Extended Monaco pour l'Entreprise

PARTENAIRE OFFICIEL

GROUPE telis

27ème atelier du numérique
GESTION DE CRISE

Le Gouvernement accompagne votre transition numérique

Une dynamique Extended Monaco pour l'Entreprise

eme.gouv.mc

Evaluer sa maturité numérique	**Se former** au numérique	**Se faire accompagner** d'un expert	**Financer** son projet
➔ Outil d'auto-diagnostic	➔ Plateau de e-learning ➔ Ateliers du numérique	➔ Annuaire d'ESN	➔ Fonds Bleu

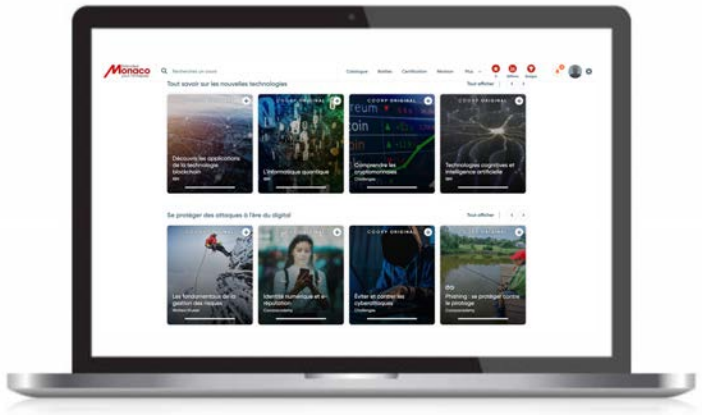
Le Gouvernement accompagne votre transition numérique

Extended Monaco pour l'Entreprise — eme.gouv.mc

Evaluer sa maturité numérique	**Se former** au numérique	Se faire **accompagner** d'un expert	**Financer** son projet

Plateau e-learning coorpacademy

- Un catalogue mis à disposition par le Gouvernement au profit des dirigeants, salariés, étudiants, jeunes diplômés
- Plus de **2000** cours
- Une formation à suivre à son rythme, à distance, selon ses besoins et ses contraintes

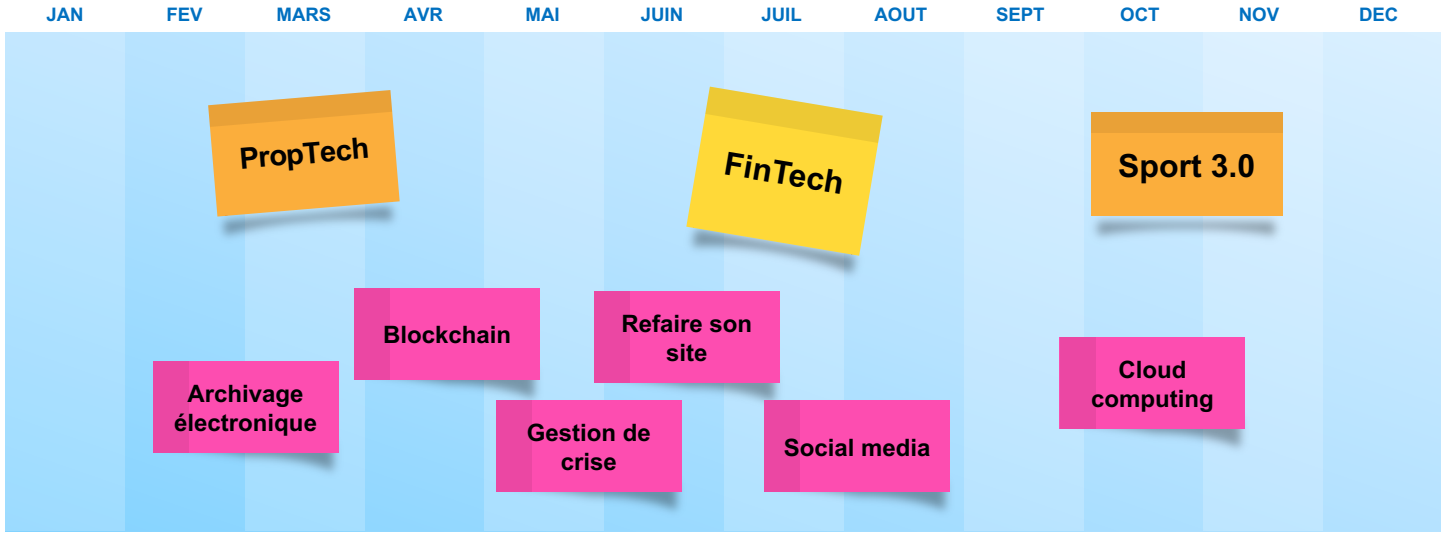


Le Gouvernement accompagne votre transition numérique

Extended Monaco pour l'Entreprise — eme.gouv.mc

Evaluer sa maturité numérique	**Se former** au numérique	Se faire **accompagner** d'un expert	**Financer** son projet

