LE SABOTAGE

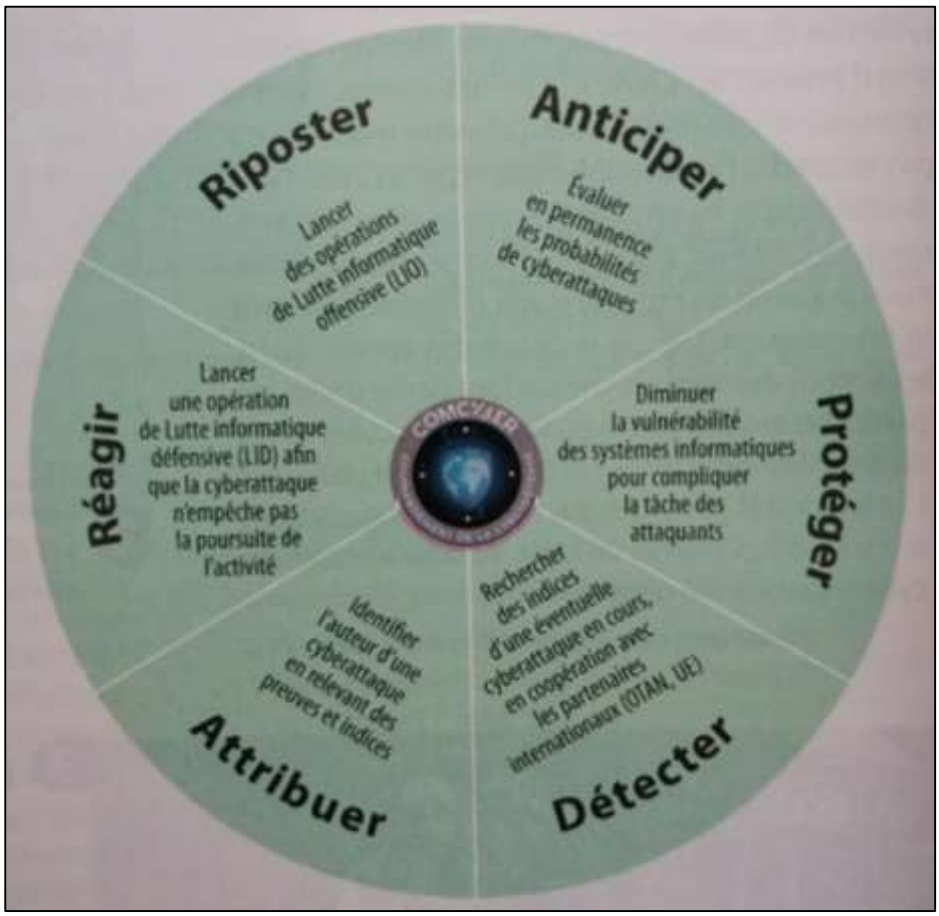
Doc1. La vulnérabilité des centrales nucléaires

La centrale *nucléaire* de Gundremmingen, située à 120 kilomètres au nord-ouest de Munich, a subi des assauts répétés de hackers. Ses systèmes informatiques ont été infectés par deux types de virus (W32.Ramnit et Conficker). Ces programmes malveillants n'ont [*cependant*] pas mis en péril les installations critiques des réacteurs […] a ainsi déclaré un porte-parole de l'entreprise.
Mais, selon nos informations, dix-huit postes ont tout de même été exposés à ces malwares [*logiciels malveillants*], connus depuis 2008 pour « collecter » des informations sensibles sur l'ensemble des réseaux connectés occidentaux. […] À ce stade, rien ne permet de relier ces attaques à d'éventuels actes terroristes. […]
Les autorités françaises, à commencer par les cinq cents experts de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI), prennent très au sérieux les risques qui pèsent sur les installations nucléaires, et les niveaux de protection ont été rehaussés depuis plusieurs mois*.

