Hach Claros
Livre blanc sur la sécurité

Présentation générale

Claros est le système intelligent d'évaluation de la qualité de l'eau de Hach®. Il est conçu pour permettre aux entreprises du secteur de l'eau de transformer en toute sécurité les données de laboratoire et de procédés en informations exploitables afin d'obtenir de meilleurs résultats. Claros regroupe les solutions Instrument Management, Data Management et Process Management de Hach sur une seule plate-forme. Hach sait que la protection des données de ses clients, le respect des réglementations de sécurité et la limitation des risques potentiels sont essentiels pour instaurer la confiance et fournir un niveau de service élevé. Hach adopte une approche d'analyse des risques pour la gestion de la sécurité. Ce document détaille les nombreuses mesures et technologies que Claros utilise pour protéger les données de ses clients.

Ce document décrit la façon dont Claros répond aux objectifs fondamentaux de la sécurité des informations, à savoir la confidentialité, l'intégrité et la disponibilité, ainsi que l'approche de Hach en matière d'architecture de sécurité et les responsabilités de ses clients. Dans le domaine de la sécurité, nous définissons la confidentialité comme l'ensemble de nos règles contrôlant l'accès aux informations, l'intégrité comme l'exactitude et la fiabilité des informations, et la disponibilité comme l'accès fiable aux informations par les utilisateurs autorisés.

Vous trouverez ci-dessous le sommaire des sujets traités dans le présent document :

L'approche de Hach

Défense en profondeur

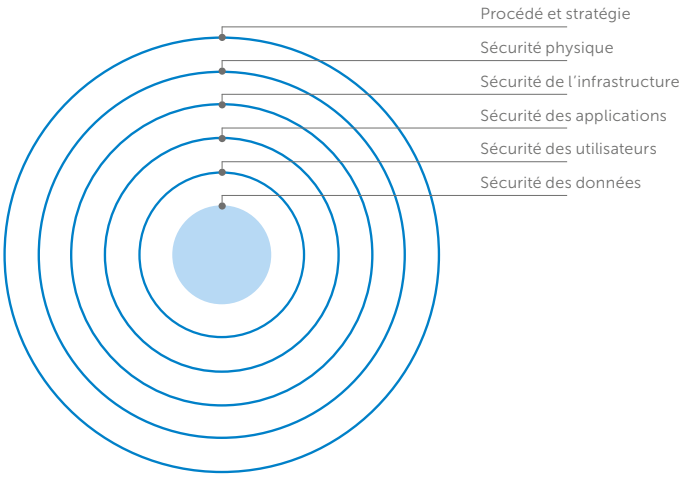
Avec Claros, il n'existe pas de couche unique qui protègerait les données des clients, mais plutôt une solution bien structurée qui prend en compte chaque couche, depuis les mesures de sécurité physique au niveau du centre de données jusqu'aux privilèges d'accès qui déterminent les données auxquelles un utilisateur peut accéder. Hach utilise cette stratégie de sécurité à plusieurs niveaux pour protéger les données des clients.

La défense en profondeur correspond à l'utilisation coordonnée de plusieurs contre-mesures de sécurité pour protéger l'intégrité des informations d'une entreprise. La stratégie est basée sur le principe militaire voulant qu'il est plus difficile pour un ennemi de vaincre un système de défense complexe et à plusieurs couches que de franchir une seule barrière.

-TechTarget

Procédé et stratégie

La première couche de défense consiste à disposer d'un ensemble complet et bien défini de stratégies et de procédés de sécurité afin de garantir la sécurité des données et des utilisateurs de nos clients. Le système de gestion de la sécurité des informations (ISMS, Information Security Management System) de Hach utilise différentes mesures des procédés et stratégies qui garantissent que la sécurité est une priorité majeure au sein même de l'entreprise, pour nos propres employés.



