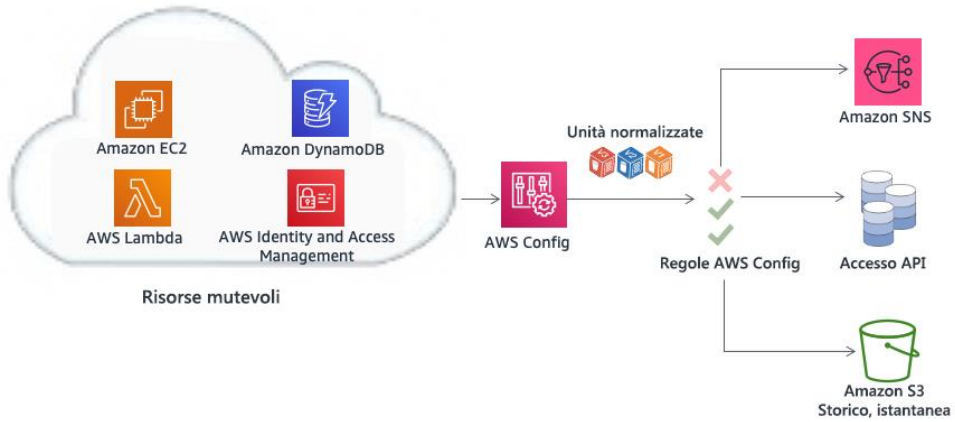

Figura 1: controllo dei cambiamenti della configurazione nel tempo con AWS Config

Per risorsa AWS si intende un'entità con la quale si può lavorare in AWS, ad esempio un'istanza EC2, un volume Amazon Elastic Block Store (Amazon EBS), un gruppo di sicurezza o Amazon Virtual Private Cloud (VPC). Per un elenco completo delle risorse AWS supportate da AWS Config, consulta i Tipi di risorse AWS supportati.

AWS Config consente di effettuare le seguenti operazioni:

- Valutare le configurazioni delle tue risorse AWS rispetto alle impostazioni desiderate.
- Ottenere un'istantanea delle configurazioni attuali delle risorse supportate associate al tuo account AWS.
- Ripristinare configurazioni di una o più risorse esistenti per il tuo account.
- Ripristinare le configurazioni preesistenti di una o più risorse.
- Ricevere una notifica ogni volta in cui una risorsa viene creata, modificata o eliminata.
- Visualizzare le relazioni fra le risorse. Ad esempio, trovare tutte le risorse che utilizzano un particolare gruppo di sicurezza.

Audit sulla conformità e analisi della sicurezza cibernetica

Con AWS CloudTrail è possibile monitorare in maniera continuativa l'attività di un account AWS. CloudTrail fornisce lo storico delle chiamate API AWS di un account, comprese quelle effettuate tramite la Console di gestione AWS, il kit SDK di AWS, gli strumenti a riga di comando e altri servizi AWS di livello superiore. Per i servizi che supportano AWS CloudTrail, è possibile identificare quali utenti e account hanno richiamato le API, l'indirizzo IP sorgente da cui sono state effettuate le chiamate e quando sono avvenute. È possibile integrare CloudTrail nelle applicazioni usando le API, automatizzare la creazione di trail per la propria organizzazione, verificarne lo stato e controllare come gli amministratori attivano o disattivano la generazione di log con CloudTrail.

I log CloudTrail possono essere aggregati da più regioni e più account AWS in un singolo bucket S3. AWS consiglia di scrivere i log, in particolare i log di AWS CloudTrail, in un bucket S3 con accesso limitato in un account AWS designato per la registrazione (Log Archive). Le autorizzazioni sul bucket devono impedire l'eliminazione dei log e devono essere cifrate a riposo utilizzando la cifratura lato server, con chiavi di cifratura gestite da Amazon S3 (SSE-S3) o chiavi gestite da AWS KMS (SSE-KMS). La conferma dell'integrità dei file di log CloudTrail può essere utilizzata per determinare se un file di log sia stato modificato, eliminato oppure sia rimasto invariato dopo la consegna da parte di CloudTrail. Questa funzione viene creata utilizzando algoritmi

standard del settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente difficile modificare, eliminare o falsificare i file di log CloudTrail senza rilevamento. È possibile utilizzare l'interfaccia a riga di comando (CLI) di AWS per convalidare i file nella posizione in cui CloudTrail li ha consegnati.

I log CloudTrail aggregati in un bucket S3 possono essere analizzati ai fini dell'audit o per attività di risoluzione dei problemi. Una volta centralizzati i log, è possibile integrarli con le soluzioni SIEM (Security Information and Event Management) o utilizzare i servizi AWS, come Amazon Athena o CloudTrail Insights, per analizzarli e visualizzarli utilizzando le dashboard Amazon QuickSight. Una volta centralizzati i log CloudTrail, è anche possibile utilizzare lo stesso account Log Archive per centralizzare i log di altre fonti, come CloudWatch Logs e i sistemi di bilanciamento del carico AWS.

Figura 2: esempio di un'architettura per audit sulla conformità e analisi della sicurezza cibernetica con AWS CloudTrail

I log AWS CloudTrail possono anche generare eventi Amazon CloudWatch preconfigurati. Questi eventi possono essere utilizzati per inviare notifiche a utenti o sistemi nel caso in cui si verifichi un evento o per richiedere azioni correttive. Ad esempio, per monitorare le attività sulle istanze EC2, è possibile creare una regola CloudWatch Event. Quando si verifica un'attività specifica sull'istanza Amazon EC2 e l'evento viene acquisito nei log, la regola attiva una funzione Lambda che invia un'e-mail di notifica sull'evento all'amministratore. (Cfr. figura 3.) L'e-mail include dettagli quali il momento in cui si è verificato l'evento, l'utente che ha eseguito l'azione, dettagli relativi a EC2 e altro ancora. Il diagramma in basso mostra l'architettura della notifica sull'evento.

