

### Description du thème

Propriétés	Description
<b>Intitulé long</b>	Gestion et Réponse aux Incidents de Cybersécurité dans un Contexte Organisationnel
<b>Formation(s) concernée(s)</b>	Cybersécurité, Systèmes Informatiques, Réseaux
<b>Matière(s)</b>	• Cybersécurité • Réseaux et Télécommunications • Gestion de la Sécurité Informatique
<b>Présentation</b>	Cette activité simule un scénario de gestion d'incident de cybersécurité dans un environnement organisationnel. Les étudiants seront divisés en plusieurs groupes représentant différents départements d'une entreprise, chacun ayant des rôles et responsabilités spécifiques pour répondre efficacement à l'incident.
<b>Savoirs</b>	<ul style="list-style-type: none"> <li>• Techniques et stratégies de réponse aux incidents de cybersécurité</li> <li>• Coordination interdépartementale en cas de crise</li> <li>• Cadre légal et réglementaire en matière de cybersécurité</li> </ul>
<b>Compétences (Bloc 3)</b>	<ul style="list-style-type: none"> <li>• Protection des données à caractère personnel</li> <li>• Préservation de l'identité numérique de l'organisation</li> <li>• Sécurisation des équipements et des usages</li> <li>• Garantie de la disponibilité, intégrité et confidentialité</li> <li>• Cybersécurisation d'une infrastructure réseau, d'un système, d'un service</li> </ul>
<b>Transversalité</b>	B3,CEJM,CEJMA
<b>Mots-clés</b>	Gestion d'incidents, Cybersécurité, Réponse à la crise, Simulation, Rôle interdépartemental, Scénarios de sécurité
<b>Durée indicative</b>	2 heures
<b>Évaluation</b>	L'évaluation sera basée sur la participation active dans le jeu de rôle, l'efficacité de la réponse à l'incident, la qualité de la communication entre les groupes, et la pertinence des stratégies de gestion de crise proposées.
<b>Ressources</b>	<ul style="list-style-type: none"> <li>■ <a href="https://www.lemondeinformatique.fr/actualites/lire-wannacry-le-ransomware-planetaire-encore-pret-a-frapper-68202.html">https://www.lemondeinformatique.fr/actualites/lire-wannacry-le-ransomware-planetaire-encore-pret-a-frapper-68202.html</a></li> <li>■ <a href="https://www.avast.com/fr-fr/c-stuxnet">https://www.avast.com/fr-fr/c-stuxnet</a></li> <li>■ <a href="https://fr.wikipedia.org/wiki/Piratage_du_PlayStation_Network#:~:text=Le%20piratage%20du%20PlayStation%20Network.original%20de%20la%20PlayStation%203.">https://fr.wikipedia.org/wiki/Piratage_du_PlayStation_Network#:~:text=Le%20piratage%20du%20PlayStation%20Network.original%20de%20la%20PlayStation%203.</a></li> <li>■ <a href="https://www.numerama.com/tech/333329-github-a-subi-ce-qui-se-semble-etre-la-plus-grosse-attaque-ddos-enregistree-jusquici.html">https://www.numerama.com/tech/333329-github-a-subi-ce-qui-se-semble-etre-la-plus-grosse-attaque-ddos-enregistree-jusquici.html</a></li> <li>■ <a href="https://www.lemonde.fr/le-piratage-ashley-madison/">https://www.lemonde.fr/le-piratage-ashley-madison/</a></li> <li>■ <a href="https://www.numerama.com/cyberguerre/1219264-cyberattaque-la-liste-des-hopitaux-touchees-en-2022.html">https://www.numerama.com/cyberguerre/1219264-cyberattaque-la-liste-des-hopitaux-touchees-en-2022.html</a></li> </ul>

## Énoncé :

Les incidents de cybersécurité sont une menace constante pour les organisations. Une réponse efficace nécessite une compréhension approfondie des différentes phases de gestion d'un incident de sécurité et une collaboration étroite entre divers départements d'une organisation.

Ce TP vise à simuler un scénario de gestion d'incident de cybersécurité à travers un jeu de rôle.

## Objectif :

Dans ce projet, vous allez endosser le rôle de professionnels de la cybersécurité au sein d'une organisation fictive confrontée à un incident de sécurité informatique.

Votre mission est de collaborer avec vos camarades pour développer et exécuter un plan d'action efficace en réponse à cet incident.

