Livre blanc AWS

Gestion de la conformité au RGPD sur AWS

Gestion de la conformité au RGPD sur AWS: Livre blanc AWS

Table of Contents

Gestion de la conformité au RGPD sur AWS

Date de publication : décembre 2020 (Révisions du document)

Résumé

Ce document fournit des informations sur les services et les ressources qu'Amazon Web Services (AWS) propose aux clients afin de les aider à se conformer aux exigences du Règlement général sur la protection des données (RGPD) pouvant s'appliquer à leurs activités. Cela comprend l'adhésion aux normes de sécurité informatique, l'attestation Cloud Computing Compliance Controls Catalog (C5) d'AWS, l'adhésion au code de conduite des fournisseurs de service d'infrastructure cloud en Europe (Cloud Infrastructure Services Providers, CISPE), des contrôles des accès aux données, des outils de surveillance et de journalisation, le chiffrement et la gestion des clés.

Présentation du Règlement général sur la protection des données (RGPD)

Le Règlement général sur la protection des données (RGPD) est une réglementation européenne relative à la protection de la vie privée (Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016) qui est entrée en vigueur le 25 mai 2018. Le RGPD remplace la directive sur la protection des données dans l'UE (directive 95/46/CE). Il vise à harmoniser les législations relatives à la protection des données dans l'ensemble de l'Union européenne (UE) en proposant une directive unique en matière de protection des données, obligatoire et directement applicable dans tout État membre de l'Union européenne.

Le RGPD s'applique à tous les traitements de données à caractère personnel, par des organisations qui possèdent un établissement au sein de l'UE ou qui traitent des données à caractère personnel de résidents de l'UE lorsqu'elles proposent des marchandises ou des services à des particuliers au sein de l'UE ou qu'elles surveillent le comportement des résidents de l'UE dans l'UE. Les données à caractère personnel comprennent toute information liée à une personne physique identifiable ou identifiée.

Changements apportés par le RGPD applicables aux organisations menant des activités au sein de l'UE

L'un des objectifs essentiels du RGPD consiste à unifier la manière dont les données à caractère personnel peuvent être traitées, utilisées et échangées de façon sécurisée dans les différents États membres de l'UE. Les organisations doivent prouver en permanence que les données qu'elles traitent sont sécurisées, ainsi que leur conformité au RGPD, en mettant en œuvre et en passant en revue régulièrement des mesures techniques et organisationnelles rigoureuses, ainsi que des politiques de conformité applicables au traitement des données à caractère personnel. En cas d'infraction au RGPD, les autorités de contrôle de l'UE peuvent infliger des amendes allant jusqu'à 20 millions d'euros, soit 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé.

Préparation d'AWS au RGPD

Les experts en conformité, en protection des données et en sécurité d'AWS collaborent avec des clients du monde entier pour répondre à leurs questions et les aider à se préparer à exécuter des

charges de travail dans le cloud conformément au RGPD. Ces équipes examinent également l'état de préparation d'AWS par rapport aux exigences du RGPD.

> **Note**
>
> Nous pouvons confirmer que tous les services AWS peuvent être utilisés en conformité avec le RGPD.

Addendum sur le traitement des données d'AWS

AWS propose un addendum sur le traitement des données (Data Processing Addendum, DPA) respectant le RGPD (DPA RGPD) qui permet aux clients de respecter les obligations contractuelles du RGPD. Le DPA RGPD d'AWS est intégré aux Conditions de service AWS et s'applique automatiquement à tous les clients dans le monde entier qui en ont besoin pour respecter le RGPD.

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt concernant le bouclier de protection des données UE-États-Unis et les clauses contractuelles types (« clauses types »). La CJUE a statué que le bouclier de protection des données UE-États-Unis n'offre plus une protection adéquate pour le transfert de données à caractère personnel de l'Union européenne (UE) vers les États-Unis. Cependant, dans le même arrêt, la CJUE a confirmé que les entreprises peuvent continuer à utiliser les clauses contractuelles types comme mécanisme de transfert de données en dehors de l'UE.

Suite à cet arrêt, les clients et partenaires AWS peuvent continuer à utiliser AWS pour transférer leur contenu de l'Europe vers les États-Unis et d'autres pays, conformément à la législation européenne en matière de protection des données, y compris au Règlement général sur la protection des données (RGPD). Les clients AWS peuvent compter sur les clauses contractuelles types incluses dans l'addendum sur le traitement des données d'AWS (DPA) s'ils choisissent de transférer leurs données en dehors de l'Union européenne conformément au RGPD. Au fur et à mesure de l'évolution du cadre réglementaire et législatif, nous nous efforcerons de faire en sorte que nos clients et partenaires puissent continuer à profiter des avantages d'AWS, où qu'ils soient. Pour en savoir plus, consultez la FAQ sur le bouclier de protection des données UE-États-Unis.

Le rôle d'AWS dans le cadre du RGPD

En vertu du RGPD, AWS agit comme un sous-traitant et comme un responsable du traitement.

D'après l'article 32, les responsables du traitement et les sous-traitants doivent « mettre en œuvre des mesures techniques et organisationnelles appropriées » en tenant compte « de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques. » Le RGPD suggère précisément quels types d'actions de sécurité sont potentiellement nécessaires, notamment :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- la capacité de restaurer la disponibilité et l'accès aux données à caractère personnel dans les temps en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

AWS en tant que sous-traitant

Lorsque les clients et le réseau de partenaires AWS (APN) utilisent les services AWS pour traiter des données à caractère personnel dans leur contenu, AWS agit comme un sous-traitant. Les clients et partenaires APN peuvent utiliser les contrôles disponibles au sein des services AWS, y compris les contrôles de configuration de la sécurité, pour le traitement des données à caractère personnel. Dans ces circonstances, le client ou le partenaire APN peut agir en tant que responsable du traitement ou que sous-traitant, et AWS agit comme un sous-traitant ultérieur. L'addendum sur le traitement des données (DPA) conforme au RGPD d'AWS intègre les engagements d'AWS en tant que sous-traitant.

AWS en tant que responsable du traitement

Lorsqu'AWS collecte des données à caractère personnel et détermine les finalités et les moyens de traitement de ces données à caractère personnel, il agit en tant que responsable du traitement. Par exemple, lorsque AWS traite des informations de compte dans le cadre de l'enregistrement de comptes, de l'administration, de l'accès aux services ou des informations de contact pour le compte AWS afin de fournir une assistance au moyen des activités du support client, AWS agit en tant que responsable du traitement.

Modèle de sécurité à responsabilité partagée

La sécurité et la conformité sont une responsabilité partagée entre AWS et le client. Lorsque les clients transfèrent leurs systèmes informatiques et leurs données vers le cloud, les responsabilités en matière de sécurité sont partagées entre le client et le fournisseur de service cloud. Lorsque les clients migrent vers le cloud AWS, AWS est responsable de la protection de l'infrastructure globale exécutant tous les services proposés dans le cloud AWS. Pour les services extraits, tels qu'Amazon S3 et Amazon DynamoDB, AWS est également responsable de la sécurité du système d'exploitation et de la plateforme. Les clients et les partenaires APN, agissant en tant que responsables du traitement ou sous-traitants, sont responsables de l'ensemble des données qu'ils placent dans le cloud ou qu'ils relient au cloud. Cette distinction des responsabilités est communément désignée comme la sécurité du cloud par rapport à la sécurité dans le cloud. Ce modèle partagé peut aider à réduire la charge opérationnelle des clients et leur fournir la flexibilité et le contrôle nécessaires pour déployer leur infrastructure dans le cloud AWS. Pour en savoir plus, consultez le Modèle de responsabilité partagée d'AWS.

Le RGPD ne change pas le modèle de responsabilité partagée AWS, qui reste pertinent pour les clients et les partenaires APN qui se concentrent sur l'utilisation des services de cloud computing. Le modèle de responsabilité partagée est une approche pratique pour illustrer les différentes responsabilités d'AWS (en tant que sous-traitant ou sous-traitant ultérieur) et des clients ou partenaires APN (en tant que responsables du traitement ou sous-traitants) dans le cadre du RGPD.

Normes de sécurité et environnement à forte conformité

D'après le RGPD, les mesures techniques et organisationnelles appropriées peuvent devoir inclure « ...des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement », ainsi que des processus de restauration, de test et de gestion globale des risques fiables.

Programme de conformité d'AWS

AWS s'impose en permanence des normes élevées en matière de sécurité et de conformité, et ce, pour toutes les opérations menées partout dans le monde. La sécurité a toujours été notre priorité absolue, notre première mission. AWS fait régulièrement l'objet d'audits d'attestation menés par des tiers indépendants afin de garantir que les activités de contrôle fonctionnent comme prévu. Plus précisément, AWS fait l'objet d'audits par rapport à divers cadres de sécurité mondiaux et régionaux en fonction de la région et du secteur d'activité. À l'heure actuelle, AWS participe à plus de 50 programmes d'audit différents.

Les résultats de ces audits sont documentés par l'organisme d'évaluation et mis à la disposition de tous les clients AWS via AWS Artifact. AWS Artifact est un portail en libre-service gratuit qui permet d'accéder à la demande aux rapports de conformité AWS. Lorsque de nouveaux rapports sont publiés, ils sont accessibles dans AWS Artifact, ce qui permet aux clients de surveiller en permanence la sécurité et la conformité d'AWS avec un accès immédiat aux nouveaux rapports.

