essensei
se concentrer sur l'essentiel

# Kill Chain Murder Party

## Un jeu immersif pour sensibiliser à la cybersécurité et découvrir les Kill Chain

**KIT DE L'ORGANISATEUR**

# Vous trouverez dans ce kit


- Licence et partage p. 2
- Présentation du jeu p. 3
- Kill Chain et cybersécurité p. 4
- Préparation du jeu p. 5
- Animation et timing p. 6
- Brief des enquêteurs-joueurs p. 9
- Briefs des personnages-acteurs p. 10
- Le contexte du jeu p. 11
- Chronologie des évènements p. 12
- Fiches personnages p. 16
- Les documents à fournir aux joueurs p. 37
- Les indices à imprimer p. 42
- Les solutions p. 63
- Les culpabilités des personnages p. 66
- Cybersécurité - Aller plus loin p. 68

# Licence et partage

**essensei** vous autorise à utiliser et à modifier ce contenu avec une licence “Attribution - Partage dans les mêmes conditions”.

Vous êtes donc libre d’adapter mais nous vous demanderons de mentionner **essensei.**

**Licence d’utilisation**
**Attribution - Partage dans les Mêmes Conditions 4.0 International (CC BY-SA 4.0)**

**Partager :** copier et redistribuer le contenu sur tout support et sous tout format, à toutes fins, même commerciales.

**Adapter :** remixer, transformer et développer le matériel à des fins diverses, même commerciales.

**Aux conditions suivantes :**

- **Attribution :** Vous devez mentionner l’auteur , fournir un lien vers la licence et indiquer si des modifications ont été apportées . Vous pouvez le faire de toute manière raisonnable, mais sans suggérer que le concédant vous approuve ou approuve votre utilisation.

- **Partage à l'identique :** Si vous remixez, transformez ou vous inspirez de ce contenu, vous devez diffuser vos contributions sous la même licence que l'original.

# Présentation du jeu

Le jeu **Kill Chain Murder Party** est une Murder Party créée intégralement par **essensei** pour sensibiliser de manière ludique aux enjeux de la cybersécurité en entreprise.

## Qu'est-ce qu'une Murder Party ?

Une **Murder Party** est une forme de jeu de rôle consistant à incarner des personnages pour résoudre une enquête.

Dans une Murder Party classique, les **joueurs** incarnent des **personnages** de l'histoire et enquêtent (ou se cachent) en fonction de leurs implication et de leurs objectifs personnels.

Dans le format Cluedo Géant, les **joueurs** prennent tous le rôle d'un **enquêteur** et vont interroger les personnages, joués par des acteurs.
**C'est le format de notre jeu Kill Chain Murder Party.**

## Logistique

- **Animateur** : 1 (potentiellement acteur également)
- **Personnages - acteurs** : 4
- **Enquêteurs - joueurs** : 30 max recommandé
- **Durée** : 1h30 - 2h
- **Lieu** : Salle avec 4 espaces isolés
- **Matériel** : Documents imprimés, papiers, stylos

# Kill Chain et cybersécurité

## Qu’est-ce qu’une Kill Chain

Une **Kill Chain** est un modèle, crée en 2011 par la société **Lockheed Martin**, permettant de décrire les 7 étapes clés d'une cyberattaque. Ce modèle a été enrichi par la suite pour donner la **Kill Chain unifiée à**18 étapes, le rendant plus pertinent et plus exploitable.

Nous nous limiterons ici au modèle traditionnel.

## Les étapes de la Kill Chain

1. **Reconnaissance** : l'attaquant sélectionne la cible, la recherche et tente d'**identifier les vulnérabilités** du réseau cible.
2. **Armement** : l'attaquant crée un **logiciel malveillant**, lui permettant d'accéder à distance à la cible en **exploitant** les vulnérabilités du système.
3. **Livraison**: l'attaquant **transmet** l'arme à la cible (via des pièces jointes de courrier électronique, des sites Web ou des clés USB par exemple)
4. **Exploitation** : le code du logiciel malveillant se déclenche et agit sur le réseau cible pour **exploiter la vulnérabilité** identifiée.
5. **Installation** : le logiciel malveillant installe un **point d'accès** utilisable par un attaquant externe.
6. **Commandement et contrôle** : le logiciel malveillant offre à l'attaquant un **accès permanent** au réseau cible.
7. **Actions sur l'objectif** : l'attaquant prend des mesures pour **atteindre ses objectifs**, tels que l'exfiltration de données, la destruction de données ou le chiffrement contre rançon.

# Préparer le jeu

## Le rôle d'animateur

Pour ce jeu, vous aurez besoin de 1 **animateur** qui se chargera des présentations initiales, qui connait le contexte, la mécanique globale et se charge du timing.

Pour ce rôle, privilégiez une personne qui est **à l'aise dans la facilitation et l'animation** et qui a **le temps d'étudier** l'ensemble du jeu dans le détail.
Une personne qui a **l'expérience de Murder Party** est un plus.

## Les personnages-acteurs

Le jeu requiert 4 **personnages-acteurs** incarnant les différents protagonistes de l'enquête. **Leur rôle est crucial** car c'est eux qui vont interagir avec les **enquêteurs-joueurs**. Ils doivent intégrer, à minima, les éléments sur leurs fiches personnages, les indices qu'ils possèdent et la timeline globale.

Pour attribuer les rôles, privilégiez des personnes à l'aise pour jouer les traits de caractères des différents personnages :

- **Robin** : Expérimenté, très volontaire, dépassé
- **Jeanne** : Business woman, très occupée, aime maitriser, préoccupée
- **Kevinn** : Inexpérimenté, nonchalant, hautain, désabusé
- **Hadrien** : Expert, réservé, antipathique, autoritaire

## Noms et genres

Les **personnages-acteurs** sont genrés et nommés dans cette version.

Cela étant, vous êtes **libres d'adapter** chaque rôle pour qu'il soit tenu par une femme ou un homme. De même, une femme ou un homme peut très bien tenir un rôle de l'autre genre sans que se soit problématique dans le cadre du jeu. Le principal étant que ça vous convienne.

Si vous modifiez un nom ou un genre, il faudra juste r**épercuter les changements** de noms ou de genre dans les documents et s'aligner avec les **personnages-acteurs** et les **enquêteurs-joueurs**.

# Animation du jeu

## Groupes de jeu

Pour le jeu, les **enquêteurs-joueurs** sont organisés en groupes homogènes de 3 à 8 personnes.

Chaque groupe recoit :

- une **Fiche enquête** à remplir
- une **Fiche Kill Chain** à remplir
- du papier pour la prise de note et un stylo.

## Déroulé du jeu

Le jeu se déroule en 3 grandes phases

### 1.Présentation et explication

- Explication du jeu et de l'animation 10 min
- Présentation du contexte général 5 min

### 2.Interrogatoires

- Premier tour d'interrogatoires 20 min
- Pause de réflexion 10 min
- Deuxième tour d'interrogatoires 20 min

### 3.Conclusions et Debrief

- Conclusions des enquêteurs 10 min
- Debrief 5 min

## Présentation

Au début du jeu, il convient **d'expliquer** rapidement aux **enquêteurs-joueurs** le fonctionnement de la partie.
Nous vous conseillons d'utiliser le brief prévu pour eux dans ce kit et d'expliquer le déroulement de la partie. Vous pouvez également leur montrer et lire la **Fiche Enquête** et le **Fiche Kill Chain**.
Prenez le temps de répondre aux questions.

Ensuite, il s'agit d'introduire le **contexte de l'enquête** en présentant les **éléments initiaux**, les différents **personnages-acteurs** et en introduisant brièvement quelques **notions de cybersécurité**, notamment la définition d'une **Kill Chain**. Vous pouvez demander au **personnage-acteur** qui joue le rôle d'Hadrien de faire la présentation sur la cybersécurité.

# Interrogatoires

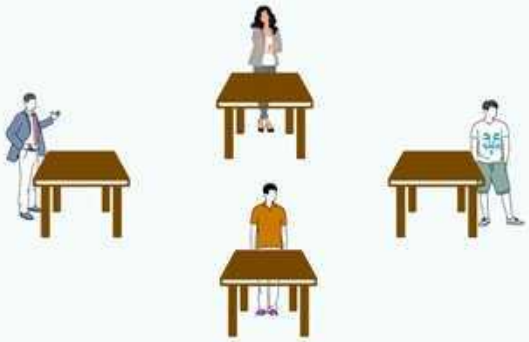
Pendant les phases d'interrogatoire, les **enquêteurs-joueurs** vont aller questionner tour à tour les différents **personnages-acteurs.**

Ils disposeront de **5 min** par **personnages-acteurs** avant de passer voir le suivant.

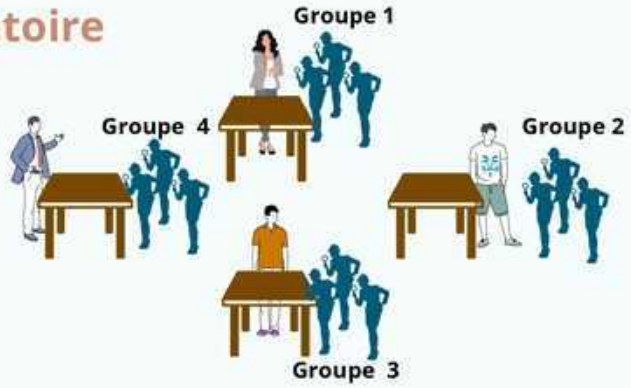
Pensez bien à laisser **10 min de réflexion** entre les deux tours d'interrogatoires pour que les groupes puissent poser leur réflexion et préparer les prochaines questions.

Nous vous conseillons de garder les **personnages-acteurs** à des endroits fixes et de faire bouger les **enquêteurs-joueurs**.

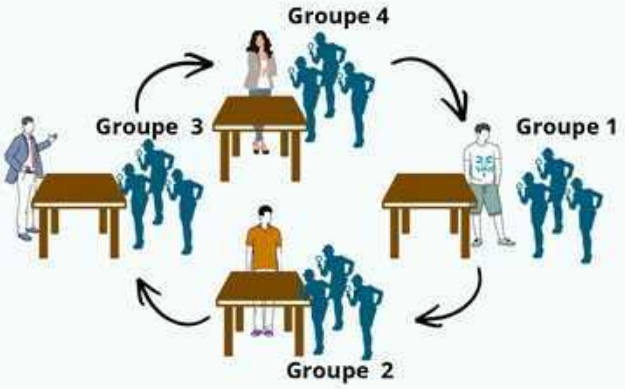
## Placement initial



## Début de l'interrogatoire




## Après 5 minutes



# Conclusion et Debrief

## Fiche enquête et fiche Kill Chain

A l'issu du deuxième tour d'intérrogatoire, laissez **5 à 10 minutes** aux groupes pour **finaliser** leur réflexion et **renseigner** la **Fiche Enquête** en répondant aux 3 questions et **remplir** la **Fiche Kill Chain** avec les détails. Puis l'**animateur** récupère les fiches des 4 groupes et prend connaissances des réponses.

En tant qu'**animateur**, parcourer les réponses et **identifier** le ou les groupes qui ont le mieux répondu en valorisant les détails.

## Révélations

Une fois toutes les fiches récupérées, vous pouvez donner les réponses attendues et **révéler la solution** de l'enquête à tous les groupes.
Profitez en pour parcourir les réponses et féliciter les groupes pour leurs réponses correctes ou originales ou farfelues.

