MINISTÈRES
SOCIAUX
Liberté
Égalité
Fraternité

Secrétariat général

Haut fonctionnaire
de défense et de sécurité

Paris, le 20 décembre 2022

Affaire suivie par : Joséphine Cossart
Courriel : HFDS@sg.social.gouv.fr
Tél. : 01 40 56 51 90
HFDS/2022/68

NOTE

à l'attention de

MESDAMES ET MESSIEURS LES CONSEILLERS DE DEFENSE ET DE SECURITE DE ZONE,
LES DELEGUES DE DEFENSE ET DE SECURITE,
LES OFFICIERS ET RESPONSABLES DE SECURITE.

Objet : Déclinaison de l'adaptation de la posture VIGIPIRATE « *Hiver 2022 – Printemps 2023* » pour les ministères sociaux.

Références :
- Partie publique du plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes n° 102000/SGDSN/PSN/PSE du 1er décembre 2016 ;
- Catalogue des fiches mesures Vigipirate (édition mai 2019) ;
- Instruction N° SG/HFDS/PDS/2018/54 du 31 janvier 2018 relative à la mise en œuvre du plan Vigipirate au sein des périmètres des ministères sociaux.

Annexe : 1. Tableau des mesures de vigilance relatives aux ministères sociaux.

Le niveau de vigilance « sécurité renforcée - risque attentat »
est maintenu sur l'ensemble du territoire national.

Cette nouvelle posture VIGIPIRATE ***« Hiver 2022 – Printemps 2023 »*** est active à compter du 21 décembre 2022.

De façon globale, elle adapte le dispositif en fonction de la période (vacances hivernales, flux touristiques, contexte social sensible) et prend en compte la reprise épidémique de COVID.

Pour la période considérée, l'accent est à porter sur la sécurité :

- des sites touristiques et des transports publics de personnes, en particulier lors des vacances scolaires et universitaires ;
- des espaces de commerce et des lieux de rassemblement, y compris les lieux de culte ;

- des bâtiments publics (services publics, locaux associatifs ou politiques, écoles et universités).

En cas d'attaque ou d'évolution significative de la menace terroriste, cette posture est susceptible de faire l'objet d'une adaptation en urgence ou de compléments (cf. bulletin d'alerte vigipirate du 13/12/2022).

I. Évaluation des menaces

Menace terroriste

La composante endogène de la menace terroriste islamiste demeure la principale menace sur le territoire national. Elle est portée par des individus souvent isolés, se réclamant de l'idéologie jihadiste mais généralement sans lien direct avec les organisations terroristes. Ces individus éprouvent souvent des difficultés d'intégration sociale et sont sensibles aux discours de haine, de violence et de déni des valeurs républicaines (sur fond de rejet des institutions). De ce fait la propagande jihadiste est de nature à mobiliser d'autres profils que ceux de la mouvance islamiste radicale, ce qui complexifie l'identification d'individus basculant soudainement dans la violence.

Les modes opératoires, souvent sommaires (armes blanches, armes par destination de type véhicule-bélier) contribuent au caractère imprévisible et aléatoire de cette menace.

Les cibles de ces attaques peuvent être indiscriminées mais revêtent généralement une certaine charge symbolique (représentant de l'État, lieux de cultes, etc). Les procès de terroristes islamistes ainsi que les journées d'hommages aux victimes du terrorisme se déroulant au cours du premier semestre 2023 peuvent constituer des opportunités d'attaques pour des individus en quête de cibles.

La libération de détenus pour terrorisme islamiste (TIS) au cours des mois à venir constitue également un enjeu de sécurité publique, tout comme le rapatriement de *returnees* depuis la zone irako-syrienne depuis juillet 2022.

En parallèle, l'accroissement des radicalités politiques conduit à une augmentation de la menace terroriste d'extrême droite et d'extrême gauche. La première, dont le taux d'armement est particulièrement élevé, est portée par des réseaux subversifs d'ultra-droite. La seconde, davantage portée sur la voie publique, pourrait profiter des futures réformes sociales et des manifestations qui en découleraient pour commettre des actions violentes.