Les clients peuvent tirer parti de certifications et d'accréditations mondialement reconnues, preuves de notre conformité par rapport à des normes internationales rigoureuses telles que la norme ISO 27017 pour la sécurité du cloud, ISO 27018 pour la confidentialité du cloud, les normes SOC 1, SOC 2 et SOC 3, la norme PCI DSS de niveau 1, et bien d'autres. AWS aide également ses clients à respecter des normes de sécurité locales, par exemple la norme Common Cloud Computing Controls Catalogue (C5) du BSI (Office fédéral de la sécurité des technologies de l'information), particulièrement soutenue par le gouvernement allemand.

Pour en savoir plus sur les programmes de certification AWS, les rapports et les attestations tierces, consultez Programmes de conformité AWS. Pour obtenir des informations spécifiques au service, consultez Services AWS concernés.

Cloud Computing Compliance Controls Catalog

Cloud Computing Compliance Controls Catalog (C5) est un système d'attestation soutenu par le gouvernement allemand qui a été introduit en Allemagne par le BSI (Office fédéral de la sécurité des technologies de l'information). Il a été créé en vue d'aider les organisations à assurer une sécurité opérationnelle contre les cyberattaques courantes dans le cadre des recommandations de sécurité pour les fournisseurs de cloud du gouvernement allemand.

Les mesures techniques et organisationnelles de protection des données et les mesures de sécurité de l'information visent à garantir la confidentialité, l'intégrité et la disponibilité des données. La norme C5 définit les exigences de sécurité qui peuvent également être pertinentes pour la protection des données. Les clients AWS et leurs conseillers en conformité peuvent utiliser l'attestation C5 comme une ressource pour comprendre les services d'assurance de sécurité informatique que propose AWS lors de la migration des charges de travail vers le cloud. La norme C5 comprend un niveau de sécurité informatique équivalent à l'IT-Grundschutz et intègre en outre des contrôles spécifiques au cloud.

La norme C5 inclut des contrôles supplémentaires qui informent sur la localisation des données, l'allocation de services, la juridiction compétente, les certifications existantes, les obligations de transparence et la description du service dans son ensemble. Grâce à ces informations, vous êtes en mesure d'évaluer les réglementations juridiques (relatives à la confidentialité des données, par exemple), vos propres stratégies et les risques d'attaques dans le cadre de votre utilisation des services de cloud computing.

Contrôles d’accès aux données

L'article 25 du RGPD stipule que le responsable du traitement « doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. » Les mécanismes de contrôle d'accès AWS ci-dessous peuvent aider les clients à se conformer à cette exigence en autorisant seulement les administrateurs, utilisateurs et applications autorisés à accéder aux ressources AWS et aux données clients.

AWS Identity and Access Management

Lorsque vous créez un compte AWS, un compte utilisateur racine est automatiquement créé pour ce compte. Ce compte utilisateur dispose d'un accès complet à tous les services et ressources AWS de votre compte AWS. Au lieu d'utiliser ce compte pour les tâches quotidiennes, vous devez l'utiliser uniquement pour créer initialement des rôles et des comptes d'utilisateurs supplémentaires, ainsi que pour les activités administratives qui l'exigent. AWS recommande d'appliquer le principe du moindre privilège dès le début, c'est-à-dire de définir différents rôles et comptes d'utilisateurs pour différentes tâches, et de spécifier l'ensemble minimum d'autorisations requises pour effectuer chaque tâche. Cette approche est un mécanisme permettant de régler un concept clé introduit dans le RGPD : la protection des données dès la conception. Le service web AWS Identity and Access Management (IAM) peut être utilisé pour contrôler en toute sécurité l'accès à vos ressources AWS.

Les utilisateurs et les rôles définissent les identités IAM avec des autorisations spécifiques. Un utilisateur autorisé peut assumer un rôle IAM pour effectuer certaines tâches. Des informations d'identification temporaires sont créées lorsque le rôle est assumé. Par exemple, vous pouvez utiliser des rôles IAM pour fournir en toute sécurité des applications qui s'exécutent dans Amazon Elastic Compute Cloud (Amazon EC2) avec les informations d'identification temporaires requises pour accéder à d'autres ressources AWS, telles que les compartiments Amazon S3 et les bases de données Amazon Relational Database Service (Amazon RDS) ou Amazon DynamoDB. De même, les rôles d'exécution fournissent des fonctions AWS Lambda avec les autorisations nécessaires pour accéder à d'autres services et ressources AWS, tels qu'Amazon CloudWatch Logs pour la diffusion de journaux ou la lecture d'un message à partir d'une file d'attente Amazon Simple Queue Service (Amazon SQS). Lorsque vous créez un rôle, vous y ajoutez des stratégies afin de définir des autorisations.

Pour aider les clients à surveiller les stratégies de ressources et à identifier les ressources dont l'accès public ou entre comptes n'est pas prévu, IAM Access Analyzer peut être activé afin de

générer des résultats exhaustifs qui identifient les ressources accessibles depuis l'extérieur d'un compte AWS. IAM Access Analyzer évalue les stratégies de ressources en appliquant une inférence et une logique mathématique pour déterminer les chemins d'accès possibles autorisés par les stratégies. IAM Access Analyzer surveille en continu les stratégies mises à jour ou nouvelles, et analyse les autorisations octroyées à l'aide des stratégies pour les rôles IAM, mais aussi pour les ressources de services telles que les compartiments Amazon S3, les clés AWS Key Management Service (AWS KMS), les files d'attente Amazon SQS, ainsi que les fonctions Lambda.

Access Analyzer pour S3 vous avertit au sujet des compartiments configurés pour autoriser l'accès à toute personne sur Internet ou à d'autres comptes AWS, y compris les comptes AWS en dehors de votre organisation. Lorsque vous examinez un compartiment à risque dans Access Analyzer pour S3, vous pouvez bloquer tout accès public au compartiment en un seul clic. AWS recommande de bloquer tous les accès aux compartiments, sauf si vous avez besoin d'un accès public pour prendre en charge un cas d'utilisation précis. Avant de bloquer tout accès public, assurez-vous que vos applications continueront à fonctionner correctement sans accès public. Pour en savoir plus, consultez la section Utilisation d'Amazon S3 pour bloquer l'accès public.

IAM présente également les dernières informations consultées afin de vous aider à identifier les autorisations inutilisées, pour que vous puissiez les supprimer des entités associées. À l'aide des dernières informations consultées, il est possible d'affiner vos stratégies et d'autoriser l'accès uniquement aux services et aux actions nécessaires. Vous êtes ainsi mieux à même de vous conformer à la bonne pratique relative au principe du moindre privilège et de l'appliquer. Vous pouvez afficher les dernières informations consultées pour les entités ou les stratégies qui existent dans IAM ou dans l'ensemble d'un environnement AWS Organizations.

Jetons d'accès temporaires via AWS STS

Vous pouvez utiliser AWS Security Token Service (AWS STS) pour créer et fournir aux utilisateurs des informations d'identification de sécurité temporaires permettant de contrôler l'accès à vos ressources AWS. Les informations d'identification de sécurité temporaires ont un fonctionnement presque identique à celui des informations d'identification des clés d'accès à long terme que vous fournissez aux utilisateurs IAM, à quelques différences près :

- Les informations d'identification de sécurité temporaires sont réservées à une utilisation à court terme. Vous pouvez configurer leur durée de validité (de 15 minutes à 12 heures maximum). Quand les informations d'identification temporaires arrivent à expiration, AWS ne les reconnaît plus ou n'autorise plus aucun type d'accès à partir des demandes d'API effectuées avec elles.

- Les informations d'identification de sécurité temporaires ne sont pas stockées avec le compte d'utilisateur. Au lieu de cela, elles sont générées dynamiquement et fournies à l'utilisateur sur demande. Lorsque les informations d'identification de sécurité temporaires arrivent à expiration (ou avant), un utilisateur peut demander de nouvelles informations d'identification, s'il est autorisé à le faire.

Ces différences présentent les avantages ci-dessous lorsque vous utilisez des informations d'identification temporaires :

- Vous n'avez pas besoin de distribuer ni d'intégrer des informations d'identification de sécurité AWS à long terme avec une application.
- Les informations d'identification temporaires servent de base aux rôles et à la fédération d'identité. Vous pouvez fournir l'accès à vos ressources AWS aux utilisateurs en définissant une identité AWS temporaire pour eux.
- Les informations d'identification de sécurité temporaires ont une durée de vie personnalisable limitée. Pour cette raison, vous n'avez pas besoin de les renouveler ni de les révoquer explicitement lorsqu'elles ne sont plus nécessaires. Quand les informations d'identification de sécurité temporaires arrivent à expiration, elles ne peuvent pas être réutilisées. Vous pouvez spécifier la durée maximale pendant laquelle les informations d'identification sont valides.