Les Ateliers du numérique en 2023



Extended Monaco pour l'Entreprise

PARTENAIRE OFFICIEL

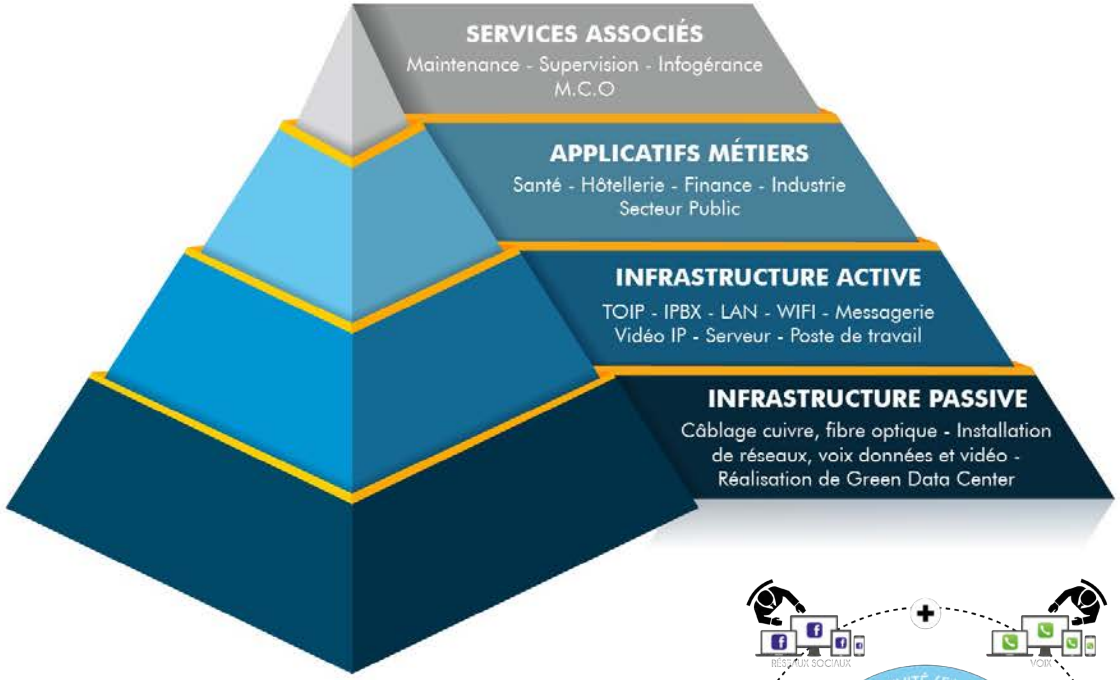
GROUPE telis

LE GROUPE TELIS ET LA GESTION DE CRISE

Communication Digitale

Solutions innovantes de communication sécurisée

- Réseaux informatiques
- Équipes de maintien en conditions opérationnelles 24/7/365
- Sécurité du SI
- Vidéo Protection



easyOne
Customized Software

GROUPE telis

Multimédia

- Applications mobiles multimédia & domotique
- Affichage dynamique et solutions interactives
- Solutions IPTV et VOD
- Smart city

Actis

DCmonaco DATACENTER

GROUPE telis

Actis

Sécurité et protection des données

- Dématérialisation et archivage numérique
- Conformité des systèmes
- Continuité d'activité et gestion de crise
- Accompagnements, sensibilisations et formations
- Cyber sécurité

DCmonaco DATACENTER

HDS CERTI TRUST

ISO 27001 CERTI TRUST

MonacoDATACENTER

- Green Data center
- Haute disponibilité
- Hébergement en Principauté
- Supervision en temps réel
- Bâtiment sécurisé 24/7/365

ACTIS ET LA GESTION DE CRISE

20 ANS
D'EXPERTISE À MONACO

4 GESTIONS DE CRISE
200+ TESTS DE GESTION DE CRISE

600M²
3 SITES EN PRINCIPAUTÉ

2 DATACENTERS
SUR LE TERRITOIRE MONÉGASQUE

LES ORIGINES D'ACTIS

Évolution de la demande clients pour des **« Plan d'urgence »** après les attentats du 11 Septembre

Création d'Actis en 2003

La demande de « Plan d'urgence s'étend aux **données**

Publication Bâle 2 et 3

Mise en place des **PCA / PRA**

Construction du **MonacoDatacenter** en plus de la salle informatique Telis

Extension des activités

Actis à la mise en conformité, la gestion de crise, la cybersécurité…

CONTINUITÉ D'ACTIVITÉ

LE SAVIEZ-VOUS

1/5 **entreprises** touchées par une attaque cyber a été menacée de fermeture.

20K$ **C'est le coût moyen/jour** d'interruption de service pour une entreprise.

Exclusif à Monaco

SITES DE REPLI

Des locaux de secours informatisés et sécurisés en principauté.

OUTILS ET PLATEFORME DE GESTION DE CRISE

Des outils de secours et une plateforme de main courante informatisée

ACCOMPAGNEMENTS DE GESTION DE CRISE

Des experts pour vous aider à prendre les bonnes décisions face à la crise.

FORMATIONS ET ENTRAÎNEMENTS

Faite l'expérience en conditions réelle et élargissez votre zone de confort.