Menace cyber

Les tendances actuelles des attaques et des vulnérabilités critiques sont marquées par :

- les attaques par rançongiciel largement utilisées par des cybercriminels et souvent couplées par une exfiltration préalable de données. Tous les secteurs publics et privés sont visés par ce type d'attaque ;
- l'exploitation massive des vulnérabilités critiques qui sont un vecteur privilégié d'intrusion initiale sur les réseaux ciblés. Des outils d'automatisation d'exploitation de vulnérabilités, développés par les cybercriminels, permettent de compromettre rapidement un grand nombre d'entités afin de sélectionner celles pouvant représenter un intérêt ;
- les attaques indirectes qui permettent, par exemple, à des attaquants étatiques de s'introduire sur les réseaux d'entités gouvernementales en compromettant les chaînes d'approvisionnement.

II. Adaptation de la posture Vigipirate pour les ministères sociaux (MINSOC)

La posture permanente de sécurité ne subit pas de modification majeure par rapport à celle de juin 2022. Le tableau en annexe récapitule les mesures devant être appliquées (activation de deux nouvelles mesures NUM additionnelles).

- Les ES et ESMS demeurent des cibles vulnérables (lieux ouverts sur l'extérieur) et doivent toujours faire l'objet d'une grande vigilance (poursuivre la mise à jour des différents plans de sécurisation, etc).
- Les opérateurs chargés de la mise en œuvre des politiques de l'emploi peuvent constituer des cibles vulnérables pour des individus en quête de cibles étatiques, dans le contexte des réformes gouvernementales à venir au printemps 2023.

Au regard du niveau actuel de la menace terroriste, une **attention particulière** est attendue sur :
- tous les opérateurs d'importance vitale et leurs prestataires (dans la continuité de la crise sanitaire actuelle) ;
- les ES accueillant des mineurs de retour des zones d'opérations de groupements terroristes dans le cadre du protocole interministériel de prise en charge ;
- les systèmes d'information qui sont des cibles régulières d'attaques du fait de leurs vulnérabilités (risque de cyberattaque majoré par un état de la menace préoccupant).

La menace cyber est actuellement particulièrement forte, néanmoins il est important de garder à l'esprit des ordres de grandeur. Pour 3000 ES publics et privés (avec obligation de déclaration des incidents) les attaques « réussies » par rançongiciel (à des degrés divers mais ayant eu un impact significatif voire total sur le SI de la structure) sont au nombre de moins de 50 incidents de sécurité sur les trois dernières années (sur respectivement 354, 349 et 700 incidents de sécurité déclarés – ce dernier chiffre tenant compte des premiers impacts systémiques liés à des incidents chez des fournisseurs en mode nuage - SAAS).

A ce jour, le système de santé français, bien que porteur de nombreuses vulnérabilités (liées à la numérisation croissante du secteur sanitaire), n'est donc pas spécifiquement ciblé mais victime d'attaques opportunistes en nombre croissant (proportionnellement à son exposition).

Parmi les différents types d'attaques, la croissance du phénomène rançongiciel n'est pas spécifique au secteur de la santé ni à la France, c'est un phénomène mondial et trans-sectoriel.

L'importance en nombre des rançongiciels et leur « industrialisation » ne doit pas masquer les autres types d'attaques (dénis de service, exfiltration de données) ou le fait que les rançongiciels embarquent maintenant fréquemment une charge d'exfiltration de données.

A ce jour il n'y a pas d'impact mesurable lié à la situation internationale toutefois ce risque ne peut être écarté.

Face à la persistance de cette menace, les administrations et opérateurs sont donc invités à maintenir élevée leur vigilance sur leurs systèmes d'information et à consulter régulièrement les alertes et la documentation mises à disposition par l'ANSSI (https://www.ssi.gouv.fr/) et le CERT/Santé (https://esante.gouv.fr/produits-services/cert-sante).

