Retours Cyber attaque

Brigitte SOR

21 Décembre 2023

SOMMAIRE

1 Analyse de la crise
Ses effets

2 Retex réponse
Analyse

3 Plan de sécurisation
Démarche remédiation

4 Bilan
Conclusions

1 Analyse de la crise

ANALYSE DE LA CRISE : CHRONOLOGIE

Attaque

Phase 1 : Crise aigue

Phase 2 : Remédiation

12 Septembre

13 au 21 Septembre

22 septembre– 30 Juin 2023

Début cryptage 21h

-> Intervention DSIN 21H30

Blocage de l'attaque 01h du matin

->Mise en place de mesures conservatoires

Situation de crise : impact global sur le fonctionnement de l'établissement

- Communication de crise
- Mise en place d'un mécanismes de pilotage de la crise
- Définition et mise en œuvre des procédures métier dégradées
- Lancement de l'analyse de l'attaque (par prestataire extérieur)

Sidération de nombreux acteurs: impact global sur les personnels

Cellule de crise (priorisations)

Tableaux de bord de suivi

- Mise en œuvre des préconisations de sécurité
- Remédiation AD (avec prestataires extérieurs)
- Information utilisateurs (bulletins hebdomadaires)
- Rétablissement progressif des services
- Retour progressif au procédures métiers normales (accompagnement par DSIN)

ANALYSE TECHNIQUE CYBERATTAQUE

Première Intrusion SI

4 Septembre

Accès via compte étudiant compromis

Plateforme A7OK

Début préparation attaque

outillage pour l'attaque déposé sur un PC enseignement (Cobalt Strike)

Préparation de l'attaque nuits et weekend suivants

Attaque

12 Septembre

Attaque latérisée sur l'ensemble des sites de l'établissement

Début du cryptage de serveurs et postes de travail

dépôt messages avec liens demandes de rançon sur le darkweb

Alerte DSIN par supervision serveurs 21h30

Début cryptage 21h
Blocage de l'attaque
01h du matin

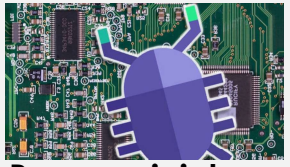
Enquête Forensic

13 au 30 Septembre

Identification
jour0, patient0

Affaire

GOLDEN SALMON



Rancongiciel

AVOS LOCKER

Identification attaquant et analyse impact attaque

Remédiation Renforcement sécurité SI

Operations de sensibilisations

1ier Octobre – 30 Juin 2023

Cellule de crise (priorisations)