* En 2020, la France compte 18 centrales nucléaires en exploitation pour un total de 56 réacteurs nucléaires de puissance.

Source : Le Point, article mis à jour le 16 avril 2016 sur le site https://www.lepoint.fr/societe/une-centrale-nucleaire-allemande-victime-d-une-cyberattaque-29-04-2016-2035939_23.php#

Doc2. Les six missions de commandement de la cyberdéfense française



Source : Ministère des Armées, 2020.

Doc3. Le cyberespace élevé au rang de priorité stratégique pour la France

Le Livre blanc sur la défense et la sécurité nationale de 2013 élève le cyberespace au rang de priorité stratégique en France. En décembre en 2016, Jean-Yves Le Drian, alors ministre de la Défense, annonce la création d'un cybercommandement. Entre 2014 et 2019, la France consacrera un milliard d'euros à la cyberdéfense et se dotera d'une cyberarmée de 3200 hommes. […] Pour le ministre, « si une attaque cyber s'apparente à un acte de guerre, une riposte adéquate s'imposera dans une logique de conflit ouvert », conformément à l'article 51 de la Charte des Nations Unies.

Source : Soline Toussaint, « Le cyberespace : champ de bataille du XXI^{ème} siècle », *Diplomates*, 19 décembre 2017.

Doc4. Expert en sécurité informatique

Étudier la fiabilité du système d'information d'une entreprise et en assurer la sûreté, telle est la mission de l'expert en sécurité informatique. Un défi pour ce spécialiste, à l'heure où les échanges de données se multiplient. - Salaire débutant 3000€ brut –

En quoi consiste ce métier ?

Ses ennemis : les virus et les hackers (pirates informatiques). Sa hantise : une faille dans le réseau. Avec des informations de plus en plus nombreuses en ligne, les virus contaminent serveurs et messageries en quelques clics. L'expert en sécurité est là pour protéger les données et traquer les failles de sécurité des réseaux Internet et intranet. Il évalue d'abord le niveau de vulnérabilité des sites, traque d'éventuels virus et met en échec les tentatives d'intrusion de hackers. Ensuite, il met en place tout un système de protection : mots de passe, cryptologie, pare-feu, antivirus, etc. Les parades ne manquent pas pour réduire les risques. Toujours au fait des dernières tendances et menaces sur le Net, cet expert est de plus en plus recherché par les entreprises. Ce métier demande de l'intégrité, de la disponibilité mais aussi un respect total de la confidentialité.

Après le bac

5 ans pour obtenir un diplôme d'ingénieur ou un master en informatique, et plusieurs années d'expérience dans les réseaux informatiques sont nécessaires.

Source : https://www.onisep.fr/Ressources/Univers-Metier/Metiers/expert-experte-en-securite-informatique

CONSIGNES :

Vous devez constituer un ensemble de 5 cartes sur le thème du sabotage :

- une carte définition,
- une carte situation,
- une carte mission,
- une carte action,
- une carte formation.

Compétences mobilisées :

* Raisonner, justifier une démarche et les choix effectués
* Analyser et comprendre un document pour en extraire des informations
* Pratiquer différents langages
* Coopérer et mutualiser

Guide sur le contenu des différentes cartes :

- Carte définition : Doc1, proposez une définition de sabotage.
- Carte situation : Doc1, résumez brièvement un cas concret de situation de sabotage.
- Carte mission : Doc2, identifiez parmi les six missions de commandement de la cyberdéfense française, celle qui vous semble être la plus efficace pour contrer le sabotage.
- Carte action : Doc3, résumez la stratégie qui peut être appliquée à l'échelle européenne pour contrer le sabotage.
- Carte formation : Doc4, présentez un métier de la cyberdéfense.

Pour compléter et affiner vos réponses vous pouvez utiliser d'autres outils : manuel, dictionnaire, ordinateur. Une fois les 5 cartes réalisées, un élève ou plusieurs élèves rapporteurs présenteront à l'oral le travail de leur groupe à l'ensemble de la classe.