Passez un peu de temps à **expliquer** la Kill Chain résolue étape par étape.

Prenez le temps de répondre aux questions des **enquêteurs-joueurs** sur le scénario complet résolu en détails.

## Culpabilités des personnages-acteurs

Une fois toute l'intrigue révélée, les **personnages-acteurs**, peuvent revenir devant les **enquêteurs-joueurs** pour exposer leurs culpabilités dans l'affaire.
Cette partie permet de **sensibiliser sur l'implication de tous** dans la cyber sécurité et de faire le lien avec une démarche agile ouverte aux enjeux cyber.

N'hésitez pas à **ajouter** ou **modifier** des éléments lié à votre contexte spécifique.

## Pour aller plus loin

Pour clôturer et inviter à aller plus loin, vous pouvez distribuer aux **enquêteurs-joueurs**, la fiche cyber sécurité.

N'hésitez pas à adaptez cette partie votre contexte pour cibler les bonnes ressources et concepts que vous voulez faire connaître.

# Brief des enquêteurs - joueurs

Vous jouer le rôle des **experts en cyber sécurité** appelés aujourd'hui pour résoudre l'affaire de la **cyber attaque** de **MonFinancement.FR**

Par **groupe**, vous aller interroger chacun des protagonistes de cette histoire pendant **5 minutes**, à **2 reprises**.

## Objectif

Votre objectif est de **comprendre** ce qu'il s'est passé en répondant aux 3 questions sur votre **Fiche Enquête** et en renseignant avec le plus de détails possible votre **Fiche Kill Chain**.

A l'issu des interrogatoires, **vos conclusions seront revues** pour déterminer le groupe gagnant.

## Quelques conseils

- Soyez dans votre rôle : **poli mais ferme** et déterminer à résoudre l'enquête.
- **Préparer** et réfléchissez à **vos questions** pour qu'elles soient les plus pertinentes possibles.
- **Utiliser toutes les informations** dont vous disposer.
- **Recoupez** les informations entre elles et utilisez les informations que vous avez obtenues d'un **personnage-acteur** pour interroger les autres.
- **Projetez** les renseignements obtenus dans la vue d'ensemble de la **Kill Chain et de la Fiche enquête.**

## Attention

Vous interrogez des **personnes**, elles peuvent **oublier** des choses, **se tromper** ou vous **mentir**. Elles ne savent pas tout et ne pourront partager que ce qu'elles connaissent des évènements.

**A vous** de faire des **recoupements** et des **déductions** pour comprendre ce qu'il s'est passé.

# Brief des personnages-acteurs

Vous incarner le rôle d'un des protagonistes de la sombre affaire de la **cyber attaque** de **MonFinancement.FR**
Vous êtes un des interlocuteurs clés et le moteur principal du jeu.
Votre rôle est essentiel pour le bon déroulement de la partie.

## Objectif

Votre objectif est de faire passer un **bon moment** aux **enquêteurs-joueurs** en les guidant dans l'enquête.
Il vous faut les **guider** en leurs distillant les bons indices **dans leur fil de réflexion** et en **ajustant** vos révélations pour les **aider**.
Attention à **ne pas en dire trop d'un coup** et les priver de la découverte.

## Quelques conseils

- Lisez la **timeline** et votre **Fiche Personnage** plusieurs fois avant la partie
- Pousser quelques indices ou recadrer les **enquêteurs-joueurs** si besoin.
- Rester fidèle au personnage : **Incarner** et **interpréter** le rôle du personnage avec son **caractère**, en réagissant comme il le ferait.
- Garder un **discours cohérent**, même si vous devez l'ajuster au fil de la partie.
- **Adapter les détails** de votre personnage pour que vous soyez à l'aise.
  Vous pouvez changer ou approfondir un peu votre personnage.
  Dans ce cas pensez à **prévenir** les autres **personnages-acteurs**.
- **Comblez les éléments manquants** avec votre créativité, soit au niveau de votre personnage, soit en réponse à des questions imprévues.
  Pensez simplement à prévenir les autres, soit à la pause, soit via l'animateur.
- **Synchronisez-vous** avec les autres **personnages-acteurs** à la pause pour les tenir informés de vos réponses et prendre connaissances des leurs.
- Restez dans votre personnage mais n'oubliez pas que **c'est un jeu** et que **l'ambiance** et la **bonne humeur** sont essentielles pour passer un bon moment.

## Pour rappel

Vous incarner une **personne**.
Vous pouvez **oublier** des choses, vous **tromper** ou **mentir**.
Vous **êtes sensé connaître UNIQUEMENT** les évènements que votre personnage connait et **pas plus**.

# Le contexte

## Vol de données et chantage chez MonFinancement.fr

### La société

Mon Financement.FR

**MonFinancement.FR** est une **petite PME** française innovante créée il y a 10 ans.
Elle compte aujourd'hui environ **60 salariés**.

### Cyberattaque et demande de rançon

La CTO de **MonFinacement.FR** à reçu ce dimanche une **demande de rançon** en échange de **données sensibles** qui ont été **chiffrées** par des hackers pendant le week-end.

### Appel des experts

Pour analyser l'attaque et avant de décider de payer ou non la rançon, l'entreprise a décidé de mandaté des experts enquêteurs-joueurs.

Leur mission est de comprendre ce qu'il s'est passé et trouver les informations à fournir aux autorités. Pour cela, l'entreprise a mobilisé 4 employés présents et actifs juste avant l'attaque :

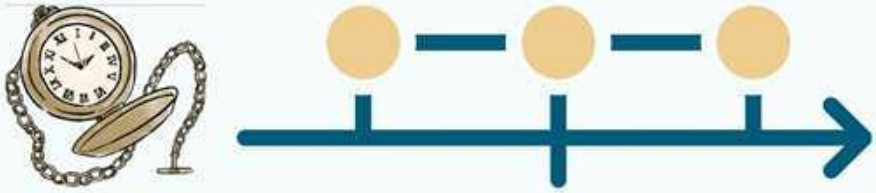
- **Robin Durant**
- **Jeanne Crespin du Bec**
- **Kevinn Raspopov**
- **Hadrien Narayana**

Les experts devront répondre aux questions suivantes :

- **Quelles données** ont été chiffrées ?
- **Qui** a permis l'attaque ?
- Quelles informations avez-vous sur **le hacker** ?

# La chronologie des évènements

## Timeline indicative



Chronologie indicative représentant l'ensemble des événements survenus.

Tous les éléments ne sont pas connus de tous les personnages et une chronologie propre leur est consacrée sur leurs **Fiches Personnage**.

Cette chronologie permet d'avoir une vision d'ensemble et d'aider à mieux appréhender l'ensemble de l'intrigue.

# Chronologie

## Le début - Il y a plusieurs années

### Il y a 6 ans

- **13 Septembre** : Arrivée de **Robin** chez **MonFinancement .FR**

### Il y a 5 ans

- **13 Mars** : Arrivée de **Hadrien** chez **MonFinancement.FR**
- **10 Juin** : Validation de la nouvelle architecture sécu
- **Septembre** : Mise en place de nouveaux firewalls et identity management
- **Novembre** : Nouvelles solutions antivirus

### Il y a 4 ans

- **Février** : mise en place du complément infra sécurité : EDR, etc.
- **16 Avril** : ouverture de route vers server 22, sans prévenir **Hadrien**
- **Hadrien** est prévenu a posteriori et ne fait rien

### Il y a 3 ans

- **Janvier** : Mise en place d'un centre d'opération de sécurité (SOC) avec des processus adapté. La cybersécurité est prise au sérieux.
- **Avril** : Mise en place d'un système de détection d'intrusion (SIEM) dans le cloud

### Il y a 2 ans

- **Février** : Arrivée de **Jeanne** en CTO chez **MonFinancement.FR**

### L'année dernière

- **Août**
  - **21 août** : **Robin** découvre le Forum Tech
  - Il y trouve des solutions techniques / donne des éléments de contexte
  - Il converse notamment avec Kevin Mitnick environ 3h / semaine

- **Septembre**
  - **20 Septembre** : **Robin** parle du Forum Tech à **Jeanne** et elle trouve ça super !

### 3 mois avant

- **1er du mois :** Arrivée de **Kevinn** chez **MonFinancement.FR** pour un stage de développeur en langage Java de 6 mois
- **5 du mois** : Kévin M parle à **Robin** de la librairie technique magique sur le forum
  - Cette librairie est adaptée au projet **SLOUP**
- **12 du mois** : **Robin** parle à **Jeanne** des contacts techniques sur le forum
- **18 du mois** : **Kevinn** fait des conneries
- **Jeanne** s'en sert comme exemple de mauvaise conduite
- **Kevinn** a reconfiguré son poste avec des outils à lui mais ne le dira à personne

# Chronologie

## Juste avant l'attaque

### 2 mois avant

- **Le 8** : **Robin** constate que **SLOUP** dérape. On ne décide rien, mais les discussions deviennent tendues et **Robin** s'inquiète.
- **Le 12** : Analyses approfondies des vulnérabilités : tout est **OK**
- **Le 17** : Mise à jour de la liste des groupes de hacker à surveiller
- **Le 18** : **Jeanne** perd son téléphoe mobile, **Kevinn** lui ramène

### Le mois précédent

- **Le 14** : Symposium "J'aime la cybersécu"
- **Le 23** : Démarrage du **nouveau projet Crypto Blockchain Data : CBD**

### Il y a 2 semaines

- **Lundi**
  - **Jeanne, Robin** et **Hadrien** sont en télétravail, **Kevinn** est sur site
  - **11h** : Comité de pilotage projet entre **Jeanne** et **Robin** - le projet **SLOUP** prend beaucoup de retard et ça se profile très mal.
  - **Jeanne** met la pression sur **Robin.** Sur proposition de **Robin**, ils décident d'utiliser la librairie préconisée par le forum technique
  - **Robin** obtient une dérogation de sécurité pour l'installation mais on oubli de prévenir **Hadrien**
  - **17h47** : **Robin** envoi un e-mail à **Kevinn** pour lui demander d'installer la librairie en urgence sur le projet **SLOUP** avec le lien de téléchargement
- **Mardi**
  - **14h** : Téléchargement de la librairie par **Kevinn** et installation sur le **serveur 22**
  - **Kevinn** rencontre beaucoup de problèmes pour l'installation alors que ça devrait être très simple...
  - Les autres sont en télétravail sur d'autres sujets...
  - **Kevinn** en profite pour prendre des cafés avec **José**

### La semaine dernière

- **Jeudi** : **Jeanne** présente les enjeux de la nouvelle initiative à la direction
- **Dimanche** : **Jeanne** reçoit un mail des cybercriminels
  - 1,244 M € à transférer en bitcoins dans 1 mois au plus tard

# Chronologie

## Le jour de la menace

### Hier

- **8h30 :** Réunion de crise avec **Jeanne**, **Robin** et **Hadrien**
  - Demande de rançon reçue !
  - Tout mettre en pause pour trouver une solution
- **9h30-10h** : **Robin** passe 15 coups de fils
  - Feux à éteindre et mise en pause des autres sujets
- **10h** : **Jeanne** informe la DAF
  - On envisage un paiement
- **11h** : **Jeanne** contacte les assurances et juristes
  - Pas de recours légaux
- **10h-12h** : **Robin** et **Hadrien** en cellule de crise.
  - Il faut agir vite et essayer de comprendre ce qu'il s'est passé
  - **Hadrien** propose de reconstituer la Kill Chain et insiste sur l'importance d'un point de vue externe
- **12h** : Réunion de crise avec **Jeanne**, **Robin** et **Hadrien**
  - Ne pas payer mais identifier la menace au préalable
- **14h** : **Robin** contact les meilleurs agents disponibles qui seront là demain
- **16h** : **José** annonce à **Kevinn** que la boîte a été hackée

### Aujourd'hui

- **Robin** dit à **Kevinn** de ne pas ébruiter l'affaire
- **Jeanne** et **Hadrien** demandent à tout le monde d'être disponible et de répondre honnêtement aux questions des experts. C'est la priorité de la journée.
- **Les meilleurs experts de cybersécurité externes** arrivent pour interroger tout le monde et reconstituer la Kill Chain de l'attaque

# Fiches Personnages

Les **Fiches Personnages** contiennent l'ensemble des informations nécessaires aux **acteurs** pour jouer leur rôle dans l'enquête.

