LIE
La lettre d'information économique
DANS LA LIGNE DE MIRE

54e Salon International de l'Aéronautique & de l'Espace (SIAE)

Sommaire

Éditorial

Mesdames, Messieurs,

La 54ème édition du Salon International de l'Aéronautique et de l'Espace (SIAE) se déroulera du 19 au 25 juin 2023 au parc des expositions du Bourget (93).

Pour vos entreprises, ce rendez-vous de renommée mondiale constitue un cadre privilégié en matière de promotion, d'échanges et d'opportunités commerciales.

Il s'inscrit également dans un contexte particulier marqué, entre autres, par la persistance des dialectiques de puissance et des enjeux de souveraineté associés, la crise ukrainienne et ses effets, les réflexions en cours sur un modèle national d'« économie de guerre » et les orientations stratégiques, capacitaires et financières de la nouvelle loi de programmation militaire.

Concentrant de multiples acteurs publics et privés dans un cadre espace-temps particulier, ce type d'évènement favorise également les tentatives d'ingérences diversifiées, tant dans leurs formes que dans leurs origines.
Celles-ci peuvent porter directement atteinte à vos intérêts économiques, commerciaux, technologiques, réputationnels ainsi qu'à ceux de vos partenaires.

Afin de concourir à la maîtrise de ces risques, la Direction du Renseignement de la Sécurité de la Défense (DRSD) vous propose dans cette lettre d'information les principales recommandations pouvant être mises en œuvre en matière de protection des personnes et des biens matériels et immatériels.
Nous vous invitons à les diffuser largement à vos collaborateurs, notamment à ceux qui participeront au salon.

En sa qualité de service de renseignement de contre-ingérence du ministère des Armées, la DRSD sera une nouvelle fois présente à vos côtés durant cette édition du SIAE.
Que ce soit avant, pendant ou après l'évènement, n'hésitez donc pas à solliciter les conseils de ses agents et à leur signaler tout fait nécessitant d'être porté à leur connaissance.

Je vous souhaite, par avance, un excellent salon.

Général de corps d'armée Philippe Susnjara
Directeur du Renseignement et de la Sécurité de la Défense

Recommandations à l'usage des exposants

AVANT LE SALON

ÉTUDIER, ÉVALUER ET ANTICIPER LA MENACE EN PRÉPARANT VOTRE PARTICIPATION EN AMONT

- [ ] Préparer minutieusement le salon avec l'ensemble des participants (internes et externes) de façon à créer une équipe soudée et cohérente.

Pour tous les participants

- [ ] Informer sa chaîne de sécurité / sûreté de sa participation ;
- [ ] Prendre en compte les retours d'expérience des précédents salons ;
- [ ] Répartir et communiquer les missions, les jours de présence et les contacts des acteurs (collaborateurs de l'entreprise, stagiaires, prestataires externes, etc.) ;
- [ ] Faire un inventaire des fournitures et matériels déployés ;
- [ ] Identifier les stands voisins, les concurrents, les sous-traitants, les délégations officielles et leurs accompagnateurs susceptibles de venir visiter le stand ;
- [ ] Disposer le matériel en fonction des angles de prise de vue ;
- [ ] Maîtriser la communication sur les réseaux sociaux autour de sa participation personnelle au salon.

Pour les équipes sûreté-sécurité

- [ ] Analyser votre implantation (orientation, ouvertures, accueil, filtrage, issue de secours) ;
- [ ] Identifier le personnel des sociétés prestataires (gardien, chauffeur, livreur, monteur du stand, etc.) ;
- [ ] Être présent lors du montage du stand et de l'installation du matériel ;
- [ ] Mettre en place un dispositif de sécurité en tout temps et prévoir son aménagement en dehors des heures d'ouverture ;
- [ ] Sensibiliser et responsabiliser les personnes présentes sur le stand (communication, commerciaux, stagiaires, etc.) sur les risques encourus ;
- [ ] Communiquer le point de contact en cas d'incident.

Pour les équipes du marketing et de la communication

- [ ] Exposer uniquement des maquettes simples et brevetées ;
- [ ] Prévoir un espace de confidentialité (si nécessaire) ;
- [ ] Préparer un argumentaire spécifique (kit de presse, carte de visite), notamment sur les sujets sensibles (innovations, business plan, etc.) ;
- [ ] Maîtriser la communication autour de la participation de sa structure, en amont et pendant le salon, sur son site et sur les réseaux sociaux ;
- [ ] Prendre connaissance de la veille média et des éventuelles atteintes (image, réputation).