Enfin, ce document interne aux MINSOC a vocation à être diffusé et/ou expliqué uniquement au personnel concerné par la mise en œuvre de cette posture. **Il ne doit, en aucun cas, être diffusé à d'autres acteurs, être affiché à la vue du public ou publié sur un site internet.**

Merci de nous faire remonter vos points d'attention et éventuelles difficultés rencontrées (hfds@sg.social.gouv.fr).

Le haut fonctionnaire adjoint
de défense et de sécurité
Général (2s) Guillaume de Marisy

Annexe 1 : Tableau des mesures de vigilance relatives aux ministères sociaux[1]

Posture Hiver 2022 – Printemps 2023

Domaine	Numéro de mesure	Type de mesure	Intitulé de la mesure	Commentaire
Alerte et mobilisation	ALR 10-01	Socle	Disposer d'une chaîne d'alerte et d'information la plus large possible. La vérifier et la tester régulièrement.	Veiller à mettre à jour régulièrement les bases de contacts.
	ALR 10-04	Socle	Signaler toute transaction, vol ou disparition de matières et de tout indice d'événement NRBC-E.	Une vigilance particulière doit porter sur le signalement de toute transaction, vol ou disparition de matière NRBC-E (précurseurs d'explosifs, acide sulfurique, bouteilles de gaz, etc.). Une fiche de recommandations pratiques, dédiée aux précurseurs d'explosifs est disponible sur le site Internet du SGDSN (http://www.sgdsn.gouv.fr/vigipirate) et rappelle le point de contact national à joindre pour signaler tout événement suspect.

[1] Seules les principales mesures publiques intéressant les secteurs des ministères sociaux sont présentées dans cette annexe. La totalité des mesures est disponible dans le catalogue des fiches mesures VIGIPIRATE (S). De plus, les numéros de mesure surlignés en jaune correspondent à celles nouvellement activées par cette posture Vigipirate.

Alerte et mobilisation	ALR 11-02	Additionnelle	Diffuser l'alerte au grand public.	Afficher le logo du niveau « sécurité renforcée – risque attentat » dans les sites accueillant du public. Ces logos doivent être visibles à l'entrée et dans les espaces d'attente des sites et peuvent être complétés d'une fiche synthétique récapitulant les conditions particulières de sécurité au sein de la structure. 
	ALR 11-04	Additionnelle	Rappeler les conduites à tenir en cas d'attaque (fusillade, attaque NRBC, colis abandonné, alerte à la bombe).	Des fiches de recommandations et de bonnes pratiques sont disponibles sur le site du SGDSN : http://www.sgdsn.gouv.fr/plan-vigipirate/
	ALR 20-01	Socle	Élaborer et mettre à jour un plan de continuité d'activité.	Il convient d'actualiser régulièrement les annuaires de crise, de sensibiliser les agents aux procédures d'alerte et d'organiser des exercices simples.
Rassemblement et zones ouvertes au public	RSB 11-01 RSB 12-01 RSB 13-01	Additionnelle	Renforcer la surveillance et le contrôle.	
	RSB 12-05	Additionnelle	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier).	Au regard de la menace associée aux attaques par véhicules-béliers, les opérateurs sont encouragés à renforcer les dispositifs de protection passive (plots, barrières, blocs en béton, etc.) sur les accès les plus fréquentés.
	RSB 20-02	Socle	Procéder à des contrôles d'identité, visite de véhicules, inspection et fouille de bagages dans les lieux identifiés (mesure de droit commun).	

