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

EUROSATORY 2024

Sommaire

Éditorial du Directeur du Renseignement et de la Sécurité de la Défense

Mesdames, Messieurs,

La prochaine édition du salon EUROSATORY se tiendra du 17 au 21 juin 2024 au parc des expositions de Villepinte, 55 ans après sa création. Événement de référence pour les industries de défense et de sécurité du combat aéroterrestre, ce rendez-vous constitue un cadre privilégié en matière de promotion industrielle et d'opportunités commerciales.

Cette édition s'inscrit toutefois dans un environnement international marqué par le conflit russo-ukrainien et une dynamique d'« économie de guerre » qui vise une plus grande résilience des capacités de production nationales de notre base industrielle et technologique de défense.

Celle-ci fait face à des convoitises croissantes de la part de nos principaux compétiteurs stratégiques, lesquelles se traduisent par des tentatives d'ingérences multiples et variées, tant par leurs modes opératoires que par les vecteurs utilisés. Ces atteintes peuvent directement porter préjudice à vos intérêts économiques, commerciaux, technologiques ainsi qu'à ceux de vos partenaires industriels. Ce faisant, elles engendrent des effets sur les capacités de nos armées à conduire leurs missions sur les théâtres d'opérations.

Face à ces menaces, la Direction du Renseignement et de la Sécurité de la Défense, pleinement investie dans sa mission de contre-ingérence économique au profit de la sphère défense, se tiendra une nouvelle fois à vos côtés pour vous accompagner lors de cet événement. À travers cette lettre d'information économique, nous souhaitons partager avec vous nos recommandations ainsi que des cas concrets d'ingérences pouvant se matérialiser pendant toute la durée du salon.

Avant, pendant et après l'évènement, nos agents se tiennent à votre disposition pour vous éclairer sur les risques d'ingérences liés aux salons, échanger avec vos équipes, traiter ensemble tout signalement que vous porteriez à leur connaissance. Pour faciliter leur travail et la remontée d'informations, nous vous invitons à diffuser largement ce support à l'ensemble de vos collaborateurs, particulièrement à ceux qui seront présents au sein des stands.

Je vous souhaite à tous une excellente édition du salon EUROSATORY 2024.

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

Maîtriser les risques

PRINCIPAUX RISQUES

- Espionnage
- Terrorisme / sabotage / subversion
- Cyber (ex : *rançongiciel*)
- Atteinte réputationnelle
- Vols de données ou de matériels

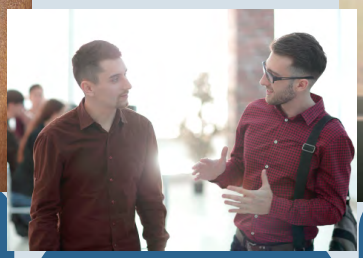
PRINCIPAUX IMPACTS

- Perte de marchés et d'avantages concurrentiels
- Perte de confiance des clients et des fournisseurs
- Perte d'avances technologiques et de capacités d'innovation
- Atteinte au patrimoine scientifique et technologique

PRINCIPAUX MODES OPÉRATOIRES CONSTATÉS

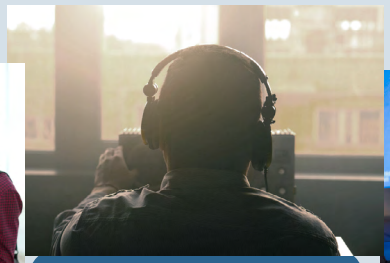
Vols

- De matériels
- De supports informatiques
- De badges d'exposant



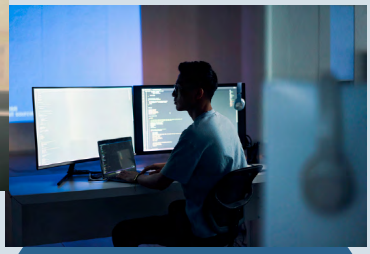
Approche humaine

- Ancien élève
- Ancien collaborateur
- Faux journaliste
- Faux stagiaire/ étudiant



Tentatives d'implantation

- De dispositifs d'écoute
- De prise de vue
- D'interception/d'intrusion



Cyber

- Usurpation de point d'accès réseaux
- Détournement du wifi
- Attaque par supports amovibles

2 QUESTIONS PRINCIPALES À SE POSER

→ **Quels sont les risques pesant sur mon dispositif déployé lors de ce salon ?**
ex. captation de savoir-faire, sabotage, tentative de débauchage d'un expert, etc.

→ **Comment puis-je réduire ces risques pour les rendre acceptables ?**
ex. sensibiliser mes collaborateurs, rester vigilant lors des visites de délégations étrangères, etc.

