Extorsion digitale

L'extorsion digitale (avec demande de rançon) est de plus en plus commune et « publique » - Elle consiste généralement en un hacking des données avec éventuellement piratage complet des systèmes et réseaux de l'organisation, et surtout « kidnapping » des données.

Qui pourront être restituées uniquement contre paiement d'une rançon, de quelques milliers d'euros à plusieurs millions

Il est ici requis d'avoir pris une approche **pro-active** de l'aspect cybersécurité non pas pour éviter cette situation mais pour en limiter l'impact si elle devait se passer.

Ne pas oublier également que les pirates peuvent également avoir l'intelligence de cibler l'un de vos salariés, lui faire du chantage, l'isoler et l'amener à de l'extorsion digitale sans que vous n'en ayez connaissance.

Ici les mesures classiques pro-actives sont principalement par le biais de mise en place de formations régulières en cybersécurité, de mise en place de politiques de changement de mot de passe et/ou de systèmes de cryptage.
Il est important d'établir dans la culture d'entreprise le réflexe de rapporter ce genre de demande de chantage afin de vérifier la réalité du risque (notamment en raison du nombre significatif de scams)

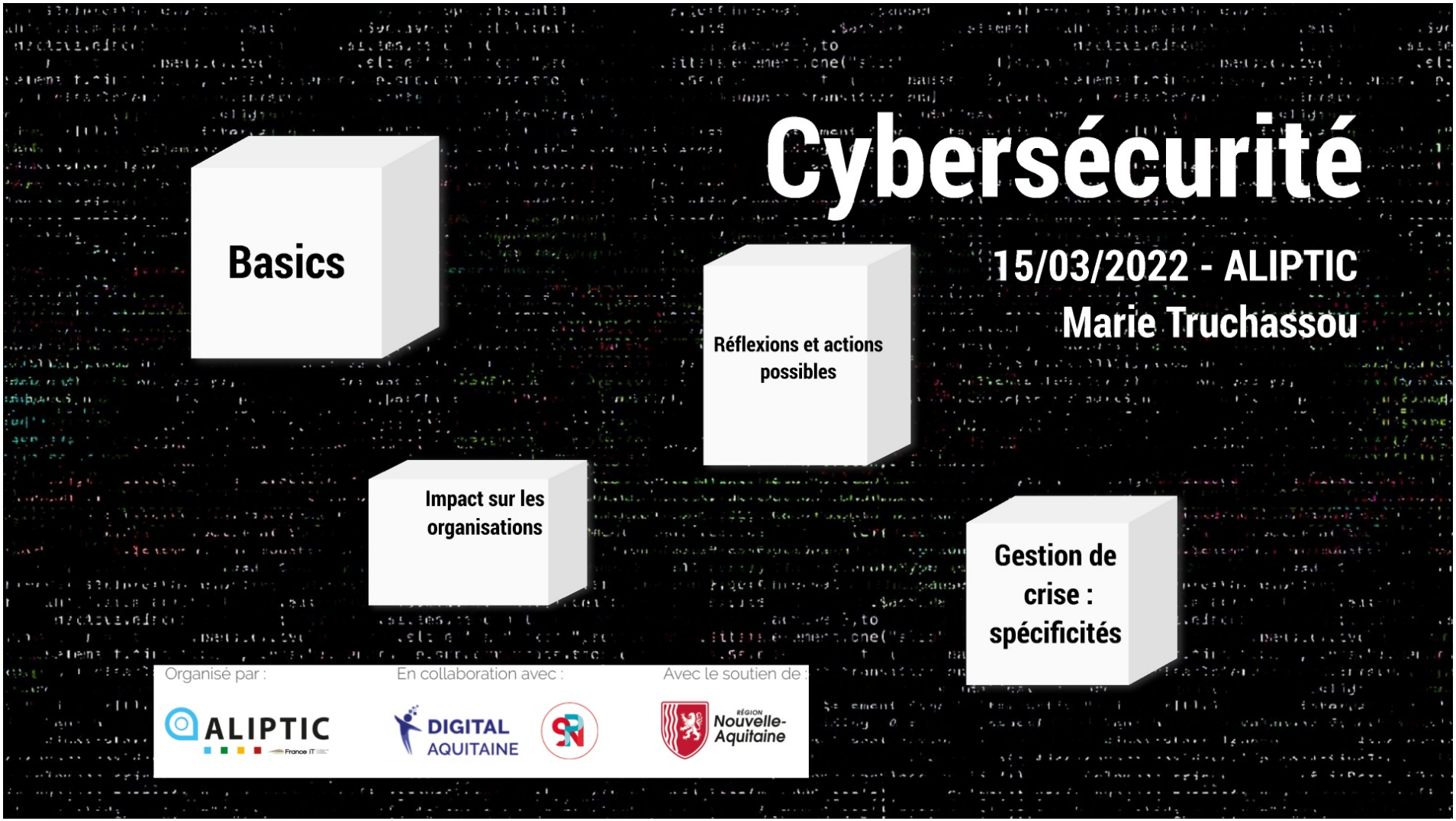
Solutions

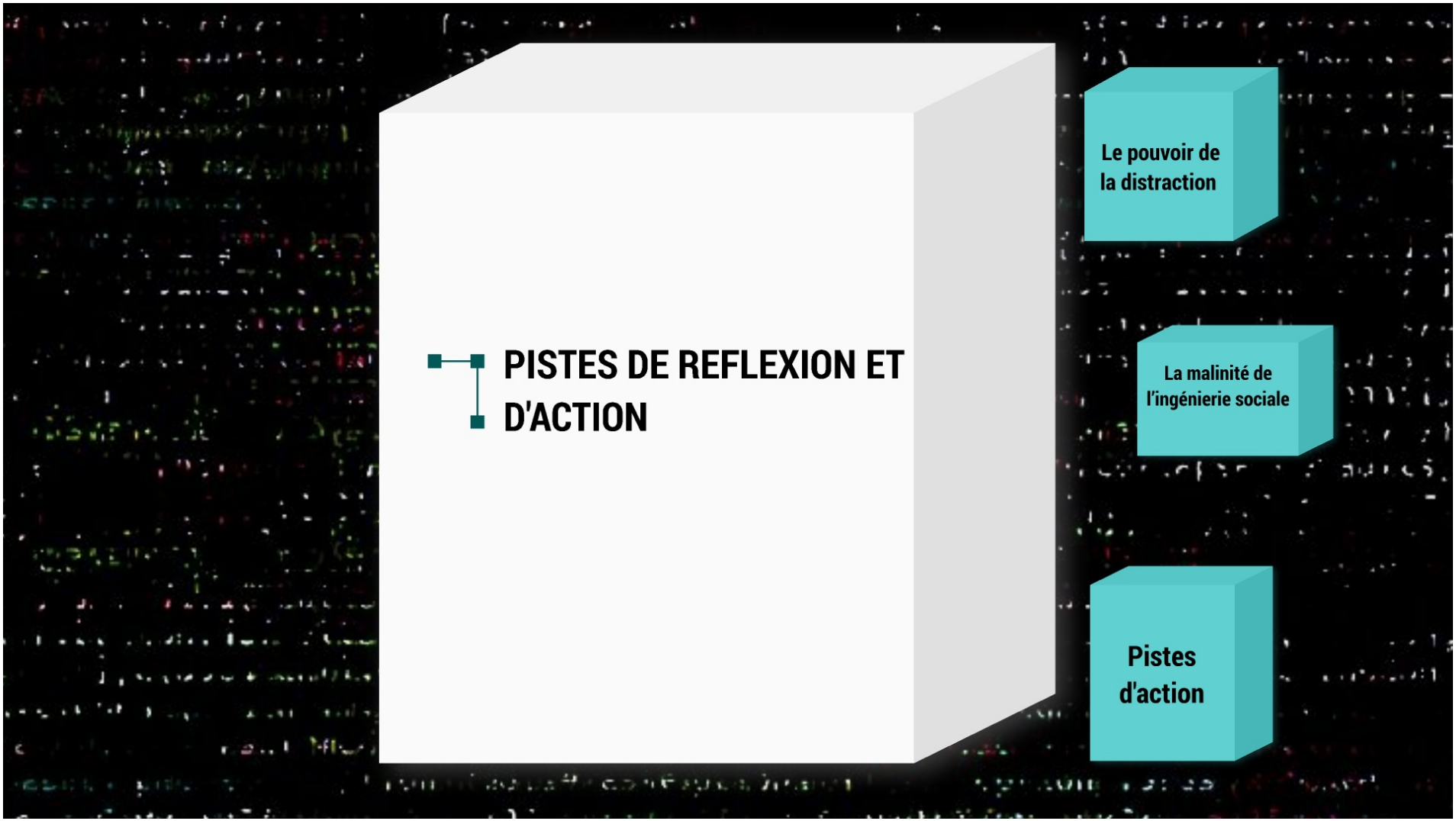
Mesures classiques pro-actives:

- mise en place de formations régulières en cybersécurité pour l'ensemble des salariés,
- mise en place de politiques de changement de mot de passe et/ou de systèmes de cryptage.

Il est important d'**établir dans la culture d'entreprise** le réflexe de rapporter ce genre de demande de chantage afin de vérifier la réalité du risque (notamment en raison du nombre significatif de scams)


