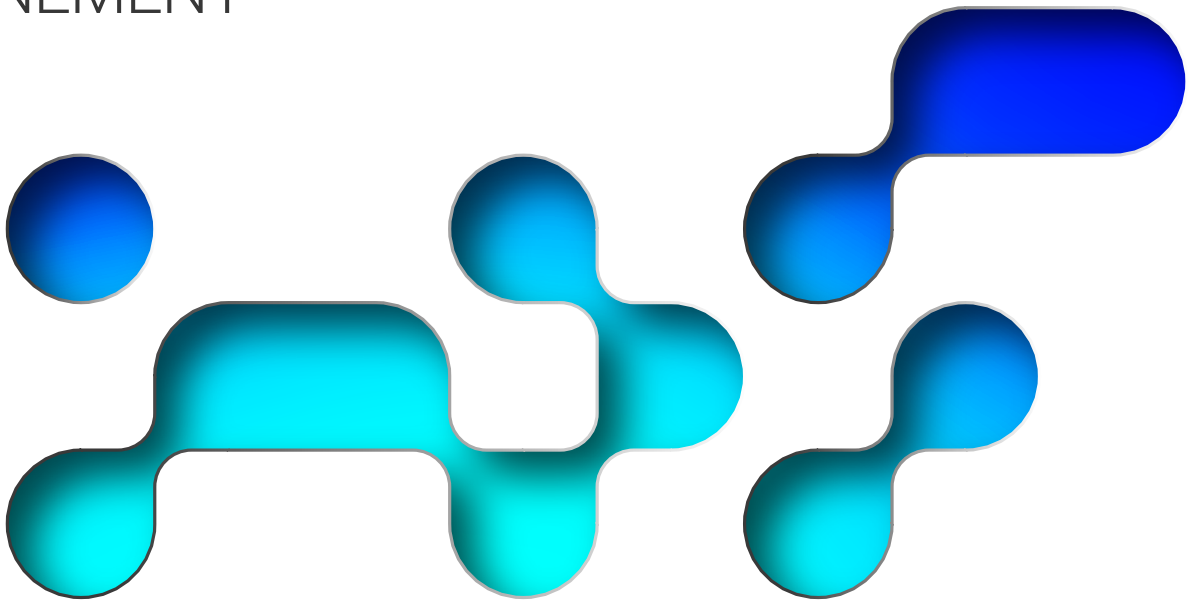
CAMPUS CYBER

FICHE MÉTHODE RANÇONGICIEL

GROUPE DE TRAVAIL : GESTION DE CRISE CYBER ET ENTRAINEMENT



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BANQUE DE FRANCE
EUROSYSTÈME

AMRAE
la Maison du risk management

CCA
Club de la Continuité d'Activité

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CESIN

CLUSIF

EXERCICE RANÇONGICIEL

DÉFINITION

Un rançongiciel (EN: *ransomware*) est un programme malveillant exfiltrant et/ou chiffrant les données du parc informatique, avec une demande de rançon.

On considèrera ici la crise par rançongiciel comme conduisant à une **indisponibilité** d'une partie significative du **parc informatique** mettant en jeu la **survie de l'organisation.**

OBJECTIFS

- **Sensibiliser les collaborateurs aux crises cyber,** et les préparer aux impacts induits par ce type d'incident ;
- **Identifier les impacts** potentiels de la diffusion d'un rançongiciel (durée, priorisation) et la **prise de décision** ;
- **Tester les procédures de réponse à incidents** vis-à-vis de la menace rançongiciel ;
- **Identifier les capacités de reconstruction,** notamment la possibilité de remonter les sauvegardes existantes sur certaines briques critiques (Active Directory, VPN, virtualisation, etc...).

DURÉE

Selon type d'exercice, une durée longue permettra d'**engager les travaux sur la continuité et la reconstruction** en y incluant les aspects de sécurisation. Un exercice d'une journée semble être une proposition convenable.

PUBLIC VISÉ

- **Cellule décisionnelle** : membres de la direction, dont communication, juridique, métiers, fonctions support (ressources humaines, etc..) ;
- **Cellules opérationnelles** : SI, SSI, Equipes métiers ;
- **Externes** : Autorités, Prestataires de crise, Assureurs, Fournisseurs (notamment sur l'interconnexion de services numériques).

IMPACTS

Internes :

- Indisponibilité (partielle ou totale) des services critiques et vitaux ;
- Désorganisation du travail voire cessation d'activité ;
- Reconstruction longue, impact financier.

Externes :

- Perte de confiance des partenaires, isolation ;
- Risques juridiques (non-conformités contractuelles / réglementaires) ;
- Dégradation d'image, dans certains cas, risques systémiques pour l'écosystème (banques, télécoms, etc.)