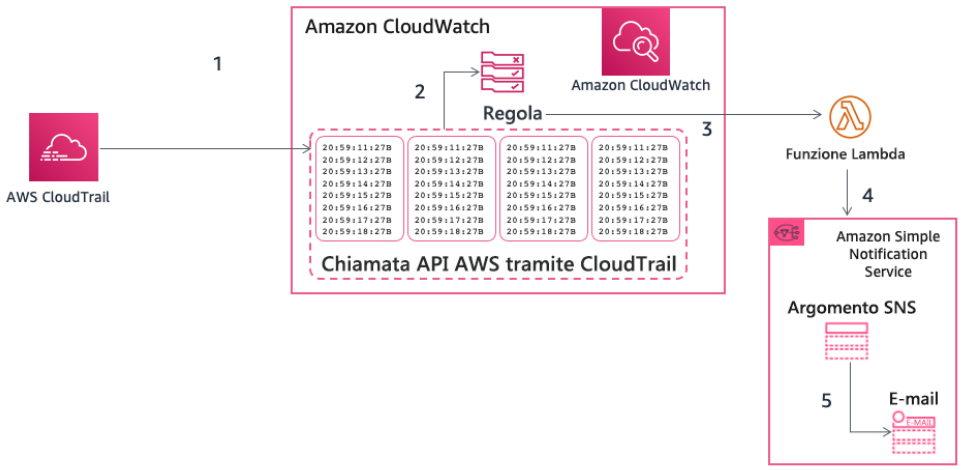

Figura 3: esempio di notifica su un evento AWS CloudTrail

Raccolta ed elaborazione di log

I log di CloudWatch possono essere utilizzati per monitorare, archiviare e accedere ai file di log da istanze EC2, AWS CloudTrail, Route 53 e altre fonti. Consulta la pagina di documentazione dei servizi AWS che pubblicano parametri CloudWatch.

Le informazioni sui log includono, ad esempio:

- Registrazione granulare di log per gli accessi a oggetti S3
- Informazioni dettagliate sui flussi nella rete tramite i log di flusso di VPC
- Controlli e azioni delle configurazioni basati su regole con regole AWS Config
- Filtraggio e monitoraggio dell'accesso HTTP alle applicazioni con funzioni firewall per applicazioni web (WAF) all'interno di CloudFront

Le metriche e i log delle applicazioni personalizzate possono anche essere pubblicati in CloudWatch Logs installando CloudWatch Agent su istanze EC2 o server in locale.

I log possono essere analizzati in modo interattivo utilizzando CloudWatch Logs Insights, eseguendo query per aiutarti a rispondere in modo più efficiente ed efficace ai problemi operativi.

I log di CloudWatch possono essere elaborati quasi in tempo reale configurando filtri di sottoscrizione e possono essere consegnati ad altri servizi come un cluster Amazon Elasticsearch Service (Amazon ES), un flusso Amazon Kinesis, un flusso Amazon Kinesis Data Firehose o Lambda per l'elaborazione, l'analisi o il caricamento personalizzati su altri sistemi.

I filtri delle metriche CloudWatch possono essere utilizzati per definire modelli da cercare nei dati di log, trasformarli in metriche numeriche di CloudWatch e impostare avvisi in base alle esigenze aziendali. Ad esempio, seguendo la raccomandazione di AWS di non utilizzare l'utente root per le attività quotidiane, è possibile impostare uno specifico filtro delle metriche CloudWatch su un log di CloudTrail (consegnato a CloudWatch Logs) per creare una metrica personalizzata e configurare un avviso, in modo da informare le parti interessate nel momento in cui vengono utilizzate le credenziali root per accedere al tuo account AWS.

Log come quelli per l'accesso al server S3 o a Elastic Load Balancing o come quelli di flusso VPC e AWS Global Accelerator possono essere consegnati direttamente a un bucket S3. Ad esempio, abilitando i log di accesso al server Amazon S3, puoi ottenere informazioni dettagliate sulle richieste che vengono fatte al tuo bucket S3. Uno storico dei log di accesso contiene i dettagli della richiesta, come il tipo di richiesta, le risorse specificate nella richiesta, ora e data in cui la richiesta è stata elaborata. Per ulteriori informazioni sui contenuti di un messaggio sui log, consulta la sezione Formato dei log di accesso al server Amazon S3 nella *guida per sviluppatori di Amazon Simple Storage Service*. I log di accesso al server sono utili per molte applicazioni, perché offrono ai proprietari del bucket informazioni sulla natura delle richieste fatte dai clienti che non sono sotto il loro controllo. Per impostazione predefinita, S3 non raccoglie i log di accesso al servizio, ma una volta abilitato il logging, S3 di solito fornisce i log di accesso al bucket entro poche ore. Se necessiti di una consegna più rapida o devi consegnare i log a più destinazioni, considera l'utilizzo di log CloudTrail o una combinazione di log CloudTrail e S3. I log possono essere cifrati a riposo configurando la cifratura degli oggetti predefinita nel bucket di destinazione. Gli oggetti vengono cifrati utilizzando la cifratura lato server con chiavi gestite da S3 (SSE-S3) o chiavi master del cliente (CMK) memorizzate all'interno di AWS Key Management Service (AWS KMS).