Authentification multifacteur

Afin de renforcer la sécurité, vous pouvez ajouter une authentification à deux facteurs à votre compte AWS et aux utilisateurs IAM. SI l'authentification multifacteur (MFA) est activée, lorsque vous vous connectez à la console de gestion AWS, vous devez entrer votre nom d'utilisateur et votre mot de passe (le premier facteur), ainsi qu'une réponse d'authentification de votre dispositif MFA AWS (le deuxième facteur). Vous pouvez activer la MFA pour votre compte AWS et pour les utilisateurs IAM individuels que vous avez créés dans votre compte. Vous pouvez également utiliser la MFA pour contrôler l'accès aux API de service AWS.

Par exemple, vous pouvez définir une stratégie qui autorise un accès complet à toutes les opérations d'API AWS dans Amazon EC2, mais refuse explicitement l'accès à des opérations d'API spécifiques, telles que `StopInstances` et `TerminateInstances`, si l'utilisateur n'est pas authentifié par 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}
               }
           }
       }
}
```

Pour ajouter une couche de sécurité supplémentaire à vos compartiments Amazon S3, vous pouvez configurer la fonction Supprimer MFA, qui nécessite une authentification supplémentaire pour modifier l'état de gestion des versions d'un compartiment et supprimer définitivement une version d'objet. La fonction Supprimer MFA renforce la sécurité en cas de mise en danger des informations d'identification de sécurité.

Pour utiliser la fonction Supprimer MFA, vous pouvez utiliser un dispositif MFA matériel ou virtuel afin de générer un code d'authentification. Consultez la page Authentification multifacteur pour obtenir la liste des dispositifs MFA matériels ou virtuels pris en charge.

Accès aux ressources AWS

Afin de mettre en œuvre un accès détaillé à vos ressources AWS, vous pouvez accorder différents niveaux d'autorisations à différentes personnes pour différentes ressources. Par exemple, vous pouvez accorder uniquement à certains utilisateurs un accès complet à Amazon EC2, Amazon S3, DynamoDB, Amazon Redshift et à d'autres services AWS.

Pour d'autres utilisateurs, vous pouvez accorder un accès en lecture seule à certains compartiments Amazon S3 uniquement, l'autorisation d'administrer uniquement certaines instances Amazon EC2 ou un accès uniquement à vos informations de facturation.

La stratégie ci-dessous est un exemple de méthode à appliquer pour autoriser toutes les actions sur un compartiment Amazon S3 spécifique et refuser explicitement l'accès à chaque service AWS qui n'est pas un service 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/*”
                 ]
               }
            ]
}
```

Vous pouvez attacher une stratégie à un compte utilisateur ou à un rôle. Pour obtenir d'autres exemples de stratégies IAM, consultez la section Exemples de stratégies basées sur l'identité IAM.

Définition des limites pour l'accès aux services régionaux

En tant que client, vous restez propriétaire de votre contenu et vous sélectionnez quels services AWS peuvent traiter, stocker et héberger votre contenu. AWS ne consulte ni n'utilise votre contenu à quelque fin que ce soit sans votre consentement. Sur la base du modèle de responsabilité partagée, vous choisissez les régions AWS dans lesquelles votre contenu est stocké et pouvez ainsi

déployer les services AWS dans les emplacements de votre choix, conformément à vos exigences géographiques spécifiques. Par exemple, si vous souhaitez vous assurer que votre contenu se trouve uniquement en Europe, vous pouvez choisir de déployer les services AWS exclusivement dans l'une des régions AWS européennes.

Les stratégies IAM fournissent un mécanisme simple de limitation de l'accès aux services dans certaines régions. Vous pouvez ajouter une condition globale (`aws:RequestedRegion`) aux stratégies IAM attachées à vos entités IAM afin de l'appliquer à tous les services AWS. Par exemple, la stratégie ci-dessous utilise l'élément `NotAction` avec l'effet `Deny`, qui refuse explicitement l'accès à toutes les actions non répertoriées dans l'instruction si la région demandée n'est pas européenne. Les actions dans les services CloudFront, IAM, Amazon Route 53 et AWS Support ne doivent pas être refusées car il s'agit de services AWS de niveau international fréquemment utilisés.

```
{
   “Version”: “2012-10-17”,
   “Statement”: [
       {
          “Sid”: “DenyAllOutsideRequestedRegions”,
          “Effect”: “Deny”,
          “NotAction”: [
               “cloudfront:*”,
               “iam:*”,
               ”route53:*”,
               “support:*”
           ],
           “Resource”: “*”,
           “Condition”: {
              “StringNotLike”: {
                  “aws:RequestedRegion”: [
                        “eu-*”
                  ]
               }
            }
      }
    ]
}
```

Cet exemple de stratégie IAM peut également être implémenté en tant que stratégie de contrôle de service dans AWS Organizations, qui définit les limites d'autorisations appliquées à des

comptes AWS ou à des unités d'organisation (UO) spécifiques au sein d'une organisation. Vous pouvez ainsi contrôler l'accès des utilisateurs aux services régionaux dans des environnements complexes à plusieurs comptes.

Il existe des fonctionnalités de géolimitation pour les régions récemment lancées. Les régions introduites après le 20 mars 2019 sont désactivées par défaut. Vous devez activer ces régions avant de pouvoir les utiliser. Si une région AWS est désactivée par défaut, vous pouvez l'activer et la désactiver à l'aide de la console de gestion AWS. Quand vous activez et désactivez des régions AWS, vous pouvez contrôler si les utilisateurs de votre compte AWS peuvent accéder aux ressources dans cette région. Pour en savoir plus, consultez Gestion des régions AWS.

Contrôle de l'accès aux applications web et mobiles

AWS fournit des services permettant de gérer le contrôle d'accès aux données au sein des applications des clients. Si vous devez ajouter des fonctions de connexion utilisateur et de contrôle d'accès à vos applications web et mobiles, vous pouvez utiliser Amazon Cognito. Les groupes d'utilisateurs d'Amazon Cognito fournissent un répertoire d'utilisateurs sécurisé qui s'étend à des centaines de millions d'utilisateurs. Vous pouvez ajouter l'authentification multifacteur (MFA) à un groupe d'utilisateurs pour protéger l'identité de ces utilisateurs. Vous pouvez également utiliser l'authentification adaptative avec son modèle basé sur le risque pour prévoir quand un autre facteur d'authentification sera nécessaire.

Grâce aux groupes d'identités Amazon Cognito (identités fédérées), vous pouvez voir qui a accédé à vos ressources et d'où provient l'accès (application mobile ou web). Vous pouvez utiliser ces informations pour créer des rôles et des stratégies IAM qui autorisent ou refusent l'accès à une ressource en fonction du type d'origine d'accès (application mobile ou web) et du fournisseur d'identité.

Surveillance et journalisation

L'article 30 du RGPD stipule que « ...chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. » Cet article comprend également des détails sur les informations qui doivent être enregistrées lorsque vous surveillez le traitement de toutes les données à caractère personnel. Puisque les sous-traitants et les responsables du traitement sont également tenus d'envoyer en temps opportun des notifications en cas de violations, il est important de détecter rapidement les incidents. Pour aider les clients à répondre à ces exigences, AWS propose les services de surveillance et de journalisation ci-après.

Gestion et configuration des ressources avec AWS Config

Grâce à AWS Config, vous bénéficiez d'un aperçu détaillé de la configuration de nombreux types de ressources AWS de votre compte AWS. Cette vue illustre la manière dont les ressources sont reliées entre elles et la façon dont elles étaient configurées précédemment, afin que vous puissiez voir la façon dont les configurations et relations changent dans le temps.

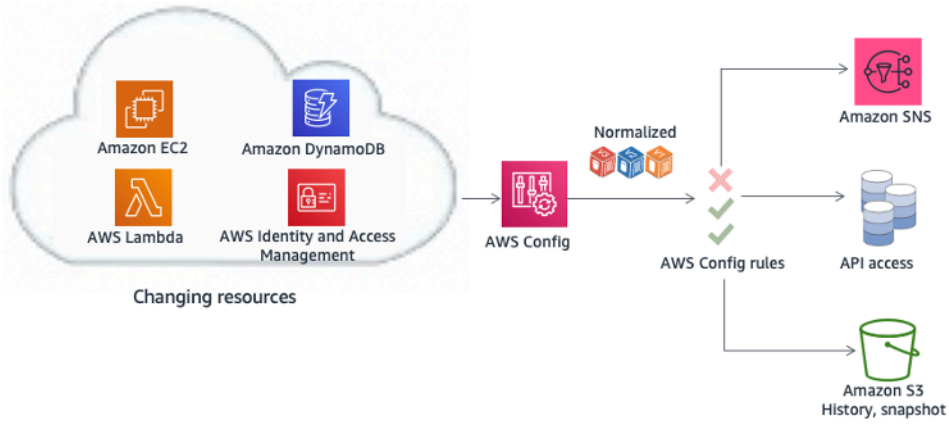

Figure 1 – Surveillance des modifications de configuration au fil du temps avec AWS Config

Une ressource AWS est une entité avec laquelle vous pouvez travailler dans AWS, comme une instance Amazon EC2, un volume Amazon Elastic Block Store (Amazon EBS), un groupe de sécurité ou un Amazon Virtual Private Cloud (Amazon VPC). Pour obtenir une liste complète des ressources AWS prises en charge par AWS Config, consultez la page Types de ressource AWS pris en charge.