Selon votre groupe, vous serez chargés d'analyser l'incident, de mettre en place des stratégies de défense, de restaurer les systèmes impactés, de coordonner les efforts de réponse entre les différents départements, et de gérer les communications ainsi que les aspects légaux de la crise. Cette simulation vous permettra de pratiquer des compétences essentielles telles que l'analyse critique, la résolution de problèmes, le travail d'équipe et la communication.

À la fin de l'exercice, nous discuterons ensemble de vos expériences, évaluerons les stratégies employées et tirerons des leçons sur les meilleures pratiques en matière de gestion d'incidents de cybersécurité.

Ce travail est conçu pour vous donner une compréhension concrète de la gestion des crises en cybersécurité et vous préparer à des situations réelles dans votre future carrière professionnelle.

## Partie 1 : Formation des Équipes et Introduction au Scénario (30 minutes)

Formez des groupes de **4 à 5 élèves**. Chaque élève se verra répartir un rôle (pour les groupes de 5, Sécurité et Personnel IT peuvent être doublés)

### Différents scénarios proposés :

#### *Scénario 1 : Attaque par Ver Informatique sur EnerTech (inspiré de l'attaque de Stuxnet sur les centrales nucléaires)*

**Type d'attaque :** Ver informatique, Sabotage

#### **Description détaillée :**

EnerTech, spécialisée dans les technologies énergétiques avancées, a été ciblée par CyberDragon, un groupe de cybercriminels. Un ver informatique, conçu pour perturber les systèmes de contrôle industriels, a été détecté dans leur réseau. Ce ver semble modifier les opérations des équipements de production d'énergie, menaçant de causer des pannes massives.



- **Tâches pour l'Équipe de Sécurité :** Identifier l'origine du ver, comprendre son fonctionnement et élaborer des contre-mesures.
- **Tâches pour le Personnel IT :** Assurer l'intégrité des systèmes opérationnels et mettre en œuvre des solutions de contournement pour maintenir la production.
- **Tâches pour la Direction :** Gérer la communication avec les parties prenantes et planifier une stratégie pour préserver la réputation de l'entreprise.
- **Tâches pour le Service Juridique :** Évaluer les implications légales de l'attaque et préparer une réponse aux enquêtes réglementaires.

## Scénario 2 : Piratage de MediaStar Entertainment (inspiré du piratage du playstation network)

**Type d'attaque :** Intrusion de réseau, Exfiltration de données

### Description détaillée :

MediaStar Entertainment, connue pour son réseau de jeux en ligne, le MediaStar Network (MSN), a été ciblée par ShadowLeague. L'attaque a entraîné une coupure prolongée du MSN, exposant les données personnelles de millions d'utilisateurs, y compris des noms, des adresses, et potentiellement des informations de carte de crédit.



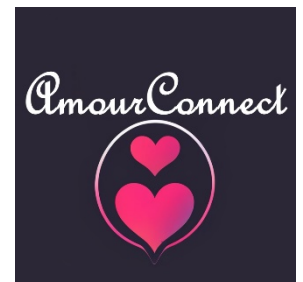
- **Tâches pour l'Équipe de Sécurité :** Investiguer sur la méthode d'infiltration utilisée par ShadowLeague et évaluer l'étendue de la fuite de données.
- **Tâches pour le Personnel IT :** Restaurer les services du MSN tout en renforçant la sécurité pour prévenir de futures attaques.
- **Tâches pour la Direction :** Gérer la crise en communiquant ouvertement avec les utilisateurs et les médias, tout en rassurant sur les mesures prises pour protéger les données des utilisateurs.
- **Tâches pour le Service Juridique :** Évaluer les implications légales de la violation de données, gérer les plaintes des utilisateurs et préparer la réponse aux autorités de régulation.

## Scénario 3 : Violation de Données chez AmourConnect (inspiré du vol de données chez Ashley Madison)

**Type d'attaque :** Violation de données, Exfiltration de données

### Description détaillée :

AmourConnect, un site de rencontres populaire, a été victime de Heartbleed Hacker. Les données personnelles, y compris des informations sensibles et des messages privés de millions d'utilisateurs, ont été exposées. L'attaque soulève des questions sur la sécurité des données et la vie privée.