C'est un guide pour aider à préparer et mener les discussions avec les **enquêteurs-joueurs** et les aider à révéler les bonnes informations sans trop en dire.
**Elle ne doit jamais être montrer directement aux enquêteurs-joueurs.**

La fiche est destinée uniquement à la personne qui jouera le rôle.

Il est conseiller de la fournir au moins la veille du jeu pour pouvoir préparer correctement le jeu.

Elle peut être imprimée sous forme de mini livret pour plus de confort.

La fiche présente les informations suivantes :

- L'histoire du personnage
- Son caractère
- Ses éléments de costumes
- Les documents en sa possession
- Un mobile possible qu'on pourrait retenir contre lui
- Ses motivations pour l'enquête
- Les évènements de son point de vue
- Ce qu'ils pensent des autres
- Ce qu'il sait du hack
- Ce qu'il va dire aux enquêteurs
  - spontanément
  - en réponse à des questions ciblées
  - ce qu'il ne dira jamais

# Robin Durant

# Fiche Perso

# Robin Durant

## Histoire du personnage

- Il a travaillé en ESN pendant 3 ans
- Puis il a intégré l'entreprise en tant que développeur il y a 8 ans
- Depuis 4 ans il est chef de projet / manager et essaie de faire tourner les projets, non sans mal
- Il soutient l'agilité mais il n'a pas encore bien compris sa place dans une organisation agile

## Caractère

Robin est **expérimenté**, **très volontaire** et positif même s'il est **complétement dépassé** par les évènements qu'il subit depuis des années et paraît souvent fatigué. Il fait tout son possible pour trouver des solutions et soutenir les équipes.

Il semble débordé et parle vite. Il propose toujours de faire lui même à la place des autres et se dévalorise très souvent.

## Costume

- Tenue formelle (mais pas trop)
- Badge accès
- Pochette avec les dossiers bien rangés (indices sur les personnages)
- Documents : 2 profils du forum, 1 conversation sur le forum, un e-mail

## Mobile possible

Une erreur dûe au surmenage ou à l'incompétence.

## Motivation pendant cette enquête

Éteindre la crise en aidant le plus possible les **enquêteurs-joueurs** et retourner au plus vite gérer ses autres problèmes...

## Les événements de son point de vue

- **L'année dernière**, pendant les vacances, avec moins d'activité sur les projets, **Robin** a entendu parler d'un **forum technique** et y a passé un peu de temps. Il a discuté avec plusieurs personnes qui l'ont beaucoup aidé et lui ont permis de trouver des solutions techniques très intéressantes pour ses projets. Il y trouve des ressources pour sa veille technologique et des conseils précieux. Il en a parlé avec **Jeanne**, la CTO, arrivée il y a 2 ans, qui était très contente. Il a partagé pas mal de sujets et d'éléments de contexte de l'entreprise pour pouvoir bénéficier de bons conseils adaptés. Il entretient des conversations régulières, environ 3h par semaine, un peu dispersées. Il converse principalement avec **Kévin Mitnick.**

- **Il y a 5 mois**, **Kévin**, son contact sur le forum, lui parle d'une **super librairie technique** qui serait très adaptée à son contexte et au projet **SLOUP** dont il lui a parlé.

- **Il y a 2 mois**, le **projet SLOUP prend pas mal de retard** notamment **à cause de** quelques difficultés du stagiaire Java, **Kevinn**. Dans l'équipe il y a Olivier, Marine, Mohamed et **Kevinn**. Il n'a rien contre **Kevinn** qui est un bon garçon mais là, il n'aide pas vraiment et nous met dans la panade. Il ne peut pas trop le protéger et même **Jeanne**, la CTO, a eu vent des retards dus au stagiaire incompétent.

- **Le mois dernier**, progressivement, **la pression est montée** pour finaliser tous les projets et consacrer une bonne partie des forces vives sur le nouveau projet innovant. La plupart des projets avancent bien et même si ça a été dur, tous avancent bien. Seul le projet **SLOUP** continue de traîner.

- **Lundi de la semaine dernière** :

  - À 11h : **Comité de Pilotage (COPIL) stratégique** avec **Jeanne** sur les encours. Le projet **SLOUP n'est toujours pas sorti** et il y a de nouveaux soucis techniques remontés. **Robin** prend une très très grosse pression. On ne le lâche pas. Il a alors l'idée de **mettre en place la librairie** dont il a entendu parlé sur le forum. Ce n'est pas l'idéal de rajouter une nouvelle librairie externe mais les gains permettront de finir le projet plus rapidement. Et c'est un sujet que même le stagiaire **Kevinn peut faire** sans problème. Il suffit d'installer et d'utiliser la librairie. En revanche, il faut une **dérogation de sécurité** pour être dans les temps. **Jeanne** est d'accord, il faut aller vite.
  - 17h47, **Robin** va voir **Kevinn** hyper stressé en disant qu'il faut absolument **installer la lib en urgence** sur le projet **SLOUP**. Malheureusement **Kevinn** est le seul sur site, étant stagiaire il n'a pas le droit au télétravail, donc c'est à lui de faire. Il lui **transmet le lien vers la librairie** que lui avait envoyé l'autre Kévin sur le forum
  - **Jusqu'à la fin de la semaine** : **Robin** a été pas mal occupé sur d'autres sujets urgents. Il court un peu partout. Vendredi il va un peu aux nouvelles sur **SLOUP** et s'aperçoit que le stagiaire n'a toujours pas fini l'installation, mais il promet de le faire très vite.

## Les événements de son point de vue - suite

- **Hier** :
  - 8h30 : il est convoqué par **Jeanne** avec **Hadrien**. Ils apprennent qu'elle a reçu une demande de **rançon** et qu'ils doivent tout mettre en pause pour trouver une solution.
  - 9h30-10h : **Robin** passe 15 coups de fils pour déléguer ou **mettre en pause** les urgences
  - 10h-12h : **Robin** et **Hadrien** se mettent en cellule de crise pour essayer d'échafauder un plan d'actions. La conclusion c'est qu'il faut **agir vite** et essayer de **comprendre** ce qu'il s'est passé. **Hadrien** parle dans son jargon de **reconstituer la Kill Chain** et de l'importance d'un **point de vue externe.**
  - 12h : Ils sont convoqués une nouvelle fois par **Jeanne**. Ils recommandent de **ne pas payer** mais d'**identifier la menace** au préalable.
  - 14h : **Robin** contacte **les meilleurs agents disponibles** qui viendront enquêter demain.

## Ce qu'il pense des autres

- **Kévinn**
  - Un bon gamin, un peu dans ses rêves. Il a de bonnes intentions mais n'est pas très réaliste. Il devrait être plus rigoureux et faire moins de bugs avant de se rêver expert. Il a encore beaucoup à apprendre.

- **Hadrien**
  - Un expert assez taciturne et pas très sympa. Il n'est pas très aidant. Il refuse même de discuter avec l'équipe pendant les sprints. Mais il produit une tonne de docs que personne ne comprend et qui sont inapplicables dans la vraie vie.

- **Jeanne**
  - La grande cheffe. Un peu dure parfois mais elle sait où elle veut aller. Si elle n'était pas aussi exigeante, il pourrait croire qu'elle le soutient mais ce n'est quand même pas facile.

## Ce qu'il sait du hack

- Pas grand chose
- Le serveur impacté est indépendant des projets en cours
- Rien n'avait vraiment commencé sur le nouveau sujet

# Robin Durant

## Ce qu'il dit aux enquêteurs

### Spontanément

- C'est **compliqué**. On avait vraiment pas besoin de ça, c'est déjà suffisamment le bazar
- L'avantage c'est que ça va mettre en lumière les **besoins en cybersécurité**. Comme **Hadrien** le dit souvent, une attaque ciblée permet à l'entreprise de prendre conscience de la vraie menace.

### Si on l'interroge spécifiquement sur

- **Le nouveau projet** : Il est très **innovant**. On ne peut pas donner trop de détails car c'est stratégique. Les données sont sur le **serveur 23**.
- **Le serveur 23** : Le serveur isolé contenant les données. À priori sécurisé
- **Le projet SLOUP** : Un projet **difficile** avec peu de personnes dédiées. On s'est appuyé sur un **stagiaire** mais il a eu **beaucoup de mal** à se mettre dans le projet et à livrer
- **La lib vérolée** : Elle lui à été conseillée par un **bon contact** sur le **forum**
- **Le lien de la lib** : Il l'a **reçu directement** sur le forum. Il peut montrer l'extrait de discussion
- **Dérogation de l'installation de la lib** : On était très en retard, il fallait qu'on fasse **vite**. Et franchement c'est pas la première fois qu'on a une dérogation
- **Son contact sur le forum** : **Kévin Mitnick**. Très compétent, sympa et serviable. Il lui ai donné pleins de solutions pragmatiques et au top des nouveautés techniques
- **Des infos détaillés sur Kévin** : Je dois pouvoir sortir son **profil sur le forum**. Je crois même qu'il y a une adresse IP associée.
- **Pourquoi avoir confié la lib et SLOUP à Kevinn** : Les autres ont été très pris sur **d'autres sujets** bien plus complexes et urgents. En plus, le **télétravail** n'aide pas. C'est plus simple avec **Kevinn** sur site. Mais finalement tous les sujets compliqués sont sortis et **SLOUP** a pris encore plus de retard.
- **Téléphone perdu de Jeanne** : Il n'a pas été au courant.
- **Les russes** : Il n'a pas d'avis
- **Le forum tech** : Un forum **très bien** avec des gens compétents et l'occasion d'obtenir de précieux conseils. En plus c'est gratuit
- **Le paiement de la rançon** : Il pense qu'il vaut mieux **ne pas payer** mais il n'a pas l'habitude de ce genre de décision

### Ce qu'il ne dira jamais

- Kévin Mitnick est suspect (il ne le crois pas d'ailleurs)
- C'est un coup des russes (il n'en sait rien du tout)

# Jeanne Crespin du Bec

# Fiche Perso

# Jeanne Crespin du Bec

## Histoire du personnage

- Une grande expérience dans des banques
- Précédemment manager de transition dans une grande banque très connue
- Elle a rejoint la société il y a 2 ans pour prendre le rôle de CTO et elle a tout remis à plat
- Elle a beaucoup d'ambition et souhaite continuer à faire évoluer sa carrière

## Caractère

De nature anxieuse, **Jeanne** est **très préoccupée** par la situation. Elle **aime contrôler** les situations et se sent très mal à l'aise quand quelque chose lui échappe. Elle est également **très occupée** et passe rarement plus de 30 minutes sur un même sujet. C'est une **business woman accomplie** et une **fine politique** qui connaît les rouages de l'entreprise. Elle sait d'ailleurs qu'une **attaque cyber peut lui coûter sa place** et entâcher très fortement sa carrière, ce qu'elle ne peut pas accepter. Elle veut montrer qu'elle **maitrise le problème** et que cela va se résoudre **grâce à elle**.