Tableaux de bord de suivi

En lien

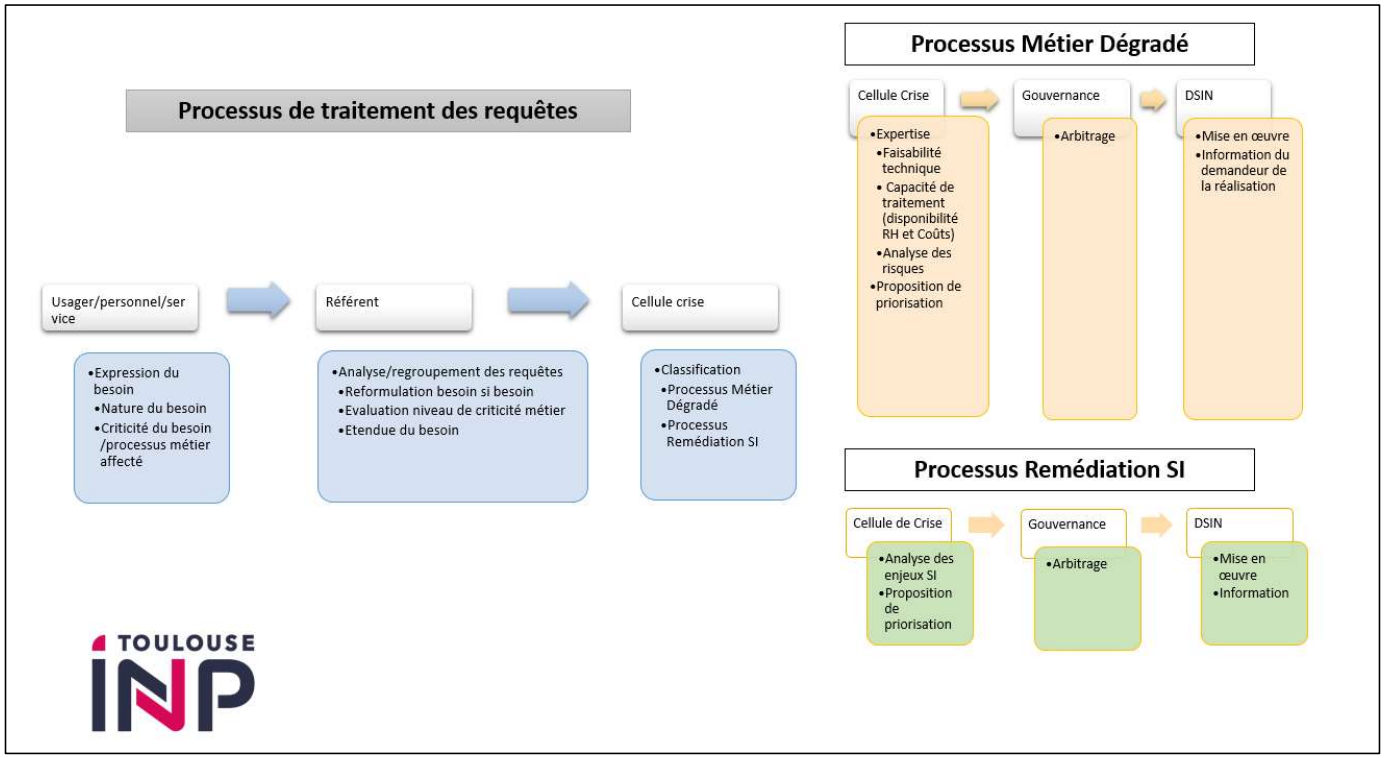
ANSSI

COSIM, CERT Renater

Remédiation de plus de 2000 postes et 600 serveurs

Phase 2: Protocole de gestion de la crise

Cellule de crise restreinte:
DGS, VP NUM, DSI/RSSI



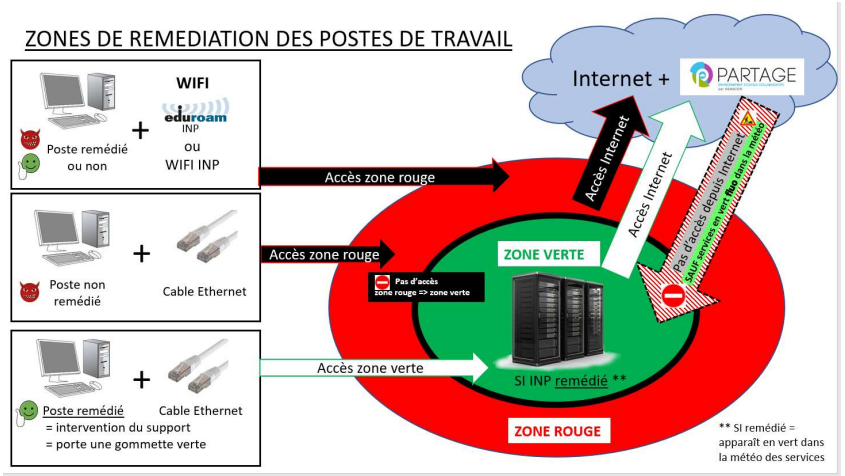
Phase 2 : Communication aux utilisateurs

- Dès le démarrage de la phase de remédiation, mise en place de la météo des services diffusée régulièrement

Nom application	Etat actuel	Description	Domaine	Fonctionnalité
OATAO		Open Archive Toulouse Archive Ouverte	Bibliothèques	
Sites Web - Intranet		Gestion de sites Web	Communication - RI	
ENT		Environnement Numérique de Travail	Communication - RI	
CAS		Central Authentication Service	Divers Services Numériques	
Compilatio		Outil d'antiplagiat	Divers Services Numériques	
Dokuwiki		Outil de documentation interne DSIN	Divers Services Numériques	
Grouper		Gestion des groupes	Divers Services Numériques	
LDAP		Annuaire	Divers Services Numériques	
LimeSurvey		Outil de questionnaire en ligne	Divers Services Numériques	
Partage		Messagerie et agendas des personnels	Divers Services Numériques	
Rainbow		Téléphonie, tchat	Divers Services Numériques	
Rocket.Chat		Outil de tchat	Divers Services Numériques	
Outils Renater: Evento, Renavisio, ... (Shibboleth)		Authentification centralisée Renater	Divers Services Numériques	
Zoom		Visio conférences (réunions administratives + enseignem	Divers Services Numériques	
Chorus Pro		Gestion des factures dématérialisées (portail du ministère	Finances - Comptabilité	
ESUP-Pay		Plateforme de paiement en ligne	Finances - Comptabilité	
MarcoWeb		Gestion des achats et marchés publics (SaaS)	Finances - Comptabilité	
SID		Système d'Information Décisionnel	Finances - Comptabilité	
SIFAC		Gestion budgétaire, financière, comptable et analytique	Finances - Comptabilité	
SIFAC Demat		Dématérialisation des factures	Finances - Comptabilité	
ADE		Gestion des emplois du temps	Formation / Scolarité	Planification
ADE		Gestion des emplois du temps	Formation / Scolarité	Consultation en ligne
Apogée		Gestion de la scolarité	Formation / Scolarité	Application tous domaines (+ dépôt PJ, envoi CVEC, SISE, ...)
Apogée		Gestion de la scolarité	Formation / Scolarité	Batchs accès exterieurs (Bourses, ParcourSup, Thèses, ...)
Apogée		Gestion de la scolarité	Formation / Scolarité	Modules Web inscriptions et PJ
Apogée		Gestion de la scolarité	Formation / Scolarité	Module Web saisie des notes
EasyID / P4P		Gestion des cartes MUT	Formation / Scolarité	