- **Tâches pour l'Équipe de Sécurité :** Identifier la brèche de sécurité et prévenir de futures fuites.
- **Tâches pour le Personnel IT :** Sécuriser les serveurs et mettre à jour les systèmes de protection des données.
- **Tâches pour la Direction :** Communiquer avec les utilisateurs affectés et le grand public.
- **Tâches pour le Service Juridique :** Gérer les implications légales de la fuite de données personnelles.

## Scénario 4 : Ransomware chez NationalRail Networks (inspiré de WannaCry contre Deutsch Bahn)

**Type d'attaque :** Ransomware, Perturbation de service

### Description détaillée :

NationalRail Networks, opérateur national ferroviaire, a été paralysé par un ransomware déployé par LockMaster. Les systèmes informatiques sont bloqués, affectant les opérations ferroviaires et les informations affichées dans les gares.



- **Tâches pour l'Équipe de Sécurité :** Analyser le ransomware et développer une stratégie de réponse.
- **Tâches pour le Personnel IT :** Restaurer les systèmes affectés et établir des communications alternatives.
- **Tâches pour la Direction :** Coordonner la réponse à l'incident et informer les passagers et le personnel.

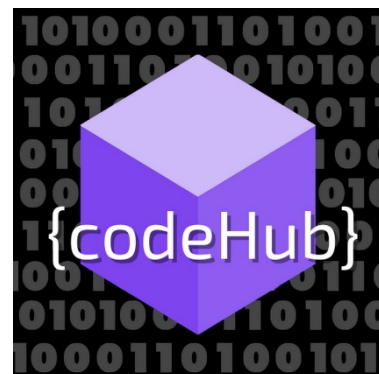
- **Tâches pour le Service Juridique** : Évaluer les conséquences légales et réglementaires de l'attaque.

### Scénario 5 : Attaque DDoS contre CodeHub (inspiré de l'attaque DDOS contre GitHub en 2018)

**Type d'attaque** : Attaque DDoS

**Description détaillée** :

CodeHub, une plateforme essentielle pour des millions de développeurs, subit une attaque DDoS massive de la part de DDoS Demons. La plateforme est devenue inutilisable, causant des perturbations majeures dans le développement de logiciels à travers le monde.



- **Tâches pour l'Équipe de Sécurité** : Mitiger l'attaque DDoS et identifier les auteurs.
- **Tâches pour le Personnel IT** : Rétablir les services et renforcer la résilience de l'infrastructure.
- **Tâches pour la Direction** : Communiquer avec les utilisateurs et les partenaires sur l'état de la situation.
- **Tâches pour le Service Juridique** : Gérer les implications juridiques et préparer la réponse aux autorités.

### Scénario 6 : Cyberattaque sur HealthNet Hospitals

**Type d'attaque** : Intrusion de réseau, Exfiltration de données, Compromission de dispositifs médicaux

**Description détaillée** :

Le réseau HealthNet Hospitals est ciblé par Medjack. Les dispositifs médicaux connectés et les systèmes d'information hospitaliers sont compromis, menaçant la sécurité des patients et la confidentialité des données de santé.



- **Tâches pour l'Équipe de Sécurité** : Identifier et isoler les systèmes affectés pour prévenir la propagation de l'attaque.
- **Tâches pour le Personnel IT** : Assurer la continuité des systèmes critiques et restaurer les opérations normales.
- **Tâches pour la Direction** : Coordonner la réponse interne et communiquer avec les patients et les autorités de santé.
- **Tâches pour le Service Juridique** : Aborder les questions de conformité et les implications légales de la violation de données de santé.

## Partie 2 : Détail des groupes de travaux

Chaque groupe doit élaborer un plan d'action spécifique en réponse à l'incident de cybersécurité, basé sur son rôle au sein de l'organisation fictive.

### 1. Équipe de Sécurité Informatique

**Nom du Service** : Sécurité Informatique

**Rôle Principal** : Protection et Réponse aux Incidents

**Tâches et Missions** (avec exemples) :

- 🖥️ Identifier la source de l'attaque (Analyser les journaux du système pour détecter l'origine de l'attaque....)
- 🖥️ Développer des contre-mesures (Mettre en place des pare-feu ou isoler des parties du réseau infecté....)
- 🖥️ Fournir des mises à jour sur l'incident : Rédiger des rapports sur l'état actuel de la sécurité et les mesures prises.