Elle emploie un ton politique qui se veut à la fois rassurant et exigeant et se met toujours en valeur elle-même.

## Costume

- Tenue sobre
- Badge accès
- Téléphone portable visible et posé sur la table
- Documents : L'e-mail de demande de rançon

## Mobile possible

Apparaître comme l'atout majeur de l'entreprise en maîtrisant une attaque cyber d'ampleur. Elle pourrait l'avoir initiée elle-même pour mieux la résoudre...

## Motivation pendant cette enquête

Gérer la crise rapidement et se montrer comme la personne clé de l'entreprise pour monter en grade.

## Les événements de son point de vue

- **Fin Q3 Y-1** (l'année dernière quoi), **Robin** lui a parlé de **contacts techniques** qui pouvaient aider et conseiller l'entreprise. C'est une **très bonne initiative.**

- **Il y a 2 mois**, elle a eu connaissance d'erreurs faites par le stagiaire **Kévinn**. Elle va s'en servir comme d'**un exemple** pour rappeler à tous le monde qu'il faut **livrer en temps et en heure**. C'est le **candidat idéal** à sacrifier pour un discours très ferme et intimidant car il n'est pas très sympathique, pas très efficace et qu'il n'est qu'en stage.

- **Depuis un mois**, il y a un fort enjeu à préparer les éléments de la nouvelle innovation technologique qui va porter la **future stratégie produit disruptive de l'entreprise**. Mais il reste quelques projets à finaliser.

- **La semaine dernière** - 11h: **Comité de Pilotage (COPIL) stratégique** avec **Robin** sur les encours. Le projet **SLOUP** n'est **toujours pas sorti** et il y a de nouveaux soucis techniques remontés. Pour assurer le nouveau sujet. Elle **met la pression à Robin** qui évoque une solution technique permettant de résoudre vite la situation. **Elle valide**, il faut vite terminer ces sujets.

- **Jeudi de la semaine dernière** : Elle a présenté les enjeux de la **nouvelle initiative** à la **direction**. Elle a la **pression** mais sait que c'est une **opportunité** très forte d'asseoir son expertise, de se positionner dans l'entreprise et d'entrer au comité stratégique voir d'être candidate au poste de **PDG** dans quelques années.

- **Dimanche dernier** : Elle reçoit un **e-mail** sur sa messagerie interne l'informant que le serveur contenant la **nouvelle initiative a été piratée** et que toutes les données sont cryptées. Elle doit transférer **1 Million €** sur un compte bancaire **avant 1 mois** si elle veut récupérer les données.

- Elle se souvient que **quelqu'un lui a pris son téléphone** il y a 2 mois et que **Kevinn**, le stagiaire, lui a ramené avec un grand sourire benêt, l'air fier de lui. Elle a des **soupçons** .

- **Hier**
  - 8h30 : elle convoque **Robin** et **Hadrien** pour exposer le problème. Il faut **absolument trouver une solution.**
  - 10h : elle **informe la direction et la DAF** pour envisager un paiement.
  - 11h : elle **contacte des assurances et juristes**, elle n'a pas de recours légaux.
  - 12h : elle refait un **point de crise** avec **Hadrien** et **Robin**. Ils décident de **ne pas payer** mais d'**identifier la menace**. **Hadrien** parle de **Kill Chain** et recommande une enquête externe, le principal fautif complice assumé ou malgré lui, est probablement ici.
  - 14h : ils contactent **les meilleurs agents disponibles** qui viendront enquêter le lendemain.

# Jeanne Crespin du Bec

## Ce qu'elle pense des autres

- **Kévinn**

Un tire au flanc un peu **rebelle**. Elle ne **l'apprécie pas** et s'en sert **d'exemple** pour montrer son autorité. C'est un stagiaire donc ça sert à ça. Et en plus il est vraiment **malpoli**.

- **Hadrien**

Un **expert**. On ne **comprend pas bien** ce qu'il raconte ni ce qu'il veut mais il **a l'air de maîtriser son affaire**. Il faut juste veiller à **ne pas exploser les coûts** en cédant à ses caprices.

- **Robin**

Un **manager utile et corvéable**. Il a réussi plusieurs fois à trouver des solutions pour sortir des projets enlisés. En le mettant **sous pression**, il peut **résoudre n'importe quel problème**, et en plus, il le fait sans se plaindre.

## Ce qu'elle sait du hack

- Pas grand chose à priori mais c'est probablement un groupe de **hackers russes**
- **Hadrien** devrait **en savoir plus très bientôt.** Elle a confiance en lui.
- D'ailleurs **Kevinn** le stagiaire est **d'origine russe** aussi, non ? Même s'il n'est pas très futé, elle ne serait pas étonné qu'il soit mêlé à cette affaire.
- **Kevinn** lui avait pris son téléphone il y a 2 mois...
- Elle sait que **Robin** a des contacts techniques sur un forum. **Peut-être pourront-ils aider** à sortir de ce guêpier ?

# Jeanne Crespin du Bec

## Ce qu'elle dit aux enquêteurs

### Spontanément

- Les **informations sont vitales** pour l'entreprise. C'est le futur de l'entreprise qui est dedans
- Il faut **absolument résoudre ce problème rapidement**. Avant le comité de direction de la semaine prochaine. Jeudi à 18h.
- C'est une **opportunité** de montrer la réactivité et la résistance de la DSI aux cyberattaques.

### Si on l'interroge spécifiquement sur

- **Le serveur 23** : Elle ne sait pas ce que c'est.

- **Téléphone perdu** : Elle a **perdu son téléphone** il y a 2 mois mais ne s'en est pas rendu compte tout de suite. **Kevinn** lui a ramené avec un **sourire louche**.

- **Les russes** : La Russie est un **pays complexe** et il est de notoriété publique que ce pays **abrite et protège des groupes de hackers** mandatés par le pouvoir pour déstabiliser l'économie mondiale. Notre entreprise, fleuron de l'économie et de la technologie française, fait donc figure de **cible idéale.**

- **Le forum tech de Robin** : **Robin** lui en a fait l'éloge. Des **conseils précieux et utiles**.

- **Le paiement de la rançon** : Ce n'est **pas la piste privilégiée** aujourd'hui. La direction n'est pas encline à faire ce transfert monétaire conséquent. La DAF **étudie cependant la question** et si les enquêteurs-joueurs pensent qu'il faut payer, elle insistera auprès de la direction.

### Ce qu'elle ne dira jamais

- Elle peut obtenir une **promotion** si elle gère bien cette crise.
- **Kevinn**, le stagiaire est le **coupable** c'est sûr.

# Kevinn Raspopov

# Fiche Perso

# Kevinn Raspopov

## Histoire du personnage

- Jeune **technicien réseau**, après 1 an, il décide de se reconvertir dans le développement informatique avec le langage de programation Java.
- C'est son **premier stage** en tant que développeur. Il y est depuis 2 mois.

## Caractère

**Désabusé**, Kevinn à l'impression d'être le **souffre-douleur**.
**Hautain**, il pense que son talent n'est pas reconnu à sa juste valeur et ça le **frustre**. Il est naturellement **nonchalant mais s'excite** si on le met en avant et qu'on parle de hackers, pour lesquels il a une vraie fascination
Il n'hésite pas à parler avec un jargon technique et en prenant les enquêteurs-joueurs de haut.

## Costume

- Tenu très (trop) décontracté
- T-Shirt en référence à des hacker (ou avec un badge ou auto collant)
- Badge accès
- Post-it collé sur le badge avec écrit : "mot de passe : QoicoubehLoL"
- Documents : L'e-mail de demande d'installation de la librairie

## Mobile possible

- Se venger de l'entreprise et de **Jeanne**, la CTO.
- Prouver sa valeur de développeur et de **hacker éthique** pour son ego

## Motivation pendant cette enquête

- **Faire la leçon** aux enquêteurs-joueurs
- Montrer que les autres sont mauvais et devraient plus le valoriser
- Se montrer comme un jeune tech efficace et reconnu

# Kevinn Raspopov

## Les événements de son point de vue

- **Depuis 2 mois** : En stage en tant que **développeur Java** dans l'équipe de **Robin**. Dans l'équipe il y a Olivier, Marine, Mohamed et lui. Tous font du télétravail mais lui n'y a pas droit. Il voulait bosser sur des technos sympas et l'IA mais on l'a mis sur des vieux projets. C'est **difficile pour lui** de rentrer dans les sujets. Il manque d'accompagnement de la part de **Robin** et du reste de l'équipe. De son point de vue, on lui a filé les **sujets pourris** et forcément **il a galéré.**
- **Lundi de la semaine dernière** : À 17h47, **Robin** lui tombe dessus hyper stressé en disant qu'il faut absolument **installer une lib en urgence** sur le projet **SLOUP**. Comme il est le seul sur site, **ça lui tombe dessus**. Une histoire de décision urgente de comité de pilotage (COPIL)
- **Mardi de la semaine dernière** : Vers 14h, il regarde l'e-mail et **télécharge la librairie**. Il commence l'installation sur le **serveur 22** et ça prend un temps fou. Il en profite pour prendre des cafés avec José, le stagiaire de la compta.
- **Jusqu'au vendredi** : **Il galère** avec pleins de petits soucis. Au début ça passait, mais vite ça devient un peu problématique. **Robin** risque de lui voler dans les plumes. Il s'est arraché et a **vraiment bossé** pour faire marcher. Il **a dû rechercher** un paquet de trucs sur Internet pour y arriver mais au final ça marche. Il est **très fier** d'avoir pu faire marcher le bouzin.
- **Hier** : **L'ambiance est bonne le matin** mais après 10h les chefs ne sont plus là et ça sent le truc pourri. **L'après-midi tout le monde fait la gueule.** À 16h, **José l'informe** que la boîte a été attaquée par des hackers. Il trouve que c'est trop cool, il se croit dans une série télé. Il pense aussi qu'on va venir lui demander de l'aide car il est très bon techniquement. **Robin** lui demande de ne pas parler du problème à qui que ce soit, à part les enquêteurs-joueurs.

# Kevinn Raspopov

## Ce qu'il pense des autres

- **Jeanne**
  - Un **tyran** qui le déconsidère. Elle **s'acharne injustement** sur lui sans comprendre que c'est lui qui peut le mieux les aider techniquement. Il essaie **au maximum de l'éviter** pour ne pas subir ses réflexions.

- **Hadrien**
  - Un vieux **un peu coincé**, pas du tout un hacker cool. Il sert surtout à mettre des **bâtons dans les roues** des développeurs mais **il s'y connaît quand même un peu** techniquement.

- **Robin**
  - Un **manager plutôt cool**. Il fait ce qu'il peut pour soutenir son stagiaire mais visiblement ça ne suffit pas. **Kevinn** aimerait beaucoup impressionner **Robin**.

## Ce qu'il sait du hack

- Pas grand chose à priori mais c'est sûrement un **groupe de hacker super cool** qui à fait ça. Peut-être le groupe de hacker russe **Akira**.