Tramite Amazon Athena è possibile utilizzare query per analizzare i log memorizzati in un bucket S3. Amazon Athena è un servizio di query interattivo che consente di analizzare i dati di S3 utilizzando SQL standard. È possibile utilizzare Athena per eseguire query ad-hoc tramite ANSI SQL, senza la necessità di aggregare o caricare i dati all'interno di Athena. Athena è in grado di elaborare set di dati non strutturati, semi-strutturati e strutturati e può essere integrata con Amazon QuickSight per una facile visualizzazione.

I log sono anche un'utile fonte di informazione per il rilevamento delle minacce. Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza cibernetica che analizza ed elabora gli eventi da diverse fonti, come i log di flusso VPC, i log eventi di gestione CloudTrail, i log eventi di dati CloudTrail S3 e i log DNS. Utilizza feed di intelligence sulle minacce (ad esempio elenchi di indirizzi IP e domini dannosi) e il machine learning per identificare attività inaspettate e potenzialmente non autorizzate e dannose all'interno dell'ambiente AWS. Quando GuardDuty è abilitato in una regione, inizia immediatamente ad analizzare i log di eventi CloudTrail. Questo sistema utilizza la gestione CloudTrail e gli eventi di dati S3 direttamente da CloudTrail attraverso un flusso indipendente e duplicativo di eventi.

Scoprire e proteggere i dati su larga scala con Amazon Macie

L'articolo 32 del GDPR stabilisce che "... il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: [...]

(b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

[…]

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento."

Avere un processo continuo di classificazione è fondamentale per adeguare l'elaborazione sicura dei dati alla natura dei dati. Se la tua organizzazione gestisce dati sensibili, controlla dove questi dati risiedono, proteggili correttamente e fornisci prova dell'applicazione di sicurezza cibernetica e privacy dei dati, come richiesto per soddisfare i requisiti di conformità alle normative. Per aiutare il cliente a identificare e proteggere i propri dati sensibili su larga scala, AWS offre Amazon Macie, un servizio di sicurezza cibernetica e privacy dei dati completamente gestito che utilizza modelli di pattern matching e machine learning per il rilevamento di informazioni a carattere personale (PII) per rilevare e proteggere i dati sensibili memorizzati nei bucket S3. Amazon Macie esegue la scansione di questi bucket e fornisce una categorizzazione dei dati utilizzando identificatori di dati gestiti che sono progettati per rilevare diverse categorie di dati sensibili. Macie è in grado di rilevare PII quali nome completo, indirizzo e-mail, data di nascita, numero di identificazione nazionale, identificazione fiscale o numero di riferimento e altro ancora.[5] Il cliente può definire identificatori di dati personalizzati che riflettono gli scenari specifici della propria organizzazione (ad esempio, numeri di account cliente o classificazione interna dei dati).

Amazon Macie valuta continuamente l'oggetto all'interno dei bucket e fornisce automaticamente un riepilogo dei risultati (figura 4) per tutti i dati non cifrati o accessibili pubblicamente che vengono individuati e che corrispondono alla categoria di dati definita. Questi dati possono includere avvisi per qualsiasi oggetto o bucket non cifrato e accessibile pubblicamente che viene condiviso con account AWS al di fuori di quelli definiti all'interno di AWS Organizations. Amazon Macie è integrato da altri servizi AWS, come AWS Security Hub, per generare risultati di sicurezza cibernetica e fornire un'azione automatica e pronta ai risultati (figura 5).

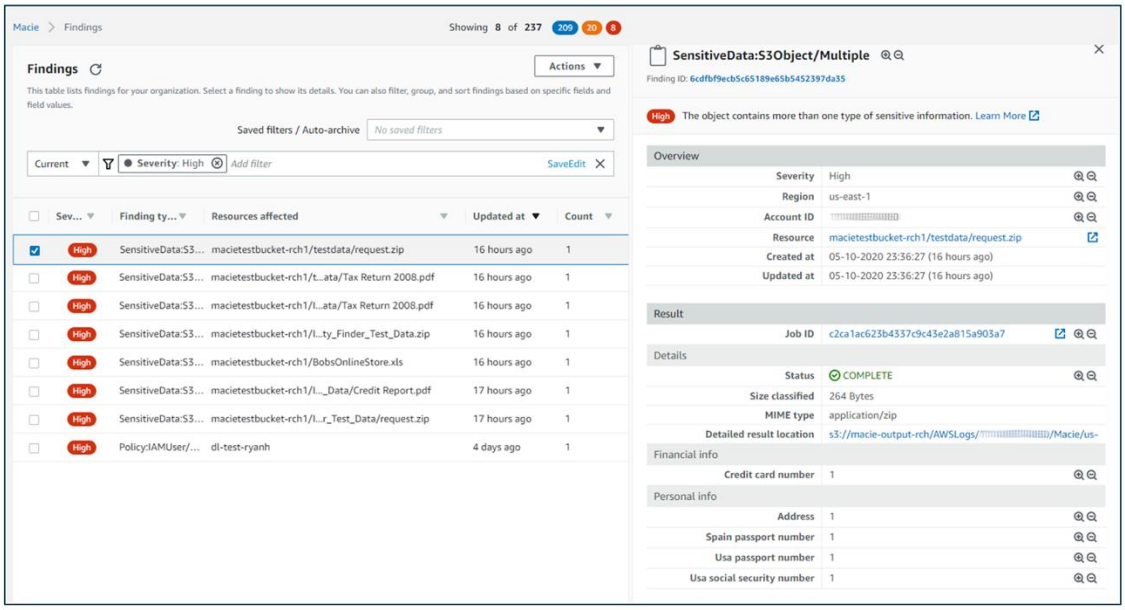

Figura 4: ispezioni dei dati ed esempio di risultati

Gestione centralizzata della sicurezza cibernetica

Molte organizzazioni si ritrovano ad affrontare sfide legate alla visibilità e alla gestione centralizzata del loro ambiente. L'aumentare delle dimensioni dell'organizzazione può rendere questa sfida più complessa, a meno che non si progetti attentamente un approccio alla sicurezza. La mancanza di conoscenza, unita a una gestione decentralizzata e disomogenea dei processi di governance e sicurezza cibernetica, può rendere un ambiente vulnerabile.