Des partenaires d'exception

DC monaco DATACENTER

JAGUARDS SECURITY OPERATION CENTER

INQUEST

PARTENAIRE : INQUEST

INQUEST

Cabinet de conseil en gestion des risques

Secteurs d'activité

Cybersécurité

Accompagner les PME/entreprises depuis la prévention

EN SAVOIR PLUS

Incendie / Explosion

Bénéficier de spécialistes des sinistres liés aux

EN SAVOIR PLUS

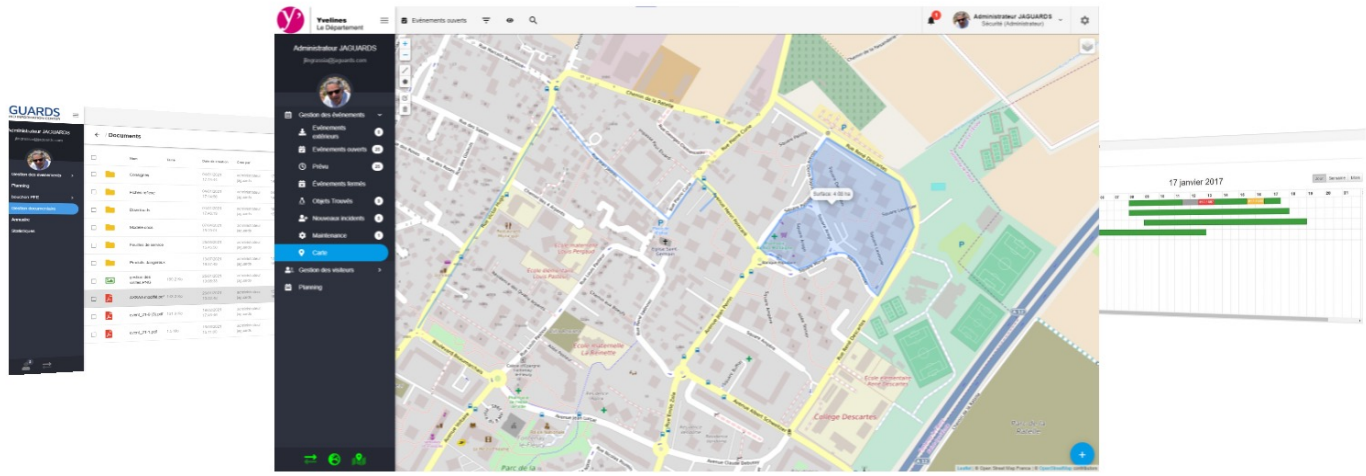
Gaël Paillet – Directeur Conseil en Cybersécurité et SI

PARTENAIRE : JAGUARDS

JAGUARDS
COMMAND INFORMATION CENTER

Main courante informatisée
Hyperviseur sureté

Communiquer – Projeter – sécuriser – Organiser – Planifier – gérér - Fluidifier



Jean-Luc Ingrassia – CEO & Product manager

QUELQUES CHIFFRES

The most important business risks in 2023: global

Ranking changes are determined by positions year-on-year, ahead of percentages.

Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*[1]	34%	*1 (44%)*	→
2	Business interruption *(incl. supply chain disruption)*	34%	*2 (42%)*	→
3	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	25%	*10 (11%)*	↑
4	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	22%	NEW	↑
5	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*[2]	19%	*5 (19%)*	→
6	Natural catastrophes *(e.g. storm, flood, earthquake, wildfire, extreme weather events)*	19%	*3 (25%)*	↓
7	Climate change *(e.g. physical, operational and financial risks as a result of global warming)*	17%	*6 (17%)*	↓
8	Shortage of skilled workforce[3]	14%	*9 (13%)*	↑
9	Fire, explosion	14%	*7 (17%)*	↓
10	Political risks and violence *(e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)*	13%	*13 (9%)*	↑

Source: (Baromètre des risques Allianz 2023)

60% des victimes de cyber attaques en 2022 sont des TPE/PME

Source: (ladepeche.fr)

27% du C.A. annuel, c'est la perte moyenne liée au temps de redémarrage du S.I. d'une PME après une attaque Cyber

Source: (ladepeche.fr)

60% des PME déposent le bilan dans les 18 mois suivants une attaque Cyber

Source: (ladepeche.fr)

QU'EST-CE QU'UNE CRISE ?

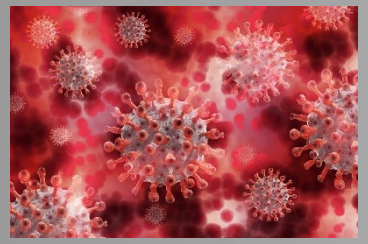
- **Souvent soudaine et brutale**
- **Forte perturbation du fonctionnement normal**
- **Menace sur la stabilité**

Quelques exemples récents


Intempéries survenues en PACA les **23 et 24 novembre 2019**.
Bilan :

- + 1000 entreprises impactées sur les zones ouest.
- Estimation moyenne des dégâts à 100 000€ et 30% de perte de CA.

(Source : CCI Nice côte d'azur – 25 novembre 2019)




Crise **Covid-19 durant l'année 2020.**
Bilan :

- Toutes les entreprises mondiales touchées
- Confinement du 17 Mars au 11 Mai : activités quasiment à l'arrêt

LES CLES DE LA PREPARATION

S'entourer de partenaires de confiance

1

Définir la stratégie et les outils de gestion de crise

2

Définir les cellules de crise

3

Identifier et cartographier les données et les compétences essentielles

4

Sensibilisation, tests et entrainements

5

Retour d'expérience, améliorations et optimisations

Actis

Etude de cas

Exemple de crise inspirée de faits réels - P1

GROUPE telis

LES FAITS : UNE ATTAQUE SURVENUE EN 2023

SOCIÉTÉ • ÉQUATEUR • MÉDIAS

Médias. Cinq journalistes équatoriens ont reçu des clés USB explosives

Une enquête pour terrorisme a été ouverte, mais les auteurs n'ont pas encore été identifiés, et leurs motivations inconnues, alors que le pays bascule chaque jour un peu plus dans la crise.

SOURCE : Courrier international

Publié le 22 mars 2023 à 11h11 Lecture 1 min.

EXEMPLE DE CRISE INSPIREE DE FAITS REELS

Date du jour de l'évènement : 28/04/2023

La **comptable** reçoit une nouvelle clé USB de certificat pour réaliser les virements bancaires.

La **comptable** reçoit également un mail du PDG lui demandant de verser les salaires au 30 Avril au lieu du 01 Mai.

Alors qu'elle est au téléphone pour confirmer les virements, **la clé USB explose**. La chaleur entraîne l'explosion de la batterie de l'ordinateur.

Le/la comptable est blessé/e,
Son ordinateur est hors service.

EXEMPLE DE CRISE INSPIREE DE FAITS REELS

Alertés par l'explosion, **les collaborateurs** avertissent les secours et maîtrisent le début d'incendie à l'aide des extincteurs.

La **direction** est informée de la situation.

La crise démarre.