Recommandations à l'usage des exposants

Sécurité numérique

- ☐ Inventorier le matériel informatique (ordinateurs, supports amovibles, téléphones) ;
- ☐ Mettre à jour les équipements informatiques ;
- ☐ Sauvegarder tous les documents sensibles nécessaires à l'activité salon sur un support amovible, et le laisser dans un coffre prévu à cet effet ;
- ☐ Protéger vos ordinateurs et tout objet connecté par un antivirus, un pare-feu et des mots de passe robustes et uniques ;
- ☐ Configurer un VPN (Virtual Private Network) en fonction des usages et l'activer systématiquement en cas de connexion à un réseau tiers ;
- ☐ Prévoir des filtres de confidentialité pour les écrans ;
- ☐ Emporter uniquement les données nécessaires à la mission.

Hors-salon : redoubler de vigilance

Les déplacements (aéroport, gare, transports en commun, navettes, parkings) en direction de et depuis le salon ainsi que **les espaces publics** (restaurant, coworking, conférence, etc.) sont propices à la captation d'informations et aux tentatives d'approche :

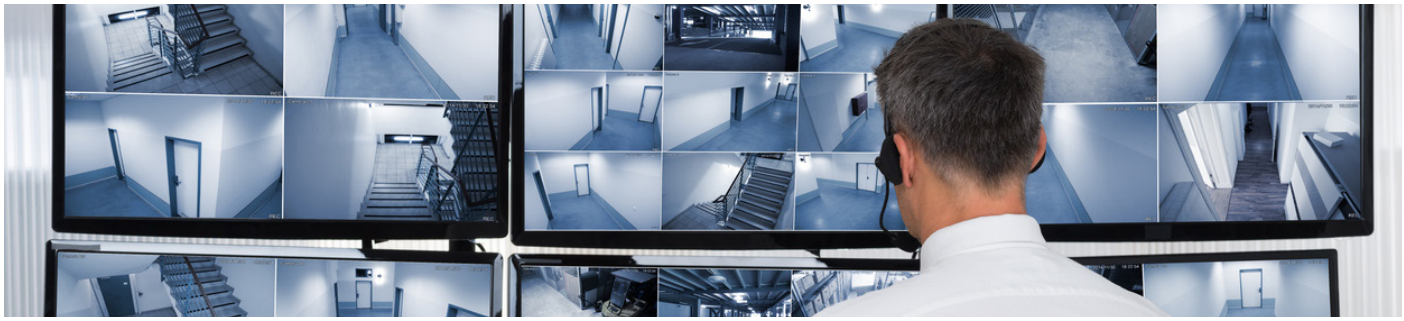
- ☐ Attention à la visibilité de votre badge ;
- ☐ Rester discret dans vos discussions ;
- ☐ Rester vigilant quant aux informations sensibles transportées (documents, ordinateur, etc.).

Si vous louez un véhicule :

- ☐ Si une connexion est nécessaire : effacer les données après utilisation.

Les évènements et les périodes entourant le salon (hôtels, à l'intérieur des halls du salon) :

- ☐ Apporter une vigilance particulière aux sollicitations « fortuites » (invitations à des repas, des « after-salon » planifiés et « non planifiés ») ;
- ☐ Rester méfiant vis-à-vis des cadeaux (ex. risque de corruption ou piégeage via les goodies) ;
- ☐ Ne jamais laisser vos outils de travail (document, ordinateur portable, etc.) sans surveillance, y compris dans les coffres de votre chambre d'hôtel ou lors des stationnements ;
- ☐ Privilégier les réseaux mobiles de votre opérateur 4G/5G.



Recommandations à l'usage des exposants

DURANT LE SALON

MAINTENIR UNE VIGILANCE CONSTANTE

Pour tous les participants

- ☐ Maintenir une personne sur le stand pendant les pauses (déjeuner, etc.) ;
- ☐ Faire preuve de prudence et de diligence quant aux éléments techniques échangés à la voix ou de manière numérique ;
- ☐ Conserver toute information sensible sur soi ou dans une armoire forte ;
- ☐ Éviter autant que possible la consultation de documents sensibles depuis des lieux publics ;
- ☐ Interdire clairement la prise de vues ou de captation audio, des prototypes et collaborateurs ;
- ☐ Vérifier systématiquement l'identité des visiteurs : demander une carte de visite (inscrire le jour, l'heure, le contact ainsi que toute information jugée utile) ;
- ☐ Surveiller et emporter le soir vos matériels et supports contenant des informations sensibles pour éviter les vols et les dégradations.