AWS offre strumenti per aiutare i clienti a soddisfare alcuni dei requisiti più complessi nella gestione e nella governance IT, oltre a strumenti per supportare un approccio alla protezione dei dati "by design", che considera la sicurezza cibernetica già dalla fase di progettazione.

AWS Control Tower permette di creare e gestire un ambiente AWS nuovo, sicuro e con più account. Automatizza la creazione di una landing zone:[6] un ambiente con account multipli creato secondo le migliori prassi e che supporta la governance attraverso l'utilizzo di "guardrails" selezionabili da una lista predefinita. I guardrail implementano regole di governance per sicurezza, conformità e operazioni. AWS Control Tower permette una gestione delle identità tramite la directory predefinita di AWS Single Sign-On (SSO) e consente l'audit tra più account con AWS SSO e AWS IAM. Centralizza, inoltre, i log provenienti da CloudTrail e AWS Config, che sono salvati all'interno di S3.

AWS Security Hub è un altro servizio che supporta la centralizzazione e può migliorare la visibilità su un'organizzazione. Security Hub centralizza e ordina in base alle priorità

i risultati sulla sicurezza cibernetica e la conformità provenienti dai vari account e servizi AWS, quali Amazon GuardDuty e Amazon Inspector. Inoltre, può essere integrato con software per la sicurezza di partner terzi per consentire l'analisi delle minacce e l'identificazione dei problemi prioritari relativi alla sicurezza.

Amazon GuardDuty è un servizio intelligente per il rilevamento delle minacce che può aiutare i clienti a monitorare e proteggere in modo più accurato e semplice i loro account AWS, i carichi di lavoro e i dati archiviati all'interno di S3. GuardDuty analizza miliardi di eventi nei tuoi account AWS da diverse fonti, tra cui eventi di gestione AWS CloudTrail, eventi di dati S3 AWS CloudTrail, log di flusso Amazon VPC e log DNS. Ad esempio, rileva chiamate API insolite, comunicazioni in uscita sospette a indirizzi IP dannosi noti o possibili furti di dati utilizzando query DNS come meccanismo di trasporto. GuardDuty è in grado di fornire risultati più accurati sfruttando l'intelligence sulle minacce basata sul machine learning e i partner terzi di sicurezza cibernetica.

Amazon Inspector è un servizio di valutazione della sicurezza cibernetica automatizzato che aiuta a migliorare la sicurezza e la conformità delle applicazioni distribuite sulle istanze EC2. Amazon Inspector analizza automaticamente le applicazioni per individuare esposizione, vulnerabilità e deviazioni dalle migliori prassi. Dopo aver eseguito una valutazione, Amazon Inspector fornisce un elenco dettagliato dei risultati di sicurezza cibernetica ordinati in base al livello di gravità.

Amazon CloudWatch Events consente di impostare su un account AWS l'invio di eventi ad altri account AWS o la ricezione di eventi inviati da altri account o organizzazioni. Questo meccanismo può essere molto utile per implementare scenari trasversali di risposta agli incidenti, in quanto permette di intraprendere rapidamente azioni correttive (ad esempio, chiamando una funzione Lambda o eseguendo un comando su un'istanza EC2) a seconda delle necessità, ogni volta che si verifica un incidente alla sicurezza.

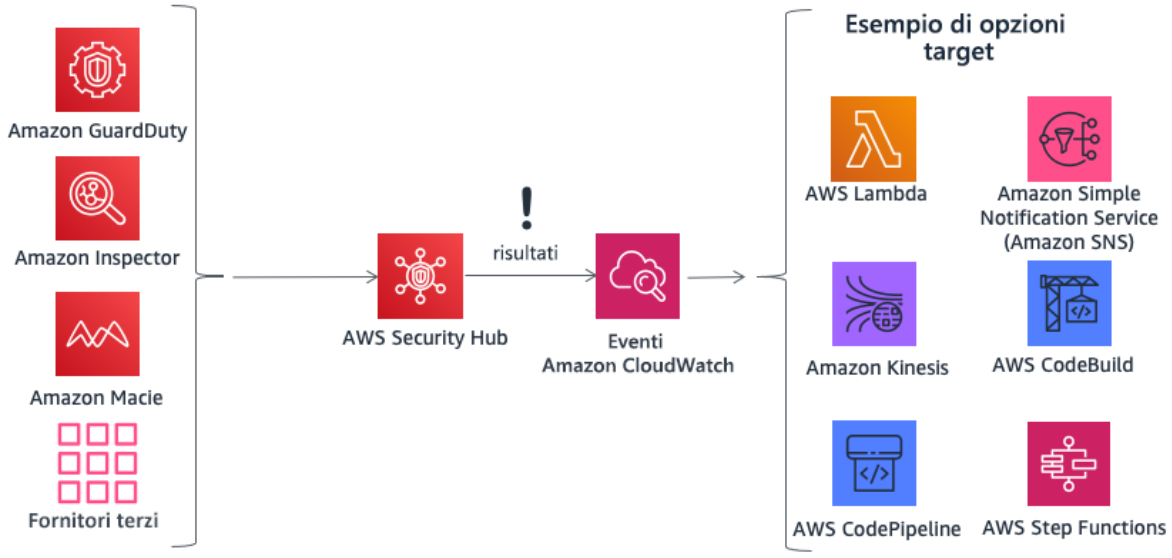

Figura 5: intraprendere azioni con AWS Security Hub e Amazon CloudWatch Events

AWS Organizations aiuta a gestire e governare ambienti molto complessi in maniera centralizzata. Permette di controllare accessi, conformità e sicurezza cibernetica in un ambiente con più account. AWS Organizations supporta le policy di controllo dei servizi (SCP), che definiscono le azioni del servizio AWS disponibili per l'utilizzo con account specifici o unità organizzative (UO) all'interno di un'organizzazione.

