



CITADELTEAM

Communication En situation de Crise



Use Case



ERCOM

Cyber Solutions by Thales

Communication en situation de crise avec Citadel Team

En cas de cyberattaque, le système d'information peut être fortement perturbé, voire totalement paralysé, rendant indisponibles les moyens de communication habituels. Pourtant, la coordination de la Direction, des équipes informatiques, métiers, juridiques et communication reste essentielle pour gérer efficacement la crise. L'enjeu est alors de garantir la continuité des échanges internes et externes grâce à une solution de messagerie sécurisée, indépendante des systèmes affectés. **Citadel Team** fournit un canal de communication résilient permettant de coordonner les équipes, de piloter la cellule de crise, de partager les informations critiques et de maintenir le lien avec les parties prenantes, même lorsque le SI n'est plus opérationnel. En assurant la continuité des communications, Citadel Team contribue à accélérer la prise de décision, à limiter l'impact de l'incident et à préserver l'activité ainsi que la réputation de l'entreprise.



Qui est concerné ?

- La cellule de crise et la Direction pour piloter la gestion de l'incident
- Les équipes IT et cybersécurité pour coordonner les actions techniques
- Les équipes communication et juridique pour diffuser les informations critiques et gérer les parties prenantes
- Les métiers et les collaborateurs concernés pour rester informés et assurer la continuité des opérations



Les objectifs :

Réagir vite, communiquer sans interruption, garder le contrôle en situation de crise !

- Activer les canaux de communication en quelques clics
- Assurer une communication autonome, indépendante du SI
- Coordonner efficacement les équipes pour une gestion optimale de la crise

Une communication en situation de crise fiable, sécurisée et toujours disponible !

a) Indépendance du SI

Une solution autonome, utilisable même si le SI est indisponible ou dégradé, pour garantir la continuité des communications critiques.

b) Sécurité et confidentialité

Chiffrement de bout en bout des échanges* pour protéger les informations sensibles.

c) Fiabilité et continuité de service

Une plateforme opérationnelle en toutes circonstances pour maintenir les échanges en situation de crise.

d) Rapidité d'activation

Diffusion en temps réel des informations et mise en relation des équipes en quelques minutes.

e) Centralisation des échanges

Un service unique pour piloter les communications, assurer le suivi et garantir la traçabilité.

f) Accessibilité multi-terminaux

Disponible sur ordinateur, mobile et tablette, pour rester connecté où que soient vos équipes.

g) Échange sécurisé en audio et visioconférence avec partage d'écran

Appels audio, visioconférences avec partage d'écran sécurisé pour coordonner efficacement les actions de crise.

*messages et appels

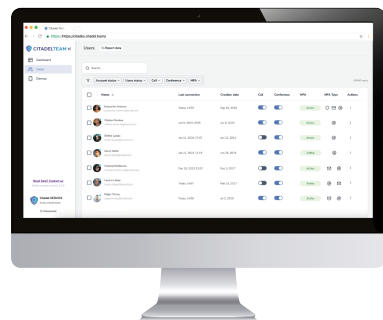


Gestion fine des utilisateurs et enrôlement même lorsque le SI n'est plus opérationnel :

Afin de garantir l'entière confidentialité et une étanchéité totale entre nos clients, chaque entreprise bénéficie d'une infrastructure dédiée, opérée par Thales et hébergée en France.

Cette approche vous offre une maîtrise totale de votre environnement. L'infrastructure est entièrement configurable afin de répondre aux exigences spécifiques de votre organisation, notamment en matière de politiques de sécurité, de gestion des identités et de contrôle des accès utilisateurs.

En cas d'incident majeur, de nouveaux utilisateurs peuvent être enrôlés même sans accès à leur email, assurant ainsi la continuité immédiate des opérations et de la cellule de crise.



Les fonctionnalités clés :



- Messagerie instantanée
- Notifications urgentes
- Partage de fichiers dans des salons chiffrés
- Téléphonie sécurisée
- Accès multi-terminaux et synchronisation (terminaux mobiles & PC)
- Disponible en SaaS sur un environnement SecNumCloud 3.2 ou Cloud Public
- Chiffrement de bout en bout* des échanges

*messagerie, appels



Les bénéfices apportés :

- Continuité des informations car cet outil est indépendant du SI
- Résilience opérationnelle et sécurité renforcée
- Réactivité accrue
- Centralisation des informations et traçabilité
- Confidentialité garantie
- Coordination optimale
- Déploiement simplifié