	RSB 20-03	Socle	Réglementer l'accès et la circulation des personnes dans le périmètre de protection fixé par un arrêté préfectoral.	Cette mesure s'applique sur le fondement de l'article L.226-1 du code de la sécurité intérieure. La communication ne doit pas faire connaître le détail, le ciblage, les moyens engagés dans la mise en œuvre de cette mesure.
Installations et bâtiments	BAT 10-01	Socle	Réglementer le stationnement et/ou la circulation aux abords des installations et bâtiments.	
	BAT 10-02	Socle	Surveiller les abords des installations et bâtiments.	Des échanges permanents doivent se tenir entre les responsables de sites et les forces de sécurité intérieure.
	BAT 10-03	Socle	Contrôler les abords des installations et bâtiments.	
	BAT 11-02 BAT 12-02 BAT 13-02	Additionnelle	Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés.	Vigilance permanente dans les domaines de la sécurisation des espaces de rassemblement (périphérie, périmétrie, intérieur).
	BAT 11-03 BAT 12-03	Additionnelle	Renforcer la surveillance aux abords des installations et bâtiments désignés.	
	BAT 12-05	Additionnelle	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier).	Se référer aux fiches de recommandations et de bonnes pratiques diffusées par le SGDSN : http://www.sgdsn.gouv.fr/plan-vigipirate/les-fiches-de-recommandations-et-de-bonnes-pratiques/
	BAT 20-01	Socle	Surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier).	Maintien du renforcement de la vigilance aux abords et des contrôles aux accès des établissements. Les mesures de contrôle peuvent notamment consister en des dispositifs de filtrage et d'inspection visuelle des sacs.
	BAT 21-01 BAT 22-01 BAT 23-01	Additionnelle	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier).	
	BAT 30-01	Socle	Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès.	La sûreté est définie en fonction de l'évaluation des risques et des menaces auxquels est soumis l'établissement.
	BAT 30-02	Socle	Surveiller la circulation interne des bâtiments et installations.	
	BAT 31-01	Additionnelle	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone).	

Installations et matières dangereuses	IMD 10-01	Socle	Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités.	Signaler tous vols, disparitions ou transactions suspectes de précurseurs d'explosifs et agents NRBC au point de contact national : pôle judiciaire de la gendarmerie nationale (pixaf@gendarmerie.interieur.gouv.fr) et au service spécialisé du HFDS (hfds@sg.social.gouv.fr).
	IMD 10-02	Socle	Établir et mettre à jour les plans particuliers de protection (PPP), les plans d'opération internes (POI), les plans d'urgence internes (PUI), les plans particuliers d'interventions (PPI), les plans de protection externes (PPE) et les plans de sûreté relatifs aux transports de marchandises dangereuses à haut risque.	S'appuyer sur la documentation communiquée par le SGDSN (exemple du PPP : http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf)
	IMD 10-03	Socle	Organiser régulièrement des exercices de test des dispositifs et de vérification de la disponibilité effective des moyens d'intervention.	
	IMD 10-07	Socle	Protéger les points névralgiques des sites désignés des véhicules béliers.	Le « guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique » publié par le ministère de l'Intérieur peut servir d'appui. Il est téléchargeable, en accès libre, au lien suivant : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique
Sécurité du numérique	NUM 11-02	Additionnelle	Rechercher sur le SI des marqueurs particuliers correspondant à une attaque	Il est recommandé de prendre régulièrement connaissances des marqueurs de vulnérabilités via le site de l'ANSSI, le CERT santé et les éditeurs et de rechercher ces indicateurs de compromission sur ses systèmes.
	NUM 21-02	Additionnelle	Consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-FR)	Accessible aux liens suivants : https://www.cert.ssi.gouv.fr/ https://www.cyberveille-sante.gouv.fr/
	NUM 31-03	Additionnelle	Absorber le trafic illégitime au niveau du réseau.	Exercer une vigilance constante sur les systèmes d'information, notamment en regard des moyens de connexion à distance.