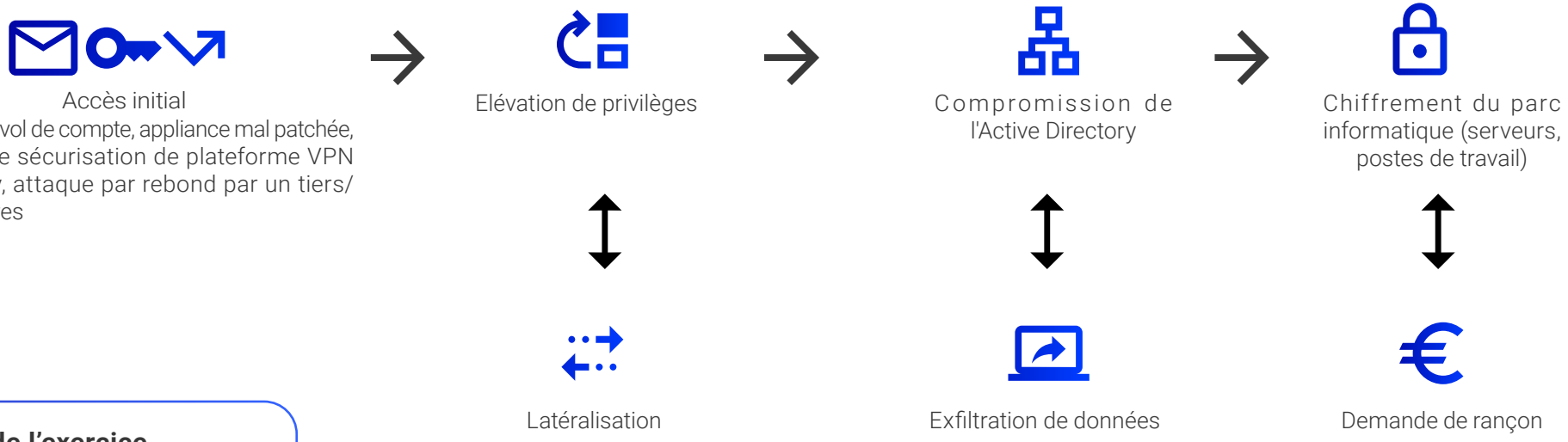
PRÉPARATION, RESSOURCES ET LOGISTIQUE

- Utilisation de **ressources documentaires** (TTPs : tactiques, techniques et procédures) et retex pour construire le scénario ;
- **Moyen d'intervention sur les datacenters** (transports, accès) si nécessaire ;
- Identification d'un **moyen d'alerte** (notamment si l'exercice est non notifié) ;
- Préparation d'**inputs techniques** afin d'alimenter les équipes ;
- Pour la reconstruction, selon la maturité, l'exercice pourra simplement évoquer cette partie, ou proposer un outillage simulant une infrastructure à reconstruire.

EXERCICE RANÇONGICIEL

Profil d'attaquants : Cybercriminel (Groupes de rançongiciel)

EXEMPLE DE KILL CHAIN *



Phases de l'exercice

1. Phase de découverte pour comprendre la situation – phase restreinte ;
2. Montée de l'attaque (signaux faibles) ;
3. Accroissement des impacts (déploiement large du rançongiciel) ;
4. Phase de remédiation.

* Pour approfondir, consulter le MITRE ATT&CK

EXERCICE RANÇONGICIEL

VARIANTES

Débutant : Exercice avec le COMEX cellule décisionnelle.

Intermédiaire : Exercice technique ou opérationnel pour la cellule de crise cyber.

Expérimenté : Exercice multi-cellules avec opérationnelle et décisionnelle.

ÉLÉMENTS ÉVALUABLES

- Bonne **compréhension** des **spécificités de la menace ransomware** ;
- Bonne **organisation de la cellule** (intégration, prise de décision, rôles, application des procédures etc.) ;
- Robustesse de la capacité de **reconstruction de l'activité informatique** et des capacités de reprise disponibles (sauvegardes immuables, bulles sécurisées, etc.) ;
- Echanges avec l'attaquant sur la rançon ;
- **Communication avec les clients** dans le contexte d'une attaque rançongiciel.

A noter : ce type de scénario se concentre généralement sur le démarrage de la crise. Il est donc peu recommandé pour évaluer la gestion de la crise dans le temps.

COMPÉTENCES DÉVELOPPÉES

- **Coordination de crise** dans un scénario extrême (cinétique rapide d'attaque, besoin d'échanger rapidement) ;
- Identification des **mesures d'isolation et de défense** (segmentation réseaux, extinction de machines ou d'application, etc.) ;
- **Coordination** des équipes CSIRT/SOC, coordination avec la communication, avec les équipes IT, etc.. ;
- Entrainement à la **remontée des sauvegardes** à large échelle ;
- Orchestration de la **reconstruction**.