Formation

Les employés de Hach autorisés à accéder à Claros suivent une formation continue leur permettant de se conformer aux stratégies de sécurité de Hach. Par exemple, le personnel des services Development Operations, Research & Development et Technical Support and Services de Hach, qui peut être amené à gérer les données et informations sensibles des clients, suit régulièrement une formation de sensibilisation à la conformité et à la sécurité qui le tient au courant des menaces de sécurité émergentes à prendre en compte.

Accès autorisé

Outre la restriction de l'accès du personnel à la zone de production, l'accès opérationnel à Claros est limité à un groupe restreint d'employés du service Development Operations de Hach. L'accès est contrôlé via le réseau d'entreprise Hach, ce qui garantit que seul le personnel autorisé peut accéder aux données. Tout le personnel Hach disposant d'un accès physique ou opérationnel aux environnements de production doit suivre une formation et toutes les activités sont consignées à des fins de traçabilité.

Contrôle des modifications

Le processus officiel de contrôle des modifications de Hach limite les risques associés aux modifications et mises à jour de Claros. Ce processus permet d'assurer le suivi des modifications apportées à Claros et de vérifier que les risques ont été évalués, que les interdépendances sont explorées et que les stratégies et procédures nécessaires ont été prises en compte et appliquées avant toute autorisation de modification. Hach documente toutes les modifications apportées dans les Notes relatives à la publication, qui sont distribuées aux clients avant toute modification ou mise à jour du système.

Durcissement des systèmes

Claros utilise de nombreuses technologies bien coordonnées pour fournir ses services, cependant certaines peuvent s'avérer inutiles. Conformément aux meilleures pratiques du secteur, le service "Claros Development Operations" inspecte de près l'ensemble de la solution afin d'identifier les services inutiles et de supprimer et/ou désactiver ces fonctionnalités pour réduire les vulnérabilités aux menaces de sécurité.

Analyses périodiques des vulnérabilités et tests de pénétration

Conformément aux stratégies internes et aux normes et cadres de cybersécurité internationaux, Hach procède régulièrement à des tests de vulnérabilité et de pénétration couvrant les failles de sécurité critiques, incluant les 10 principaux risques OWASP, afin de garder une longueur d'avance sur les menaces de sécurité.

Correctifs de sécurité

Hach a mis en place des stratégies et des procédures rigoureuses pour mettre à jour tous les composants de Claros, notamment les systèmes d'exploitation, les hyperviseurs de machines virtuelles, les intergiciels, les bases de données, les applications mobiles, etc., avec les correctifs de sécurité des fournisseurs. Ces activités de correctifs de sécurité sont soumises à l'audit du cycle de vie du développement des produits sécurisé CEI62443-4-1 et à des normes rigoureuses.

Confidentialité

Authentification

L'architecture Claros repose sur une structure de sécurité centralisée d'authentification et d'autorisation pour contrôler l'accès au service et aux appareils sur le terrain. Cette structure de sécurité permet d'appliquer des stratégies de sécurité en demandant aux algorithmes d'efficacité des mots de passe de définir la longueur et la complexité minimales du mot de passe.

Cryptage en transit

L'ensemble du trafic entrant et sortant de Claros est crypté afin d'assurer la sécurité des communications. Ce cryptage utilise un protocole TLS/SSL (Transport Layer Security/ Secure Sockets Layer) qui exploite les algorithmes SHA-2 (Secure Hash Algorithm 2) ou AES (Advanced Encryption Standard). Cela signifie qu'aucune donnée ne quitte ou n'atteint l'un des points finaux de confiance sans être cryptée lors de la navigation sur Internet.

Cryptage au repos

Hach ne prend aucun risque avec les données au repos des clients. Toutes les données Claros sont stockées sur des serveurs Microsoft Azure et cryptées à l'aide de la norme de cryptage AES 256 bits. Par conséquent, même si quelqu'un accède aux données sur les serveurs, celles-ci sont totalement brouillées et non identifiables.

