FAIRE FACE ENSEMBLE

La sensibilisation de tous à la menace terroriste.

En proposant cette plateforme, le Secrétariat Général de la Défense et de la Sécurité Nationale offre à chacun la possibilité de mieux comprendre les enjeux de vigilance, de prévention et de protection face à la menace terroriste, pour adopter les bonnes pratiques et contribuer à la sécurité de tous.

DÉCOUPAGE PÉDAGOGIQUE

Environ **8h00** de contenu pédagogique dont **3h00** spécifiquement à destination des professionnels, avec par unité :

une vidéo introductive par un grand témoin

un questionnaire pour tester ses connaissances

le développement des notions clés du chapitre

des ressources complémentaires diversifiées en consultation libre

LA SENSIBILISATION À LA MENACE TERRORISTE EN 3 MODULES

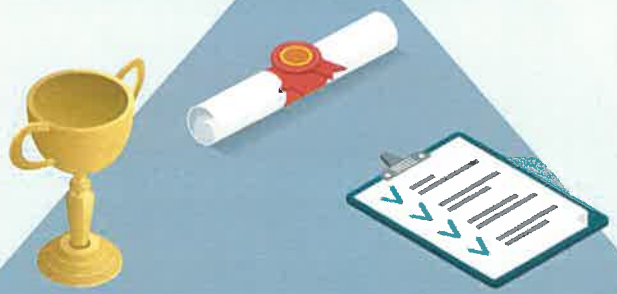
Construits autour de thématiques prioritaires, les 3 modules de 3 ou 4 unités chacun permettent :

- Pour le grand public, d'avoir une vue d'ensemble du plan VIGIPIRATE, de la menace terroriste en France, et des réflexes à adopter en conséquence ;
- Pour les professionnels, de mieux connaitre leurs responsabilités et d'acquérir les outils pour y faire face.

UN OUTIL PÉDAGOGIQUE ET ACCESSIBLE À TOUS

Le MOOC* « Faire Face Ensemble » est un outil de sensibilisation en ligne gratuit et accessible à tous vous permettant d'accéder à votre rythme **à un large contenu pédagogique.**

Une attestation délivrée dès :



80% de réussite

à toutes les unités

*MOOC : Massive Open Online Course. Formation en ligne ouverte à tous.

FAIRE FACE ENSEMBLE

WWW.VIGIPIRATE.GOUV.FR

REJOIGNEZ-NOUS

FAIRE FACE ENSEMBLE

WWW.VIGIPIRATE.GOUV.FR

MODULE 1

Comprendre la menace terroriste et le dispositif VIGIPIRATE

- **Unité 1 :** comprendre la menace terroriste
- **Unité 2 :** qu'est-ce que VIGIPIRATE ?
- **Unité 3 :** comment fonctionne VIGIPIRATE ?

MODULE 2

Tous impliqués face à la menace terroriste !

- **Unité 1 :** se préparer en tant que citoyen
- **Unité 2 :** prévenir un acte terroriste
- **Unité 3 :** réagir
- **Unité 4 :** gérer l'après-attentat

MODULE 3

Sensibilisation des professionnels

(responsables d'établissements ou de sites recevant du public)

et des élus locaux.

- **Unité 1 :** recommandations à destination des responsables d'établissements recevant du public
- **Unité 2 :** recommandations à destination des organisateurs de rassemblements
- **Unité 3 :** sensibilisation des élus locaux à la menace terroriste