Hot topic pour les organisations
Story
Extorsion digitale

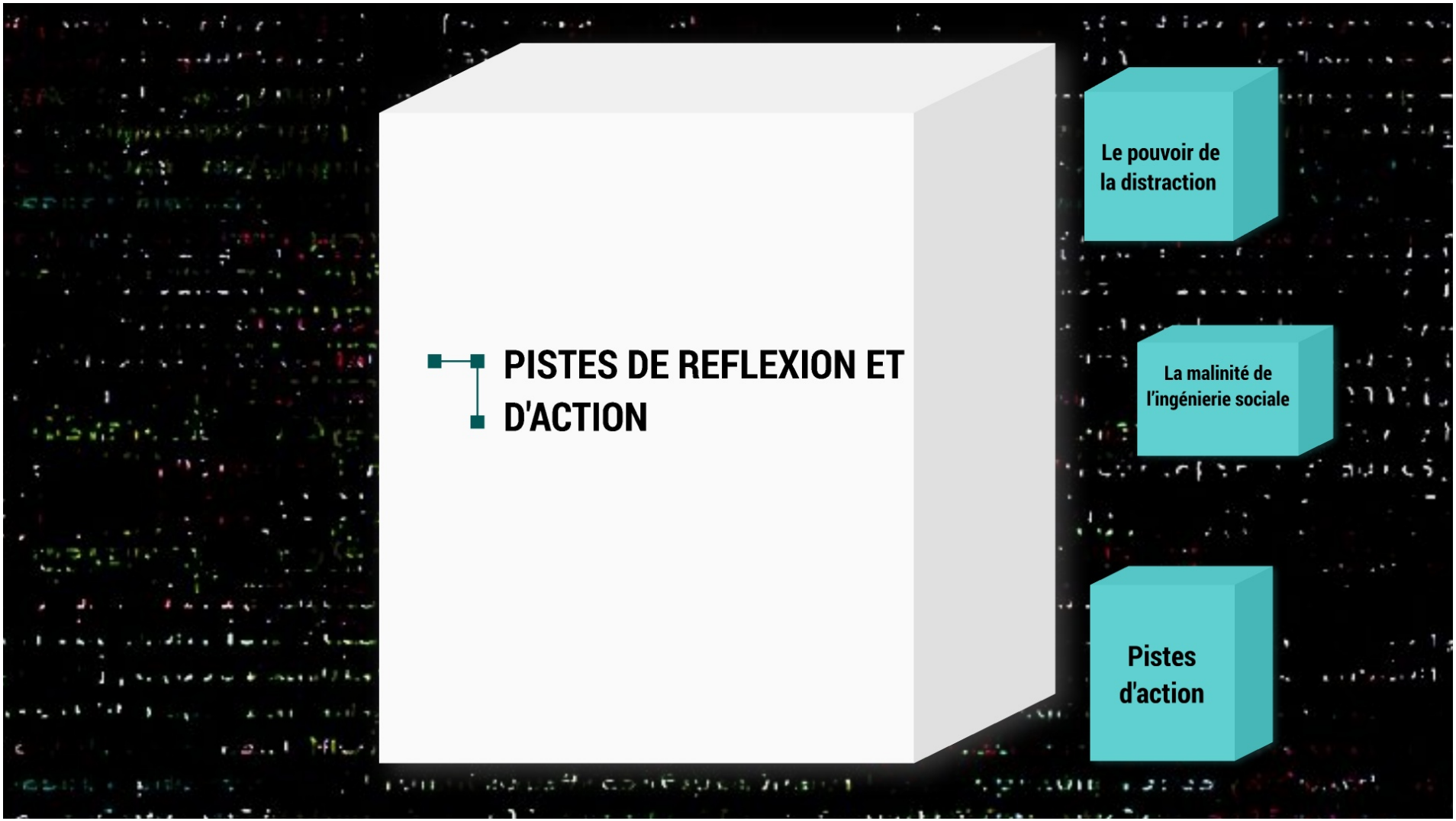

Cybersécurité
15/03/2022 - ALIPTIC
Marie Truchassou
Basics
Réflexions et actions possibles
Impact sur les organisations
Gestion de crise : spécificités
Organisé par :
ALIPTIC
France IT
En collaboration avec :
DIGITAL AQUITAINE
Avec le soutien de :
Région Nouvelle-Aquitaine


PISTES DE REFLEXION ET D'ACTION
Le pouvoir de la distraction
La malinité de l'ingénierie sociale
Pistes d'action

Le pouvoir de la distraction

Le rapport annuel State of Work (US) de 2020, réalisé par le spécaliste du logiciel Workfront estime qu'en Moyenne, les salaries sont interrompus environ 14 fois par jour, principalement par des interactions technologiques (email, social media, notifications etc)

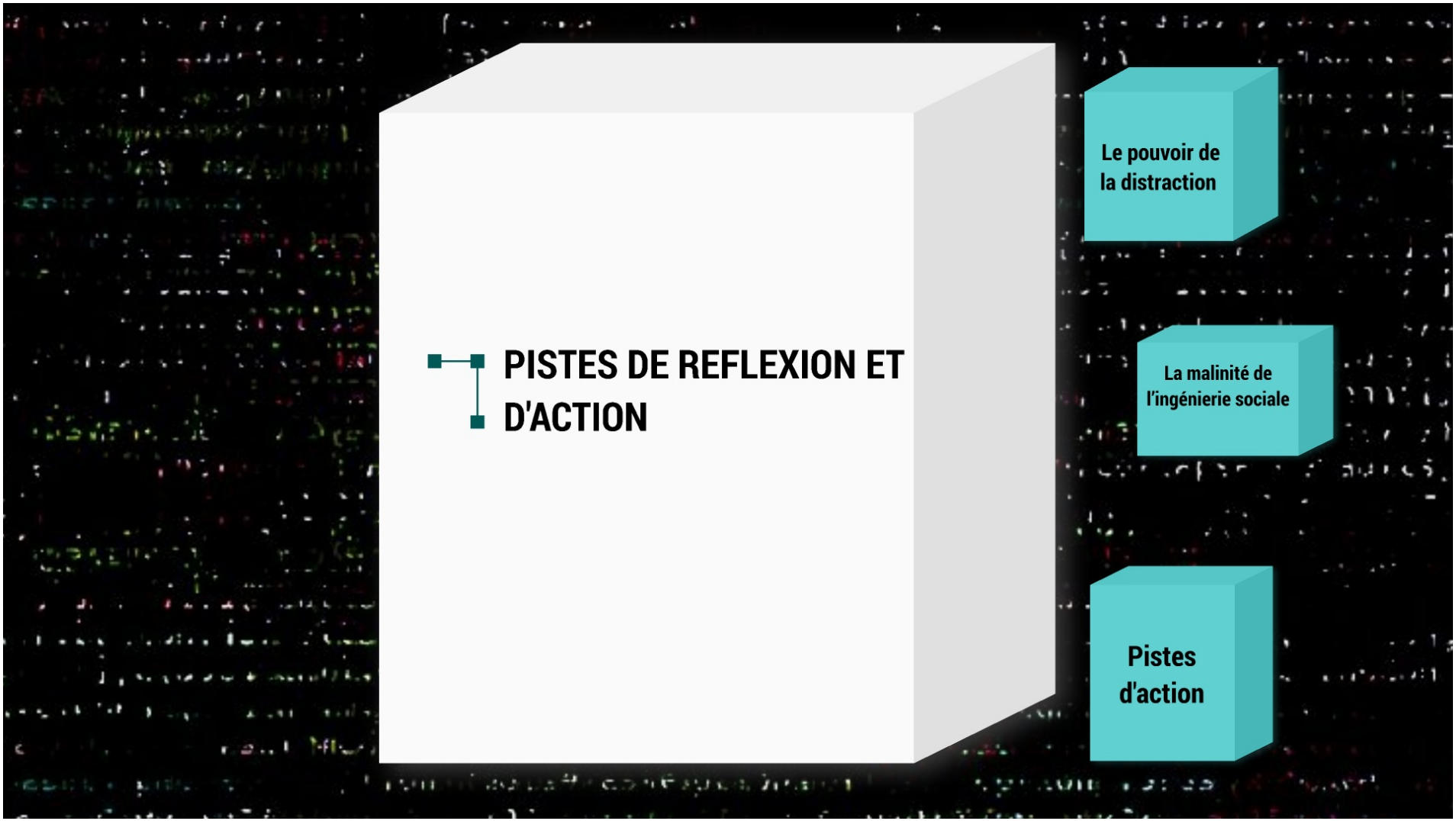
Cette même enquête établi qu'il faut parfois jusqu'à 20 minutes après une telle interruption de la tâche initiale.