Légende état actuel
Etat avant la cyberattaque
Remédié partiellement
Non remédié
Remédiation prévue la semaine prochaine

Statut du mardi 11 octobre 2022



Phase 2: Acompagnement les différents métiers

Mise en place d'échanges systématisés personnalisés avec les chefs de service (dans les écoles et en central) sur :

- Liste des activités qui restent possibles
- Liste des activités qui fonctionnent en mode dégradé
- Liste des activités qui ne sont plus possibles
- Liste des demandes, des priorités
- Inquiétudes
- Informations de la DSIN

Permet :

Accompagnement au mode dégradé

Priorisation des actions de remédiation ou de mise en place de mode dégradé

Vue globale de la situation des métiers à destination de la gouvernance

Effets induits par la crise : Perturbations majeures activités métiers

- Formation et scolarité:
  - Accès salles TP informatiques
  - Absence ADE et Moodle pour les étudiants
  - Inscriptions d'étudiants manquantes
    - Mode dégradé : recensement des inscriptions déjà faites, recueil manuel des informations pour les autres
  - Emploi du temps :
    - Affichage papier quand la récupération n'est pas possible dans les agendas
    - Problème de traçabilité des heures d'enseignement effectuées (surtout vacataires)
- Finances, DAFA :
  - Factures en attente
  - Inquiétude sur la sortie du compte financier de l'établissement
  - Chiffres imprécis car pas de vision des budgets
- Pilotage
  - Organisation des élections sans pouvoir recenser les électeurs dans le SI
- Logistique
  - Contrôle d'accès aux bâtiments désactivé
- Communication
  - Déréférencement des sites INP
  - Tous les sites indisponibles
- Patrimoine
  - Plateformes GTC, SI Patrimoine indisponibles
- DRH
  - Reconduction de la paie de septembre pour les personnels gérés administrativement
  - Pas de paie pour les vacataires
- Formation continue
  - Difficultés de poursuivre les formations à distance sans Moodle
- …

Effets induits : DSIN

- Mise en évidence de faiblesses techniques et organisationnelles
- Charge RH DSIN
  - Enorme charge de travail et de charge mentale sur peu d'agents (3 à 4) de la DSIN durant la phase 1 de crise aigue
  - Très forte pression des usagers sur les services support de proximité durant la phases 1
  - Activités remédiation, pilotage gestion de crise, accompagnement utilisateurs aux usages en mode dégradé **> 1800 j/h DSIN (>8 ETP)**

  - Déficit postes, compétences – difficultés à recruter (domaine en tension extrême)
  - Risque épuisement de certains personnels vu la durée
  - Tensions
- Financier
  - Sous-traitance (enquête Forensic, expertise ingénierie windows) : 250K€
  - Outillages (détection, remédiation) : sondes, EDR, XDR

- Retards projets / MCO

Effets induits: Enjeux humains

- Effet de sidération de la plupart des agents de l'établissement (phase 1 surtout)

  -> inquiétude, désarroi des personnels, sentiment d'impuissance, d'empêchement de faire leur travail, colère chez certains (complotisme parfois…)

  -> difficulté à se représenter la nature exacte de l'évènement

- Stress induit par le fonctionnement en mode dégradé

2 Retex Réponse

Retex: Enjeux organisationnels

- Structure de prise de décision et d'arbitrage (situation de crise)

  -> Tâtonnement dans la mise en place de l'organisation de crise dans un établissement se vivant comme « fédéral »

  -> clarifier les modes de prise de décision en situation de crise

- Organisation interne de la DSIN

  -> Service Central depuis 3 ans mais transformation de l'organisation incomplètement déployée

  -> Flottement au démarrage dans l'application des directives en composantes

  -> Personnels soumis à des injonctions contradictoires (DSIN vs environnement local)

  -> Pb de souveraineté sur le SI à corriger impérativement (SDN)

Retex : Communication interne

- Communication interne personnels

  Doctrine: transparence, réassurance, responsabilisation

  - Courriels Présidente, DGS, DSIN, Services centraux
  - Réunion CHSCT
  - Réunions d'informations en présentiel sur chacun des sites
  - Webinaire de présentation des conclusions de l'analyse Forensic (gouvernance, DSIN)
  - Courriel hebdomadaire de météo de la remédiation

  -> Effet très positif de la communication en particulier en présentiel

- Communication interne étudiants
  - Courriels Présidente
  - Informations pratiques par les DE et équipes enseignantes

  -> pas de problème identifié

Retex: Communication externe

- Communication institutionnelle

  - Tutelles partenaires essentiels (Rectorat, CNRS,…) : Présidente et DGS
  - Organes techniques des tutelles (COSSIM, ANSSI, Cert Renater, PJ…) : Directrice DSIN

  - Partenaires spécifiques : en direct par les personnes concernées

  -> pas de problème identifié

- Communication « grand public »

  Doctrine: frugalité, transparence

  -> éviter l'emballement médiatique

  -> fuite sur les réseaux sociaux en phase 1 – pression médiatique induite

  -> mise en place d'une page web à l'adresse de notre site institutionnel
  -> centralisation de la communication
  -> Interview AEF (VP numérique)

  -> bons retours externes

Retex: Enjeux fonctionnels

- Fort impact sur l'ensemble des métiers

- Pas de procédures de fonctionnement en mode dégradé prédéfinies

  -> mise en place de procédures en mode dégradé en période de crise

  -> Assez rapide pour les services centraux

  -> plus difficile dans les composantes

  -> hésitation sur la doctrine (Quels relais en composates ? Procédure unique à déployer partout vs procédure définies localement? …)

  -> travailler à la définition de procédures de fonctionnement dégradées

3 Stratégie sécurisation SI

Les grandes étapes

1 - **ENDIGUEMENT DE L'ATTAQUANT :** pour empêcher l'aggravation de l'incident.