AWS Systems Manager offre visibilità e controllo dell'infrastruttura su AWS. È possibile visualizzare i dati operativi di più servizi AWS da una console unificata e automatizzare le attività operative su di essi. Fornisce informazioni sulle attività API recenti, le modifiche alla configurazione delle risorse, gli avvisi operativi, l'inventario del software e lo stato di conformità delle patch. Integrando questo servizio con altri servizi AWS, è anche possibile agire sulle risorse in base alle tue esigenze operative, per rendere conforme il tuo ambiente.

Ad esempio, integrando Amazon Inspector con AWS Systems Manager, le valutazioni di sicurezza cibernetica sono semplificate e automatizzate, perché è possibile installare l'agente Amazon Inspector automaticamente utilizzando Amazon EC2 Systems Manager nel momento in cui viene avviata un'istanza EC2. Puoi anche eseguire riparazioni automatiche per i risultati di Amazon Inspector utilizzando le funzioni EC2 System Manager e Lambda.

Protezione dei dati in AWS

L'articolo 32 del GDPR prevede che le organizzazioni debbano «... [mettere in] atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono [...] la pseudonimizzazione e la cifratura dei dati personali

[...]” Inoltre, le organizzazioni devono salvaguardarsi dalla divulgazione non autorizzata o dall’accesso ai dati personali.

La cifratura riduce i rischi associati alla conservazione dei dati personali, perché rende i dati illeggibili, salvo possesso della chiave corretta. Una strategia di cifratura a 360° può aiutare a ridurre l’impatto degli incidenti di sicurezza, inclusi alcune violazioni della sicurezza cibernetica.

Cifratura di dati a riposo

La cifratura di dati a riposo è un processo vitale per la conformità normativa e la protezione dei dati. Aiuta a far sì che i dati sensibili salvati su dischi non siano accessibili a utenti o applicazioni non in possesso di un chiave valida. AWS offre varie opzioni per la cifratura dei dati a riposo e la gestione delle chiavi di cifratura. Ad esempio, è possibile utilizzare un kit SDK di cifratura AWS con una CMK creata e gestita in AWS KMS per cifrare dati arbitrari.

I dati cifrati possono essere conservati a riposo in modo sicuro e la loro decrittazione può avvenire solo da parte di un soggetto con accesso autorizzato alla CMK. Il risultato è la cifratura envelope dei dati confidenziali, un meccanismo di policy per l’autorizzazione e la cifratura autenticata oltre a un logging di audit tramite AWS CloudTrail. Alcuni servizi base di AWS integrano le funzioni di cifratura di dati a riposo, fornendo l’opzione di cifrare i dati prima di scriverli in archivi non volatili. Ad esempio, è possibile cifrare i volumi Amazon EBS e configurare i bucket S3 per la cifratura lato server (SSE) utilizzando la cifratura AES-256. S3 supporta anche la *cifratura lato client*, che consente di cifrare i dati prima di inviarli a S3. I kit SDK AWS supportano la cifratura lato client per facilitare le operazioni di cifratura e decrittazione degli oggetti. Amazon RDS supporta anche Transparent Data Encryption (TDE).

È possibile cifrare i dati negli instance store Linux EC2 utilizzando le librerie Linux incorporate. Questo metodo consente di cifrare i file in modo trasparente, proteggendo i dati riservati. Di conseguenza, le applicazioni che trattano i dati ignorano la cifratura esistente a livello del disco.

È possibile usare due metodi per cifrare file negli instance store:

- **Cifratura a livello del disco:** con questo metodo, l’intero disco (o un blocco all’interno del disco) viene cifrato utilizzando una o più chiavi di cifratura. La cifratura del disco opera al di sotto del livello file system, non si basa su un sistema operativo specifico e nasconde informazioni su directory e file, come nome e dimensione. Encrypting File System, ad esempio, è un’estensione Microsoft del New Technology File System (NTFS) del sistema operativo Windows NT che fornisce la cifratura del disco.

- **Cifratura a livello di file system:** Questo metodo realizza una cifratura dei file e delle directory, ma non di tutto il disco o di tutta la partizione. La cifratura a livello di file system opera sul file system ed è trasferibile da un sistema operativo all'altro.

Per volumi di instance store SSD di tipo Non-Volatile Memory express (NVMe), la *cifratura a livello del disco* è un'opzione predefinita. I dati dello storage dell'istanza NVMe sono cifrati utilizzando una cifratura a blocchi XTS-AES-256 implementato su un modulo hardware sull'istanza. Le chiavi di cifratura vengono generate utilizzando il modulo hardware e sono univoche per ogni dispositivo dello storage dell'istanza NVMe. Tutte le chiavi di cifratura vengono distrutte quando l'istanza viene arrestata o terminata e non possono essere recuperate. Non è possibile usare chiavi di cifratura personali.

Cifratura di dati in transito

AWS consiglia caldamente di cifrare i dati in transito da un sistema all'altro, includendo risorse all'interno e all'esterno di AWS.