Contact :
courrier.sgdsn@sgdsn.gouv.fr

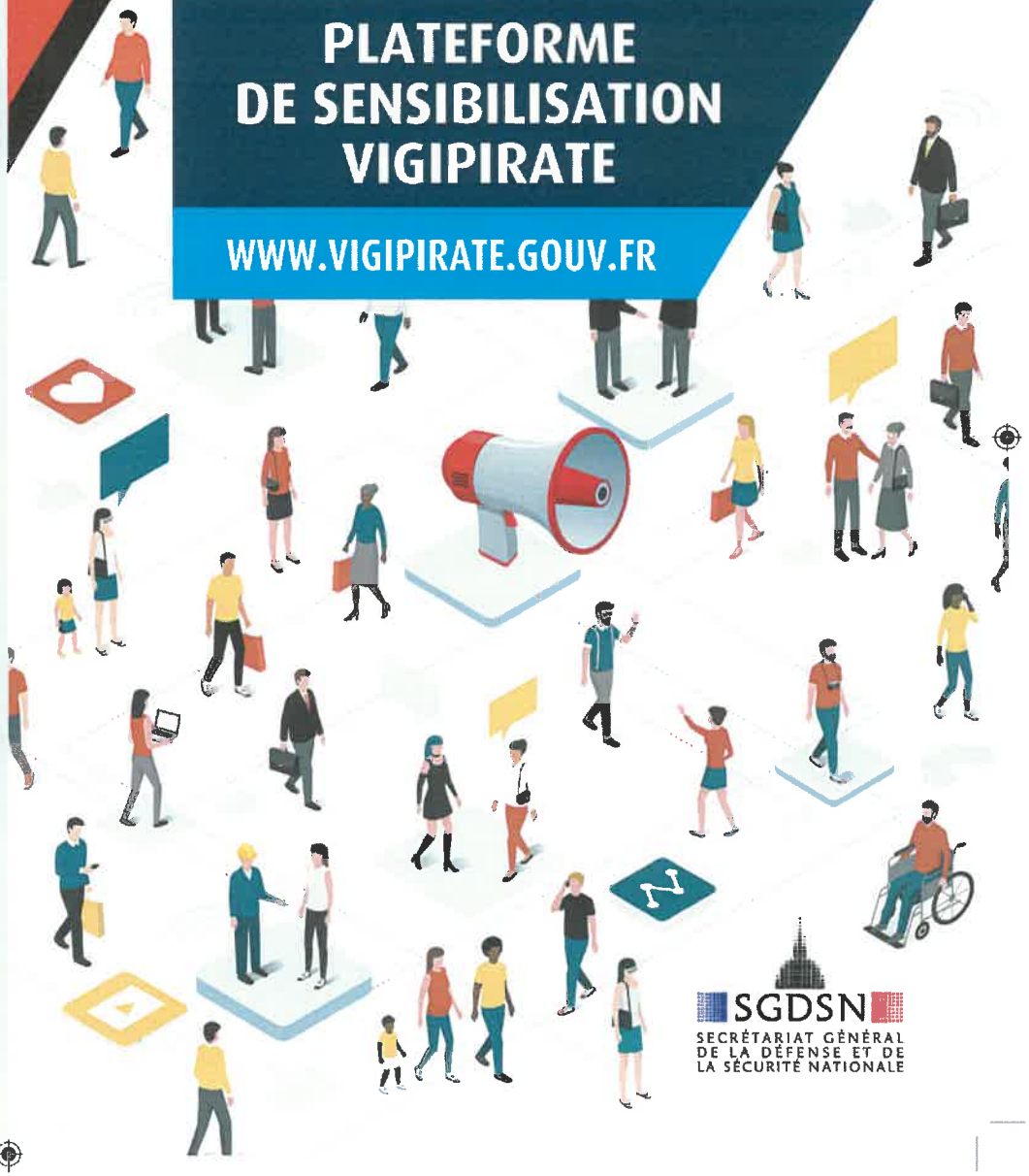
SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE
51, boulevard de La Tour-Maubourg
75700 Paris SP 07
www.sgdsn.gouv.fr

Maquette : PôleGraphisme, Fabrication, Images – DSAF/DPSG – Septembre 2019

FAIRE FACE ENSEMBLE

PLATEFORME DE SENSIBILISATION VIGIPIRATE

WWW.VIGIPIRATE.GOUV.FR



SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE
RETROUVEZ DE LA VISIBILITÉ SUR VOTRE ANNUAIRE

Cible : Administrateurs AD, CHAINE SSI

- L'ANSSI met à disposition des opérateurs stratégiques de l'État une capacité d'audit des annuaires Active Directory (et Samba) au travers du service ADS (Active Directory Security).
- Cette capacité vise à redonner de la visibilité aux opérateurs stratégiques de l'État (ministères, OIV, OSE, etc.) sur le niveau de sécurité de leur annuaire et à les accompagner dans son durcissement par l'application progressive de mesures adéquates. Cette prestation est basée sur l'expérience et l'expertise du bureau audits sur les sujets d'Active Directory (AD), et enrichie par les différentes opérations de cyberdéfense auxquelles le bureau participe.
- Le service ADS permet ainsi à la fois d'objectiver le niveau de sécurité et d'accompagner progressivement les opérateurs vers un niveau de sécurité à l'état de l'art. Cette capacité est pensée à la fois pour les chaînes SSI et pour les chaînes exploitation. Pour les unes, l'application présente les tableaux de bord avec les indicateurs ; pour les autres, elle présente les recommandations détaillées à appliquer et accompagne les bénéficiaires dans le pilotage de leurs prestataires.