2 - **ÉVICTION DE L'INTRUS DU CŒUR DU SI :** pour recréer une base de confiance d'où mener la reconstruction.

3 - **ÉRADICATION DES EMPRISES DE L'ADVERSAIRE :** pour éliminer les capacités de retour de l'attaquant par des portes dérobées laissées lors de l'intrusion.

Source : ANSSI

Quel scénario de reprise?

Scénario 1 - « Restaurer au plus vite des services vitaux »

Face à un péril immédiat pour votre organisation, un nombre restreint de services doivent impérativement être redémarrés. Toutefois, cette approche ne traitera ni les causes racines de l'incident, ni ne protégera d'une résurgence de l'attaque à moyen terme. La survie de votre organisation reste en question.

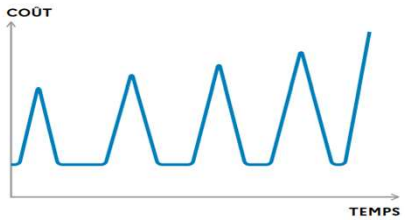
Scénario 2 - « Reprendre le contrôle du SI »

Vous privilégiez un retour le plus rapide possible à l'état de fonctionnement antérieur de la totalité du système d'information. Il n'est pas restructuré. Votre organisation reste à risque, tant que des changements substantiels n'auront pas été réalisés (protection de l'administration, détection...).

Scénario 3 - « Saisir l'opportunité pour préparer une maîtrise durable du SI »

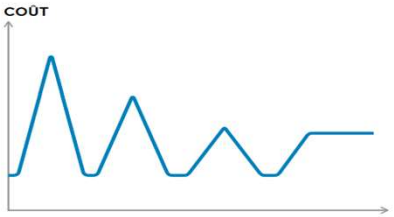
Quitte à réaliser des changements majeurs dès la remédiation, vous transformez votre posture de sécurité. Vous choisissez d'investir durablement pour vous réapproprier le pilotage et la défense de votre système d'information. Cette approche permet d'adopter un modèle de sécurité proactif, plutôt que réactif.

Scénario 1



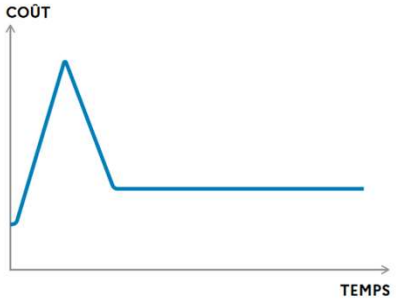
Le redémarrage d'urgence des services vitaux est faiblement coûteux, mais les risques de résurgence sont élevés. D'autres remédiations ultérieures seront alors nécessaires, ce qui génère un coût total très élevé pour l'organisation.

Scénario 2



L'état fonctionnel du SI est ramené à la situation précédant la compromission, dès la première remédiation. Néanmoins, le plan de sécurisation s'étalera sur la durée et aura à nouveau des impacts sur l'activité métier.