- Il sait qu'il a téléchargé une **librairie sur un site** par le lien fourni par **Robin**.

- Il a installé la librairie mais **il a eu pas mal de problèmes**. Il a galéré à débugguer l'installation avec des problèmes non documentés. Finalement ça a fini par marcher. Il demande aux joueurs-enquêteurs de ne pas parler des soucis qu'il a eu à **Robin**.

# Kevinn Raspopov

## Ce qu'il dit aux enquêteurs

### Spontanément

- **Trop cool cette cyber attaque !** On dirait une **série d'espionnage** et en plus, ils ont autre chose à faire que de lui tomber dessus.

- Les **enquêteurs-joueurs** sont des **experts en cybersécurité comme lui**. Ils sont un peu des **hackers éthiques comme lui**.

- **J'aurais pu pirater l'entreprise** moi aussi ! J'ai carrément le niveau.

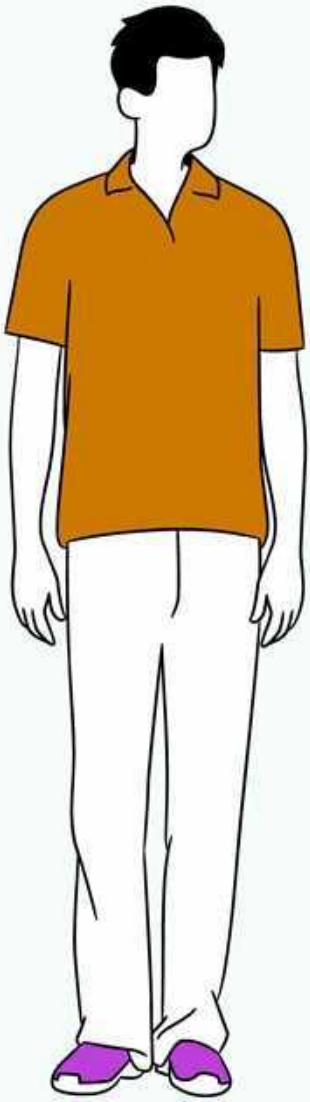
### Si on l'interroge spécifiquement sur

- **Jeanne, la CTO** : Trop relou. Elle **lui en veut** personnellement sans raison.
- **Le téléphone de Jeanne** : Oui, il a **retrouvé** le téléphone de **Jeanne à la cafétéria**. La boloss l'avait oublié. Il lui a ramené et elle a à peine dit merci. Abusé...
- **Les hackers** : Les hackers sont **trop cool** !
- **Ses parents** : **Russes** d'origines mais en France depuis 25 ans maintenant. Heureusement qu'ils ont déménagés sinon il aurait été obligé de passer dans un char en Ukraine...
- **L'installation de la lib** : Oui il a **installé** sur le **serveur 22**. J'ai galéré mais **j'ai réussi parce que je suis fort.**
- **La récupération de la lib** : Il a utilisé le lien de téléchargement de l'**e-mail** de **Robin**. Il peut retrouver cet e-mail.
- **Son mot de passe sur le post-it** : Lol. Des fois il l'oublie mais bon **ça ne risque pas grand chose**.
- **Akira** : Un groupe de **hacker russe hyper forts**
- **Le serveur 23** : Un **serveur isolé** avec des données **sensibles**
- **Le serveur 22** : Le serveur **SLOUP**
- **Les russes** : Ne le répétez pas mais **ça craint un peu** en Russie avec les manœuvres spéciales et le président qui reste à vie. On est mieux en France. Enfin **côté hacking** c'est quand même autre chose les russes.

### Ce qu'il ne dira jamais

- Il a été **nul**
- Les **hackers ont eu tort** de pirater l'entreprise

# Hadrien Narayana



# Fiche Perso

# Hadrien Narayana

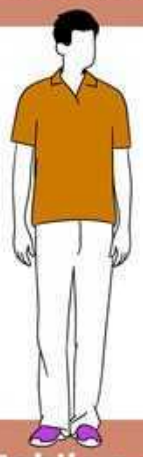
## Histoire du personnage

- Il a fait de **longues études en informatique** et a passé un **doctorat** en cybersécurité à l'UEIRB, en **Bielorussie.**
- Il a travaillé en tant qu'**expert en cybersécurité** pour un grand groupe Hongrois (Videoton Holding) pendant 4 ans. Il a habité en **Hongrie.**
- Il a rejoint l'entreprise **il y a 5 ans** en tant qu'**expert cybersecurité** pour remettre un peu les choses au carré.

## Caractère

Hadrien est d'un **naturel réservé**. Il est **expert** de son sujet et **veut être reconnu** comme tel. Il n'aime pas qu'on remette **ses décisions et son autorité** en cause. Mais aujourd'hui il se sent **dans son élément**. Il a fait venir des externes , les **enquêteurs-joueurs**, et veut les aider à trouver ce qu'il s'est passé.
Il s'exprime avec le ton d'un **professeur**, **sûr de lui**. Il n'est **pas très sympathique** ni drôle. Il aide les **enquêteurs-joueurs** en les considérant comme des experts comme lui.

## Costume



- Chemise sombre : il veut être pris au sérieux
- Lunettes
- Badge accès
- Pochette avec les dossiers
- Documents : Programme du symposium, cartographie des serveurs, liste des hackeurs, analyse traceroute, Un rapport des menaces (National Vulnerability Database (NVD)), Explication du scanning.

## Mobile possible

**Mobiliser l'entreprise** sur les enjeux de la cybersécurité pour provoquer un éléctrochoc : les menaces sont réelles et sont au coin de la rue.

## Motivation pendant cette enquête

**Identifier** l'assaillant et **comprendre** ce qu'il s'est passé, surtout pour l'intérêt intellectuel.

# Hadrien Narayana

## Les événements de son point de vue

- **Depuis 5 ans**, il **assure la cybersécurité** des systèmes informatiques de MonFinancement.fr. Il à remis beaucoup de choses en place, ce n'était pas glorieux. Maintenant,de son point de vue, **c'est acceptable.**

- **Il y a 2 ans**, remise à jour de la **documentation** de sécurité cyber de l'entreprise.

- **En début d'année dernière**, les **analyses approfondies** des vulnérabilités (scans) ont été lancées sans détecter de faille. Les analyses régulières sont lancées au moins une fois par semaine. **Aucune alerte**.

- **Il y a 3 mois**, il a remis à jour la **liste des groupes de hacker** à surveiller.

- **Il y a 2 mois**, nouvelles **procédures** de validation d'ouverture de flux internes et externes.

- **Le mois dernier,** il a participé au **symposium "J'aime la cybersecu".**

- **Hier** :
  - 8h30, :il est convoqué par **Jeanne** avec **Robin**. Ils apprennent qu'elle a reçu une **demande de rançon** et qu'ils doivent tout mettre en pause pour trouver une solution.

  - 9h30-10h : **Robin** passe 15 coups de téléphone.

  - 10h-12h : **Robin** et **Hadrien** se mettent en **cellule de crise** pour essayer d'échafauder un plan d'actions. La conclusion c'est qu'il faut **agir vite** et essayer de **comprendre** ce qu'il s'est passé. **Hadrien** propose de **reconstituer la Kill Chain** et insiste sur l'importance d'un **point de vue externe.**

  - 12h : Ils sont convoqués une nouvelle fois par **Jeanne**. Ils recommandent de **ne pas payer** mais d'**identifier la menace** au préalable.

  - 14h, **Robin** contacte les meilleurs agents disponibles pour enquêter aujourd'hui

# Hadrien Narayana

## Ce qu'il pense des autres

- **Kevinn**
  - Il ne le **connaît pas**. C'est un **stagiaire qui n'a pas compris** les enjeux de la sécurité et qui est plutôt un **risque** pour l'entreprise.

- **Robin**
  - Il a l'air **souvent dépassé** par les enjeux mais il est **sympa** et **agit**. Il ne prend pas assez en compte les procédures de sécurité de l'entreprise. On a beau lui rappeler régulièrement les procédures, **son équipe ne les respecte pas.**

- **Jeanne**
  - Une **politique**. Elle n'a **pas bien compris les enjeux de la cybersécurité** et néglige trop ce poste. Cependant **elle écoute** et va quand même souvent dans son sens, sauf quand il faut mettre la main au portefeuille...

## Ce qu'il sait du hack

- Il a beaucoup œuvré pour **sécuriser** les systèmes de l'entreprise. C'est aujourd'hui relativement sécurisé même si on peut mieux faire.

- Le **serveur impacté est indépendant** des projets en cours.

- Les premières analyses montrent que **l'attaque proviendrait de Russie,** peut-être d'un groupe nommé **Cozy Bear.** Mais cela reste à confirmer avec des analyses plus poussées.

- Il **ne sait pas** comment l'intrusion a eu lieu. Il faut **reconstituer la Kill Chain**, principalement la **livraison** qui va exposer la faille. Il sait que souvent la défaillance provient du Social Engineering, c'est à dire les **gens qui ne font pas attention**.

# Hadrien Narayana

## Ce qu'il dit aux enquêteurs

### Spontanément

- **J'étais sûr** qu'on subirait une attaque. J'avais prévenu.
- C'est une **super opportunité.** Il voulait vraiment mesurer son infrastructure à une attaque réelle. Il est **très excité** par cette enquête.
- Il faut **procéder méticuleusement et par étape**. Il faut construire la **Kill Chain** pour comprendre ce qu'il s'est passé, identifier le ou les points faibles (c'est probablement un employé) et cibler l'attaquant.
- **Parlons** ensemble de **cybersécurité** en général: la théorie, les concepts, l'actualité, les menaces

### Si on l'interroge spécifiquement sur

- **Le nouveau projet** : Il ne connaît pas le détail. Les données sont sur le **serveur 23.**
- **Le serveur 23** : Le serveur **isolé** contenant les données. À priori **sécurisé**
- **La connectivité du serveur 23** : Isolé je vous dit. **Aucun accès vers l'extérieur**. Ni même interne ! **Attendez** je regarde sur la carto... **Ah non tiens**, on avait ouvert un pont vers les serveur 21, 22 et 24 au moment du COVID pour les accès distants de la gestion du parc informatiques... On aurait dû les supprimer.
- **Le projet SLOUP** : Il ne le connaît pas. **Serveur 22** je crois
- **La librairie vérolée** : Ah oui celle là elle est **signalée** dans les derniers rapports NVD
- **Dérogation de l'installation de la lib** : Il n'a **jamais été informé** de cette installation. Elle aurait dû passer par son service pour être validée.
- **Le forum de Robin** : Il ne le **connaît pas**
- **Des infos sur Kevin Mitnick** : C'est drôle. **Le porteur de ce pseudo est un comique**, c'est le nom d'un célèbre hackeur mort en 2023.
- **Téléphone perdu de Jeanne** : Il n'a **pas été au courant**. Elle aurait dû le prévenir pour faire une vérification.
- **Les russes** : Une **nation active** en termes de **cyberattaques** mais c'est loin d'être la seule. D'ailleurs les nations n'ont pas beaucoup de contrôles sur ces groupes qui sont souvent transnationaux.
- **Le paiement de la rançon** : Il serait mieux de **ne pas payer mais** il va être compliqué de récupérer les données. Ce sera peut être nécessaire

### Ce qu'il ne dira jamais

- **Kevinn** et **Robin** savent ce qu'ils font et sont **professionnels**.
- L'attaque n'est **pas mérité** car l'entreprise était suffisament sécurisé.