Intégrité

Accès contrôlé et basé sur les rôles

Tous les accès des clients à Claros sont contrôlés par le biais d'interfaces utilisateur (IU), d'API (interface de programmation d'applications) et/ou d'outils dédiés. L'utilisation de l'une de ces méthodes d'accès nécessite un nom d'utilisateur et un mot de passe disposant des privilèges appropriés pour l'accès demandé. Chaque administrateur de compte Claros peut définir les autorisations des comptes d'utilisateur, appelés Contrôle d'accès basé sur les rôles (RBAC). Le RBAC étant appliqué à l'ensemble de l'infrastructure Claros, les clients ne disposent d'aucun accès root ou administratif à une quelconque partie de l'infrastructure technologique Claros, et l'accès est autorisé uniquement via la couche d'application Claros (IU ou API).

Accès aux applications

Les données des clients sont uniquement accessibles via l'application Claros. Que cet accès se fasse via les interfaces utilisateur ou via les API disponibles, il applique le RBAC pour limiter l'accès aux données des clients au personnel et aux utilisateurs autorisés. Par conséquent, Claros ne fournit pas d'accès direct aux bases de données. Cette approche empêche les services ou systèmes non autorisés de récupérer ou de modifier accidentellement ou de manière malveillante les données des clients.

Communication

Toutes les communications avec Claros sont initiées par les appareils sur le terrain, afin que le client puisse suivre toutes les tentatives de communication de son propre réseau vers le monde extérieur et ajouter des mesures de sécurité supplémentaires à son réseau environnant. L'authenticité de toute tentative de communication vers et depuis les appareils sur le terrain vers les données Claros est validée.

Pare-feu

Tous les accès réseau depuis et vers les appareils sur le terrain sont protégés par un pare-feu à plusieurs couches fonctionnant en mode « Tout refuser ». L'accès à Internet est uniquement autorisé sur les ports explicitement ouverts pour un sous-ensemble d'hôtes virtuels spécifiés seulement. Tous les serveurs de base de données fonctionnent derrière un pare-feu supplémentaire, ajoutant ainsi une couche de sécurité.

Ports et services inutiles

Tous les ports et services sur les serveurs et appareils sur le terrain intégrés qui ne sont pas requis pour le fonctionnement de Claros sont désactivés, ce qui élimine les possibilités supplémentaires d'intrusion externe. Seuls quelques ports et points finaux doivent être ouverts sur le réseau du client pour utiliser Claros. Le tableau suivant présente les ports et services utilisés par Claros :

Port	Direction	Service	Objectif
1194 (UDP)	Sortie	VPN	Accès à distance pour les techniciens de maintenance Hach
5671 (TCP)	Sortie	AMQPS	Transmettre/recevoir des messages à/de Claros
123 (UDP)	Sortie/Entrée	NTP	Obtenir la date et l'heure actuelles à partir du serveur horaire externe
80 (TCP)	Sortie	HTTP	Obtenir des mises à jour de micrologiciel hachées et signées à partir du répertoire
443 (TCP)	Sortie	HTTPS	Accéder à l'interface utilisateur Claros

Disponibilité

Microsoft Azure

Claros exploite le Cloud computing Microsoft Azure pour fournir ses services. Tous les clients de Claros bénéficient donc de l'accord de niveau de service (SLA) Microsoft Azure, qui garantit une disponibilité supérieure ou égale à 99,95 % de tous les principaux services Azure.

Infrastructure

L'infrastructure qui prend en charge notre solution se situe entre la couche physique du centre de données et la couche applicative de Claros. Dans toute l'infrastructure, la sécurité est mise en œuvre de manière complète et coordonnée afin d'améliorer la sécurité des données des clients.

Conformité

Afin d'aider nos clients à se conformer aux exigences nationales, régionales et sectorielles régissant la collecte et l'utilisation des données individuelles, Microsoft Azure propose l'ensemble le plus complet d'offres de conformité dans le domaine de la fourniture de services Cloud standard.