AWS Config permet d'effectuer les actions suivantes :

- Évaluer les configurations de vos ressources AWS pour vérifier que les paramètres sont corrects.

- Obtenir un instantané des configurations actuelles des ressources prises en charge qui sont associées à votre compte AWS.
- Récupérer des configurations d'une ou plusieurs des ressources qui existent dans votre compte.
- Récupérer les historiques de configuration d'une ou plusieurs ressources.
- Recevoir une notification quand une ressource est créée, modifiée ou supprimée.
- Afficher les relations entre les ressources. Par exemple, vous pouvez rechercher toutes les ressources qui utilisent un groupe de sécurité particulier.

Audits de conformité et analyse de sécurité

Grâce à AWS CloudTrail, vous pouvez surveiller en permanence l'activité du compte AWS. Un historique des appels d'API AWS pour votre compte est capturé, notamment les appels d'API effectués à l'aide de la console de gestion AWS, des kits SDK AWS, des outils de ligne de commande, ainsi que des services AWS de plus haut niveau. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé les API AWS pour des services prenant en charge CloudTrail, l'adresse IP source d'origine des appels, ainsi que le moment où les appels ont eu lieu. Vous pouvez intégrer CloudTrail dans des applications utilisant l'API, automatiser la création de journaux d'activité pour votre organisation, vérifier le statut des journaux d'activité et contrôler de quelle manière des administrateurs activent et désactivent la journalisation de CloudTrail.

Les journaux CloudTrail peuvent être agrégés à partir de plusieurs régions et de plusieurs comptes AWS dans un seul compartiment Amazon S3. AWS recommande de rédiger des journaux, en particulier des journaux AWS CloudTrail, dans un compartiment Amazon S3 avec un accès restreint dans un compte AWS désigné pour la journalisation (Log Archive). Les autorisations sur le compartiment doivent empêcher la suppression des journaux et ils doivent également être chiffrés au repos à l'aide du chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) ou des clés gérées par AWS KMS (SSE-KMS). La validation de l'intégrité des fichiers journaux CloudTrail peut être utilisée pour déterminer si un fichier journal a été modifié ou supprimé, ou s'il reste inchangé après avoir été livré par CloudTrail. Cette fonction est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est alors difficile de modifier, de supprimer ou de falsifier des fichiers journaux de CT par traitement informatique sans détection. Vous pouvez utiliser l'interface de ligne de commande AWS (AWS CLI) pour valider les fichiers à l'emplacement où CloudTrail les a livrés.

Les journaux CloudTrail agrégés dans un compartiment Amazon S3 peuvent être analysés à des fins d'audit ou pour des activités de dépannage. Une fois les journaux centralisés, vous pouvez intégrer

des solutions SIEM (solutions de gestion des événements et informations de sécurité) ou utiliser des services AWS, tels qu'Amazon Athena ou CloudTrail Insights, pour les analyser et les visualiser à l'aide des tableaux de bord Amazon QuickSight. Une fois que vous avez centralisé les journaux CloudTrail, vous pouvez également utiliser le même compte Log Archive pour centraliser les journaux provenant d'autres sources, telles que CloudWatch Logs et les équilibreurs de charge AWS.

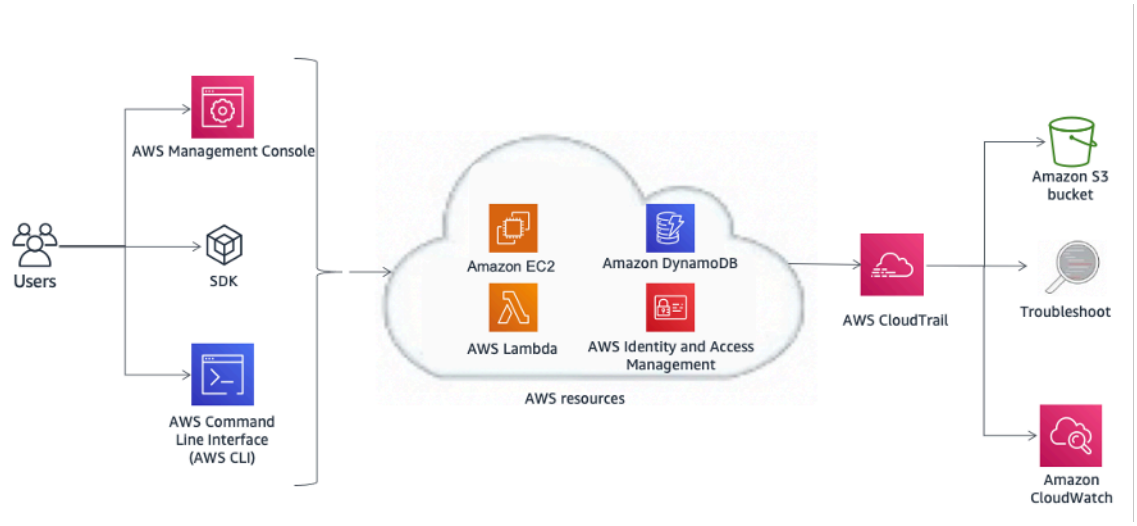

Figure 2 – Exemple d'architecture pour l'audit de conformité et les analyses de sécurité avec AWS CloudTrail

Les journaux AWS CloudTrail peuvent également déclencher des événements Amazon CloudWatch préconfigurés. Vous pouvez utiliser ces événements pour informer les utilisateurs ou les systèmes qu'un événement s'est produit, ou pour des actions de remédiation. Par exemple, si vous souhaitez surveiller les activités sur vos instances Amazon EC2, vous pouvez créer une règle CloudWatch Event. Lorsqu'une activité spécifique se produit sur l'instance Amazon EC2 et que l'événement est enregistré dans les journaux, la règle déclenche une fonction AWS Lambda, qui envoie à l'administrateur une notification par e-mail concernant l'événement. (Voir la figure 3.) L'e-mail comprend des détails tels que le moment où l'événement s'est produit, l'utilisateur qui a effectué l'action, les détails Amazon EC2, etc. Le diagramme suivant montre l'architecture de la notification d'événement.

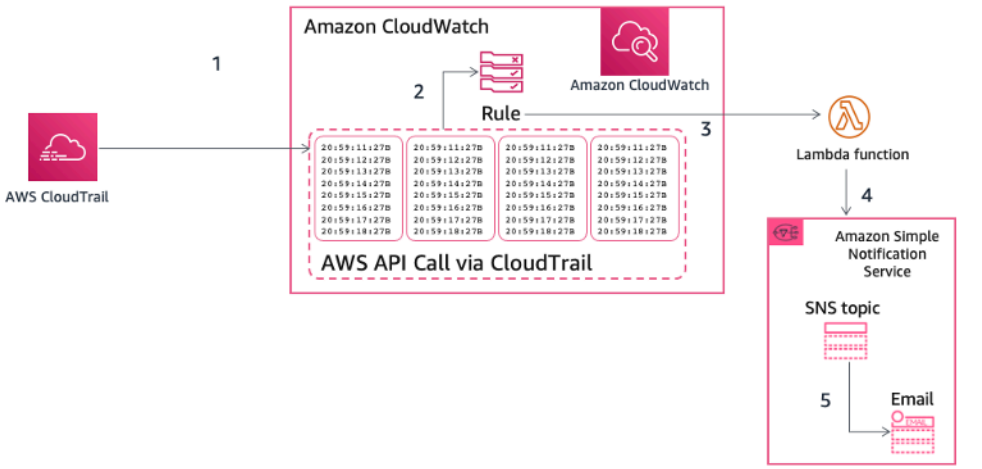

Figure 3 – Exemple de notification d'événement AWS CloudTrail

Collecte et traitement des journaux

CloudWatch Logs peut être utilisé pour surveiller et stocker vos fichiers journaux, et y accéder, à partir d'instances Amazon EC2, AWS CloudTrail, Route 53 et d'autres sources. Consultez la page de documentation sur les services AWS qui publient des journaux dans CloudWatch Logs.

Les informations dans les fichiers journaux incluent, par exemple :

- la journalisation granulaire des accès aux objets Amazon S3 ;
- des informations détaillées sur les flux du réseau via VPC-FlowLogs ;
- la vérification de la configuration basée sur des règles et les actions avec des règles AWS Config ;
- le filtrage et la surveillance de l'accès HTTP aux applications avec les fonctions de pare-feu d'application web (WAF) dans CloudFront.

Les métriques et les journaux d'application personnalisés peuvent également être publiés dans CloudWatch Logs en installant CloudWatch Agent sur des instances Amazon EC2 ou des serveurs sur site.

Les journaux peuvent être analysés de manière interactive à l'aide de CloudWatch Logs Insights, en effectuant des requêtes pour vous aider à répondre plus efficacement aux problèmes opérationnels.

Les journaux CloudWatch Logs peuvent être traités en quasi-temps réel en configurant des filtres d'abonnement et transmis à d'autres services tels qu'un cluster Amazon OpenSearch Service

(OpenSearch Service), un flux Amazon Kinesis, un flux Amazon Kinesis Data Firehose ou une fonction Lambda pour des applications personnalisées de traitement, d'analyse ou de chargement vers d'autres systèmes.