**Interactions** :




Collaboration étroite avec le Personnel IT et mise à jour régulière de la Direction.

## 2. Personnel IT

**Nom du Service :** Technicien IT

**Rôle Principal :** Gestion des Systèmes et Infrastructures

**Tâches et Missions (avec exemples) :**

-  Restauration des systèmes informatiques (Restaurer les données à l'aide des copies de sauvegarde)
-  Mettre en œuvre des solutions de contournement (Établir des serveurs provisoires pour maintenir les services en ligne)
-  Renforcer les défenses : (Installer des mises à jour de sécurité et des correctifs sur les systèmes.)

**Interactions :**




Coordination avec la Sécurité Informatique pour les aspects techniques et mise à jour de la Direction.

## 3. Direction

**Nom du Service :** Direction Générale

**Rôle Principal :** Gestion Stratégique et Communication

**Tâches et Missions (avec exemples) :**

-  Gestion de la communication de crise (Organiser une conférence de presse pour informer le public et les clients.)
-  Supervision de la coordination (Organiser des réunions régulières pour suivre les progrès des équipes...).
-  Gestion des relations externes (Communiquer avec les actionnaires pour expliquer les mesures prises)

**Interactions :**




Reçoit des informations et dirige la stratégie en collaboration avec le Service Juridique.

## 4. Service Juridique

**Nom du Service :** Département Juridique

**Rôle Principal :** Conseil Légal et Conformité

**Tâches et Missions (avec exemples) :**

-  Évaluer les implications légales (Analyser les violations potentielles de données en vertu du RGPD...)
-  Préparation pour les enquêtes (Rassembler des documents et des preuves pour répondre aux autorités de régulation....)
-  Conseiller sur les aspects légaux (Fournir des recommandations sur la communication publique pour éviter les litiges....)

**Interactions :**

Collaboration avec la Direction pour les décisions légales et recevoir des informations des équipes techniques.

## Partie 3 : Simulation de la Réponse à l'Incident

### Objectif

Mettre en pratique les plans élaborés dans la Partie 2 en simulant une gestion active de l'incident de cybersécurité selon le scénario choisi.

## Déroulement

### 1. Mise en Situation

Chaque groupe est placé dans une "salle de crise" fictive (un îlot de tables) .  
Le professeur annonce le début de l'incident (fournissant éventuellement des détails supplémentaires)

### 2. Réponse de l'Équipe de Sécurité Informatique

**Tâches** : Débuter l'analyse de l'incident, identifier les systèmes affectés et initier les premières mesures de confinement.

**Exemple** : Utiliser des tableaux blancs ou des logiciels pour tracer la propagation de l'attaque et décider des actions immédiates pour la contenir.

### 3. Actions du Personnel IT

**Tâches** : Commencer les opérations de restauration et de sauvegarde, et assurer que les services vitaux restent opérationnels.

**Exemple** : Simuler la restauration des systèmes à partir de sauvegardes et établir des communications de secours.

### 4. Gestion de Crise par la Direction

**Tâches** : Coordonner la réponse globale, décider des communications officielles, et superviser les actions des différents groupes.

**Exemple** : Organiser des briefings réguliers pour tenir informés tous les membres et planifier des annonces publiques.

### 5. Support du Service Juridique

**Tâches** : Conseiller sur les aspects légaux, préparer la documentation pour la conformité réglementaire, et gérer les implications légales de l'incident.

**Exemple** : Rédiger des notices légales et préparer des stratégies pour les enquêtes potentielles.

### 6. Interaction et Coordination

**Réagissez** en temps réel aux informations fournies par le modérateur.

**Communiquez** activement au sein de votre groupe et avec les autres groupes.

**Adaptez** votre stratégie en fonction des développements de la situation.

## Résultats Attendus

- 🔧 **Équipe de Sécurité Informatique** : Un rapport sur l'incident, incluant l'origine, l'impact, et les mesures prises.
- 🔧 **Personnel IT** : Un plan détaillé des opérations de restauration et des mesures de continuité mises en place.
- 🔧 **Direction** : Un résumé des décisions prises, des communications établies et de la gestion globale de la crise.
- 🔧 **Service Juridique** : Un aperçu des implications légales et des documents préparés.
- 🔧 **Tout le monde** : Un débriefing commun où chaque groupe présente ses actions et découvertes