# Les documents à fournir aux enquêteur-joueurs

- La Fiche Enquête
- La Fiche Kill Chain format Portrait
- La Fiche Kill Chain format Paysage

# Kill Chain Murder Party

une conférence immersive mortelle

# Fiche Enquête

Nom du groupe :

Quelles données ont été chiffrées ?

Qui à permis l'attaque ?

Quelles informations détaillées sur le hacker pouvez-vous fournir ?

essensei

se concentrer sur l'essentiel

# Kill Chain Murder Party

une conférence immersive mortelle

## Fiche Kill Chain

Nom du groupe :

1 **Reconnaissance** : c'est la phase de collecte d'informations et de planification permettant à l'attaquant de cibler son attaque.

2 **Armement** : L'attaquant prépare une arme sur mesure pour être utilisée innocemment par la cible et ouvrir les portes à l'attaquant.

3 **Livraison** : L'attaquant transmet directement (lien social, fishing...) ou indirectement (faux site...) l'arme qu'il a préparée.

4 **Exploitation** : L'arme est déclenchée, souvent par la cible elle-même, et donne un accès interne à l'attaquant.

essensei

se concentrer sur l'essentiel

# Kill Chain Murder Party

## une conférence immersive mortelle

5 **Installation** : L'attaquant, par le biais de l'arme installe un accès permanent dans le système d'information de la cible.

6 **Command & control** : L'attaquant ouvre des canaux de commande dans le SI lui permettant d'opérer.

7 **Actions** : L'attaquant opère dans le système : reconnaissance interne, récupération d'informations, destruction.

1.Reconnaissance

3.Livraison

5.Installation

7.Actions

2.Armement

4.Exploitation

6.Contrôle

essensei
se concentrer sur l'essentiel

# Indices des personnages-acteurs à imprimer

**Dans les affaires de Robin**

- Un badge (format A5)
- Une discussion sur le Forum Tech avec Kevin
- Le profil de Robin sur le Forum Tech
- Le profil de Kevin sur le Forum Tech
- L'e-mail de demande d'installation de la librairie

**Dans les affaires de Jeanne**

- Un badge (format A5)
- L'e-mail de demande de rançon

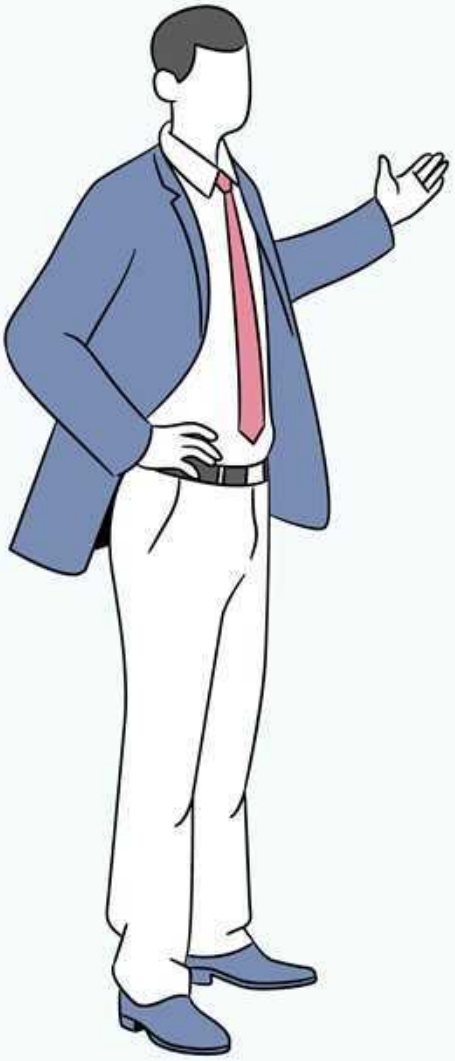
**Dans les affaires de Kevinn**

- Un badge (format A5)
- L'e-mail de demande d'installation de la librairie

**Dans les affaires d'Hadrien**

- Un badge (format A5)
- Le programme du symposium J'aime la Cybesecu
- La cartographie des serveurs
- Une liste de groupe de hacker à surveiller
- Une analyse de l'origine de l'e-mail de rançon
- Un rapport de vulnérabilités
- Une explication du scanning

# Dans les affaires de Robin Durant



# Robin Durant

Mon Financement.FR

**Robin** (Moi)

Bonjour Kévin. Je me permet de vous contacter pour notre contexte MonFinancement.fr . Nous avons un projet JAVA en cours, assez simple, mais qui doit avancer vite et avec un stagiaire qui n'est pas très dégourdi. Comment pourrions nous nous assurer que le code est complet et facile à produire par un débutant ? Est-ce que vous auriez des astuces magiques ?

Bonjour Robin, quand tu dis simple, on parle principalement de POJO ?

**Kévin**

**Robin** (Moi)

Oui en grande partie.

Alors j'ai un truc magique pour toi si tu ne connais pas. La librairie Lombok permet de générer automatiquement tout un ensemble de lignes de code avec toutes les bonnes pratiques. C'est un must have. Ton stagiaire devra juste mettre les bonnes annotations et après la majorité du code sera générée automatiquement à la volée en tissage orienté aspect : getter/setter, constructeurs, equals… ça fait gagner un temps fou.

**Kévin**

**Robin** (Moi)

C'est super. Je pense que c'est exactement ce qu'il nous faut oui. Je ne connais pas trop la programmation orienté aspect

Tu peux télécharger la lib directement ici http://projetlombork.org/downloads/lombok.jar

**Kévin**

FORUM TECH

# Kévin Mitnick

Tech All Star

2 854 recommandations

1 304 contributions

connection details : Melun, France
Routeur IP : 195.205.38.43
last connected : 1 week ago - 22h17

FORUM TECH

Robin

# Robin Durant

Tech Noob

0 recommandations

42 contributions

connection details : La Ferté-Macé, France
Routeur IP : 201.148.111.302
last connected : 2 weeks ago - 16h17

Robin

De: robin.durant@monfinancement.fr
À : kevinn.raspopov-stagiaire@monfinancement.fr

(il y a 8 jours)

Hi Kevinn !

Ca farte ? LoL ptdr

Pourrais-tu je te prie récupérer le lien de la librairie Lombok.
http://projetlombork.org/downloads/lombok.jar

Un fois installée, il faut que tu ajoutes les annotations @Data et @Non-Null aux bons endroits pour consolider le code.
Ca devrait résoudre les derniers problèmes et nous permettre de livrer rapidement.

Si tu as des soucis d'installation, tu peux contacter Marine pour t'aider.
Elle devrait avoir un peu de temps cette semaine.

Merci
Bien cordialement
Robin

# Dans les affaires de Jeanne Crespin du Bec

De: JeVousAiEu
À : jeanne.crespin_du_bec@monfinancement.fr

(il y a 2 jours)

Vous ne savez pas qui je suis.

Mais vous savez ce que sont les données du projet **CBD**.
Pour être plus exact, le projet  Crypto Blockchain Data

J'ai pris soin de crypter toutes vos données et de les rendre inutilisables pour vous.

Je peux vous envoyer la clé permettant de décrypter et récupérer toutes vos données.
Sans cette clé, toutes vos données seront définitivement perdues.

Je vous demande juste 1,236 Millions € en Bitcoin.

A vous de décider.

# Jeanne Crespin du Bec

**Direction**

Mon Financement.FR

# Dans les affaires de Kevinn Raspopov

# Kevinn Raspopov

STAGIAIRE

Mon Financement.FR

Robin

De: robin.durant@monfinancement.fr
À : kevinn.raspopov-stagiaire@monfinancement.fr

(il y a 8 jours)

Hi Kevinn !

Ca farte ? LoL ptdr

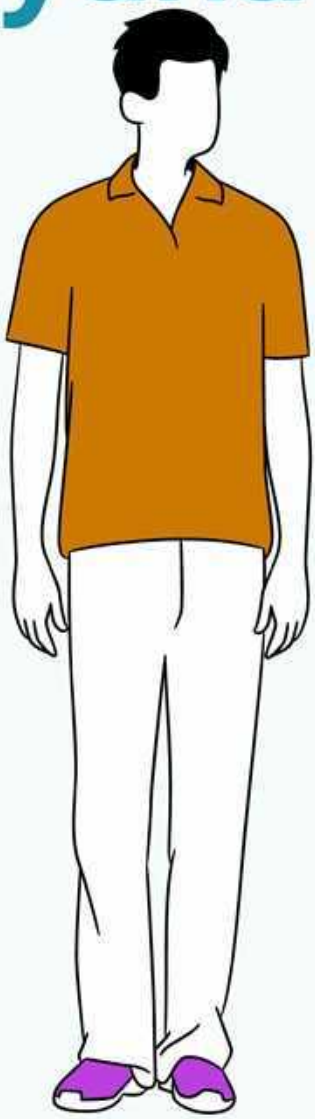
Pourrais-tu je te prie récupérer le lien de la librairie Lombok.
http://projetlombork.org/downloads/lombok.jar

Un fois installée, il faut que tu ajoutes les annotations @Data et @Non-Null aux bons endroits pour consolider le code.
Ca devrait résoudre les derniers problèmes et nous permettre de livrer rapidement.

Si tu as des soucis d'installation, tu peux contacter Marine pour t'aider.
Elle devrait avoir un peu de temps cette semaine.