Pour les équipes sûreté-sécurité

- ☐ Surveiller les comportements des personnes (notamment des délégations étrangères, ainsi que de leur accompagnant - traducteur) ;
- ☐ Matin et soir : « briefer / débriefer » les participants sur la protection de l'information, les événements à venir et constatés ;
- ☐ Noter les anomalies rencontrées pendant la journée sur un « carnet de bord » ;
- ☐ Faire remonter toute information ou doute à la DRSD sous forme de compte-rendu détaillé (Qui, Quoi, Où, Quand, Comment, Pourquoi).

Sécurité numérique

- ☐ Sécuriser les postes informatiques dédiés au salon (câble antivol) ;
- ☐ Contrôler vos supports amovibles en station blanche ;
- ☐ Rester vigilant en cas d'échanges via des applications (ex. Skype) ;
- ☐ Échanger uniquement avec un mail professionnel ;
- ☐ Désactiver les fonctionnalités non nécessaires sur vos objets connectés et smartphones (ex. la géolocalisation).

En cas de sollicitation pour une entrevue - un sondage ou des enquêtes multiples

- ☐ Éviter de donner des interviews d'initiative ;
- ☐ Utiliser une adresse email éphémère (durée de vie limitée) ;
- ☐ Transmettre uniquement les données nécessaires.

LORS DE LA CLÔTURE ET APRÈS LE SALON

En fin de salon, fatigue et routine aidant, le niveau de sécurité baisse et les actions de captation élémentaire sont fréquentes et s'appuient souvent sur des repérages réalisés en amont.

- ☐ Rester présent lors du démontage du stand ;
- ☐ Vérifier l'intégrité des dispositifs de protection avant la remise en mode transport ;
- ☐ Vérifier l'ensemble des matériels et documentations (exhaustivité et conformité de l'état de colisage, des inventaires).

Après le salon :

- ☐ Effectuer, dès le retour dans vos locaux, un inventaire exhaustif des matériels et documents.

- **Rapport d'étonnement :**

- ☐ Rédiger un rapport d'étonnement avec les participants (points positifs, problèmes rencontrés, axes d'amélioration) en séparant le point « sécurité et sûreté » du point « commercial et attendus ».

L'analyse de ces informations permettra à votre hiérarchie et votre chaîne de sécurité et sûreté de comprendre les incidents, en identifiant notamment les éventuels risques et signaux faibles, ainsi que d'avoir un retour d'expérience pour préparer les prochains salons.

- **Sécurité numérique :**

- ☐ Faire vérifier tous les supports numériques par le responsable SSI ;
- ☐ Contrôler l'intégrité des moyens informatiques ayant servi sur le salon ;
- ☐ Effectuer une analyse antivirale avant de blanchir le matériel.

SI VOUS CONSTATEZ

- Comportements étranges et / ou suspects ;
- Questionnements intrusifs (notamment lors des évènements hors salon) ;
- Prises de photographies précises et / ou intempestives ;
- Vol (matériels, documentations, etc.) ou intrusion d'un support numérique (ex. clé USB) :

notez le maximum d'informations et de précisions sur le/les individus et leurs agissements afin de les communiquer à votre chaîne sécurité, aux organisateurs et à votre référent DRSD !

CAS CONCRETS d'ingérences constatées à l'occasion de salons d'armements

Communication en amont du salon mal maîtrisée

Faits : Un directeur commercial, utilisateur régulier des réseaux sociaux, notamment professionnels, communique, sous son nom propre, sur ses responsabilités managériales en lien avec un programme d'armement. En juin, il annonce sa participation à un salon international afin de signer un contrat « majeur ». En parallèle, son fils (même patronyme) organise un évènement festif sur Facebook dans un groupe non privé. En effet, son père partant pour un déplacement professionnel, il organise une soirée. À cette fin, il transmet les codes d'accès de l'immeuble. À son retour, le père constate que son ordinateur a « disparu » et que son bureau a été fouillé.

Analyse : S'il s'agit de rester prudent quant au caractère ciblé ou opportuniste de ce vol, force est de constater que les communications, volontaires et non maîtrisées, ont peut-être facilité ce vol sans effraction apparente.

Impact : Les conséquences pour l'entreprise sont difficiles à évaluer précisément, le directeur commercial n'étant pas en capacité d'inventorier tous les fichiers ayant pu être compromis.