PISTES DE REFLEXION ET D'ACTION
Le pouvoir de la distraction
La malinité de l'ingénierie sociale
Pistes d'action

La malinité de l'ingénierie sociale

L'ingénierie sociale peut être définie comme une stratégie amenant à la mise en place d'une opération méthodique utilisée pour tromper les êtres humains afin qu'ils divulguent des informations sensibles, sans exploiter le système informatique ou le réseau en question

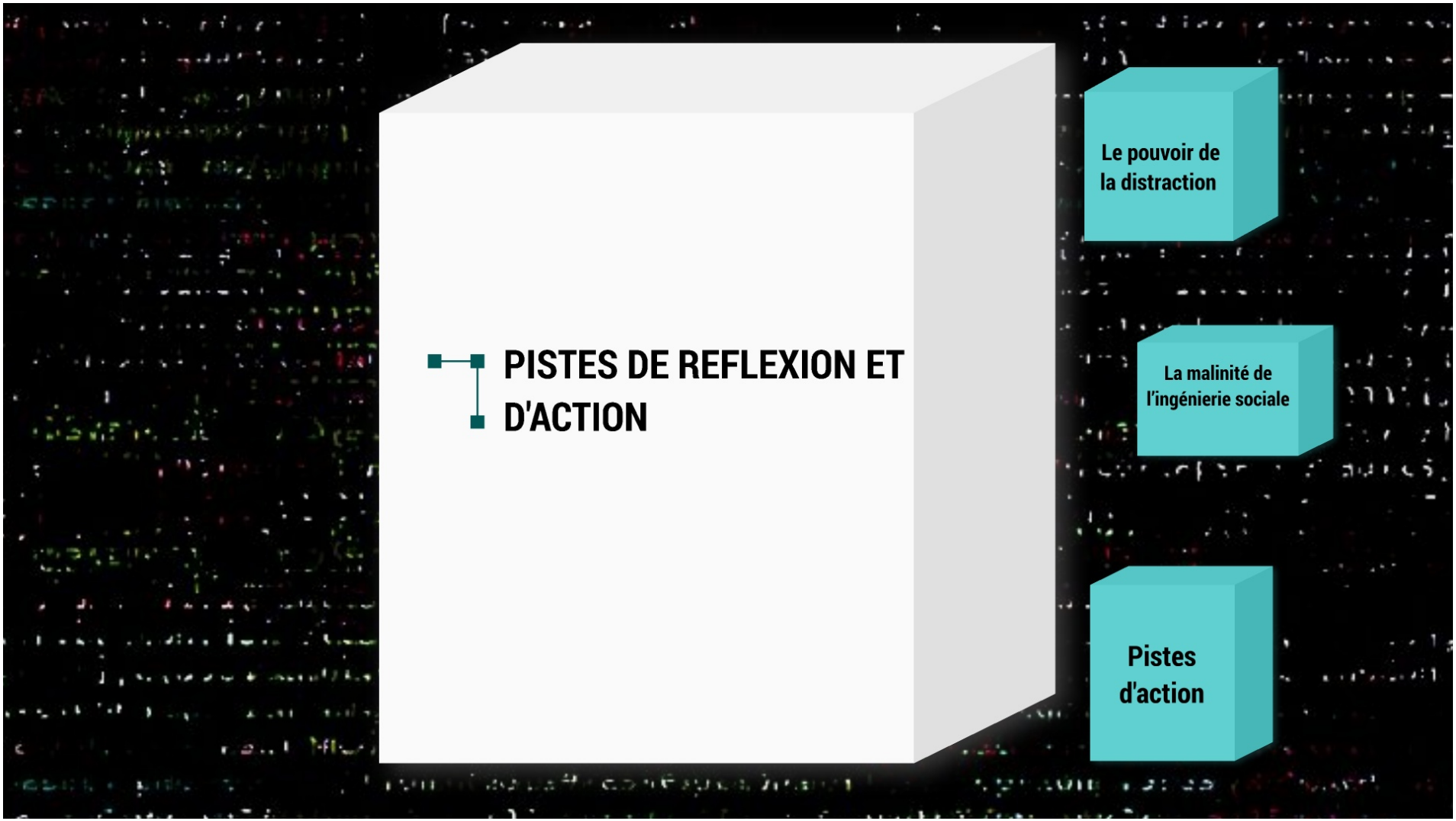
De fait, les salaries sont les principales proies de l'ingénierie sociale.