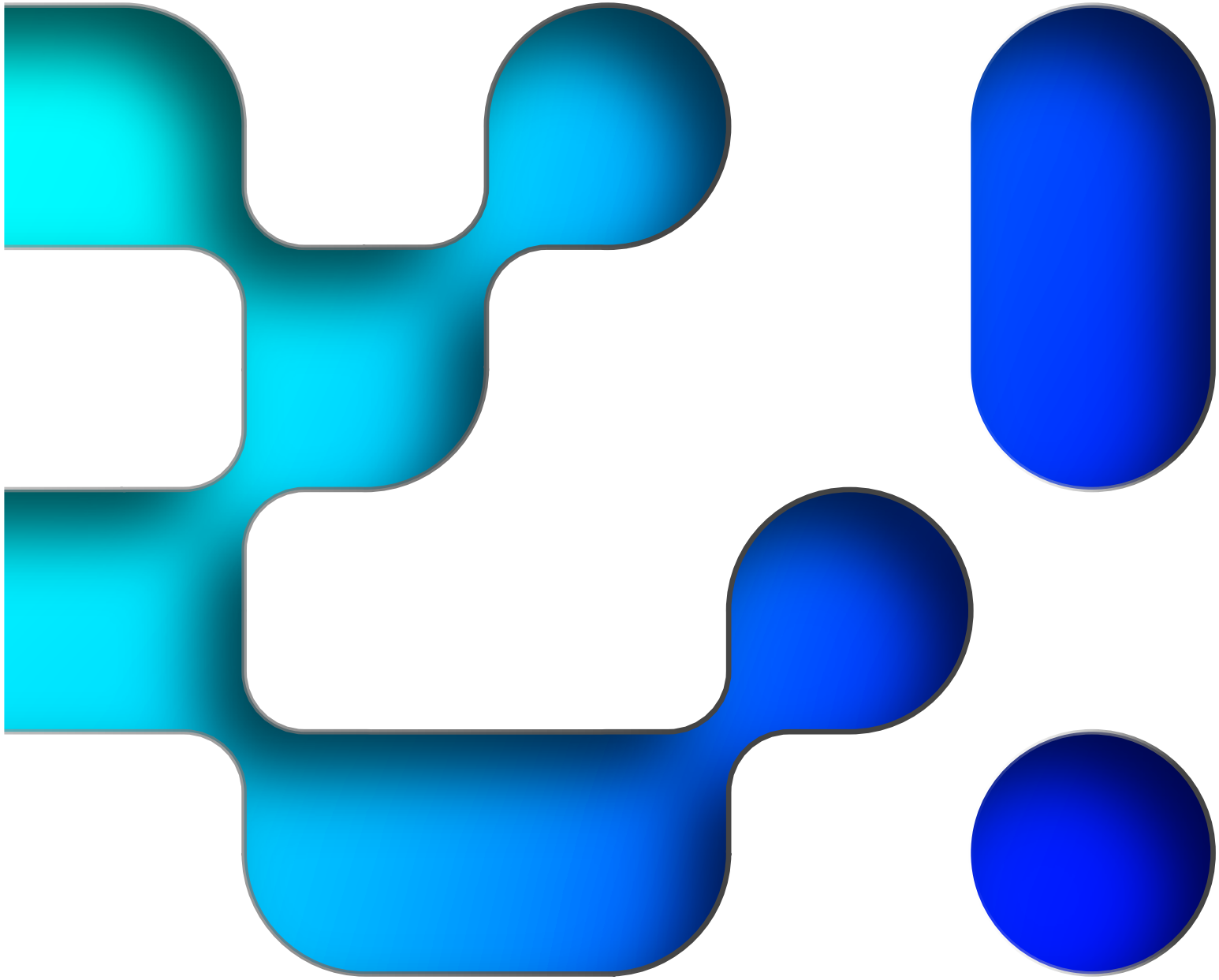
BÉNÉFICES ATTENDUS

- Aider à la **construction** ou la **mise à jour de fiches réflexes** ou d'identification de listes de **ressources critiques** et des mesures à mettre en œuvre pour les protéger ;
- Construire une **stratégie de communication** et l'outillage / la documentation associés ;
- Identifier des **points d'amélioration** dans l'outillage et **tester la bascule vers l'outillage de gestion de crise** ;
- Créer une **meilleure appréhension de la crise** et du stress par les collaborateurs / gestionnaires de crise ;
- Travailler sur les **interfaces du dispositif** de crise en place ;
- Construire une **liste de tiers partie** (clients, partenaires, fournisseurs, etc).

POSSIBLES DIFFICULTÉS ET BIAIS

- Choix du scénario d'exercice entre **propagation de l'attaque par les équipes techniques** (protection & défense). Ceci peut conduire à un différentiel entre les attendus de l'exercice vs ceux des participants ;
- Scénario extrême à tous les niveaux d'organisation pouvant générer un niveau de **stress** important ;
- Echanges entre experts uniquement / **biais de confirmation** : la technique peut prendre le pas sur le décisionnel sans tenir compte des impacts sur les activations métiers, seulement à l'écoute des experts ;
- **Focus de défense** plutôt que de circonscrire l'attaque ou encore la reprise d'activité ;
- Impact minoré si les stimulis ne mettent pas en lumière les **impacts métiers/entreprise** ;
- Risque de **prise de décision rapide sans analyse d'impact** (ex : coupure d'accès sans concertation) ;
- **Incompréhension entre cellule technique et non technique** sans effort de vulgarisation et de synthèse.

Contributeurs : Accenture, Airbus, ANSSI, BNP Paribas, Bouygues Telecom, Deloitte, Française des Jeux, SUEZ



CAMPUS CYBER
5 - 7 RUE BELLINI
92800
PUTEAUX

https://campuscyber.fr/