Tentative de captation de données sur un ordinateur d'exposant

Contexte : Deux individus de nationalité étrangère se sont présentés sur un stand d'une entreprise du domaine de l'aviation. Sensibilisé en amont du salon, le commercial a répondu de façon élémentaire aux questions posées puis a demandé aux interlocuteurs leurs identités. Durant la conversation, le commercial a constaté que l'un des visiteurs essayait de connecter une clé USB à l'ordinateur de présentation. S'étant interposé, les deux individus, qui s'exprimaient jusqu'alors dans un anglais approximatif, se sont mis à converser entre eux dans leur langue natale et ont quitté le stand.

Analyse : L'ordinateur approché est utilisé à des fins de démonstration et aucune action n'est possible dessus (ports USB bloqués, mots de passe robuste changés à chaque déplacement). L'ordinateur ne représente aucune vulnérabilité et le risque pour la défense a donc été écarté.

Mesures : Le commercial ayant remonté l'information à sa chaîne de sécurité/sûreté, cette dernière a rendu compte de façon détaillée aux agents de la DRSD sur place. La DRSD a alors pu investiguer sur les individus et sensibiliser les autres exposants français pouvant être ciblés.

N'hésitez pas à contacter votre chaîne de sûreté/sécurité au sein de votre structure et votre agent DRSD référent afin de faire remonter toute ingérence ou atteinte (physique, économique, juridique, cybernétique, etc.) dont vous penseriez être victimes.

Soyez assurés que la DRSD et chacun des agents présents se tiennent à vos côtés.

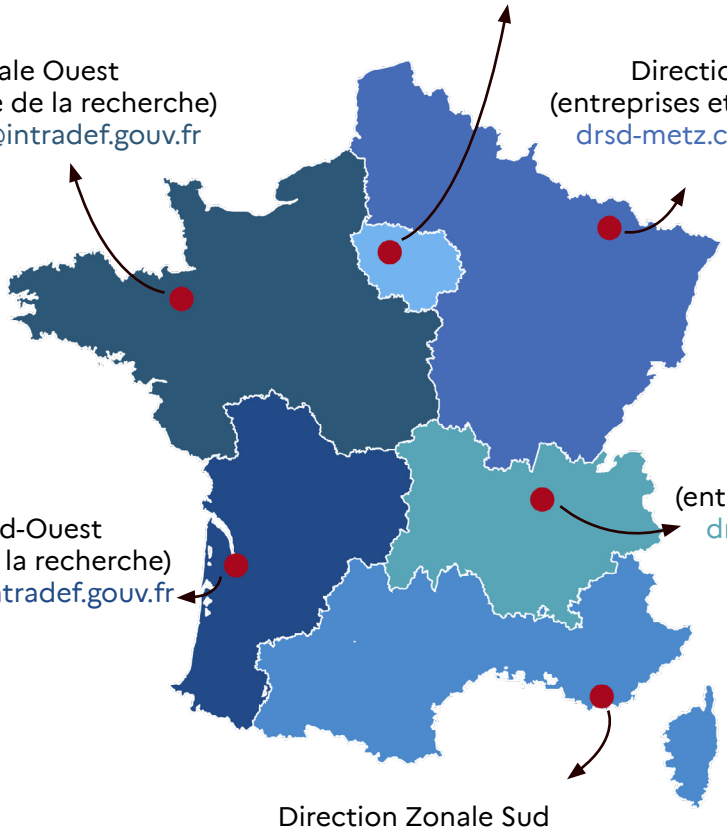
Gardons le contact

Direction Centrale
Section « Sensibilisation »
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Directions Zonales Ile-de-France
Entreprises : drsd-dsezp-4.cds.fct@intradef.gouv.fr
Instituts et écoles de recherche : drsd-idf.cmi.fct@intradef.gouv.fr

Direction Zonale Ouest
(entreprises et monde de la recherche)
drsd-rennes.cmi.fct@intradef.gouv.fr

Direction Zonale Nord-Est
(entreprises et monde de la recherche)
drsd-metz.cmi.fct@intradef.gouv.fr



Direction Zonale Sud-Est
(entreprises et monde de la recherche)
drsd-lyon.cmi.fct@intradef.gouv.fr

Direction Zonale Sud-Ouest
(entreprises et monde de la recherche)
drsd-bordeaux.cmi.fct@intradef.gouv.fr

Direction Zonale Sud
(entreprises et monde de la recherche)
drsd-toulon.cmi.fct@intradef.gouv.fr