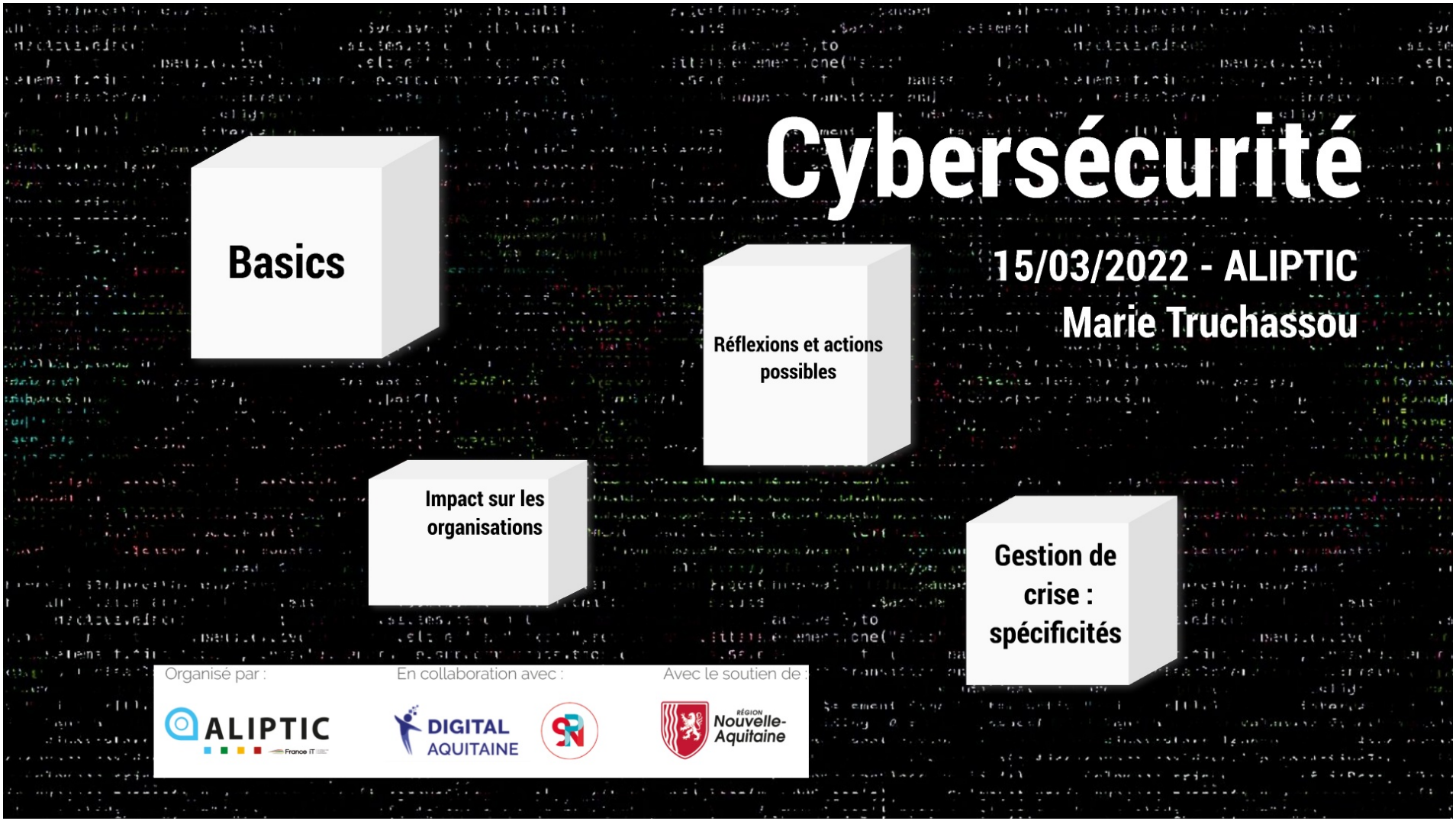

PISTES DE REFLEXION ET D'ACTION
Le pouvoir de la distraction
La malinité de l'ingénierie sociale
Pistes d'action