1 Bénéficier du service ADS ?

Pour bénéficier du service, la procédure à suivre est particulièrement simple.

1. Télécharger la dernière version de l'outil de collecte ORADAD (Outil de récupération automatique de données de l'*Active Directory*) sur GitHub [**https://github.com/ANSSI-FR/ORADAD/releases**].
2. Extraire les fichiers exécutables (exécutable ORADAD.exe et fichier de configuration).
3. Ouvrir un terminal et exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine. Le fichier de configuration doit être positionné dans le dossier contenant l'exécutable ORADAD.exe [commande à lancer : ORADAD.exe <outputDirectory>].
4. Envoyer l'archive tar contenant les résultats de la collecte (et présent dans le répertoire outputDirectory) à l'adresse club@ssi.gouv.fr. Si la taille du fichier est supérieure à 10 Mo, l'ANSSI met à disposition un serveur d'*upload* sur lequel déposer le fichier. L'URL et les comptes permettant d'accéder au serveur sont fournis à la demande (email à adresser à l'adresse **club@ssi.gouv.fr**)

Dès réception du fichier de collecte, l'ANSSI lancera les analyses et en partagera les résultats dans un délai de 15 jours, sous forme d'un rapport détaillé présentant les différents points de contrôle qui ont révélé des défauts de configuration pouvant entrainer des risques de sécurité.

2 ADS pour les nuls

L'annuaire AD, centre névralgique de la sécurité des systèmes d'information Microsoft

L'annuaire Active Directory est l'élément qui permet de gérer de manière centralisée l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI.

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE
RETROUVEZ DE LA VISIBILITÉ SUR VOTRE ANNUAIRE

Le faible niveau de sécurité des annuaires met en danger les systèmes d'information

Les prestations d'audit effectuées par l'ANSSI auprès de ses bénéficiaires font apparaître un manque de maturité critique récurrent sur la sécurité des annuaires Active Directory. Ce défaut de sécurité affaiblit significativement le niveau global de sécurité de ces SI. Cette observation est confortée par la connaissance acquise au contact des différents réseaux compromis sur lesquels l'agence est intervenue lors d'opérations de cyberdéfense. Au-delà du manque de maturité, le bureau Audits constate par ailleurs que le niveau de sécurité des annuaires Active Directory décroît en fonction du temps et du cycle de vie du SI.

Développement d'une capacité spécifique et ouverture d'un service

Au sein de l'agence, les prestations d'audit sur un système d'information donnent habituellement lieu à la rédaction d'un rapport détaillé, répertoriant à un temps t les vulnérabilités qui touchent le système d'information, les recommandations correspondantes et la priorité de leur déploiement. Ces rapports, souvent volumineux, ne permettent pas toujours de prioriser avec aisance les actions à mener. Par ailleurs, si un audit donne une idée du niveau de sécurité à un instant donné, il ne mesure pas durablement l'évolution du niveau de sécurité.

Face à ce constat, le bureau Audits a développé une nouvelle capacité dont l'objectif est d'auditer, à la demande du bénéficiaire et de manière autonome, le niveau de sécurité des Active Directories des ministères.

Une approche ludique et personnalisée

Les résultats sont rendus disponibles depuis une interface web qui répertorie et ordonne les vulnérabilités et recommandations afférentes. Lors de chaque audit, le niveau de sécurité de la configuration de l'Active Directory est traduit par un niveau sur une échelle de 1 à 5. Le niveau obtenu découle immédiatement de la gravité des vulnérabilités trouvées le niveau 1 étant synonyme de défauts critiques et le niveau 5 d'un niveau à l'état de l'art.