Actis

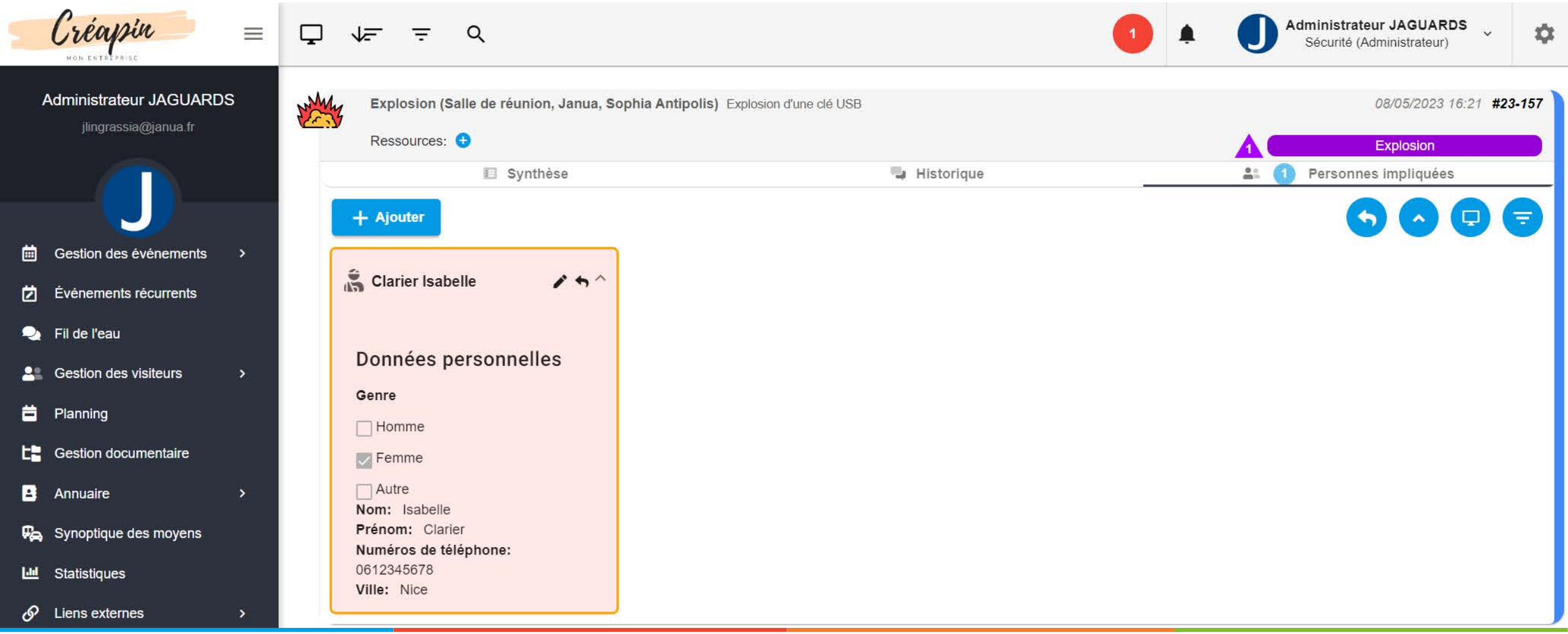
Etude de cas : Démonstration

Gérer la crise avec Jaguards, Hyperviseur sureté, main courante informatisée

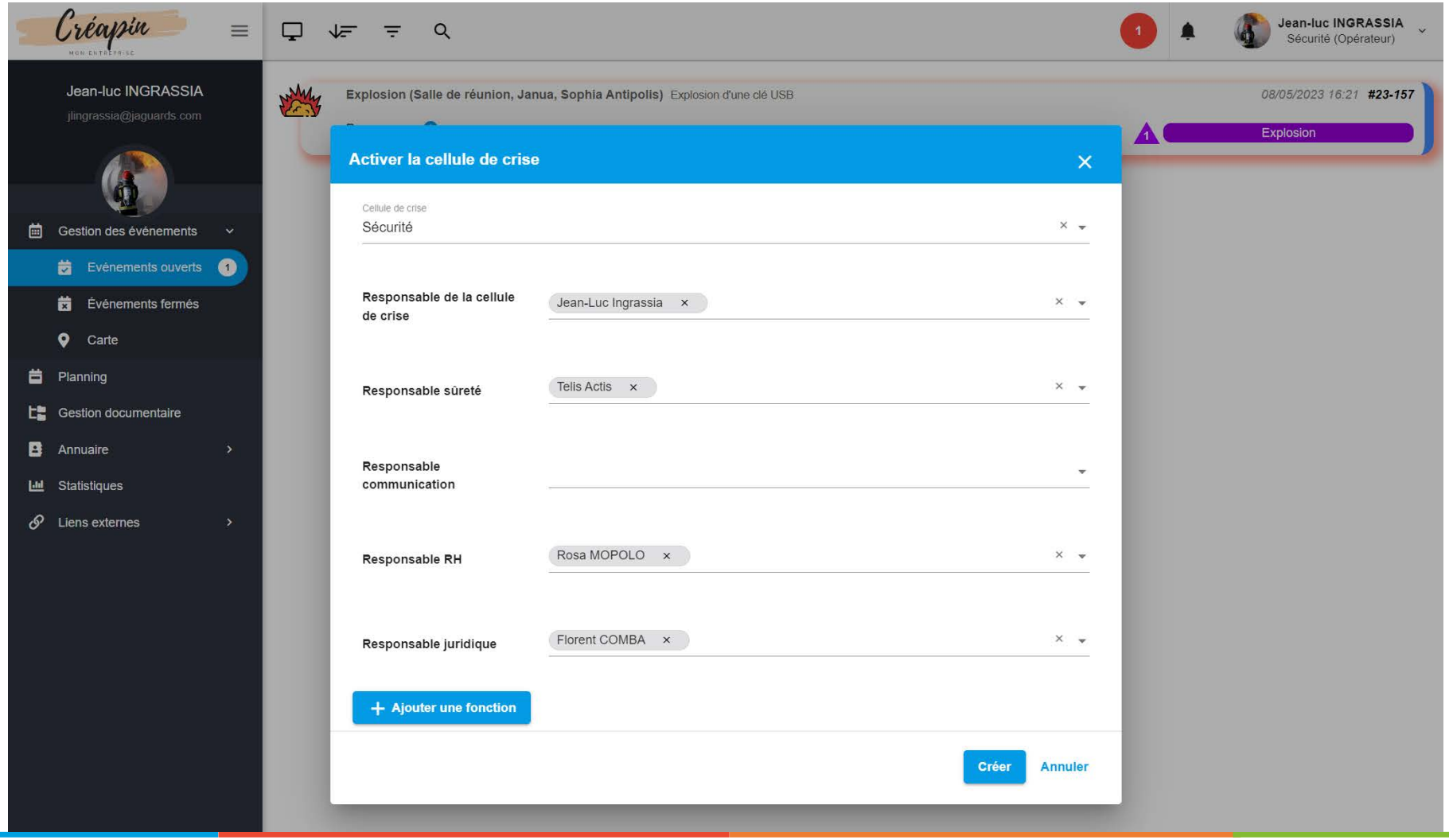
GROUPE telis

JAGUARDS
COMMAND INFORMATION CENTER

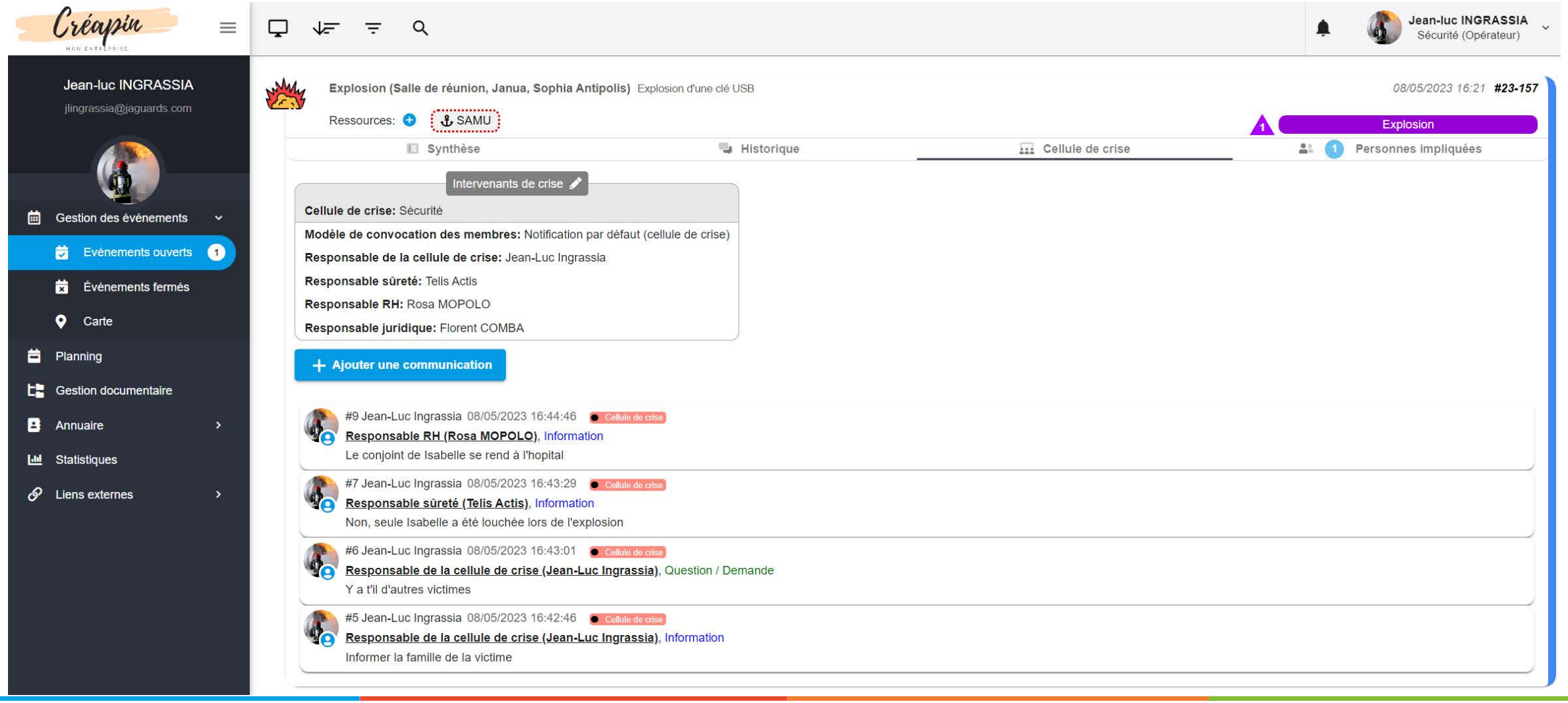
Création de l'événement sûreté explosion de la clé USB avec 1 victime en UR



Activation de la cellule de crise Sûreté



Toutes les informations de la cellule de crise sont tracées dans l'outil



Actis

Etude de cas

Exemple de crise inspirée de faits réels - P2

GROUPE telis

LES FAITS : INFECTION VIRALE SURVENUE EN 2023

Windows 10 et 11 : gare à ce malware qui attaque incognito et se propage sur clé USB

PAR BRUNO MATHIEU
LE 30/01/2023

0 COM

Des chercheurs ont découvert une nouvelle méthode de diffusion du malware PlugX, qui utilise une faille dans de l'Explorateur de fichiers de Windows. En conséquence de quoi, le logiciel malveillant opère de manière totalement invisible pour l'utilisateur.

EXEMPLE DE CRISE INSPIRÉE DE FAITS RÉELS

Les secours ont pris en charge **le/la comptable**
Le choc passé, certains **collaborateurs** retournent à leur poste.