Quando viene creato un account AWS, a esso viene riservata una sezione logicamente isolata del cloud AWS, chiamata Amazon Virtual Private Cloud (Amazon VPC). In quest'area è possibile lanciare risorse AWS in una rete virtuale definita dal cliente. Questi ha il controllo completo sull'ambiente virtuale di rete. Ciò permette di selezionare l'intervallo di indirizzi IP, creare sottoreti e configurare tabelle di routing e gateway di rete. Inoltre, è possibile creare una connessione VPN hardware tra il data center aziendale e Amazon VPC per utilizzare il cloud AWS come estensione del data center aziendale.

Per proteggere la comunicazione tra Amazon VPC e il data center aziendale, è possibile scegliere, tra diverse opzioni di connettività VPN, quella che meglio soddisfa le proprie necessità. AWS Client VPN consente un accesso sicuro alle risorse AWS attraverso servizi VPN basati sul client. È anche possibile utilizzare un'appliance VPN software di terze parti disponibile in AWS Marketplace, installabile su un'istanza EC2 all'interno di Amazon VPC. In alternativa, è possibile creare una connessione VPN IPsec per proteggere la comunicazione tra VPC e la rete remota. AWS Direct Connect consente di creare una connessione privata dedicata da una rete remota ad Amazon VPC. Questa connessione può essere abbinata a una connessione Site-to-Site VPN di AWS per creare una connessione privata con cifratura IPsec.

AWS fornisce degli endpoint HTTPS tramite il protocollo TLS (Transport Layer Security) per le comunicazioni, il che offre una cifratura in transito quando si usano le API AWS. Il servizio AWS Certificate Manager (ACM) consente di generare, gestire e distribuire certificati privati e pubblici da utilizzare per stabilire un trasferimento cifrato tra i sistemi tra i quali si muove un carico di lavoro. Amazon Elastic Load Balancing, integrato in ACM, può essere utilizzato come supporto per i protocolli HTTPS. Se un contenuto viene distribuito tramite Amazon CloudFront, supporta gli endpoint cifrati.

Strumenti di cifratura

AWS offre diversi servizi, strumenti e meccanismi di cifratura di dati altamente scalabili, che aiutano a proteggere i dati archiviati ed elaborati in AWS. Per informazioni sulle funzionalità dei servizi AWS e sulla privacy, consultare Funzionalità del servizio AWS per considerazioni sulla privacy.[7]

I servizi di cifratura di AWS utilizzano un ampio ventaglio di tecnologie per la cifratura e l'archiviazione, progettate per mantenere l'integrità e la riservatezza dei dati a riposo o in transito. AWS offre quattro servizi e strumenti principali per le operazioni di cifratura:

- **AWS Key Management Service** (AWS KMS) è un servizio gestito da AWS che crea e gestisce sia chiavi master sia chiavi dati. AWS KMS è integrato in diversi servizi AWS, per offrire una cifratura dati lato server tramite le chiavi KMS dagli account dei clienti. I moduli hardware per la sicurezza KMS (HSMs) sono validati al livello 2 FIPS 140-2.
- **AWS CloudHSM** offre HSM validati a livello 3 di FIPS 140-2. Consentono l'archiviazione di una gamma di chiavi di cifratura autogestite, tra cui chiavi master e chiavi dati.
- **Servizi e strumenti di cifratura AWS**
  - **AWS Encryption SDK** offre una libreria di cifratura lato client per permettere di implementare la cifratura e la decrittazione di *tutti* i tipi di dati.
  - **Amazon DynamoDB Encryption Client** fornisce una libreria di cifratura lato client per la cifratura delle tabelle dati prima che queste vengano inviate a un servizio di database, come Amazon DynamoDB.

AWS Key Management Service

AWS Key Management Service (AWS KMS) è un servizio gestito che facilita la creazione e la gestione delle chiavi di cifratura utilizzate per cifrare i dati. Sfrutta gli Hardware Security Modules (HSMs) per proteggere la sicurezza delle chiavi. AWS KMS si integra con numerosi altri servizi AWS per consentire di proteggere i dati archiviati in tali servizi. AWS KMS è integrato anche con AWS CloudTrail per fornire i log dell'utilizzo di tutte le chiavi e consentire di soddisfare i requisiti normativi e di conformità.

Permette di creare, importare e modificare regolarmente le chiavi master e definire policy di utilizzo e monitorarne l'uso tramite la Console di gestione AWS, il kit SDK o l'interfaccia a riga di comando di AWS.

Le chiavi master all'interno di AWS KMS, siano esse importate da te o create per tuo conto da AWS KMS, vengono conservate in archivi estremamente durevoli in formati cifrati, per fare in modo che possano essere usate quando servono. AWS KMS può

eseguire la rotazione automatica delle chiavi master create all'interno di KMS una volta all'anno senza dover cifrare nuovamente i dati già cifrati con la tua chiave master. Non è necessario tenere traccia delle versioni precedenti delle chiavi master perché risulteranno sempre disponibili all'interno di AWS KMS per decrittare i dati precedentemente cifrati.

L'utente può decidere chi ha accesso a ciascuna chiave master di KMS e per quali servizi queste chiavi possono essere utilizzate. Per fare ciò, sono disponibili una serie di controlli accessi, tra cui concessioni e condizioni di policy delle chiavi all'interno delle policy delle chiavi o delle policy IAM. È anche consentito importare chiavi dalla propria infrastruttura di gestione delle chiavi per impiegarle su KMS.