Un niveau donne ainsi accès à un lot de recommandations adaptées. Une fois ces dernières mises en œuvre, des scripts de contrôle sont aussitôt référencés dans l'interface pour permettre à l'administrateur de contrôler de manière autonome et indépendante la bonne application des recommandations.

L'évolution relative à chaque niveau est objectivée par un score et représentée sur l'interface graphique par une barre de progression. Même si elle ne permet pas toujours d'accéder aux vulnérabilités et recommandations du niveau suivant, la correction progressive des vulnérabilités à un niveau donné, se traduit néanmoins par l'obtention de points. L'administrateur peut ainsi justifier de manière objective que ses actions améliorent significativement le niveau de sécurité de l'AD et donc du SI.

Considérant l'enjeu majeur pour un réseau qu'est la bonne sécurisation de son AD (et son maintien), l'idée de l'ANSSI est d'accompagner progressivement vers un niveau de sécurité à l'état de l'art grâce à l'application de recommandations adéquates et dans un contexte plus ludique (*gamification*).

3 En savoir plus

Envoyer un email à club@ssi.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle Graphisme, Fabrication, Image – DSAF/DPSG – Octobre 2019.

CONDUITE A TENIR LORS D'UN ÉVÉNEMENT BIOLOGIQUE OU CHIMIQUE

Fiche pratique à destination des responsables de sécurité et de sûreté des établissements recevant du public (ERP)

(Fiche actualisée en date du 7 mai 2019)

Cette fiche décrit les bons réflexes à adopter en cas de survenue d'un événement de type biologique ou chimique au sein d'un ERP afin de limiter au maximum le nombre de victimes et de préparer au mieux l'arrivée des services spécialisés. Elle ne vise pas à faire de chaque agent de sécurité un spécialiste des risques biologiques et chimiques. Elle vient en complément de la fiche de sensibilisation du grand public sur cette thématique déjà accessible sur le site du gouvernement : https://www.gouvernement.fr/partage/10904-que-faire-en-cas-d-exposition-a-un-produit-toxique-ou-contaminant-reagir-attaque-chimique

- Les criminels et les terroristes ont démontré leur capacité à fabriquer des explosifs ou des substances chimiques en utilisant des produits chimiques courants.
- La fabrication et la volonté des terroristes à utiliser des armes biologiques ou chimiques est aujourd'hui avérés. Plusieurs tentatives d'attentats ont été déjouées par les autorités ces dernières années :
- **Eté 2017 :** arrestation d'individu préparant un attentat chimique en Australie ;
- **Mars 2018 :** tentative d'assassinat au novitchok au Royaume-Uni ;
- **Mai 2018 :** découverte de tutoriels de fabrication d'explosifs et de ricine (toxine) lors d'une perquisition en France ;
- **Juin 2018 :** découverte d'un laboratoire clandestin de production de ricine en Allemagne.
- **Novembre 2018 :** arrestation en Italie d'un suspect souhaitant commettre un attentat à la ricine.

En cas d'événement de nature biologique ou chimique, une bonne organisation préalable de vos établissements ainsi qu'une réaction adaptée de vos personnels peuvent sauver des vies.

1 Généralités sur la menace biologique et chimique

La menace biologique se caractérise par l'utilisation de deux types d'agents :

- les agents infectieux (virus, bactéries, champignons). Ils peuvent être :
  - **contagieux.** Quelques agents suffisent alors pour provoquer une épidémie si la maladie n'est pas détectée à temps ;
  - **peu ou pas contagieux (bacilles du charbon).** Ces agents peuvent exceptionnellement se transmettre lorsqu'ils sont, par exemple, sous forme sous forme de poudre fine volatile. La dispersion initiale peut passer inaperçue. La maladie se déclare alors après une période d'incubation pouvant aller de un à dix jours, compliquant d'autant plus l'identification de son origine.
- **les toxines sont des substances toxiques produites par des organismes vivants** (ricine par la graine de ricin, toxine botulique par le bacille *clostridium botulinum*). Elles peuvent être :
  - inhalées par les voies respiratoires, leur action nocive peut alors survenir en quelques minutes ;
  - ingérées par voie alimentaire ou hydrique, leur action peut survenir en quelques heures, voire davantage. La survie des personnes intoxiquées tient alors essentiellement à l'identification très rapide de l'agent et, souvent, à l'administration, en extrême urgence, du traitement adéquat.