Les filtres de métriques CloudWatch peuvent être utilisés pour définir des modèles à rechercher dans les données de journal, les transformer en métriques CloudWatch numériques et configurer des alarmes en fonction des besoins de votre entreprise. Par exemple, conformément à la recommandation d'AWS de ne pas utiliser l'utilisateur racine pour les tâches quotidiennes, il est possible de configurer un filtre de métrique CloudWatch spécifique sur un journal CloudTrail (envoyé à CloudWatch Logs) afin de créer une métrique personnalisée et de configurer une alarme pour notifier le parties prenantes lorsque les informations d'identification racine sont utilisées pour accéder à votre compte AWS.

Les journaux tels que les journaux d'accès au serveur Amazon S3, les journaux d'accès Elastic Load Balancing, les journaux de flux VPC et les journaux de flux AWS Global Accelerator peuvent être envoyés directement dans un compartiment Amazon S3. Par exemple, lorsque vous activez les journaux d'accès au serveur Amazon Simple Storage Service, vous pouvez obtenir des informations détaillées concernant les demandes adressées à votre compartiment Amazon S3. Un enregistrement du journal d'accès contient des détails sur la demande, tels que le type de demande, les ressources spécifiées dans la demande, ainsi que l'heure et la date du traitement de la demande. Pour en savoir plus sur les contenus d'un fichier journal, consultez Format des journaux d'accès au serveur Amazon Simple Storage Service dans le manuel du développeur Amazon Simple Storage Service. Les journaux d'accès au serveur sont utiles pour de nombreuses applications, car ils fournissent aux propriétaires du compartiment des renseignements sur la nature des demandes effectuées par les clients qu'ils ne contrôlent pas. Par défaut, Amazon S3 ne collecte pas les journaux d'accès au service. Toutefois, lorsque vous activez la journalisation, Amazon S3 transmet habituellement les journaux d'accès à votre compartiment en quelques heures. Si vous avez besoin d'une livraison plus rapide ou si vous devez envoyer des journaux vers plusieurs destinations, envisagez d'utiliser des journaux CloudTrail ou une combinaison de journaux CloudTrail et Amazon S3. Les journaux peuvent être chiffrés au repos en configurant le chiffrement des objets par défaut dans le compartiment de destination. Les objets sont chiffrés au moyen du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) ou des clés principales client (clés CMK) stockées dans AWS Key Management Service (AWS KMS).

Les journaux stockés dans un compartiment Amazon S3 peuvent être interrogés et analysés à l'aide d'Amazon Athena. Amazon Athena est un service d'interrogation interactif qui permet d'analyser des données dans Amazon S3 à l'aide d'une requête SQL standard. Vous pouvez utiliser Athena pour exécuter des requêtes ad hoc à l'aide du langage SQL ANSI, sans avoir besoin d'agréger ou

de charger les données dans Athena. Athena peut traiter des jeux de données non structurés, semi-structurés et structurés et s'intègre à Amazon QuickSight pour une visualisation facile.

Les journaux constituent également une source d'informations utile pour la détection automatique des menaces. Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les événements provenant de plusieurs sources, telles que les journaux de flux VPC, les journaux d'événements de gestion CloudTrail, les journaux d'événements de données CloudTrail Amazon S3 et les journaux DNS. Il utilise des flux de détection de menaces, comme les listes d'adresses IP et de domaines malveillants, ainsi que le machine learning pour identifier toute activité inattendue et potentiellement non autorisée et malveillante au sein de votre environnement AWS. Lorsque vous activez GuardDuty dans une région, il commence immédiatement à analyser vos journaux d'événements CloudTrail. Il consomme la gestion CloudTrail et les événements de données Amazon S3 directement à partir de CloudTrail via un flux d'événements indépendant et dupliqué.

Découverte et protection des données à grande échelle avec Amazon Macie

L'article 32 du RGPD stipule que « ...le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : [...]

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

[...]

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

Il est essentiel de disposer d'un processus continu de classification des données pour adapter le traitement des données de sécurité à la nature des données. Si votre organisation gère des données sensibles, surveillez les emplacements de stockage de ces données, protégez ces dernières comme il se doit et démontrez que vous appliquez les contrôles de sécurité et de confidentialité des données nécessaires pour répondre aux exigences de conformité réglementaire. Afin d'aider le client à identifier et à protéger ses données sensibles à grande échelle, AWS propose Amazon Macie, un service totalement géré de sécurité et de confidentialité des données qui utilise des modèles de correspondance de modèles et de machine learning pour la détection des données d'identification personnelle (PII) en vue de détecter et de protéger les données sensibles stockées dans des

compartiments S3. Amazon Macie analyse ces compartiments et fournit une catégorisation des données à l'aide d'identificateurs de données gérés conçus pour détecter plusieurs catégories de données sensibles. Macie peut détecter les données d'identification personnelle telles que le nom complet, l'adresse e-mail, la date de naissance, le numéro d'identification national, d'identification ou de référence du contribuable, etc. Le client peut définir des identificateurs de données personnalisés qui reflètent les scénarios particuliers de son organisation (par exemple, les numéros de compte client ou la classification interne des données).

Amazon Macie évalue en permanence l'objet à l'intérieur des compartiments et fournit automatiquement un résumé des résultats (figure 4) pour toutes les données non chiffrées ou accessibles au public découvertes qui correspondent à la catégorie de données définie. Ces données peuvent inclure des alertes pour tout objet ou compartiment non chiffré et accessible au public partagé avec des comptes AWS en dehors de ceux que vous avez définis dans AWS Organizations. Amazon Macie est intégré à d'autres services AWS, tels que AWS Security Hub, afin de générer des résultats de sécurité exploitables et de fournir une action automatique et réactive en fonction dudit résultat (figure 5).

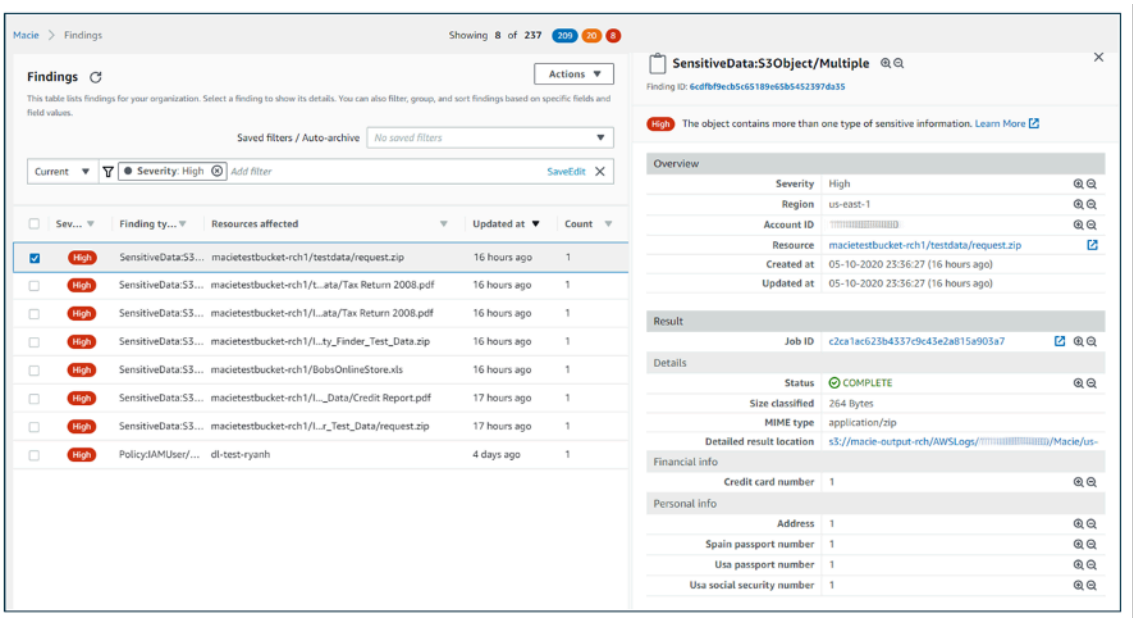

Figure 4 – Inspections des données et exemple de résultats

Gestion centralisée de la sécurité

De nombreuses organisations sont confrontées à des difficultés liées à la visibilité et à la gestion centralisée de leurs environnements. À mesure que votre empreinte opérationnelle croît, ces difficultés peuvent s'aggraver si vous n'évaluez pas attentivement vos systèmes de sécurité. Le

manque de connaissances, combiné à une gestion décentralisée et inégale des processus de gouvernance et de sécurité, peut rendre votre environnement vulnérable.

Certains outils fournis par AWS aident à répondre à certaines des exigences les plus complexes en matière de gestion et de gouvernance informatiques, tandis que d'autres prennent en charge une approche de protection des données dès la conception.