Ils constatent alors **des lenteurs sur le réseau, certains fichiers partagés sont inaccessibles**.

Le RSSI est informé et prévient la **direction.**
La crise évolue.

Actis

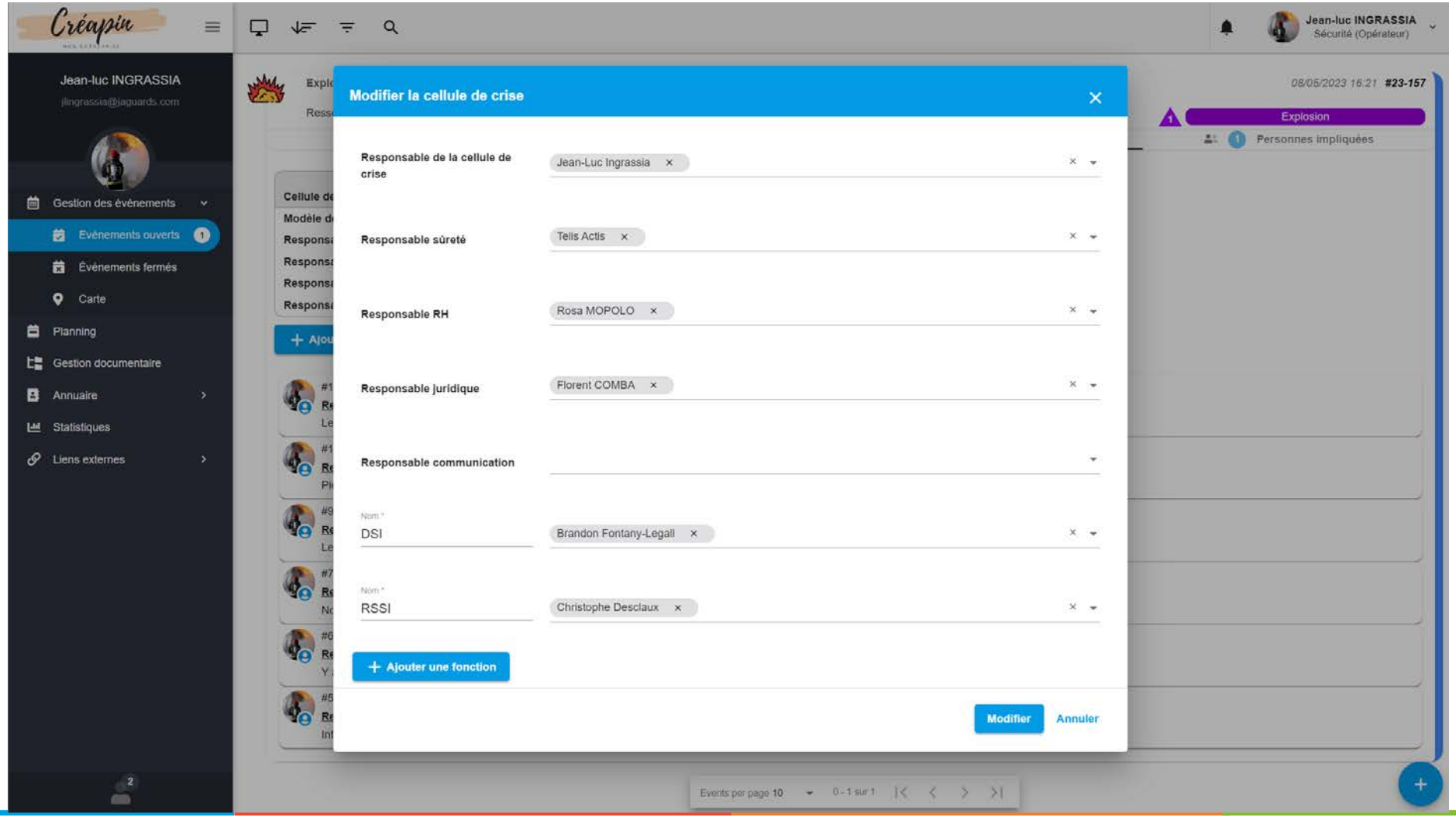
Etude de cas : Démonstration