La menace chimique est liée à l'utilisation de produits toxiques qui sont **inhalés par les victimes** (gaz ou aérosols de fines gouttelettes), **qui pénètrent à travers la peau ou qui sont ingérés** (aliments, boissons).

Si **leur action est généralement rapide** (quelques secondes à quelques minutes), ils peuvent toutefois entraîner des effets secondaires très graves qui n'apparaissent que plusieurs heures après l'agression (phosgène, chlore, etc.).

Certains de ces produits sont très répandus dans l'industrie (chlore, cyanures), d'autres sont uniquement fabriqués à des fins offensives (sarin, ypérite, etc.).

Si certains toxiques se dispersent assez rapidement (acide cyanhydrique, chlore), d'autres, moins volatiles, sont dits « persistants » et peuvent maintenir le danger pendant plusieurs heures, voire plusieurs jours. Ces derniers sont généralement « contaminants » : ils se déposent sur le corps, les vêtements, les objets et peuvent se transférer d'une personne à l'autre.

CONDUITE A TENIR LORS D'UN ÉVÉNEMENT BIOLOGIQUE OU CHIMIQUE

FICHE PRATIQUE À DESTINATION DES RESPONSABLES DE SÉCURITÉ

(Fiche actualisée en date du 7 mai 2019)

2

Un événement biologique ou chimique, qu'il soit intentionnel ou accidentel, peut être détecté par **l'observation concomitante de certains indices** (odeur inhabituelle, déversement d'une substance liquide, nuage de fumée, etc.) **et de symptômes identiques sur plusieurs personnes.** Sans disposer de matériel de détection spécifique, cette concomitance d'indices et de symptômes doit alerter et pousser les agents de sécurité d'un ERP à réagir afin de limiter au maximum le nombre de victimes. **Le tableau ci-dessous récapitule :**

- **les principaux symptômes aisément détectables** chez une personne soumise à l'action d'un agent biologique ou d'une substance chimique ;
- **les principales actions à réaliser** afin limiter le nombre de victimes et préparer l'arrivée des services de secours spécialisés.

ÉLÉMENTS D'ALERTE

LES SYMPTOMES : OBSERVÉS SUR PLUSIEURS PERSONNES À LA FOIS, ILS DOIVENT VOUS ALERTER

- Angoisse, agitation
- Chute brutale
- Tremblements, convulsions, crampes
- Suffocation
- Difficulté pour respirer
- Toux
- Larmoiements, sueurs
- Douleur aux yeux
- Ecoulement nasal et/ou salivaire
- Irritation, brûlure de la peau
- Sensation de brûlure, de douleur
- Sensation de poids sur la poitrine
- Sensation de brûlure dans la gorge
- Douleur abdominale
- Nausées, vomissements
- Diminution du diamètre de la pupille

PRINCIPALES ACTIONS À RÉALISER

ALERTER LES SECOURS

- Alertez, ou demandez à votre poste de sécurité d'alerter les services de secours (18, 15 ou 112).
- Donner, si possible, un bilan d'ambiance à votre service de sécurité et décrivez-lui succinctement la situation (contexte et symptômes observés, gravité et ampleur de ces symptômes, nombre et état des victimes).

PROTÉGER / RASSURER LE PUBLIC

- Faites évacuer le public de la zone soumise à un risque et guidez le vers un point de regroupement identifié, si possible aéré.
- Evitez que d'autres personnes non exposées ne viennent dans la zone concernée.
- Demandez aux personnes de limiter les contacts entre elles, de ne pas boire, manger ou fumer.
- Tentez de limiter les phénomènes de panique en rassurant les victimes et les personnes dans l'attente des secours.

PREPARER L'ARRIVÉE DES SECOURS

- Coupez les systèmes de ventilation et de climatisation propres au bâtiment touché afin de limiter la diffusion d'air vicié.
- Encouragez les victimes à rester sur place, au point de regroupement.
- Faites retirer les vêtements (manteau, blouson, pantalon, etc.) présentant des tâches de contamination (liquide/poudre).
- Si vous pensez être contaminé, signalez-vous aux services d'incendie et de secours ou au service d'urgence et réanimation (SMUR).

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Maquette : Pôle graphique, fabrication, image – DSAF/DPGS – Avril 2019.