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 constituer une équipe soudée et cohérente.

Pour tous les participants

- [ ] Informer sa chaîne de sécurité / sûreté de la participation de la société ;
- [ ] 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.), afin d'éviter les intervalles et déficits de couverture ;
- [ ] Faire un inventaire des fournitures et matériels déployés et en contrôler quotidiennement l'intégrité ;
- [ ] Identifier les stands voisins, les concurrents, les sous-traitants, les délégations officielles et leurs accompagnateurs susceptibles de venir visiter le stand ;
- [ ] Disposer le matériel de façon à éviter toute prise de vue qui permettrait de capter des mots de passe et informations sensibles (ex : tourner tous les ordinateurs de manière à empêcher la visibilité de l'écran et du clavier).

Pour les équipes sûreté-sécurité

- [ ] Analyser son 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 constant 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 existants ;
- [ ] Communiquer les coordonnées du point de contact à prévenir 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 via les plateformes sécurisées ;
- ☐ Sauvegarder tous les documents sensibles nécessaires à l'activité salon sur un support amovible et le stocker dans un coffre prévu à cet effet ;
- ☐ Protéger les ordinateurs et tout objet connecté par un antivirus, un pare-feu et des mots de passe robustes, uniques et de circonstance (pour l'événement) ;
- ☐ Configurer un VPN (*Virtual Private Network*) en fonction des usages et l'activer systématiquement en cas de connexion à un réseau tiers ;
- ☐ Prévoir, si possible, des filtres de confidentialité pour les écrans et téléphones portables ;
- ☐ Emporter uniquement les données nécessaires à la mission. Présenter uniquement les projets brevetés.

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 :

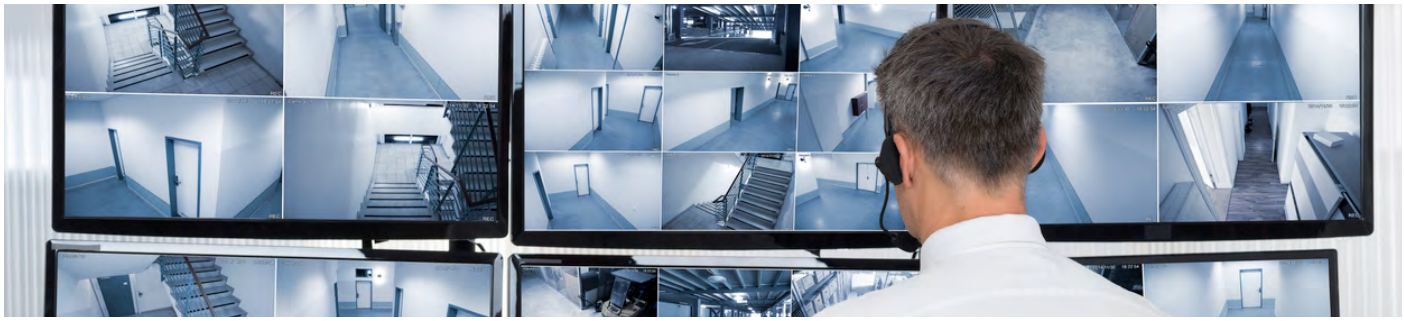
- ☐ Attention à la visibilité de son badge ;
- ☐ Rester discret dans ses discussions ;
- ☐ Rester vigilant quant aux informations sensibles transportées (documents, ordinateur, etc.).

En cas de location d'un véhicule :

- ☐ Si une connexion (Bluetooth ou autre) est nécessaire : effacer les données du tableau de bord avant de rendre le véhicule de location.

Les événements et la vie courante 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 ses outils de travail (documents, ordinateur portable, etc.) sans surveillance, y compris dans les coffres des chambres d'hôtel ou lors des stationnements (lieux cibles les plus évidents) ;
- ☐ Privilégier aux wi-fi localisés (hôtel ou restaurant) les réseaux mobiles de son opérateur 4G/5G.



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 quant aux détails techniques échangés à la voix ou de manière numérique ;
- ☐ Conserver toute information sensible sur soi ou dans une armoire forte dédiée le cas échéant (hors hôtel) ;
- ☐ 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 des 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, hors créneaux d'ouverture du salon, les 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).

Sécurité numérique

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

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

- ☐ Éviter de donner des entrevues d'initiative, non préparées ;
- ☐ Utiliser une adresse mail éphémère (durée de vie limitée) ;
- ☐ Transmettre uniquement les informations nécessaires.