Tous les centres de données Microsoft Azure sont certifiés conformément aux principales normes de sécurité des informations répertoriées dans le tableau suivant :

CDSA	Azure est certifié par l'association internationale de protection et de sécurité du contenu, Content Delivery and Security Association.
Attestation CSA STAR	Azure et Intune ont reçu l'attestation STAR de la Cloud Security Alliance basée sur un audit indépendant.
GxP	Les services Cloud de Microsoft respectent les bonnes pratiques cliniques, de laboratoire et de fabrication (GxP).
ISO 9001	Microsoft est certifié pour sa mise en œuvre de ces normes de gestion de la qualité.
ISO 20000-1:2011	Microsoft est certifié pour sa mise en œuvre de ces normes de gestion des services.
ISO 22301	Microsoft est certifié pour sa mise en œuvre de ces normes de gestion de la continuité de l'activité.
ISO 27001	Microsoft est certifié pour sa mise en œuvre de ces normes de gestion de la sécurité des informations.
ISO 27017	Les services Cloud de Microsoft ont mis en œuvre ce Code de pratiques pour les contrôles de sécurité des informations.
ISO 27018	Microsoft a été le premier fournisseur de Cloud à respecter ce code de pratiques en matière de confidentialité du Cloud.
MPAA	Azure a réussi une évaluation officielle menée par la Motion Picture Association of America.
Evaluations partagées	Microsoft fait la démonstration de l'adéquation d'Azure avec ce programme dans la version 3.0.1 de CSA CCM.
SOC 1	Les services Cloud de Microsoft sont conformes aux normes de contrôle de l'organisation de service en matière de sécurité opérationnelle.
SOC 2	Les services Cloud de Microsoft sont conformes aux normes de contrôle de l'organisation de service en matière de sécurité opérationnelle.
SOC 3	Les services Cloud de Microsoft sont conformes aux normes de contrôle de l'organisation de service en matière de sécurité opérationnelle.
WCAG 2.0	Les services Cloud de Microsoft sont conformes aux directives Web Content Accessibility Guidelines 2.0.

Déploiements régionaux

L'implantation de Microsoft Azure à l'échelle mondiale est plus importante que celle de tout autre fournisseur de Cloud, offrant ainsi l'évolutivité nécessaire pour rapprocher les applications Claros des utilisateurs du monde entier, tout en préservant la résidence des données et en proposant des options complètes de conformité et de résilience aux clients. Afin d'aider les clients à préserver la souveraineté de leurs données et à se conformer aux réglementations régionales, Hach utilise pour ses clients des centres de données Microsoft Azure se trouvant dans leurs régions ou aussi près que possible de celles-ci.

50 Sites sans le monde **140** Disponible dans 140 pays

Source : Microsoft

Tous ces centres de données disposent également d'un système de chauffage, ventilation et climatisation redondant N+1, et d'une alimentation sans coupure (ASC).

La sécurité physique est conforme aux meilleures pratiques du secteur et comprend :

- Protocoles de carte d'accès, protocoles d'identification biométrique et surveillance interne et externe 24 heures sur 24
- Accès limité au personnel autorisé du centre de données : personne ne peut entrer dans la zone de production sans autorisation préalable et escorte appropriée
- Chaque employé d'un centre de données doit se soumettre à des contrôles de sécurité minutieux

Responsabilités du client

Accès et configuration contrôlés

Afin de garantir la sécurité des données, Hach attend également de ses clients qu'ils respectent les normes de sécurité. Hach compte sur ses clients pour s'assurer que chaque compte Claros est configuré avec les autorisations et l'accès appropriés pour chaque utilisateur. Il incombe à chaque client d'identifier les personnes au sein de la station disposant d'un accès administratif et de gérer ces comptes dans la durée.

Protection physique

Les clients sont responsables de la protection physique de leur infrastructure d'instrumentation et de sécurité Hach. Chaque station est responsable du contrôle des accès à celle-ci, aux instruments Hach concernés (transmetteurs et capteurs, par exemple) et aux réseaux de communication.

Connectivité

La connectivité des instruments Hach à Claros sur chaque site client relève de la responsabilité du client. Pour que Claros fonctionne efficacement, les instruments nécessitent généralement une connexion cellulaire ou réseau que le client doit maintenir et protéger efficacement.

DOC180.77.10159.Feb19