Sécurité du numérique	NUM 31-06	Additionnelle	Sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter.	Effectuer des rappels réguliers sur les risques liés aux « messages piégés » (phishing), qui constituent le premier vecteur d'infestation virale, notamment de « rançongiciels ».
	NUM 31-09	Additionnelle	Rappeler l'importance d'une mesure d'hygiène ou sectorielle existante.	Pour sécuriser les accès à distance des systèmes d'information en cas de télétravail, il est recommandé de recourir à une authentification multi facteurs (https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/), afin d'éviter une authentification depuis un poste attaqué, volé ou perdu et s'assurer du caractère sécurisé de la connexion réseau à travers Internet lorsqu'un utilisateur a besoin de se connecter au système d'information de l'entité à distance. Au regard des menaces d'attaque par hameçonnage, il importe de sensibiliser les utilisateurs à être particulièrement attentifs aux courriels qu'ils reçoivent, les inciter à ne pas activer les macros dans les pièces jointes et mettre en place des mesures pour limiter l'exécution des macros. La fiche « hameçonnage » du SGDSN est une ressource utile : http://www.sgdsn.gouv.fr/vigipirate/securite-du-numerique-lhameconnage-ou-phishing/
	NUM 41-01	Additionnelle	Valider et appliquer un correctif de sécurité.	Face aux vulnérabilités critiques et à l'état de la menace, il est impératif d'appliquer, dans les plus brefs délais, les correctifs de sécurité mentionnés dans les bulletins d'alerte de sécurité du CERT-FR. Les correctifs référencés dans les alertes doivent, si cela est nécessaire et pour des raisons d'urgence et de criticité, être appliqués en dehors des processus de maintien en condition de sécurité des systèmes d'information. De même, les correctifs mentionnés dans les avis de sécurité et qui correspondent à la veille sur plus d'une centaine de produits, doivent également être appliqués dans le cycle habituel de maintien en condition de sécurité des systèmes
	NUM 41-02	Additionnelle	Vérifier la correction effective d'une vulnérabilité.	

				d'information. L'exploitation de certaines des vulnérabilités référencées permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La bonne application des correctifs de sécurité référencés doit être régulièrement contrôlée et validée. Les bulletins d'alerte de sécurité et les avis de sécurité sont disponibles sur le site www.cert.ssi.gouv.fr.
Sécurité du numérique	NUM 51-01	Additionnelle	Vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés	S'assurer que la capacité de communication entre le personnel en charge de réponse à la crise sera maintenue : vérifier les annuaires de crise et s'assurer qu'ils sont correctement diffusés. Il est également nécessaire de tester régulièrement les moyens de communication alternatifs et sécurisés qui pourront être utilisés dans le cas d'une attaque impactant les outils de communication nominaux.
	NUM 51-02 NUM 52-02	Additionnelle	Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace.	Compte tenu des menaces cyber persistantes, il est essentiel de s'assurer que les outils et dispositifs de réponse à incident sont opérationnels et adaptés à la menace numérique et que le personnel chargé de le mettre en œuvre soit familiarisé avec celui-ci. Le guide de l'ANSSI sur la thématique de la gestion de crise cyber aide les organisations à organiser leur dispositif : https://www.ssi.gouv.fr/uploads/2021/12/anssi-guide-gestion_crise_cyber.pdf Il est également important que la baisse des effectifs liés aux congés estivaux n'impacte pas l'organisation de ce dispositif. Il est par ailleurs recommandé d'effectuer un exercice d'activation du PCA ou de gestion de crise cyber si le dernier exercice a été effectué il y a plus d'un an.
	NUM 51-05	Additionnelle	Réaliser des tests de restauration des sauvegardes	Il convient d'organiser régulièrement des tests de restauration des sauvegardes réalisées sur les systèmes d'information. Ces tests (effectués sur les sauvegardes en ligne et hors-ligne) sont un moyen de vérifier la présence