AWS Control Tower fournit le moyen le plus simple de configurer et de gérer un nouvel environnement AWS multicomptes sécurisé. Il automatise la configuration d'une zone de destination, qui est un environnement multicomptes basé sur de bonnes pratiques, et permet la gouvernance à l'aide de barrières de protection que vous pouvez choisir parmi une liste prédéfinie. Les barrières de protection mettent en œuvre des règles de gouvernance pour la sécurité, la conformité et les opérations. AWS Control Tower fournit la gestion des identités à l'aide du répertoire par défaut AWS IAM Identity Center (IAM Identity Center) et permet l'audit entre comptes en utilisant IAM Identity Center et IAM. Il centralise également les journaux provenant de CloudTrail et les journaux AWS Config, qui sont stockés dans Amazon S3.

AWS Security Hub est un autre service qui prend en charge la centralisation et peut améliorer la visibilité au sein d'une organisation. Security Hub centralise et hiérarchise les résultats de sécurité et de conformité de l'ensemble des comptes et services AWS, tels qu'Amazon GuardDuty et Amazon Inspector. Il peut être intégré à un logiciel de sécurité de partenaires tiers afin de vous aider à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires.

Amazon GuardDuty est un service intelligent de détection des menaces qui peut aider les clients à surveiller et à protéger de manière plus précise et facile leurs comptes et charges de travail AWS, ainsi que leurs données stockées dans Amazon S3. GuardDuty analyse des milliards d'événements sur vos comptes AWS à partir de plusieurs sources, notamment les événements de gestion AWS CloudTrail, les événements de données CloudTrail Amazon S3, les journaux de flux Amazon Virtual Private Cloud et les journaux DNS. Par exemple, il détecte les appels d'API inhabituels, les communications sortantes suspectes vers des adresses IP malveillantes connues ou les vols de données potentiels utilisant des requêtes DNS comme mécanisme de transport. GuardDuty est en mesure de fournir des résultats plus précis en tirant parti des renseignements sur les menaces récupérés par machine learning et des partenaires de sécurité tiers.

Amazon Inspector est un service automatique d'évaluation de la sécurité qui permet d'améliorer la sécurité et la conformité des applications déployées sur les instances Amazon EC2. Amazon Inspector évalue automatiquement les applications afin de déterminer leur exposition et de détecter les éventuelles failles ou les écarts par rapport aux bonnes pratiques. Après avoir effectué

une évaluation, Amazon Inspector produit une liste détaillée de constatations en matière de sécurité, classées par niveau de gravité.

Amazon CloudWatch Events permet de configurer votre compte AWS pour envoyer des événements vers d'autres comptes AWS ou pour devenir un récepteur d'événements provenant d'autres comptes ou organisations. Ce mécanisme peut être très utile pour mettre en œuvre des scénarios de réponse aux incidents entre comptes, en prenant des mesures correctives opportunes (par exemple, en appelant une fonction Lambda ou en exécutant une commande sur une instance Amazon EC2) chaque fois qu'un incident de sécurité se produit.

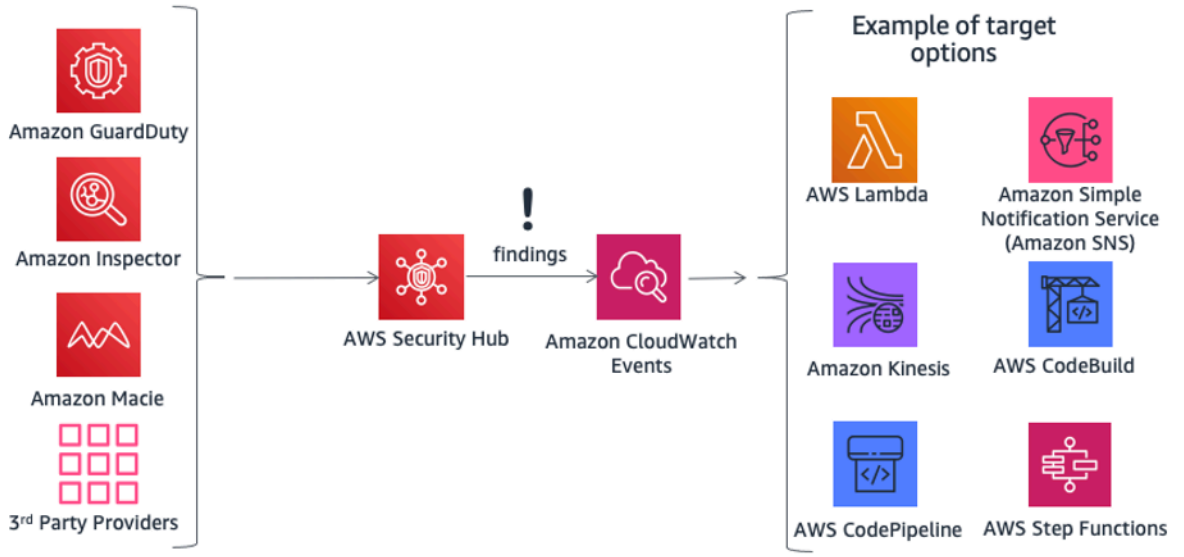

Figure 5 – Mesures prises avec AWS Security Hub et Amazon CloudWatch Events

AWS Organizations vous aide à gérer et à gouverner de manière centralisée des environnements complexes. Il permet de contrôler l'accès, la conformité et la sécurité dans un environnement multicomptes. AWS Organizations prend en charge les politiques de contrôle des services, qui définissent les actions de service AWS disponibles pour une utilisation avec des comptes ou des unités d'organisation (UO) spécifiques au sein d'une organisation.

AWS Systems Manager vous donne la visibilité et le contrôle de votre infrastructure sur AWS. Vous pouvez afficher les données opérationnelles de plusieurs services AWS à partir d'une console unifiée et automatiser les tâches opérationnelles entre ces services. Vous pouvez obtenir des informations à propos des activités d'API récentes, des modifications de configuration des ressources, des alertes opérationnelles, de l'inventaire des logiciels et de l'état de conformité des correctifs. Grâce à l'intégration à d'autres services AWS, vous pouvez également prendre des mesures sur les ressources en fonction de vos besoins opérationnels, afin de rendre votre environnement conforme.

Par exemple, en intégrant Amazon Inspector à AWS Systems Manager, les évaluations de sécurité sont simplifiées et automatisées, car vous pouvez installer l'agent Amazon Inspector automatiquement à l'aide d'Amazon Elastic Compute Cloud Systems Manager lorsqu'une instance Amazon EC2 est lancée. Vous pouvez également effectuer des corrections automatiques par rapport aux résultats d'Amazon Inspector à l'aide des fonctions Amazon EC2 System Manager et Lambda.

Protection de vos données sur AWS

L'article 32 du RGPD stipule que les organisations doivent mettre « ...en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris (...) la pseudonymisation et le chiffrement des données à caractère personnel [...]. » En outre, les organisations doivent assurer une protection contre la « divulgation non autorisée de données à caractère personnel (...) ou l'accès non autorisé à de telles données. »

Le chiffrement réduit les risques associés au stockage des données à caractère personnel car ces données sont illisibles sans la bonne clé. Une stratégie de chiffrement complète peut aider à atténuer l'impact de divers événements de sécurité, y compris certaines failles de sécurité.

Chiffrement des données au repos

Le chiffrement des données au repos est essentiel pour la conformité réglementaire et la protection des données. Il permet de garantir que les données sensibles stockées sur des disques ne sont pas lisibles par des utilisateurs ou des applications sans une clé valide. AWS propose plusieurs options de chiffrement au repos et de gestion des clés de chiffrement. Par exemple, vous pouvez utiliser le kit SDK AWS Encryption avec une clé CMK créée et gérée dans AWS KMS pour chiffrer des données arbitraires.

Les données chiffrées peuvent être stockées en toute sécurité au repos ; seule une partie disposant d'un accès autorisé à la clé CMK peut les déchiffrer. En conséquence, vous obtenez des données confidentielles chiffrées par enveloppe, des mécanismes de stratégie pour l'autorisation et le chiffrement authentifié, ainsi que la journalisation d'audit par AWS CloudTrail. Certains services de base AWS disposent de fonctions de chiffrement au repos intégrées, offrant la possibilité de chiffrer les données avant qu'elles ne soient écrites sur un espace de stockage non volatil. Par exemple, vous pouvez chiffrer des volumes Amazon EBS et configurer des compartiments Amazon S3 pour un chiffrement côté serveur (SSE) en utilisant un chiffrement AES-256. Amazon S3 prend également en charge le chiffrement côté client, qui permet de chiffrer les données avant de les envoyer à Amazon S3. Les kits SDK AWS prennent en charge le chiffrement côté client afin de faciliter les opérations de chiffrement et de déchiffrement des objets. Amazon RDS prend également en charge le chiffrement transparent des données (Transparent Data Encryption ou TDE).

Il est possible de chiffrer les données des stockages d'instance Linux Amazon EC2 à l'aide de bibliothèques Linux intégrées. Cette méthode permet de chiffrer les fichiers de façon transparente, ce

qui protège les données confidentielles. Par conséquent, les applications qui traitent les données ne remarquent pas le chiffrement au niveau du disque.

Vous pouvez employer deux méthodes pour chiffrer des fichiers sur des stockages d'instances.