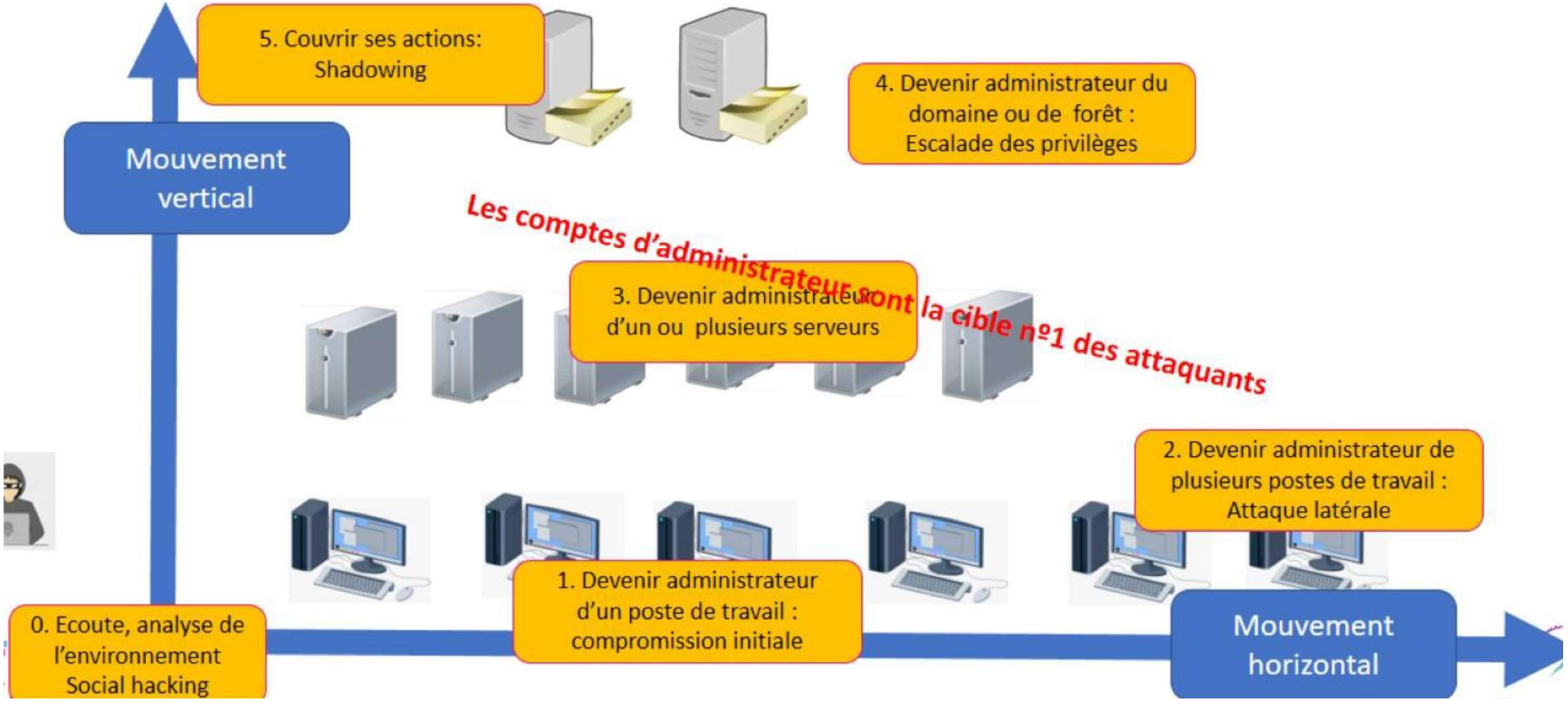
Scénario 3



Le coût de la première remédiation est élevé, mais elle constitue une opportunité majeure pour poser les bases d'une sécurité à l'état de l'art. À terme, cet investissement aura été très rentable. L'organisation maîtrise durablement sa sécurité.

Source ANSSI

Scénario d'attaque



Active Directory : Cible des attaquants !

Compromissions favorisées par :

- Des systèmes Windows non mis à jour avec des vulnérabilités non patchées
- Méconnaissance ou mauvaises configurations d'Active Directory

Se protéger contre les attaques latérales

Limiter le nombre des comptes administrateurs locaux et mettre en place des critères de responsabilité

- Charte de Co-administration
- Deux comptes distinct pour l'utilisateur :
  - Un compte utilisateur du domaine
  - Un compte personnel pour des taches d'administration (membres administrateurs local)

Analyser, surveiller et mettre à jour les systèmes d'exploitation

- Limiter les versions obsolètes et favoriser les mises à jour

Sécuriser les postes avec l'antivirus centralisé

- Ajouter progressivement sur l'ensemble des appareils l'EDR (Endpoint Detection and Response)

Se protéger contre les attaques latérales

Objectif

- Eviter qu'une machine compromise ne puisse être utilisée pour contaminer les autres grâce à un mot de passe ou un hash du compte administrateur local identique

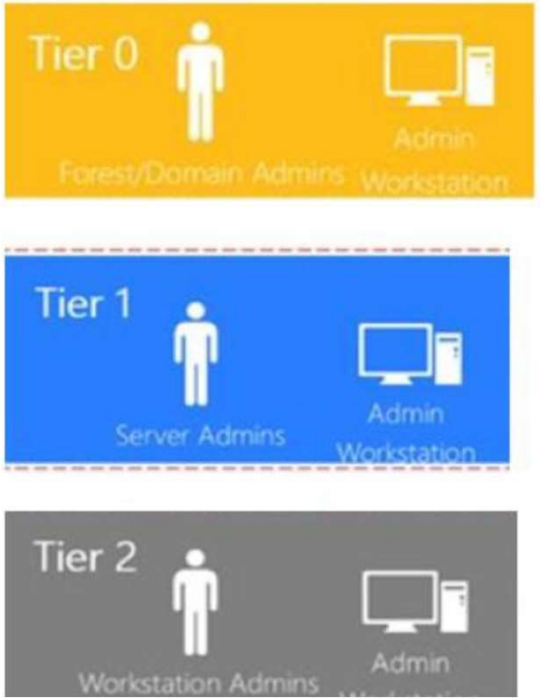
Mise en œuvre

- Mettre en œuvre LAPS « Local Admin Password Solution » :
  - Affecte automatiquement un mot de passe complexe à un compte administrateur local de chacun des serveurs membres et workstations qui sera différent pour chacun d'eux
  - Change régulièrement ce mot de passe
  - Le stocke dans un emplacement sécurisé tel qu'un attribut du compte machine dans l'AD (ms-Mcs-AdmPwd)