				des sauvegardes, leur qualité et l'aptitude à restaurer un système d'information à partir de ces dernières. Pour plus de renseignements sur ce sujet, consulter le guide « d'hygiène numérique » de l'ANSSI : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
	NUM 51-06	Additionnelle	Procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques	En cas d'attaque par rançongiciel, de destruction ou d'altération des données, il est important de pouvoir restaurer le bon fonctionnement des systèmes les plus critiques en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration. Le guide de l'ANSSI « Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ? » aide les entités à réduire le risque d'attaque et réagir lorsque celle-ci réussie : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide attaques_par_rancongiciels_tous_concernes-v1.0.pdf/
Secteur Santé	SAN 10-01	Socle	Assurer une veille sanitaire permanente visant à détecter l'utilisation d'un agent NRBC contre la population et une capacité analytique permanente permettant d'identifier un agent NRBC dans le domaine sanitaire.	
	SAN 20-01	Socle	Assurer une capacité permanente de prise en charge de victimes d'actes de terrorisme (blessés ou malades).	Les agences régionales de santé (ARS) veillent, d'une part, à bien articuler le schéma ORSAN AMAVI avec le plan ORSEC des préfectures et, d'autre part, à organiser le dispositif sanitaire des grands événements à sensibilité particulière selon les orientations des préfets.
	SAN 30-01	Socle	Assurer le fonctionnement nominal des chaînes de production des produits de santé et l'approvisionnement en matières premières pharmaceutiques au niveau des opérateurs du secteur des produits de santé.	

	SAN 30-02	Socle	S'assurer de la permanence des capacités de distribution des produits de santé, équipements et matériels sanitaires.	
	SAN 40-01	Socle	Assurer une sécurisation permanente des établissements de santé et médicaux-sociaux.	Les directeurs des établissements de santé doivent poursuivent les efforts de sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurité d'établissement (PSE) et la mise en œuvre d'actions de formations à l'intention de l'ensemble de leurs personnels.
Réseaux d'eau	EAU 20-01	Socle	Connaître l'autonomie de fonctionnement et s'assurer de la disponibilité de stocks suffisants de réactifs.	
	EAU 20-02	Socle	Établir et mettre à jour l'évaluation des besoins en eau en fonction des usages et des besoins prioritaires de la population.	
	EAU 20-03	Socle	Recenser et informer les populations sensibles.	
Réseaux d'eau	EAU 20-04	Socle	Établir, mettre à jour et tester les possibilités de secours, de substitution et d'interconnexion.	
	EAU 20-05	Socle	Organiser le dispositif de veille, d'alerte, d'astreinte, de permanence et de gestion de crise et maintenir le réseau de contacts avec les autorités.	
	EAU 20-06	Socle	Établir, mettre à jour et tester périodiquement les plans d'opération internes (POI), plans particulier d'intervention (PPI), plans particulier de protection (PPP) et plans de protection externes (PPE), garantir les capacités d'intervention.	
	EAU 20-07	Socle	Etre en mesure de mettre en œuvre les consignes de sur-chloration dans les délais impartis.	

	EAU 20-08	Socle	Définir le programme d'analyses périodiques de l'eau.	
	EAU 20-09	Socle	À chaque livraison, contrôler systématiquement la conformité des réactifs nécessaires au traitement de l'eau.	
	EAU 20-10	Socle	Surveiller les points les plus vulnérables du réseau d'alimentation en eau.	
	EAU 20-11	Socle	Effectuer les études de vulnérabilité et des auto-diagnostics.	
	EAU 20-12	Socle	Porter à la connaissance des autorités tout incident pouvant avoir des conséquences sur la santé publique.	
	EAU 20-13	Socle	Mettre en place une astreinte ou une permanence dans les laboratoires des exploitants et les laboratoires agréés en charge du contrôle sanitaire des eaux.	
L'étranger	EXT 10-05	Socle	S'inscrire sur Ariane (voyageurs).	Ces mesures de précaution permettent de : - recueillir les numéros utiles, prendre connaissance des consignes de sécurité et les conserver pendant toute la durée d'un séjour à l'étranger ; - recevoir des recommandations de sécurité par courriels si la situation le justifie ; - être contacté en cas de crise dans le pays de destination ; - prévenir, en cas de besoin, la personne contact désignée sur Ariane.
	EXT 10-06	Socle	Consulter le site « conseils aux voyageurs » (voyageurs).	