- Chiffrement de disque : grâce à cette méthode, le disque, ou le bloc dans le disque, est chiffré à l'aide d'une ou plusieurs clés de chiffrement. Le chiffrement de disque se fait sous le niveau du système de fichiers, ne dépend pas du système d'exploitation et cache les informations des répertoires et fichiers, comme leur nom et leur taille. Par exemple, l'Encrypting File System est une extension Microsoft pour le système NTFS (New Technology File System) du système d'exploitation Windows NT qui permet de chiffrer un disque.
- Chiffrement du système de fichiers : grâce à cette méthode, au lieu de chiffrer tout le disque ou toute la partition, seuls les fichiers et les répertoires sont chiffrés. Le chiffrement au niveau du système de fichiers fonctionne sur le système de fichiers et est portable sur différents systèmes d'exploitation.

Pour les volumes de stockage d'instance SSD NVMe (Non-Volatile Memory Express), le chiffrement du disque est l'option par défaut. Les données dans le volume de stockage d'instance NVMe sont chiffrées à l'aide d'un chiffrement par blocs XTS-AES-256 implémenté dans un module matériel sur l'instance. Les clés de chiffrement sont générées à l'aide du module matériel et sont uniques pour chaque périphérique de stockage d'instance NVMe. Toutes les clés de chiffrement sont détruites lorsque l'instance est arrêtée ou résiliée et ne peuvent pas être récupérées. Vous ne pouvez pas utiliser vos propres clés de chiffrement.

Chiffrement des données en transit

AWS recommande vivement de chiffrer les données en transit entre deux systèmes, y compris les ressources internes et externes à AWS.

Lorsque vous créez un compte AWS, une portion du cloud AWS isolée logiquement, à savoir Amazon Virtual Private Cloud (Amazon VPC), y est allouée. Vous pouvez y lancer des ressources AWS dans un réseau virtuel que vous définissez. Vous conservez ainsi la totale maîtrise de votre environnement de mise en réseau virtuel, y compris pour la sélection de votre propre plage d'adresses IP, la création de sous-réseaux et la configuration de tables de routage et de passerelles réseau. En outre, vous pouvez créer une connexion VPN (Virtual Private Network) matérielle entre le centre de données de votre entreprise et votre Amazon VPC, et exploiter ainsi le cloud AWS comme une extension de votre centre de données d'entreprise.

Pour protéger la communication entre votre Amazon VPC et votre centre de données d'entreprise, vous pouvez choisir, parmi plusieurs options de connectivité VPN, celle qui correspond le mieux à vos besoins. Le VPN client AWS peut être utilisé pour autoriser un accès sécurisé à vos ressources AWS à l'aide de services VPN basés sur le client. Il est également possible d'utiliser une appliance VPN logicielle tierce disponible sur AWS Marketplace, à installer sur une instance Amazon EC2 de votre Amazon VPC. Sinon, vous pouvez créer une connexion VPN IPsec afin de protéger la communication entre votre VPC et votre réseau distant. Vous pouvez aussi utiliser AWS Direct Connect pour établir une connexion privée dédiée depuis un réseau distant vers votre Amazon VPC. Cette connexion peut être combinée à un AWS Site-to-Site VPN afin de créer une connexion privée à chiffrement IPsec.

AWS fournit des points de terminaison HTTPS utilisant le protocole TLS pour la communication, qui permet le chiffrement en transit lorsque vous utilisez des API AWS. Il est aussi possible d'utiliser le service AWS Certificate Manager (ACM) afin de générer, de gérer et de déployer les certificats privés et publics que vous utilisez en vue d'établir un transport chiffré de vos charges de travail entre les systèmes. Elastic Load Balancing est intégré à ACM pour prendre en charge les protocoles HTTPS. Si votre contenu est distribué via Amazon CloudFront, les points de terminaison chiffrés sont pris en charge.

Outils de chiffrement

AWS propose divers services, outils et mécanismes évolutifs de chiffrement des données afin que vous puissiez protéger vos données stockées et traitées sur AWS. Pour en savoir plus sur les fonctionnalités et la confidentialité du service AWS, consultez Capacités de service AWS pour la protection de la vie privée.

Les services de chiffrement d'AWS utilisent un large éventail de technologies de chiffrement et de stockage conçues pour préserver l'intégrité de vos données au repos ou en transit. AWS propose quatre principaux outils destinés aux opérations de chiffrement.

- AWS Key Management Service (AWS KMS) est un service géré AWS qui génère et gère des clés principales et des clés de données. AWS KMS est intégré à de nombreux services AWS afin de fournir un chiffrement des données côté serveur à l'aide de clés AWS KMS provenant de comptes clients. Les modules de sécurité matériels AWS KMS sont certifiés FIPS 140-2 niveau 2.
- AWS CloudHSM fournit des modules de sécurité matériels certifiés FIPS 140-2 niveau 3. Ceux-ci stockent en toute sécurité diverses clés de chiffrement autogérées, y compris les clés principales et les clés de données.

- Services et outils de chiffrement AWS
  - Le kit SDK AWS Encryption fournit une bibliothèque de chiffrement côté client permettant d'implémenter des opérations de chiffrement et de déchiffrement sur tous les types de données.
  - Amazon DynamoDB Encryption Client fournit une bibliothèque de chiffrement côté client permettant de chiffrer les tables de données avant de les envoyer à un service de base de données, tel qu'Amazon DynamoDB.

AWS Key Management Service

AWS Key Management Service est un service géré qui facilite la création et le contrôle des clés de chiffrement utilisées pour chiffrer vos données, et utilise des modules de sécurité matériels (HSM) pour protéger la sécurité de vos clés. AWS KMS est intégré à plusieurs autres services AWS afin que vous puissiez protéger les données que vous stockez avec ces services. AWS KMS est également intégré à AWS CloudTrail de façon à vous fournir des journaux de toutes vos utilisations de clés selon vos besoins réglementaires et de conformité.

Vous pouvez en toute simplicité créer, importer et renouveler des clés, mais aussi définir des stratégies d'utilisation et réaliser un audit de l'utilisation à partir d'AWS Management Console, ou encore à l'aide du kit SDK AWS ou de l'interface de ligne de commande AWS (AWS CLI).

Les clés CMK dans AWS KMS, qu'elles soient importées par vos soins ou créées pour vous par KMS, sont conservées dans un stockage hautement durable et dans un format chiffré, ce qui permet de les utiliser quand cela est nécessaire. Vous pouvez configurer KMS afin qu'il effectue une rotation automatique des clés CMK créées dans KMS une fois par an, sans que vous ayez à chiffrer de nouveau les données déjà chiffrées à l'aide de votre clé principale. Vous n'avez pas besoin de garder une trace des anciennes versions de vos clés CMK, puisque KMS les conserve pour le déchiffrement automatique des données préalablement chiffrées.

Pour n'importe quelle clé CMK dans AWS KMS, vous pouvez contrôler qui a accès à ces clés et les services avec lesquels elles peuvent être utilisées au moyen d'un certain nombre de contrôles d'accès, y compris des autorisations et des conditions de stratégie de clé au sein de stratégies de clés ou de stratégies IAM. Vous pouvez également importer des clés depuis votre propre infrastructure de gestion de clés et les utiliser dans KMS.