Se protéger contre les attaques verticales

Délégation d'administration en 3 Tiers : Modèle de Tiering

- S'applique également dans toute architecture autre qu'un Active Directory

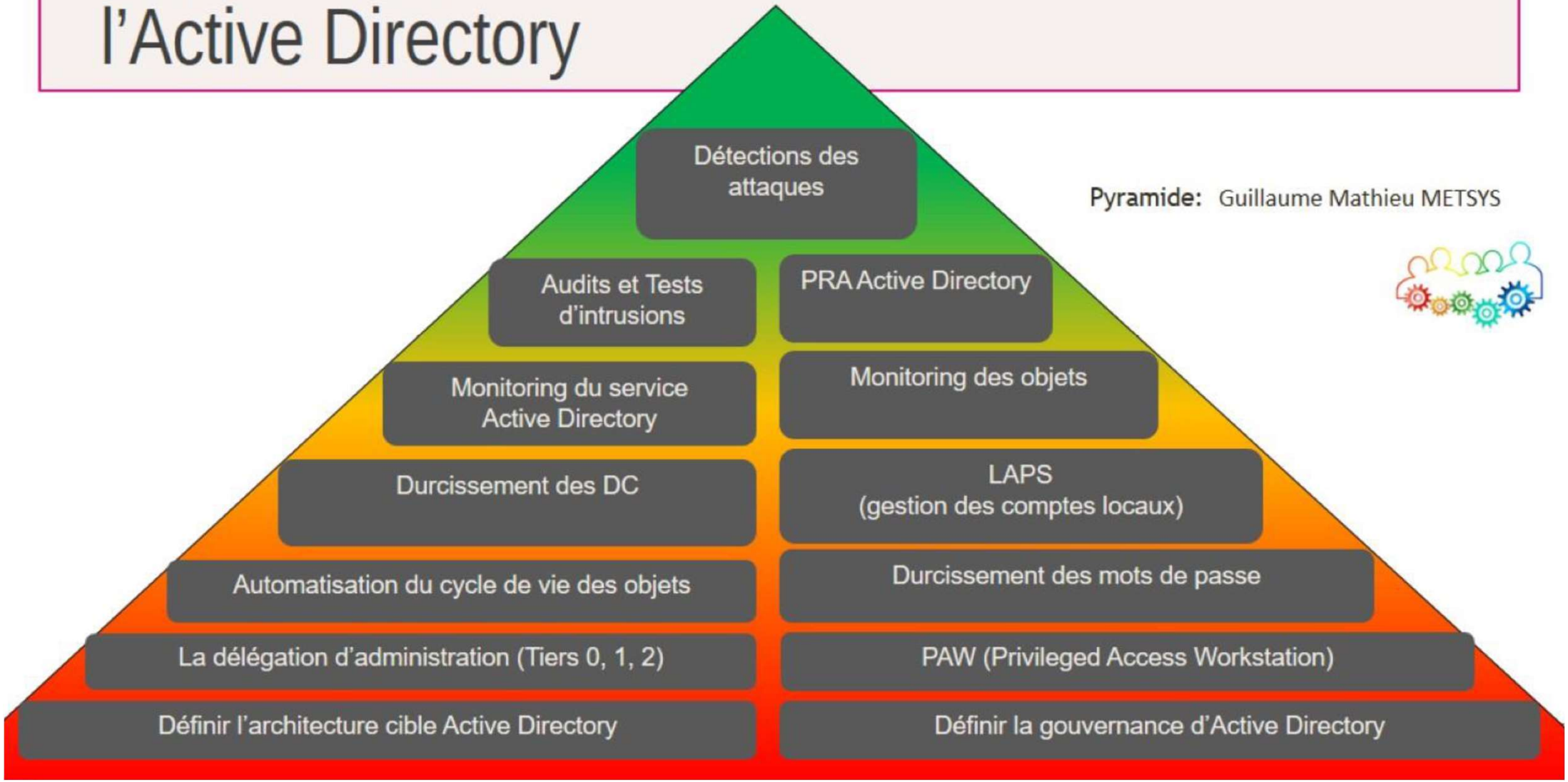


Tier 0 : serveurs très critiques
- administrateurs de domaine
- domaine Contrôleurs de domaines, PKI interne…)
- administrateurs de comptes, GPO et serveurs critiques

Tier 1 :
- serveurs applicatifs (Impression, WSUS, KMS…)
- administrateurs des serveurs et des applications

Tier 2 :
- administrateurs des stations de travail et applicatifs
- postes clients (Laptop, Desktop, imprimantes…)