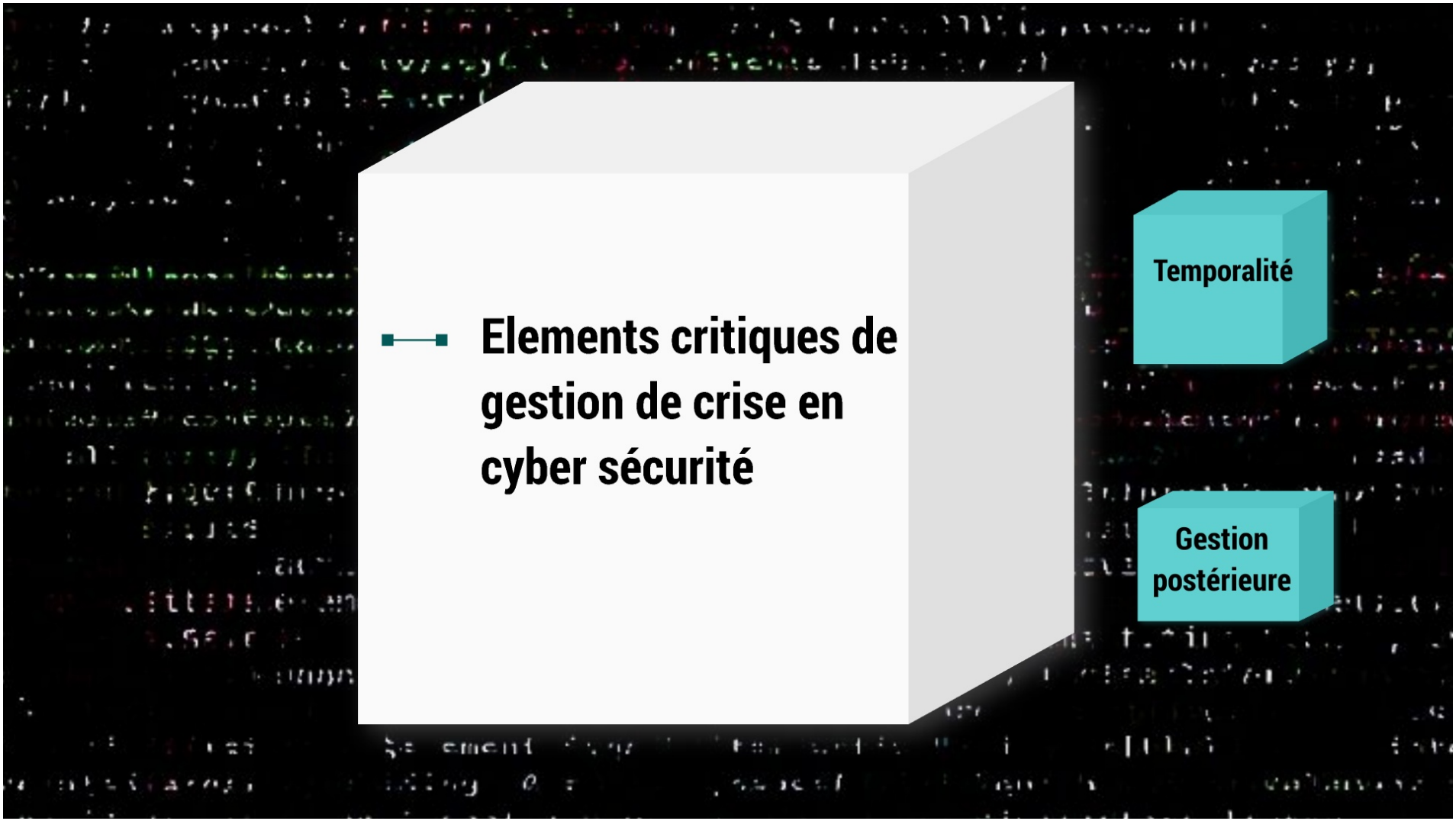
Pistes d'action

2 groupes :

- le développement de bonnes pratiques et de bons reflexes intégrées dans la culture d'entreprise
- la gestion d'un incident de cybersécurité avec mise en place d'un processus, interlocuteurs et responsabilités.


PISTES DE REFLEXION ET D'ACTION
Le pouvoir de la distraction
La malinité de l'ingénierie sociale
Pistes d'action


Cybersécurité
15/03/2022 - ALIPTIC
Marie Truchassou
Basics
Réflexions et actions possibles
Impact sur les organisations
Gestion de crise : spécificités
Organisé par :
ALIPTIC
France IT
En collaboration avec :
DIGITAL AQUITAINE
Avec le soutien de :
Région Nouvelle-Aquitaine


Elements critiques de gestion de crise en cyber sécurité
Temporalité
Gestion postérieure

