TC-01

SÉCURITÉ

Bonnes pratiques de sécurité

Guide opérationnel à destination des utilisateurs de la plate-forme CEREBRO et de leurs organisations.

Résumé exécutif

> /// EXECUTIVE SUMMARY
>
> La sécurité d'une plateforme critique ne tient jamais qu'à son infrastructure. Elle se construit aussi côté utilisateur : dans la manière dont les comptes sont protégés, dont les sessions sont gérées, et dont les incidents sont signalés.
>
> Ce document décrit les pratiques attendues de la part des organisations qui utilisent CEREBRO, et les responsabilités partagées entre CaliaLabs et ses clients en matière de sécurité opérationnelle.
>
> Il ne remplace pas la politique de sécurité interne de votre organisation. Il vient la compléter sur les aspects spécifiques à l'utilisation de la plateforme.

Points clés

AUTHENTIFICATION FORTE

MFA obligatoire pour tous les comptes administrateurs et sensibles

GESTION DES ACCÈS

Principe du moindre privilège appliqué par défaut à chaque rôle

SIGNALEMENT D'INCIDENT

Canal dédié 24/7 pour toute suspicion de compromission

RESPONSABILITÉ PARTAGÉE

CaliaLabs protège la plateforme, le client protège ses accès

Responsabilité partagée

La sécurité d'une utilisation de CEREBRO repose sur un modèle de responsabilité partagée entre CaliaLabs et les organisations clientes.

CaliaLabs est responsable de la sécurité de la plateforme elle-même : infrastructure, code, chiffrement des données au repos et en transit, surveillance des menaces, gestion des vulnérabilités, et continuité opérationnelle.

Les organisations clientes sont responsables de la sécurité de leurs propres accès : gestion des identités de leurs collaborateurs, activation de l'authentification multi-facteurs, configuration des rôles selon le principe du moindre privilège, et sensibilisation de leurs équipes.

Ce partage n'est pas une clause contractuelle abstraite. C'est une réalité opérationnelle : même la meilleure infrastructure ne peut rien contre un mot de passe réutilisé sur un autre service compromis.

Authentification et gestion des comptes

L'authentification multi-facteurs (MFA) est obligatoire pour tous les comptes disposant de privilèges d'administration, et fortement recommandée pour l'ensemble des utilisateurs.

Les méthodes MFA supportées sont : applications d'authentification (TOTP), clés physiques FIDO2/WebAuthn, et codes de secours à usage unique. Les SMS ne sont pas recommandés comme second facteur en raison des risques connus (SIM swap, interception).

Les mots de passe doivent respecter les critères suivants : longueur minimale de 12 caractères, complexité mélangée, absence de réutilisation entre services, renouvellement uniquement en cas de compromission suspectée (pas de rotation calendaire forcée, conformément aux recommandations NIST SP 800-63B).

La création d'un compte sur CEREBRO est soumise à validation par un administrateur de l'organisation cliente. Chaque compte est nominatif : les comptes partagés entre plusieurs personnes sont interdits.

Gestion des rôles et privilèges

Les rôles dans CEREBRO suivent le principe du moindre privilège : chaque utilisateur ne dispose que des droits strictement nécessaires à sa mission opérationnelle.

Trois grandes familles de rôles existent : opérationnels (traitement des flux, validation ex-ante), gouvernance (supervision, arbitrage, overrides), et administration (configuration système, gestion des utilisateurs, intégrations).

Les privilèges d'administration font l'objet d'une traçabilité renforcée : chaque action administrative génère un événement de journalisation inaltérable (WORM), horodaté et attribuable à l'identité ayant effectué l'action.

Les organisations sont encouragées à revoir périodiquement les droits accordés (au minimum tous les trimestres), à retirer les accès des collaborateurs qui ont changé de mission, et à désactiver immédiatement les comptes en cas de départ.

Sessions et accès distants

Les sessions CEREBRO expirent automatiquement après une période d'inactivité définie dans la configuration de l'organisation (par défaut : 30 minutes pour les comptes standards, 15 minutes pour les comptes administrateurs).

Les connexions depuis un nouveau terminal ou une nouvelle adresse IP déclenchent une vérification additionnelle selon la politique de l'organisation.

L'accès à CEREBRO est uniquement possible via HTTPS avec TLS 1.3 ou supérieur. Les requêtes non chiffrées sont systématiquement rejetées au niveau du reverse proxy.

L'utilisation de réseaux publics non chiffrés (Wi-Fi ouvert, hotspot non identifié) pour accéder à la plateforme est déconseillée, y compris pour les utilisateurs disposant d'une connexion VPN d'entreprise.

Signalement d'incident de sécurité

Toute suspicion de compromission — perte de terminal, mot de passe potentiellement divulgué, courriel suspect reçu par un utilisateur, activité anormale dans les journaux — doit être signalée sans délai.

Le canal dédié est disponible 24 heures sur 24, 7 jours sur 7, à l'adresse security@calialabs.com. En cas d'incident majeur confirmé, une ligne téléphonique d'urgence est communiquée aux référents sécurité des organisations clientes.

Les délais d'engagement sont les suivants : accusé de réception sous 1 heure pour les incidents critiques, sous 4 heures pour les incidents de niveau élevé. Une première analyse est communiquée sous 24 heures.

Conformément aux obligations RGPD et DORA applicables, CaliaLabs s'engage à notifier les clients concernés dans les délais réglementaires en cas de violation de données personnelles ou d'incident opérationnel significatif.

Sensibilisation et formation

Les attaques les plus fréquentes contre les plateformes critiques ne visent pas la plateforme elle-même, mais ses utilisateurs : hameçonnage, ingénierie sociale, usurpation d'identité.

Nous recommandons aux organisations clientes de sensibiliser leurs équipes aux signaux faibles : demandes inhabituelles, urgence fabriquée, canaux de communication non habituels, pièces jointes inattendues.

CaliaLabs met à disposition, sur demande, des ressources de sensibilisation adaptées au contexte d'utilisation de la plateforme, ainsi que des simulations d'hameçonnage sur mesure.

En cas de doute sur l'authenticité d'une communication prétendant venir de CaliaLabs, vérifiez systématiquement via le canal de contact officiel avant d'agir.

Révision et mise à jour

Ce document est révisé au minimum une fois par an, et à chaque évolution significative de la plateforme ou du paysage de menaces. La version en vigueur est celle publiée sur le Trust Center.

Les organisations clientes sont informées des changements majeurs par les canaux de communication contractuels.