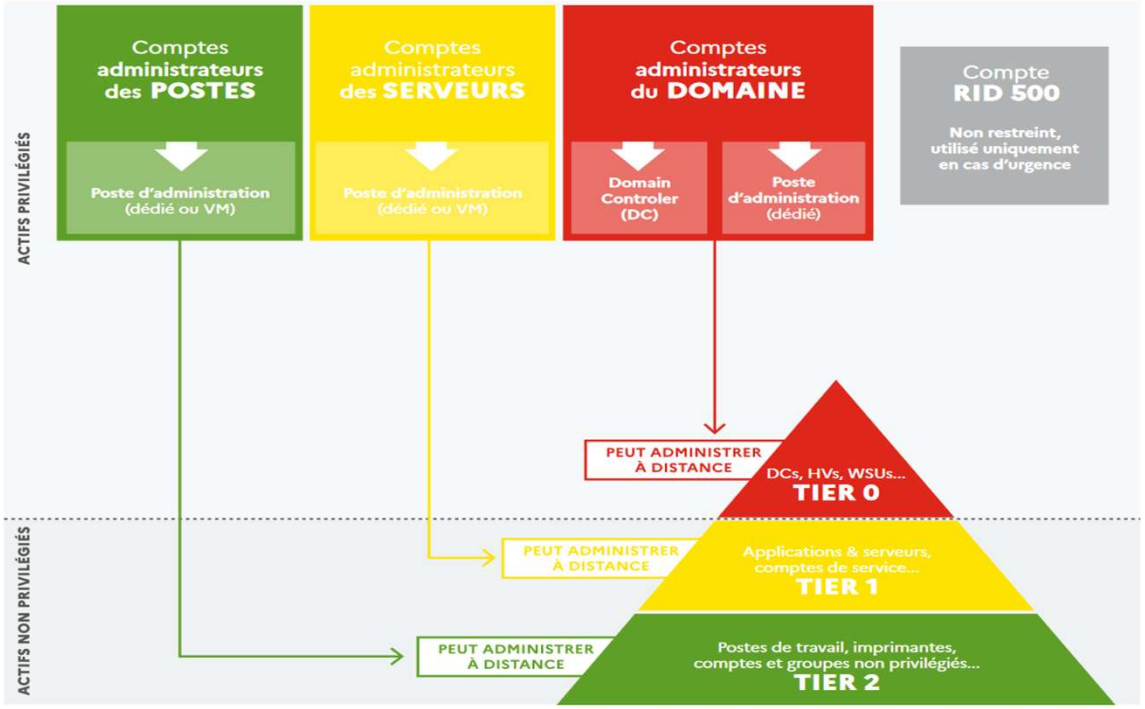
Approche pyramidale du durcissement de l'Active Directory



Pyramide: Guillaume Mathieu METSYS

Concepts clés de la remédiation 1/2

Règles du moindre privilège - impact fort pour les administrateurs au quotidien !



Concepts clés de la remédiation 2/2

- Journalisation de TOUS les évènements (conservation 1 an) - Indexation dans un puits de log (SIEM)
  - Pour détecter au plus tôt les signaux faibles et garantir la complétude d'analyses ou enquêtes type Forensic
- Segmentation système/réseau à accroître
  - Cloisonner pour limiter la diffusion des attaques (cloisonnement physique ou logique)
  - Domaines formation/administration/recherche – SI à risques (SIFAC'demat, Abyla, …)
- Recourir à l'IA (EDR/XDR)
  - Surveillance 24/7 (préparation des attaques nuits, week-ends, périodes de vacances)
  - Apprentissage situation « normale » pour détection comportements nouveaux et/ou à risque – possibilité de réponses automatisées avec risques faux positifs
- Sécuriser les connexions à distance sur les briques SI (accès VPN, VDI) :
  - Mise en œuvre d'authentification à double facteur (code sur télephone, clef physique « Yubikey »

Plan de sécurisation de notre SI

MESURES TECHNIQUES

- Mesurer, Evaluer (PinkCastle, Purple Knight, ORADAD, …)
- **Réduire la dette technologique** en lien avec l'ingénierie du poste de travail et infrastructures Windows (architecture 3 tiers -- règles du moindre privilège) porte d'entrée principale des attaques
- **Cloisonner** les réseaux, **sécuriser les accès distants** (authentification à double facteur pour les télétravailleurs et usages nomades personnels etudiants)
- **Recourir à l'IA** pour détecter les attaques et les bloquer (déploiement EDR Crowdstrike, sondes XDR : Darktrace …)

FORMATION, SENSIBILISATION, RH

- **Formation** des agents de la DSIN
- **Sensibilisation** des utilisateurs (formations, mises en situation régulières)
- Pallier aux **difficultés de recrutement** par de la sous-traitance – attention à la perte de compétences!

MESURE, SUIVI DU NIVEAU DE SECURITE

- Souscription services ANSSI
- **ADS** : évaluation mensuelle sécurité AD
- **SILENE** : évaluation mensuelle exposition internet

A venir : labellisation applications avant mise en production (cf directive européenne NS2)

ASSURER LA SOUVERAINETE DU SI ET DE SA GOUVERNANCE

- **Affermissement modèle de gouvernance** du numérique (Circuits décisionnels, comitologie),
- **standardisation et uniformisation** des infrastructures et services,

STRATÉGIE

S'appuyer sur les recommandations ANSSI et résultats d'analyse

Renforcer la sécurité du SI en réduisant la dette technique tou en renforçant la sensibilisation de tous les acteurs (cybersécurité, RGPD)

Utiliser l'IA pour détecter les activités réseaux suspectes et les bloquer en 24/7