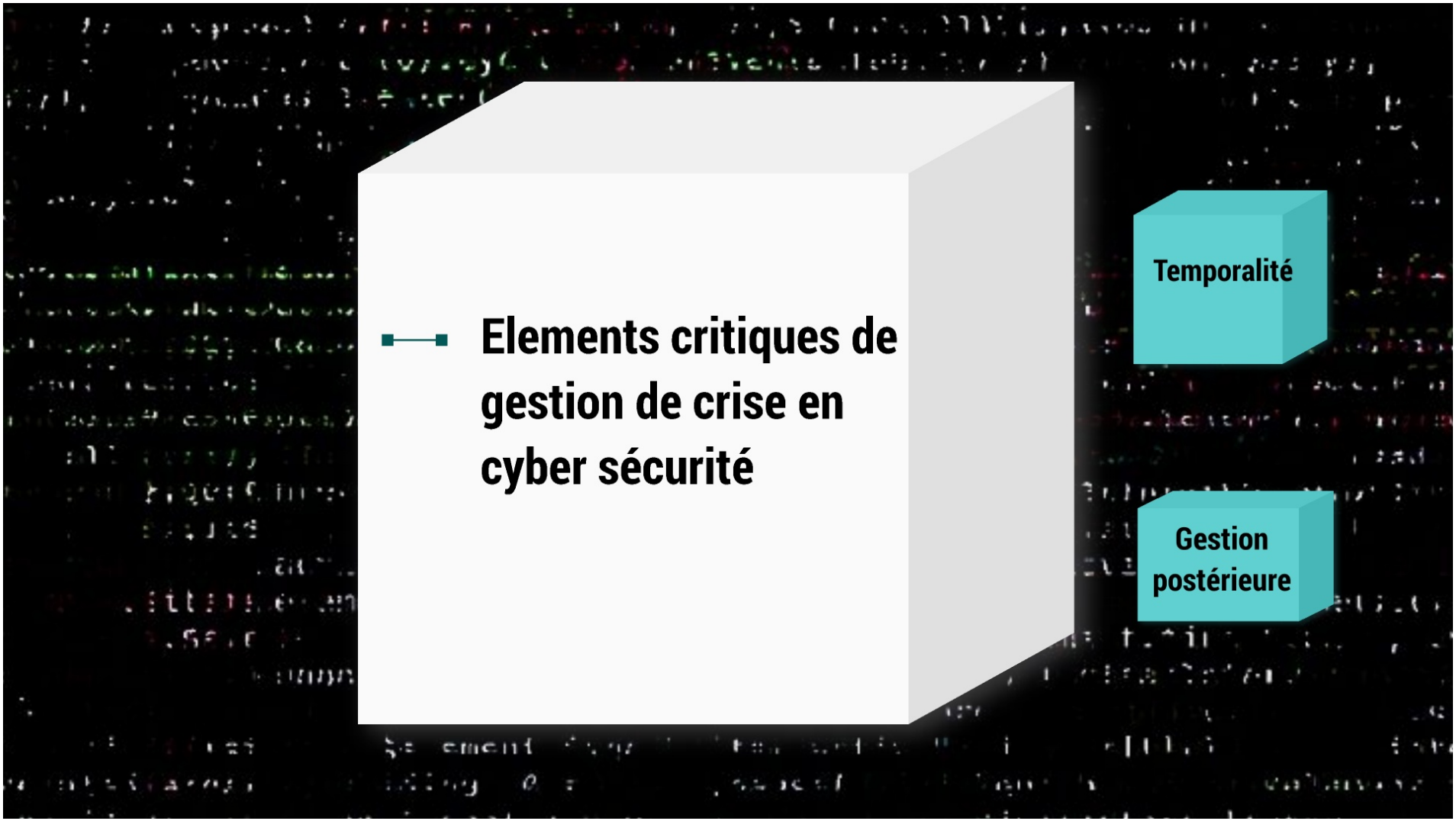
Temporalité

- En general la temporalité est critique ici (il peut s'agir parfois de quelques minutes) et de ce fait la connaissance préalable par les salaries des étapes à prendre est critique ici.

Il est donc recommandé que le salarié ait connaissance des process et contacts référents, ce qui induit une formation préalable, récurrente et continue mais également la mise en place de supports de rappel de ces procédures (disponibles rapidement, en format papier, carte contact mise sur le bureau etc)

- En function du type de cyberattaque, il peut être necessaire de déconnecter du réseau ou de prendre d'autres mesures protectrices. Ces dernières doivent être identifiées. La cybersécurité étant une forme de criminnalité, il ne faut pas oublier l'aspect "enquête" que certaines stuations vont engendrer,
mais également de faire une analyse des reseaux et certains systemes ne sont alors pas disponibles.

- L'approche pro-active de la cybersécurité permet de bénéficier de l'avantage de pouvoir estimer le temps necessaire pour la realisation de cette étape d'évaluation, et également de pouvoir identifier comment la continuité/l'ajustement de l'activité peut être anticipée. La communication vis à vis du client, des prestataires, mais également pour l'enquête (ANSSI, police etc) peut également être anticipée et permettre une "limitation" de l'impact de l'inconfort d'une telle situation.

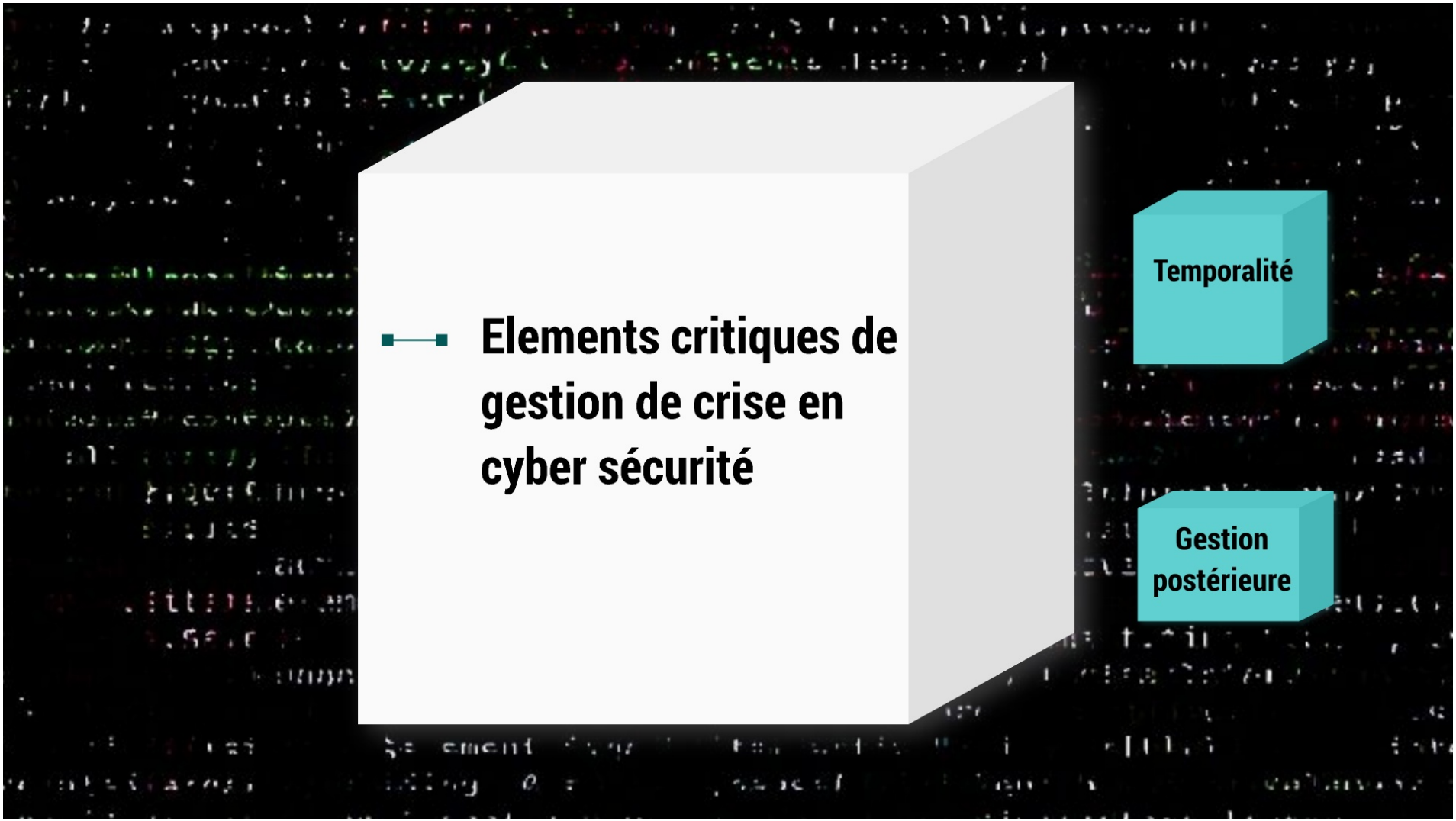

Elements critiques de gestion de crise en cyber sécurité
Temporalité
Gestion postérieure