Merci
Bien cordialement
Robin

# Dans les affaires de Hadrien Narayana



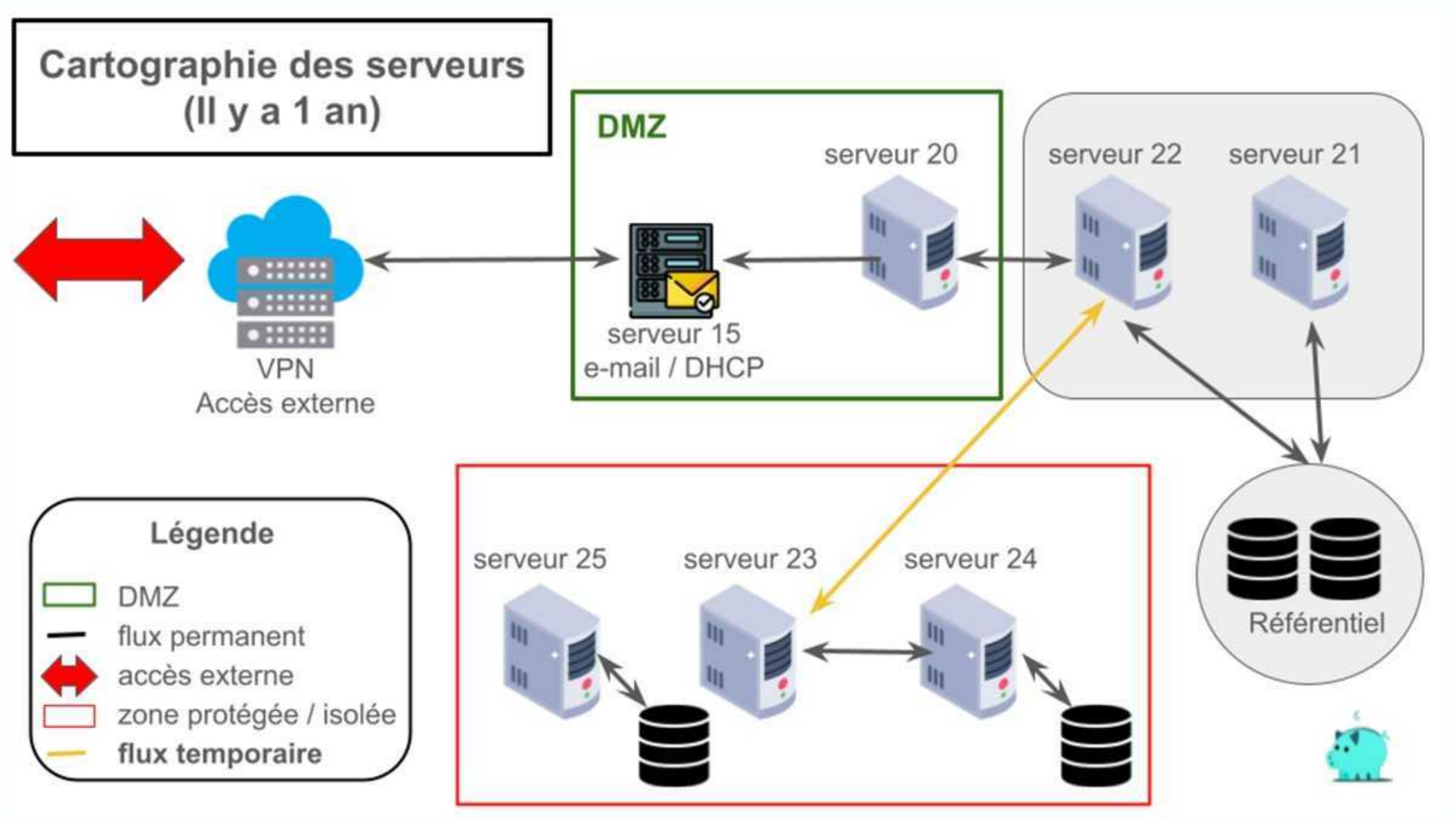
# Hadrien Narayana

Mon Financement.FR

# Symposium bi annuel des experts et professionnels de la cybersécurité

sponsored by Microsoft

| | Salle Microsoft | Salle Guillaume Poupard | Salle Daniel Guinier | Salle Laurent Bloch et Christophe Wolfhugel |
|---|---|---|---|---|
| 9h15-11h | Les enjeux de la cybersécurité de demain | Portraits des intrus aux systèmes d'informations | La documentation au centre de la cyberdefense | Green cybersécurité par les plantes |
| 11h12-12h57 | Les outils Microsoft à votre disposition pour la cybersécurité | Surveiller tous les utilisateurs | Documenter sa documentation cyberdéfense | Sécuriser par la suppression des accès |
| 14h08-15h53 | Le service Microsoft | Pourquoi moi non plus je ne devrais pas accéder aux systèmes | Processer son process de cybersécurité | Comment gérer une direction qui n'a plus accès à l'informatique |
| 16h05-17h20 | Comment prendre rendez-vous avec un commercial Microsoft | Qu'est-ce qu'on fait là ? | Documenter le process de documentation des processus | Postuler en tant qu'expert cybersecurité |
| 17h20-17h34 | Pot convivial de clôture de fin | | | |


Cartographie des serveurs
(Il y a 1 an)
DMZ
serveur 20
serveur 22
serveur 21
serveur 15
e-mail / DHCP
VPN
Accès externe
Légende
DMZ
flux permanent
accès externe
zone protégée / isolée
flux temporaire
serveur 25
serveur 23
serveur 24
Référentiel

# Liste des groupes de hackers
# Menaces à surveiller cette année

## Niveau 0

**RUSSIE**

- FANCY BEAR / APT28
- COZY BEAR / APT29

**EUROPE DE L'EST**

- DARKSIDE

**GRANDE BRETAGNE**

- LAPSUS$

## Niveau 1

**INTERNATIONAL**

- ANONYMOUS
- TELECOMIX
- HACKING FOR GIRLIEZ (HFG)

**PAYS-BAS**

- LIZARD SQUAD

**ÉTATS-UNIS**

- GOATSEE SECURITY

**ALLEMAGNE**

- CHAOS COMPUTER CLUB

## Niveau 2

**INTERNATIONAL**

- THE DARK OVERLORD

**ÉTATS-UNIS**

- EQUATION / SHADOW BROKERS
- LULZ SECURITY / LULZSEC
- UGNAZI

**CORÉE DU NORD**

- BUREAU 121
- LAZARUS GROUP / APT38

**ISRAËL**

- UNIT 8200

```
> emailheader -c email_rancon.eml > header.txt
...
> Received: by a05:af26:b0:ee04:8adc with SMTP id it38csp873644pxb; sunday last week 21:34:22 (PST)
X-Received: by 2002:a1f:e7c3:0:b0:230c:1143 with SMTP id
e186-20020a1fe7c3000000b0040c1143mr1354415vkh.10.170748080274; sunday last week 21:34:22 -0800 (PST)
Received: from mail-sor-f69.google.com (mail-sor-f69.google.com. [209.85.220.69]) by mx.google.com with
SMTPS id v123-20020a1fde81000000b004c03edabcd1sor537020vkg.1.2024.02.09.04.13.22  for
<jeanne.crespin_du_bec@monfinancement.fr> (Transport Security); sunday last week 21:34:22 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning jeanne.crespin_du_bec@monfinancement.fr)
client-ip=209.85.220.69;

> traceemailsource -f header.txt
...
tracing route to JeVousAiEu <alias>
*** VPN detected ***
the result can be inaccurate or irrelevant
********************
The IP source of this e-mail is 106.10.142.38

> iplookup -s 106.10.142.38

Country : Russia
City : Nijni Novgorod
Lat : 56° 18' 40,32" N
Long : 43° 55' 50,88" E
```

Russe ? Cozy Bear ?

Information Technology Laboratory

# NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

## CVEs Received and Processed

| Time Period | New CVEs Received by NVD | New CVEs Analyzed by NVD | Modified CVEs Received by NVD | Modified CVEs Re-analyzed by NVD |
|---|---|---|---|---|
| Today | 0 | 0 | 0 | 0 |
| This Week | 1 | 1 | 1 | 1 |
| This Month | 1461 | 1250 | 0 | 722 |
| Last Month | 2609 | 2790 | 0 | 360 |
| This Year | 4070 | 4040 | 0 | 1082 |

## CVSS V3 Score Distribution

| Severity | Number of Vulns |
|---|---|
| CRITICAL | 23003 |
| HIGH | 60873 |
| MEDIUM | 59809 |
| LOW | 2526 |

| Last 20 Scored Vulnerability IDs & Summaries | CVSS Severity |
|---|---|
| **CVE-2024-24822** - Une librairie du projet java Lambok permet de scanner un réseau interne et d'installer des logiciels de cryptage de données. Des pirates peuvent exiger des rançons pour fournir une clé de décryptage et restaurer les données.. lire CVE-2024-24822<br>**Published:** yesterday; 5:12:08 PM -050 | CRITICAL |
| **CVE-2024-24821** - Composer is a dependency Manager for the PHP language. In affected versions several files within the local working directory are included during the invocation of Composer and in the context of the executing user. As such, under certain conditions... read CVE-2024-24821<br>**Published:** last week; 7:15:08 PM -050 | MEDIUM |

# Qu'est-ce que les cyber attaques de Scanning ?

Lors du attaque de type Scanning, divers paquets de données sont envoyés au système ou au réseau pour identifier les services et les ports accessibles.

Le procédé est le suivant :

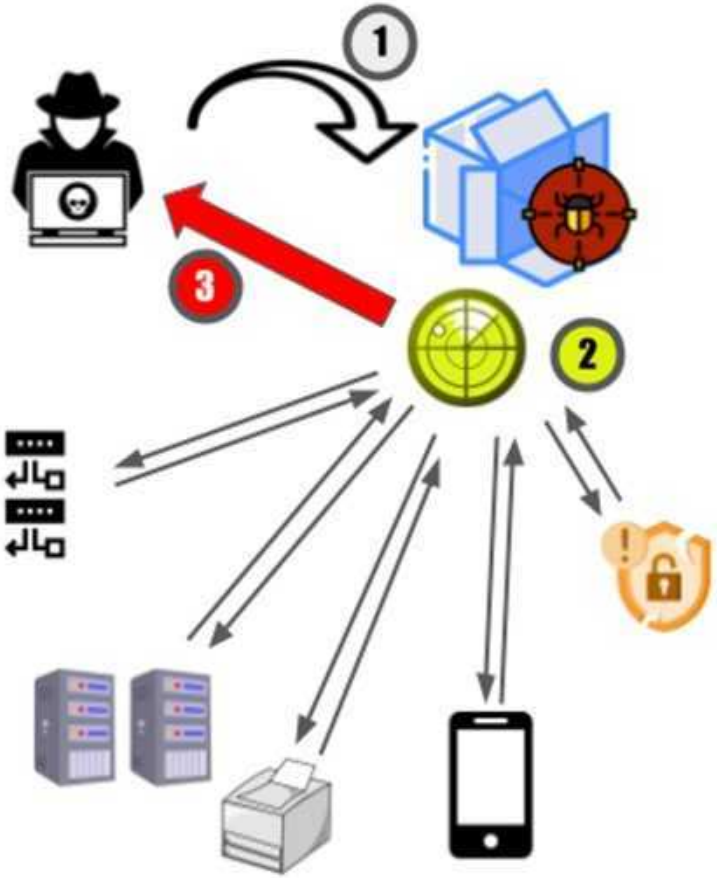
1. Livraison d'un logiciel vérolé
2. Un programme s'exécute et sonde le réseau
3. Le programme envoi un rapport à l'adresse programmé

Cela peut être fait manuellement, mais les attaquants s'appuient généralement sur des outils automatisés qui vont sonder et balayer différentes vulnérabilités.

Différents types de Scanning existent

- **Port Scanning** : Recherche des ports ouverts et accessibles
- **Network Scanning** : Recherche des services et matériels accessibles
- **Vulnerability Scanning** : Recherche des failles à partir d'une liste standard

Les attaques de type Scanning  constituent une menace sérieuse pour tous les systèmes et réseaux, mais avec les mesures et outils de sécurité appropriés, votre organisation peut rester en sécurité contre elles.
Les pare-feu, les systèmes de détection et de prévention des intrusions et les outils de gestion des vulnérabilités sont des étapes importantes pour parvenir à une cyberdéfense solide.



# Solutions

Vous trouverez ici les solutions de l'enquête avec la **Fiche Enquête** et la **Fiche Kill Chain** remplies.

Ne les communiquer pas aux **enquêteurs-joueurs** avant la fin de partie. Attention, notamment à ne pas laisser ses **documents imprimés visibles** lors de la partie.

Vous trouverez également les **culpabilités** des **personnages-acteurs** pour la clôture.