Gérer la crise avec Jaguards, Hyperviseur sureté, main courante informatisée

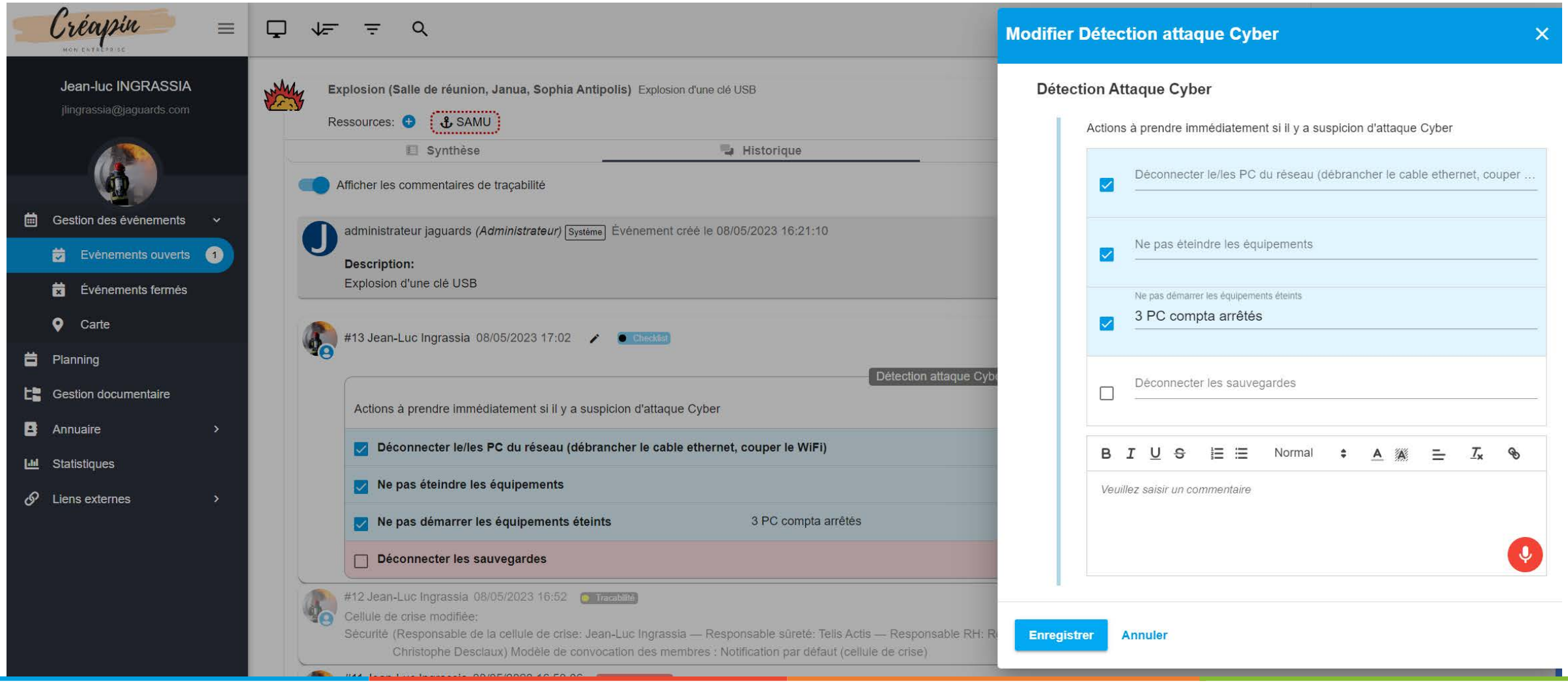
GROUPE telis

JAGUARDS
COMMAND INFORMATION CENTER

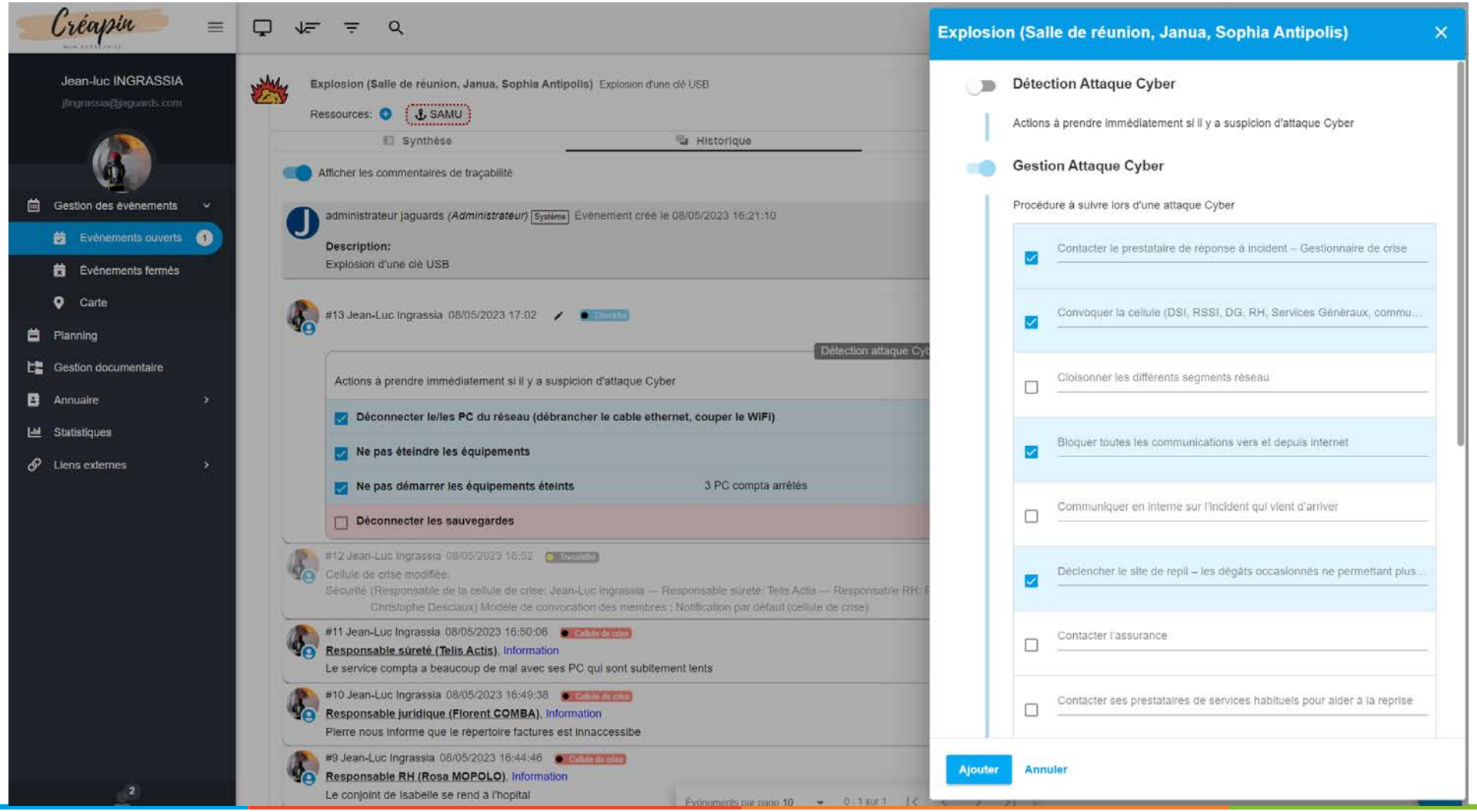
Suite au signalement du service compta, on active la cellule de crise cyber (ajout RSSI et DSI)