Ad esempio, la policy in basso sfrutta la condizione `kms:ViaService` per consentire l'utilizzo di una CMK gestita da un cliente per azioni specifiche solo per richieste provenienti da Amazon EC2 o Amazon RDS in una regione specifica (*us-west-2*) per conto di un utente specifico (`ExampleUser`).

```
{
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Effect": "Allow",
                 "Principal": {
                     "AWS":
"arn:aws:iam::111122223333:user/ExampleUser"
                  }
                 "Action": [
                      "kms:Encrypt*",
                      "kms:Decrypt",
                      "kms:ReEncrypt*",
                      "kms:GenerateDataKey*",
                      "kms:CreateGrant",
                      "kms:ListGrants",
                      "kms:DescribeKey"
                  ],
                  "Resource": "*",
                  "Condition": {
                     "ForAnyValue:StringEquals": {
                         "kms:ViaService": [
                               "ec2.us-west-2.amazonaws.com",
                               "rds.us-west-2.amazonaws.com"
                         ]
```

```
                    }
                }
}
```

Integrazione di servizi AWS

AWS KMS è integrato a una serie di servizi AWS: consulta il sito web KMS per un elenco completo dei servizi integrati. Grazie a queste integrazioni, è possibile utilizzare le chiavi master di AWS KMS per cifrare i dati archiviati con tali servizi. Oltre a una chiave master gestita dal cliente, una serie di servizi integrati permettono di usare una CMK gestita da AWS, creata e gestita per te in modo automatico, ma valida solo per lo specifico servizio per cui è stata creata.

Funzionalità di audit

AWS CloudTrail registra ogni utilizzo di una chiave memorizzata all'interno di KMS in un file di log che viene consegnato al bucket S3 specificato nella configurazione di CloudTrail. Le informazioni registrate includono i dettagli relativi all'utente, la data e l'ora di utilizzo, l'operazione eseguita e la chiave utilizzata.

Sicurezza cibernetica

AWS KMS è stato progettato in modo da non consentire a nessuno di accedere alle chiavi master di un cliente. Il servizio è stato sviluppato su sistemi progettati per mantenere al sicuro le chiavi master con tecniche di protezione avanzate, ad esempio salvando su disco solo chiavi master cifrate, disattivandone l'archiviazione in memoria e selezionando i sistemi accessibili all'host che le utilizza. L'accesso al software di aggiornamento viene monitorato mediante un processo di controllo multilaterale che viene tenuto sotto controllo e verificato da un gruppo indipendente interno di AWS.

Per ulteriori informazioni su AWS KMS, consulta il whitepaper *AWS Key Management Service*.

AWS CloudHSM

AWS CloudHSM è un modulo di sicurezza hardware su cloud (HSM) che contribuisce a soddisfare i requisiti di conformità aziendali, contrattuali e normativi per la sicurezza dei dati, consentendo di generare e utilizzare le chiavi di cifratura su un hardware validato al livello 3 FIPS 140-2.

CloudHSM consente di controllare le chiavi e le operazioni di cifratura eseguite da HSM.

I partner di AWS e AWS Marketplace offrono un'ampia gamma di soluzioni per la protezione dei dati sensibili all'interno della piattaforma AWS. Tuttavia, per applicazioni e dati soggetti a obblighi contrattuali o normativi relativi alla gestione delle chiavi di

cifratura, può essere necessaria una protezione aggiuntiva. Fino ad ora, l'unica opzione era quella di memorizzare i dati sensibili (o le chiavi di cifratura che proteggono i dati sensibili) nei data center in locale. Ciò comporta un possibile impedimento nella migrazione di queste applicazioni nel cloud o un rallentamento notevole delle loro prestazioni. Il servizio AWS CloudHSM consente di proteggere le chiavi di cifratura all'interno di moduli HSM progettati e convalidati secondo gli standard governativi per la gestione sicura delle chiavi. È possibile generare, archiviare e gestire in modo sicuro le chiavi usate per la cifratura dei dati, in modo che tu sia l'unico utente autorizzato ad accedervi. AWS CloudHSM aiuta a soddisfare i rigorosi requisiti di gestione delle chiavi senza compromettere le prestazioni dell'applicazione.

Il servizio AWS CloudHSM funziona con Amazon VPC. Il provisioning delle istanze CloudHSM viene effettuato all'interno di Amazon VPC con un indirizzo IP specificato dall'utente, fornendo una connettività di rete semplice e privata alle istanze EC2. Poiché le istanze CloudHSM si trovano vicino alle istanze EC2, il loro utilizzo garantisce una latenza di rete inferiore, migliorando le performance dell'applicazione. AWS fornisce un accesso dedicato ed esclusivo (a tenant singolo) alle istanze CloudHSM, che sono isolate da altri clienti AWS. Disponibile in più regioni e zone di disponibilità, CloudHSM permette di aggiungere un archivio di chiavi sicuro e durevole alle tue applicazioni.

Integrazione con servizi AWS e applicazioni di terze parti

CloudHSM può essere utilizzato con Amazon Redshift, Amazon RDS for Oracle o applicazioni di terze parti (come ad esempio SafeNet Virtual KeySecure) come radice di attendibilità, Apache (terminazioni SSL) o Microsoft SQL Server (cifratura dei dati in modo trasparente). È anche possibile utilizzare CloudHSM per la scrittura di applicazioni e per continuare a utilizzare le librerie di cifratura standard usate abitualmente, incluse PKCS#11, Java JCA/JCE, Microsoft CAPI e CNG.

Attività di audit

Per monitorare le modifiche alle risorse o controllare le attività di audit su sicurezza cibernetica e conformità, è possibile esaminare tutte le chiamate API CloudHSM effettuate dal tuo account tramite AWS CloudTrail. Inoltre, è possibile controllare le operazioni sull'appliance HSM usando o inviando messaggi syslog al raccoglitore di log.