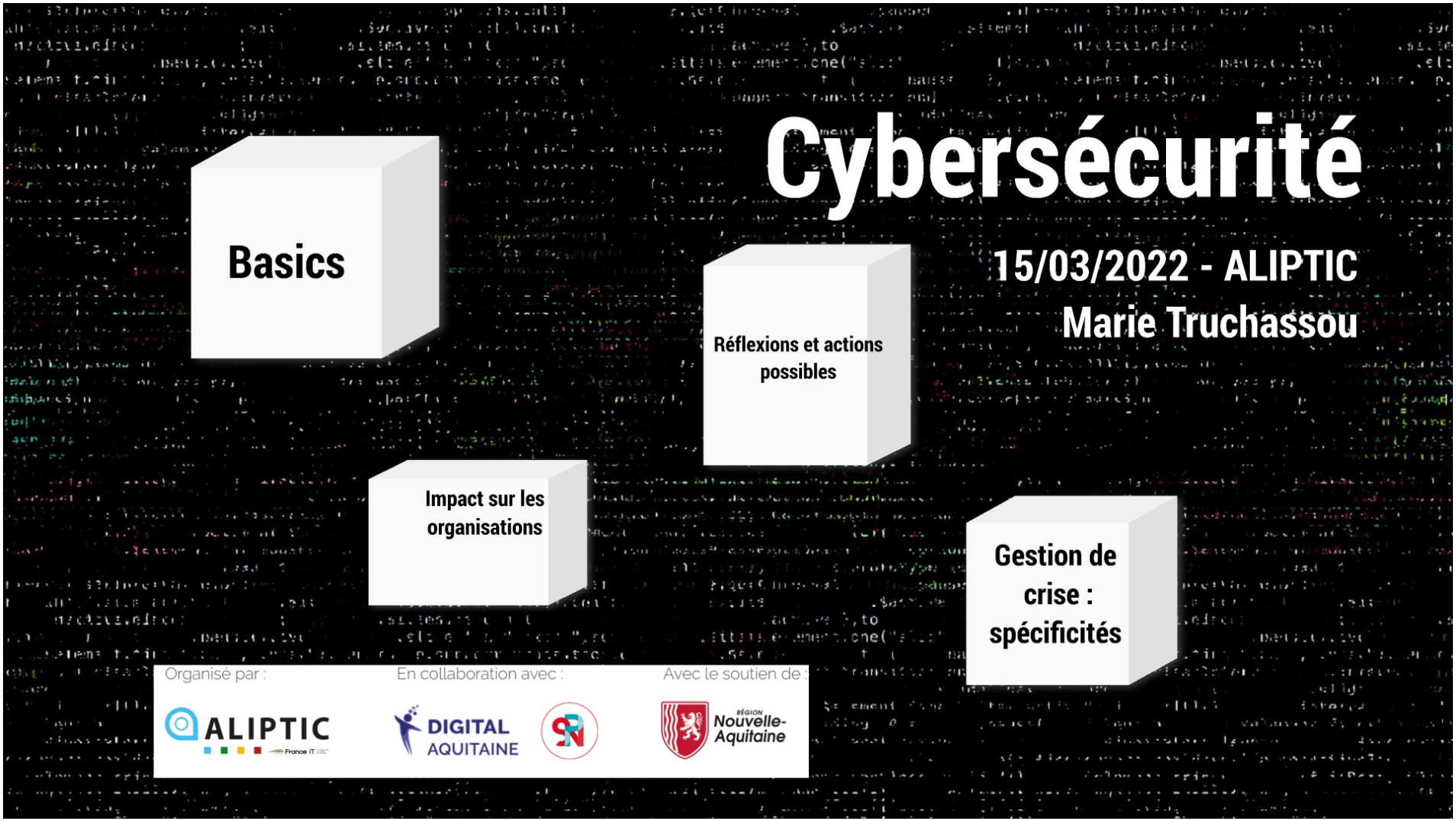
Récupérer, Reporter, S'inspirer

- Si la crise de cybersécurité implique de récupérer les données, elles peuvent ensuite récupérées à partir de la sauvegarde la plus récente. Encore faut il avoir une sauvegarde ! C'est un point crucial à intégrer dans les procédures et approches de la cybersécurité au sein de votre organisation.

- Il est important d'avoir conscience qu'un piratage des données implique des obligations de communication auprès du client final, des individus dont les données ont pu être piratées en cas de données individuelles. Selon le type de données, cela peut créer un risque legal et financier non négligeable (confère RGPD notamment)

- S'inspirer : Chaque crise est l'occasion de s'inspirer pour améliorer le process existant - l'étape d'analyse a posteriori et d'ajustement des approches et procédures existantes est primordiale. Encore plus dans le domaine de la cybersécurité ou la technicité et complexité du domaine implique des changements et ajustements constants.


Elements critiques de gestion de crise en cyber sécurité
Temporalité
Gestion postérieure


Cybersécurité
15/03/2022 - ALIPTIC
Marie Truchassou
Basics
Réflexions et actions possibles
Impact sur les organisations
Gestion de crise : spécificités
Organisé par :
ALIPTIC
France IT
En collaboration avec :
DIGITAL AQUITAINE
Avec le soutien de :
Région Nouvelle-Aquitaine