Activation de la procédure détection attaque Cyber



Application de la procédure de crise cyber



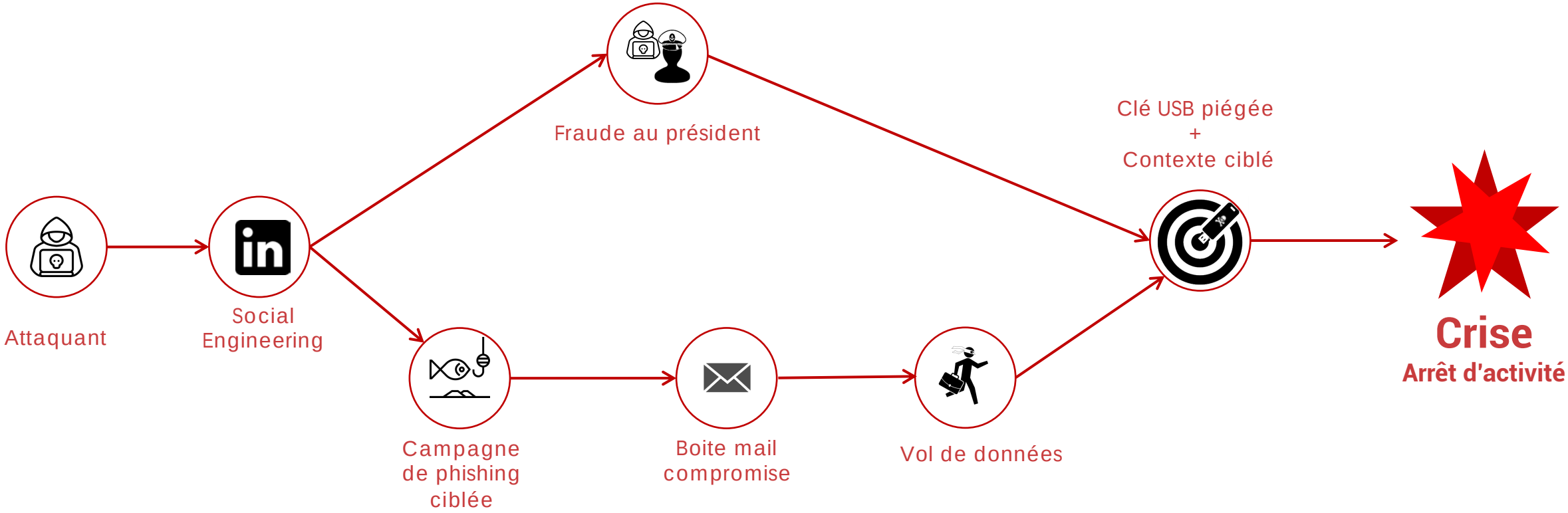
Actis

Etude de cas : Bilan

Comment réagir efficacement face à cette crise ?

GROUPE telis

KILL CHAIN INCIDENT



Quelles sont les conséquences directes de l'attaque ayant provoqué la crise ?

Bilan Humain

- 1 Collaborateur clé blessé

⇨ Durée du parcours de recrutement : Jusqu'à 11 semaines
33% des recruteurs abandonnent devant la difficulté.

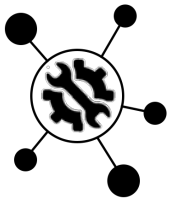
Bilan 2022 APEC

- Les équipes sont choquées

⇨ Minimum 3 mois avec suivi psychologique
Jusqu'à 20% auront des séquelles à vie

Deuxièmeavis.fr – Les conséquences du stress post traumatique

Quelles sont les conséquences directes de l'attaque ayant provoqué la crise ?



Bilan Technique

- Indisponibilité d'une partie des locaux

⇨ Durée de l'enquête
Expertise assurance
Durée des travaux

- Le réseau et le SI sont compromis et inutilisables en l'état

⇨ 1 semaine de black out minimum
Temps nécessaire au redémarrage du S.I. :
- 80% sous 3 mois
- 100% sous 6 mois

INQUEST – Bilan 2022

EXEMPLE DE CRISE INSPIREE DE FAITS REELS

Quelles sont les conséquences directes de l'attaque ayant provoqué la crise ?

Bilan Financier

- 27% du C.A. perdu en moyenne
- Coût de la gestion de crise : 200-250k€
- Coût des prestations d'aide au redémarrage du SI : 200-250k€

⇨ Incertitude sur la pérennité de l'entreprise

Dans 60% des cas : dépôt de bilan après 18 mois

QUEL EST LE COÛT DE LA CRISE?

Perte de CA + Perte de productivité + Coût de la restauration + Frais Indirects + Impact sur l'image de marque

Perte de CA

CA horaire x Temps d'interruption x Pourcentage d' indisponibilité

Perte de productivité

(Salaire horaire de l'employé n°1 x % de productivité) + (Salaire horaire de l'employé n°2 x % de productivité) + etc (autant de fois que vous avez d'employés)

Coût de restauration

Facture de votre prestataire informatique et/ou charge salariale de votre service IT pour la restauration de votre système d'information et de vos données.

Frais indirects

Coût de relocalisation, + Coût de logistique et d'intendance + Coût de votre communication de crise + application du RGPD + frais liés à la gestion de crise.

Impact sur l'image

Image pénalisante auprès du public / Perte de clients potentiels / Départ de clients dus à la crise.

Actis à votre service

Contacter Actis:

Par téléphone : +377 97.98.18.18

Par Mail : contact@actis.mc

Plus d'infos : www.actis.mc

RELATION CLIENTS

Thierry **LERAY**

Marion **SOLER**

Jean-Pierre **BALLET**

Gwendoline **GIANANGELI**

Alexandre **AVID**

Damien **ENGRAND**

Suivez notre actualité :

@Actis SAM @ActisMonaco