Servizi e strumenti di cifratura AWS

AWS offre meccanismi che soddisfano un'ampia gamma di standard di sicurezza cibernetica che puoi usare per implementare una cifratura che rispetti le migliori prassi. AWS Encryption SDK[8] è una libreria di cifratura lato client disponibile in Java, Python, C, JavaScript e un'interfaccia a riga di comando che supporta Linux, macOS e Windows. AWS Encryption SDK offre opzioni avanzate per la protezione dei dati, tra cui suite di chiavi di algoritmi simmetriche, sicure e autenticate, come 256-bit AES-GCM con chiavi di derivazione e accesso. Poiché è stato specificamente progettato per applicazioni che sfruttano Amazon DynamoDB, DynamoDB Encryption Client[9] permette

agli utenti di proteggere le loro tabelle dati prima che vengano inviate al database. Permette, inoltre, di verificare e decrittare dati quando vengono richiamati. Il client è disponibile in Java e Python.

Infrastruttura Linux DM-Crypt

Dm-crypt è un meccanismo di cifratura Linux a livello di kernel che permette agli utenti di montare un file system cifrato. Montare un file system è un processo che consiste nel collegare un file system a una directory (punto di montaggio), mettendolo a disposizione del sistema operativo. Dopo il montaggio, tutti i file nel file system sono disponibili per le applicazioni senza ulteriori interazioni. Tuttavia, questi file sono cifrati quando vengono archiviati nel disco.

Il device mapper è un'infrastruttura nel kernel Linux 2.6 e 3.x che fornisce un metodo generico per creare layer virtuali di dispositivi a blocchi. Il target crypt del device mapper fornisce una cifratura trasparente di dispositivi a blocchi usando l'API di cifratura del kernel. La soluzione in questo post prevede l'utilizzo di dm-crypt in combinazione con un file system su supporto disco mappato a un volume logico dal Logical Volume Manager (LVM). L'LVM fornisce gestione di volumi logici per il kernel Linux.

Protezione dati fin dalla progettazione (by design) e per impostazione predefinita (by default)

AWS riceve una richiesta ogni qualvolta un utente o un'applicazione cerchino di usare la Console di gestione AWS, le API AWS o la CLI AWS. Il servizio AWS riceve la richiesta ed esegue una serie di passaggi per determinare se la richiesta può essere accettata o rifiutata, secondo una specifica logica di valutazione della policy. Ad eccezione delle richieste di credenziali di root, tutte le richieste su AWS vengono negate per impostazione predefinita (viene applicata la policy *deny* predefinita). Ciò significa che tutto ciò che non viene esplicitamente autorizzato dalla policy, viene rifiutato. Come migliore prassi, nella definizione delle policy, AWS consiglia di applicare il principio del privilegio minimo, che implica che ogni componente (come utenti, moduli o servizi) deve essere in grado di accedere solo alle risorse necessarie per completare le rispettive attività.

Questo approccio riflette l'articolo 25 del GDPR, che stabilisce che il titolare del trattamento "mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento."

AWS fornisce strumenti per implementare l'*infrastruttura come codice,* che è un potente meccanismo per includere la sicurezza cibernetica già dalle prime fasi di progettazione di un'architettura. AWS CloudFormation offre un linguaggio comune per descrivere e permettere il provisioning di tutte le risorse delle infrastrutture, incluse le policy e i processi di sicurezza cibernetica. Grazie a questi strumenti e queste pratiche,

la sicurezza cibernetica entra a far parte del codice e può essere aggiornata, monitorata e modificata (con un sistema di versioni multiple), a seconda delle esigenze dell'organizzazione. Ciò favorisce un approccio di *protezione dei dati fin dalla progettazione*, in quanto i processi e le policy di sicurezza possono essere inclusi nella definizione dell'architettura oltre a poter essere monitorati in maniera continuativa da misure di sicurezza cibernetica nell'organizzazione.

Il supporto di AWS

Tabella 1: il contributo dato da AWS per gestire la conformità al GDPR

Area	Descrizione	Servizi e strumenti AWS
Solido framework di conformità	Può essere necessario includere nelle misure tecniche e organizzative appropriate "La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento."	SOC 1 / SSAE 16 / ISAE 3402 (precedentemente SAS 70) / SOC 2 / SOC 3 PCI DSS Livello 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Cloud Computing Compliance Controls Catalog (C5)
Controllo dell'accesso ai dati	Il titolare del trattamento "mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento."	 AWS Identity and Access Management (IAM)  Amazon Cognito  AWS Shield e WAF  AWS Resource Access Manager  AWS Organizations  AWS CloudFormation  AWS CloudTrail  AWS Config

Area	Descrizione	Servizi e strumenti AWS
Monitoraggio e logging	"ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento di cui sono responsabili." "[...] il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio [...]"	 Amazon CloudWatch  AWS Control Tower  Amazon GuardDuty  Amazon Inspector  Amazon Macie  AWS Systems Manager  AWS Security Hub
		 AWS Tools e SDK
Protezione dei dati in AWS	Le organizzazioni devono "[mettere in] atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono [...] la pseudonimizzazione e la cifratura dei dati personali."	 AWS Certificate Manager  AWS CloudHSM  AWS Key Management Service

Collaboratori

Hanno collaborato alla stesura di questo documento:

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Public Sector Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services
- Luca Iannario, Public Sector Solutions Architect, Amazon Web Services

Revisioni del documento

Data	Descrizione
Novembre 2017	Prima pubblicazione
Dicembre 2020	Aggiornamento per l'aggiunta di nuovi servizi e funzionalità AWS.

Notes

[1] https://ec.europa.eu/info/law/law-topic/data-protection_it

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] https://cispe.cloud/

[4] https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

[5] https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html#managed-data-identifiers-pii

[6] https://aws.amazon.com/solutions/aws-landing-zone/

[7] https://aws.amazon.com/compliance/data-privacy/service-capabilities/

[8] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-encrypt.html

[9] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-ddb-client.html