Toutes vos réponses doivent être rédigées sur les patrons de cartes ci-dessous.

LE SABOTAGE

① Carte définition

Est considéré comme un acte de sabotage, **une attaque informatique perpétrée par des hackers dans le but de diffuser des virus et des programmes ou logiciels malveillants afin de rendre inopérant un système informatique**. Le sabotage peut prendre l'aspect d'assauts répétés.

Par cette action, les pirates peuvent récupérer des informations confidentielles voire sensibles ou classées « *secret défense* ».

Source : Le Point, article mis à jour le 16 avril 2016 sur le site https://www.lepoint.fr/societe/une-centrale-nucleaire-allemande-victime-d-une-cyberattaque-29-04-2016-2035939_23.php#

LE SABOTAGE

② Carte situation

Le 16 avril 2016, **la centrale nucléaire de Grundremingen** en Allemagne a subi « *des assauts répétés de pirates informatiques* ». Les systèmes informatiques ont été infectés de virus et de nombreux postes de la centrale ont été exposés à des logiciels malveillants.

La situation aurait été particulièrement dangereuse si les pirates avaient pris le contrôle de la centrale et de ses réacteurs.

Source : Le Point, article mis à jour le 16 avril 2016 sur le site https://www.lepoint.fr/societe/une-centrale-nucleaire-allemande-victime-d-une-cyberattaque-29-04-2016-2035939_23.php#

LE SABOTAGE

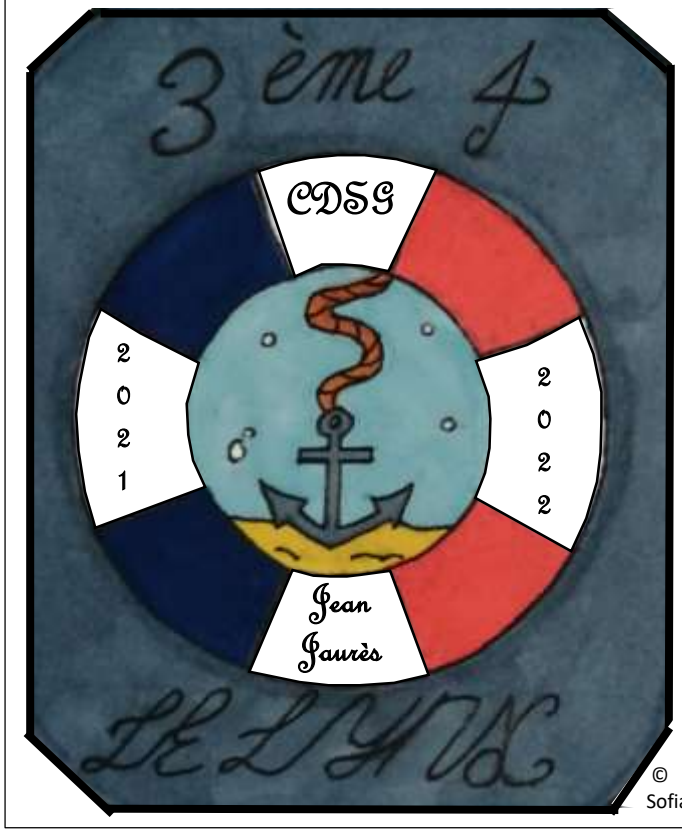
③ Carte mission

Source : Ministère des Armées, 2020.

LE SABOTAGE

④ Carte action

Source : Soline Toussaint, « Le cyberespace : champ de bataille du XXI[ème] siècle », *Diplomates*, 19 décembre 2017.



© Sofia

LE SABOTAGE

⑤ Carte formation

Source : https://www.onisep.fr/Ressources/Univers-Metier/Metiers/expert-experte-en-securite-informatique