Dans une logique d'amélioration continue, interroger l'équilibre entre sécurité SI, souveraineté et usages
(au bureau, en situation de TLT, en mobilité)

4 Bilan

Bilan

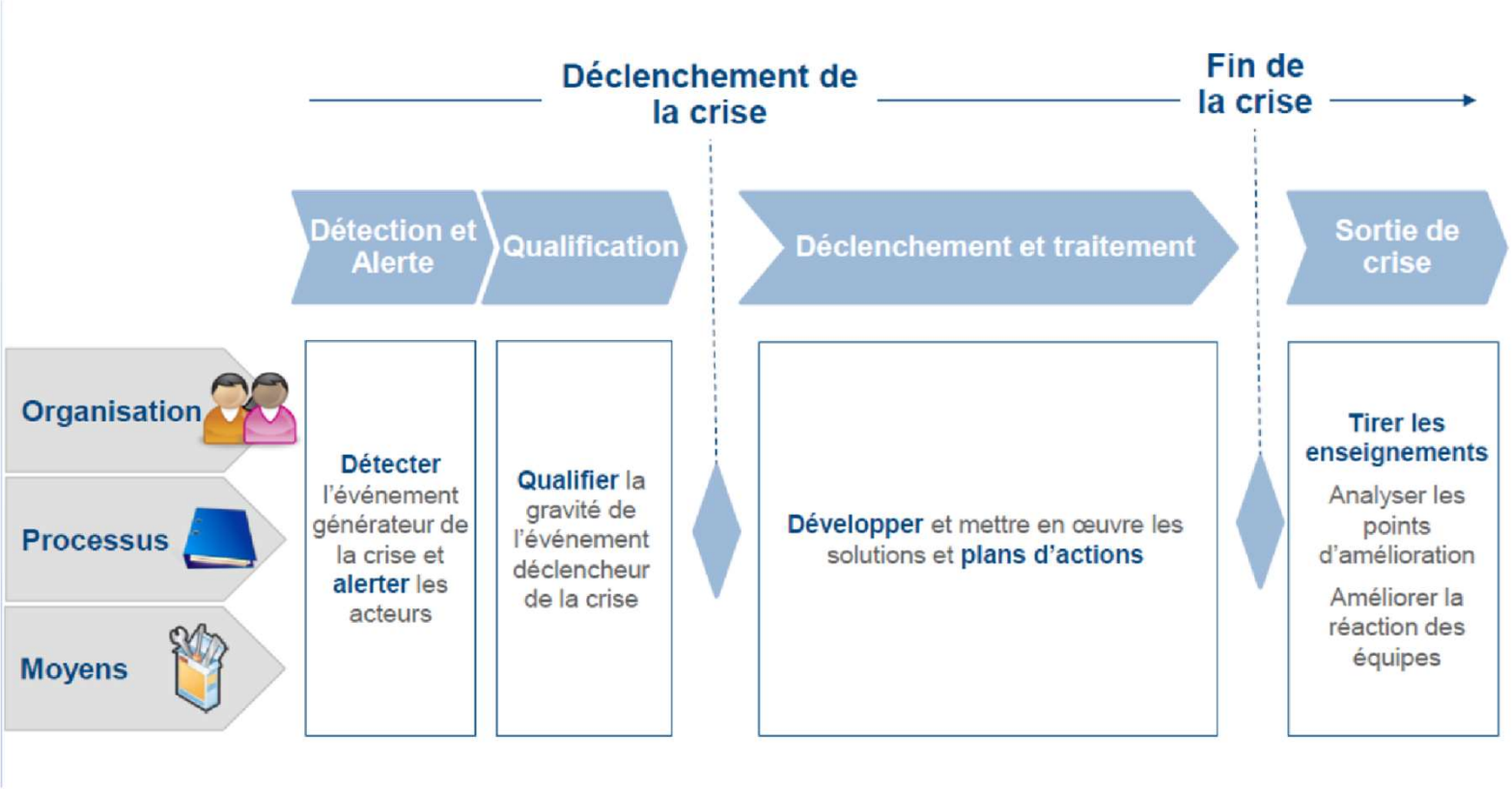
- Caractéristiques de l'attaque
  - -> Attaque interrompue par la DSIN
  - -> Impact sur l'ensemble du SI de l'établissement
  - -> Peu de chiffrage de données abouti
  - -> Pas d'exfiltration de données hors annuaire (surveillance darkweb)
  - -> Pas de pertes de données (sauvegardes saines)
  - -> Moyens de communication préservés : messagerie Partage utilisable sans lien SI actif, solution communication unifiée Rainbow

- Réponse de la DSIN jugée satisfaisante

- Fort impact sur le fonctionnement de l'établissement (ensemble du spectre des missions)
- Fort stress sur les personnels
- Mise en évidence de problèmes de souveraineté du SI

- Mise en place d'un plan de sécurisation du SI (dès la phase de remédiation)
- Prise en compte des risques de cyberattaque dans notre nouveau schéma directeur du numérique

Important: Fin de crise à prononcer !



Merci!
Questions?

Intervenante :
Brigitte Sor – ***Toulouse INP***
21/12/2023