# KILL CHAIN MURDER PARTY

une conférence immersive mortelle

# Fiche Enquête

Nom du groupe : **Soluces**

## Quelles données ont été chiffrées ?

Toutes les données du projet stratégique confidentiel CBD

## Qui à permis l'attaque ?

Kevinn a installé l'outil utilisé pour l'attaque en utilisant le lien fourni par Robin

## Quelles informations détaillées sur le hacker pouvez-vous fournir ?

Le hacker est très probablement le pseudo Kevin Mitnick du forum Tech, associé à l'adresse IP 195.205.38.43 localisée à Melun et une dernière connexion la semaine dernière à 22h17

essensei

se concentrer sur l'essentiel

essensei
se concentrer sur l'essentiel

**1. Reconnaissance**
Discussions sur Forum Tech

**2. Armement**
Lien lib Lombok vérolée

**3. Livraison**
Installation de la librairie par Kevinn

**4. Exploitation**
Scan du réseau
Serveurs accessibles

**5. Installation**
Installation de l'outil de chiffrement

**6. Contrôle**
Allocation de privilèges
Accès aux données

**7. Actions**
Demande de rançon par e-mail

# Culpabilités

## Les fautes de Robin

Je suis coupable

- D'excès de **confiance**
- D'absence de **collaboration** avec mon responsable cybersécurité

J'aurais dû m'appuyer sur les valeurs agiles

- **Les interactions plutôt que les processus :** en obtenant une dérogation de sécurité en urgence, j'ai négligé la communication avec mon responsable cybersécurité.

- **La transparence** : en ne mesurant pas le risque à utiliser une librairie fournie par un inconnu, je n'ai pas rendu visible ce problème de sécurité.

- **Fournir le soutien** dont a besoin l'équipe, en ne laissant pas un stagiaire tout seul dans son coin pour redresser un projet sous pression.

## Les fautes de Jeanne

Je suis coupable

- D'un manque de **vigilance** concernant le partage des enjeux et des contraintes
- D'un manque de **transparence** et de **confiance** envers mes équipes

J'aurais dû m'appuyer sur les valeurs agiles

- **Les personnes avant les processus** : s'en prendre publiquement au stagiaire pour non respect des mesures élémentaires de sécurité au lieu de faire en sorte de le sensibiliser / responsabiliser sur les enjeux et contraintes s'est révélé contre productif …

- **La collaboration avec le client** : mettre sous pression les équipes a conduit à des choix malheureux faits dans l'urgence. Pourquoi ne pas explorer les alternatives en terme d'architecture, de roadmap, etc. sans dégrader la qualité ?

# Culpabilités

## Les fautes de Kevinn

Je suis coupable

- De manque de **transparence**, de cacher mes erreurs et difficultés
- De **naïveté**, manque de **vigilance** sur les menaces cyber et **contournement** des bonnes pratiques

J'aurais dû m'appuyer sur les valeurs agiles

- **Les personnes avant les processus** pour échanger tous ensemble sur mes problématiques et bénéficier des retours et alertes collectives que je n'aurais pas vu

- **Transparence, Inspection, Adaptation** pour mettre en visibilité ce qui est fait, identifier les risques et corriger les erreurs

## Les fautes d'Hadrien

Je suis coupable

- D'une posture d'expert, **dogmatique** et **intransigeante**, sans me soucier des nécessités de l'entreprise

J'aurais dû m'appuyer sur les valeurs agiles

- **Les personnes avant les processus**, plutôt que d'envoyer mes recommandations sur l'ingénierie sociale, impliquer tous les acteurs de l'entreprise pour qu'ils s'approprient ces concepts et les attitudes à adopter

- **La collaboration avec le client** (dans ce cas précis les autres équipes), pour les aider à mettre en place les chaînes de build sécurisant la construction, l'intégration de binaires et le suivi de vulnérabilité. Puis les rendre autonomes pour la suite

# Flyer cybersécurité

## Pour aller plus loin

Pour continuer à **sensibiliser** et donner des éléments aux participants pour **aller plus loin** dans leur compréhension et leur apprentissage de la cybersécurité, nous vous proposons un petit document à imprimer pour qu'ils puissent l'emporter et le relire.

Bien entendu, vous êtes libres de **créer votre propre document** insistant sur les éléments pertinents pour votre contexte.

## LOCKHEED MARTIN Kill Chain

1. **Reconnaissance** : c'est la phase de collecte d'informations et de planification permettant à l'attaquant de cibler son attaque.
2. **Armement** : L'attaquant prépare une arme sur mesure pour être utilisée innocemment par la cible et ouvrir les portes à l'attaquant.
3. **Livraison** : L'attaquant transmet directement (lien social, fishing...) ou indirectement (faux site...) l'arme qu'il a préparée.
4. **Exploitation** : L'arme est déclenchée, souvent par la cible elle-même, et donne un accès interne à l'attaquant.
5. **Installation** : L'attaquant, par le biais de l'arme installe un accès permanent dans le système d'information de la cible.
6. **Command & control** : L'attaquant ouvre des canaux de commande dans le SI lui permettant d'opérer.
7. **Actions** : L'attaquant opère dans le système : reconnaissance interne, récupération d'informations, destruction.

## Principes fondamentaux de la cyberagilité

Au sein des équipes, nous ne pouvons pas tous être des experts cybersécurité, mais tous doivent y être **acculturés**.

Les mesures de protection les plus pertinentes se font au sein des **équipes produit**, en connaissant la criticité des données et des services.

Les équipes d'expertises cyber **collaborent** avec les équipes produit et les aident à monter en compétence. Leur succès se mesure au travers du succès de ces équipes produit.

Les activités de cybersécurité doivent être menées **le plus tôt possible** dans le cycle de développement et au **plus près** des équipes produit.

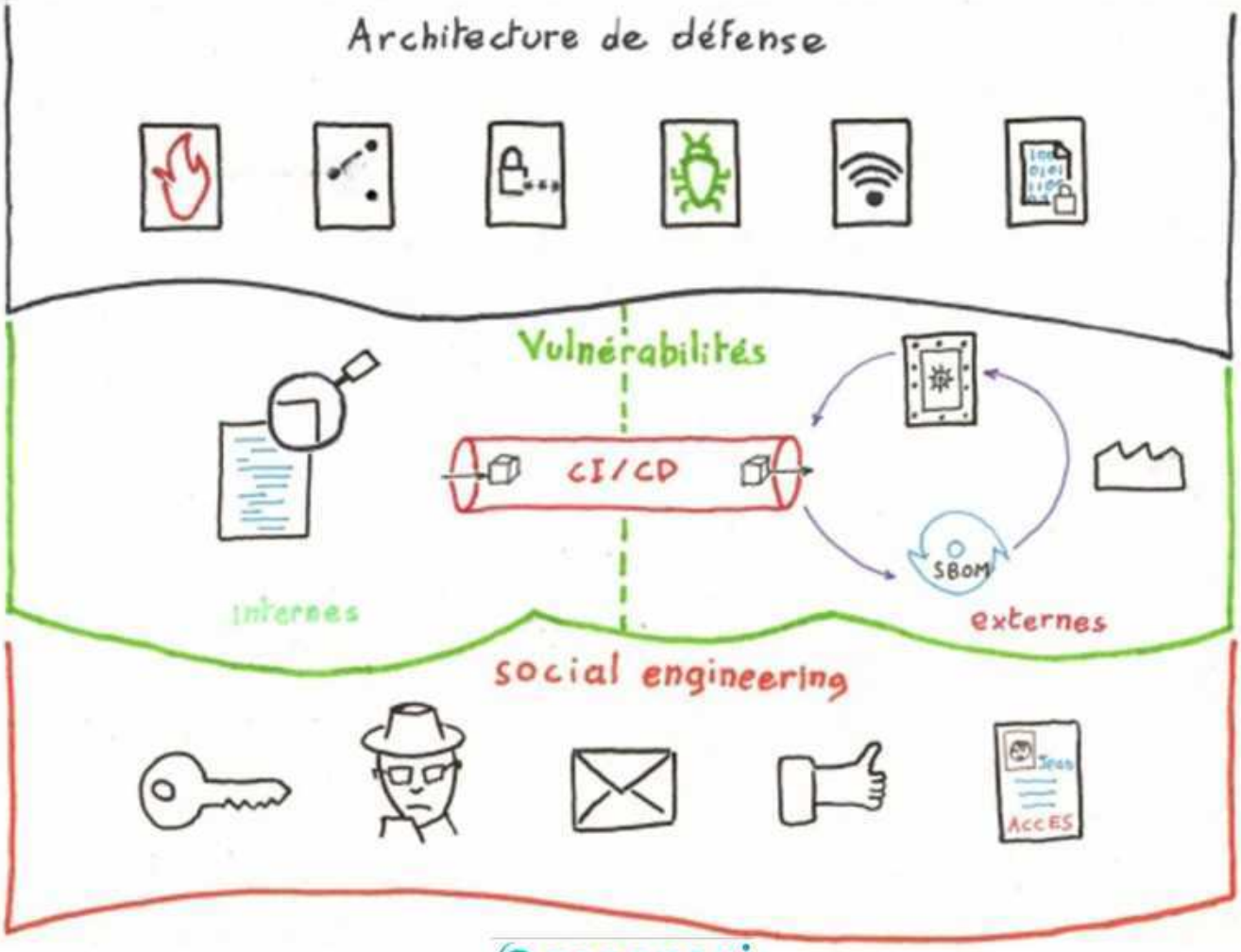
La "securité by design" s'adresse **en continu** durant toute la réalisation du produit. La CI/CD y est un élément majeur, mais pas le seul.

Les vulnérabilités sont **intégrées au backlog**, au même titre que les autres éléments à intégrer au produit, priorisées par le PO avec l'éclairage des experts.

Commencer par mettre en oeuvre les basiques de Rob Joyce :

- Patch management
- Least privilege administration
- Multi-factor authentication
- Know your network
- Daily backup
- White listing
- Enable logging / do analysis
- Harden (Flash, Java, etc.)
- Data encryption

essensei
se concentrer sur l'essentiel




essensei
se concentrer sur l'essentiel

## Les menaces sur le SI

Le **script kiddie** pratique le hacking pour le sport et le challenge. Il utilise des outils sur étagère. Ces attaques sont faciles à contrer mais très nombreuses, et il suffit d'une fois...

Les **hacktivistes** sont organisés en communautés. Ils défendent une cause et attaquent leurs cibles à des fins de divulgation de manière assez élaborée

Les **cybercriminels** pratiquent le racket auprès d'entreprises dont les services et données sont critiques. Très organisés, leur pratique principale est le chiffrement de données sensibles.

Les **APT** (advanced persistent threats) sont la crainte des états. Ce sont des groupes militarisés élaborant des attaques très techniques sur le long terme.

**L'ingénierie sociale** se focalise sur l'exploitation des travers du comportement humain, pour s'introduire physiquement ou numériquement dans l'entreprise ou accéder à des informations importantes.

**Le traitement des vulnérabilités** adresse les faiblesses de conception et de réalisation des produits face aux attaques connues. Il traite aussi les plans de remédiation face à l'apparition de vulnérabilités identifiées dans les produits ou composants utilisés

**L'architecture de défense** la stratégie et l'organisation des éléments de sécurisation de l'entreprise, au niveau réseau, infrastructure et doctrine.

https://www.essensei.fr/ressources/article/cyberagilite

# Vos retours sont précieux

**Merci** d'avoir téléchargé ce kit et de faire vivre ce jeu de sensibilisation à la cybersécurité.

Nous espérons qu'il aura répondu à vos attentes.

Pour **corriger** et continuer à **améliorer** ce jeu
pour vous, pour nous et pour tous les futurs participants,
nous avons besoin de vos retours,
positifs comme négatifs.

Ecrivez-nous à l'adresse suivante :

**contact@essensei.fr**

Nous sommes aussi disponibles, dans la mesure du possible, pour répondre à vos questions et vous aider à animer votre session.