Par exemple, la stratégie ci-dessous utilise la condition `kms:ViaService` afin d'autoriser l'utilisation d'une clé CMK gérée par le client pour les actions spécifiées uniquement lorsque la demande provient d'Amazon EC2 ou d'Amazon RDS dans une région spécifique (us-west-2) au nom d'un utilisateur spécifique (`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”
                        ]
                     }
               }
}
```

Intégration des services AWS

AWS KMS est intégré à un certain nombre de services AWS. Consultez le site web de KMS pour obtenir la liste complète des services intégrés. Grâce à ces intégrations, vous pouvez utiliser facilement des clés CMK AWS KMS afin de chiffrer les données que vous stockez auprès de ces services. Outre l'utilisation d'une clé CMK gérée par le client, un certain nombre de services intégrés permettent d'utiliser une clé CMK gérée par AWS qui est créée et gérée automatiquement en votre nom, mais qui peut être utilisée uniquement dans le service spécifique qui l'a créée.

Capacités d'audit

AWS CloudTrail enregistre chaque utilisation d'une clé que vous stockez dans AWS KMS dans un fichier journal transmis au compartiment Amazon S3 que vous avez spécifié dans votre configuration

de CloudTrail. Les informations enregistrées incluent les détails concernant l'utilisateur, l'heure, la date, l'opération et la clé utilisée.

Sécurité

AWS KMS est conçu de manière à ce que personne ne puisse accéder à vos clés principales. Le service repose sur des systèmes conçus pour protéger vos clés principales à l'aide de techniques de renforcement approfondies. Il s'agit notamment d'éviter le stockage de clés principales intelligibles sur un disque dur ou leur conservation en mémoire, et de limiter le nombre de systèmes pouvant accéder aux hôtes qui utilisent les clés. Tout accès destiné à mettre à jour le logiciel sur le service est contrôlé par un contrôle d'accès multipartite qui est vérifié et examiné par un groupe indépendant au sein d'AWS.

Pour en savoir plus sur AWS KMS, consultez le livre blanc AWS Key Management Service.

AWS CloudHSM

AWS CloudHSM est un module de sécurité matériel (HSM) basé sur le cloud, conçu pour vous aider à répondre aux exigences de conformité, contractuelles et réglementaires de l'entreprise en matière de sécurité des données, en vous laissant générer et utiliser vos clés de chiffrement sur un matériel certifié FIPS 140-2 niveau 3.

Avec AWS CloudHSM, vous contrôlez les clés et les opérations de chiffrement effectuées par le HSM.

AWS et les partenaires AWS Marketplace proposent différentes solutions de protection des données sensibles sur la plateforme AWS. Toutefois, dans le cas d'applications et de données soumises à des exigences contractuelles ou réglementaires très strictes en termes de gestion des clés de chiffrement, une protection supplémentaire peut s'avérer nécessaire. Auparavant, la seule option proposée consistait à stocker les données sensibles (ou les clés de chiffrement protégeant ces données) dans des centres de données sur site. Cette solution pouvait entraver la migration de ces applications vers le cloud, ou ralentissait fortement leurs performances. Grâce à AWS CloudHSM, vous pouvez protéger vos clés de chiffrement dans des HSM conformes aux normes gouvernementales relatives à la gestion sécurisée des clés. Vous pouvez générer, stocker et gérer de manière sécurisée les clés de chiffrement utilisées pour le chiffrement des données, afin que vous soyez la seule personne pouvant accéder à ces clés. Grâce à AWS CloudHSM, vous êtes en mesure de respecter les exigences strictes en termes de gestion des clés sans que les performances de vos applications en pâtissent.

Le service AWS CloudHSM fonctionne avec Amazon VPC. Les instances AWS CloudHSM sont déployées dans votre Amazon VPC avec l'adresse IP que vous indiquez. Vous disposez ainsi d'une connexion réseau simple et privée pour vos instances Amazon EC2. Lorsque vous localisez vos instances HSM à proximité de vos instances Amazon EC2, vous réduisez la latence du réseau, ce qui peut améliorer les performances des applications. AWS fournit un accès dédié et exclusif (locataire unique) aux instances HSM, qui sont isolées des autres clients AWS. Disponible dans plusieurs régions et zones de disponibilité, AWS CloudHSM permet d'ajouter un stockage de clés durable et sécurisé à vos applications.

Intégration aux services AWS et aux applications tierces

Vous pouvez utiliser CloudHSM avec Amazon Redshift, Amazon RDS pour Oracle ou des applications tierces (telles que SafeNet Virtual KeySecure) comme racine de confiance, pour Apache (terminaison SSL) ou Microsoft SQL Server (chiffrement transparent de données). Vous pouvez également utiliser AWS CloudHSM pour développer vos propres applications, tout en continuant à utiliser les bibliothèques de chiffrement standard, telles que PKCS#11, Java JCA/JCE, Microsoft CAPI et CNG.

Activités d'audit

Si vous avez besoin de suivre l'évolution de vos ressources ou d'auditer les activités à des fins de sécurité et de conformité, vous pouvez passer en revue les appels d'API de gestion via AWS CloudHSM effectués à partir de votre compte à l'aide d'AWS CloudTrail. De plus, vous pouvez auditer des opérations sur l'appliance HSM à l'aide de syslog ou envoyer des messages de journal syslog à votre propre collecteur de journaux.

Services et outils de chiffrement AWS

AWS propose des mécanismes conformes à un large éventail de normes de sécurité de chiffrement que vous pouvez utiliser pour mettre en œuvre un chiffrement conforme aux meilleures pratiques. Le kit SDK AWS Encryption est une bibliothèque de chiffrement côté client, disponible en Java, Python, C, JavaScript, et dans une interface de ligne de commande qui prend en charge Linux, macOS et Windows. Il offre des fonctions avancées de protection des données, notamment des suites d'algorithmes de clés symétriques sécurisées et authentifiées, comme les clés AES-GCM 256 bits avec dérivation de clés et signature. Puisqu'il a été spécialement conçu pour les applications qui utilisent Amazon DynamoDB, le client de chiffrement DynamoDB permet aux utilisateurs de protéger leurs données de table avant qu'elles ne soient envoyées à la base de données. En outre, il vérifie et déchiffre les données lorsqu'elles sont récupérées. Le client est disponible en Java et en Python.

Infrastructure Linux DM-Crypt

Dm-crypt est un mécanisme de chiffrement au niveau du noyau Linux qui permet aux utilisateurs de monter un système de fichiers chiffré. Le montage d'un système de fichiers consiste à attacher ce système de fichiers à un répertoire (point de montage) afin de le rendre disponible pour le système d'exploitation. Après le montage, tous les fichiers du système de fichiers sont disponibles pour les applications sans aucune interaction supplémentaire. Ces fichiers sont toutefois chiffrés lorsqu'ils sont stockés sur le disque.

L'outil de mappage des périphériques est une infrastructure dans le noyau Linux 2.6 et 3.x qui fournit un moyen générique de créer des couches virtuelles de périphériques de stockage en mode bloc. La cible de chiffrement de l'outil de mappage des périphériques fournit un chiffrement transparent des périphériques de stockage en mode bloc en utilisant l'API de chiffrement du noyau. La solution présentée ici utilise dm-crypt conjointement avec un système de fichiers sur disque mappé à un volume logique par le gestionnaire de volumes logiques (LVM). Le LVM permet une gestion des volumes logiques pour le noyau Linux.

Protection des données dès la conception et par défaut

Chaque fois qu'un utilisateur ou une application tente d'utiliser AWS Management Console, l'API AWS ou l'interface de ligne de commande AWS CLI, une demande est envoyée à AWS. Le service AWS reçoit la demande et exécute plusieurs autres étapes afin de déterminer s'il faut autoriser ou refuser la demande, conformément à une logique d'évaluation de stratégies précise. À l'exception des demandes d'informations d'identification racines, toutes les demandes sur AWS sont refusées par défaut (la stratégie de refus par défaut est appliquée). Cela signifie que tout ce qui n'est pas explicitement autorisé par la stratégie est refusé. AWS recommande d'appliquer dans la définition des stratégies le principe du moindre privilège, c.-à-d. que chaque composant (tel que les utilisateurs, les modules ou les services) doit pouvoir accéder uniquement aux ressources nécessaires à l'exécution de ses tâches.

Cette approche est conforme à l'article 25 du RGPD, qui stipule que le responsable du traitement « doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. »

AWS fournit également des outils permettant de mettre en œuvre le puissant mécanisme Infrastructure as Code, qui permet de tenir compte de la sécurité dès le début de la conception d'une architecture. AWS CloudFormation fournit un langage commun pour décrire et allouer toutes

les ressources d'infrastructure, y compris les stratégies et les processus de sécurité. Grâce à ces outils et pratiques, la sécurité fait partie intégrante de votre code et peut être gérée par version, surveillée et modifiée (à l'aide d'un système de gestion des versions) en fonction des exigences de votre organisation. Cela permet de protéger les données dès la conception, car les processus et les stratégies de sécurité peuvent être inclus dans la définition de votre architecture. Ils peuvent aussi être surveillés en permanence par des mesures de sécurité dans votre organisation.

Dans quelle mesure AWS peut vous aider

Tableau 1 – Dans quelle mesure AWS peut vous aider à vous conformer au RGPD

Domaine	Description	Services et outils AWS
Cadre de conformité stricte	Les mesures techniques et organisationnelles appropriées peuvent devoir inclure « des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement. »	SOC 1 / SSAE 16 / ISAE 3402 (anciennement SAS 70) / SOC 2 / SOC 3 PCI DSS, niveau 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5)
Contrôle d'accès aux données	Le responsable du traitement doit mettre « ...en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield et AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations

Domaine	Description	Services et outils AWS
	les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. »	AWS CloudTrail

Domaine	Description	Services et outils AWS
Surveillance et journalisation	« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. » « ...le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque [...] »	AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub Outils et kits SDK AWS

Domaine	Description	Services et outils AWS
Protection de vos données sur AWS	Les organisations doivent « mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris (...) la pseudonymisation et le chiffrement des données à caractère personnel (...). »	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

Participants

Ont contribué à la préparation du présent document :

- Tim Anderson, spécialiste du secteur technique, Amazon Web Services
- Carmela Gambardella, architecte de solutions pour le secteur public, Amazon Web Services
- Giuseppe Russo, directeur de l'assurance de la sécurité, Amazon Web Services
- Marta Taggart, directrice des programmes, Amazon Web Services
- Luca Iannario, architecte de solutions pour le secteur public, Amazon Web Services

Révisions du document

Date	Description
Novembre 2017	Première publication
Décembre 2020	Mise à jour afin d'inclure l'ajout de nouveaux services et fonctionnalités AWS.

Mentions légales

Les clients sont responsables de leur propre évaluation indépendante des informations contenues dans ce document. Le présent document : (a) est fourni à titre informatif uniquement, (b) représente les offres et pratiques actuelles de produits AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part d'AWS et de ses sociétés apparentées, fournisseurs ou concédants de licences. Les produits ou services AWS sont fournis « en l'état » sans garantie, représentation ou condition, de quelque nature que ce soit, explicite ou implicite. Les responsabilités et obligations d'AWS envers ses clients sont déterminées par les contrats AWS, et le présent document ne fait pas partie d'un contrat entre AWS et ses clients, ni le modifie.