LORS DE LA CLÔTURE ET APRÈS LE SALON

En fin de salon, au moment du démontage, fatigue et routine aidant, le niveau de sécurité baisse et les actions de captation élémentaire sont alors plus fréquentes, s'appuyant 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 les locaux de la société, 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 !

CONTACT DRSD SUR LE SALON : 01 46 73 56 65 / 06 33 71 01 07

CAS CONCRETS d'ingérences constatées lors du dernier salon EUROSATORY 2022

Questions intrusives

Contexte : une jeune femme d'une vingtaine d'années, ressortissante d'un pays d'Asie du Sud-Est, s'est présentée en tant qu'étudiante auprès de l'un des commerciaux d'une entreprise de la BITD qui développait une technologie innovante dans le domaine de l'optronique. Prétextant rédiger un mémoire de recherche, elle a longuement échangé avec cet agent commercial, alternant questions techniques et personnelles.

Semblant satisfaite des réponses obtenues à ses questions, la jeune femme a fini par quitter le stand avant de revenir quelques minutes plus tard pour converser avec le même collaborateur. Elle a profité de cette nouvelle occasion pour lui demander des noms de contacts, ingénieurs ou responsables travaillant sur des programmes sensibles en cours afin de s'entretenir avec eux, toujours dans le cadre de la rédaction de son travail de recherche. Lors de ce second entretien, ses questions se sont avérées plus précises sur le matériel exposé. Interloqué, le commercial de l'entreprise a décidé de couper court à leur conversation et de rédiger un rapport d'étonnement à sa chaîne sécurité.

Conséquences : à la suite des investigations conduites par la DRSD, il s'est avéré que la jeune femme avait échangé en toute discrétion avec un individu défavorablement connu du Service entre ses deux conversations sur le stand de l'entreprise française.
Le commercial, qui a répondu par deux fois aux questions de la jeune femme, a reconnu avoir manqué de vigilance face à l'attitude entreprenante de son interlocutrice pour obtenir des informations.
L'équipe de la DRSD présente sur le salon a sensibilisé les collaborateurs de l'entreprise aux risques de rattrapage technologique que pouvaient représenter les réponses à ces questions intrusives.

Prises de vue

Contexte : deux commerciaux d'une entreprise étrangère ont tenté de s'immiscer au sein d'un événement privé organisé par une entreprise française spécialiste des blindages. Cette présentation, située en salle arrière du stand de l'exposant, devait donner lieu à l'avant-première de la présentation de leur nouveau matériel. Leur intrusion a heureusement été déjouée par la vigilance des agents de sécurité présents sur le stand, qui ont strictement fait appliquer la consigne du badge apparent. Or, les deux employés, conscients de ne pas figurer sur la liste des personnes autorisées à cet événement avaient tenté de dissimuler leur badge pour masquer leur identité. Ces individus ont alors été priés de quitter le stand.
En fin de journée, anticipant vraisemblablement la relève des équipes de sécurité, les mêmes individus ont été repérés par les agents de la DRSD en train de photographier discrètement les matériels exposés sur le stand ouvert au public, malgré le panneautage prohibant cette pratique.

Conséquences : l'officier de sécurité de l'entreprise a fait remonter cet incident à la DRSD. Il ressort des premières investigations que les deux individus appartiennent à l'un des services de renseignement d'un pays fortement intéressé par le nouveau matériel développé par l'entreprise.

CAS CONCRETS d'ingérences constatées lors du dernier salon EUROSATORY 2022

Visite de délégation étrangère

Contexte : à l'occasion d'une visite de délégation étrangère sur le stand d'une entreprise de la BITD, le directeur commercial s'est aperçu qu'un individu inconnu s'était greffé au groupe invité. L'homme semblait particulièrement attentif aux propos du directeur lorsque celui-ci évoquait certaines spécificités du matériel que son entreprise commercialise dans le domaine de l'artillerie. Sensibilisé en amont du salon, le directeur a interrompu ses explications et demandé à l'homme de quitter le stand. Visiblement gêné, celui-ci s'est exécuté.

Conséquences : après cet incident, la chaine sécurité de l'entreprise de la BITD a fait remonter aux équipes de la DRSD cette information. Les investigations ont révélé que l'individu appartenait à une entreprise étrangère travaillant sur les mêmes briques technologiques que l'entreprise française.
Les équipes de la DRSD présentes sur le salon ont ensuite sensibilisé les entreprises de la BITD travaillant dans le secteur de l'artillerie afin d'éviter toute nouvelle tentative de captation d'informations.

Comportement anormal d'une hôtesse

Contexte : le comportement d'une hôtesse d'accueil, recrutée par l'intermédiaire d'une agence d'intérim, a attiré l'attention des collaborateurs de l'entreprise exposante pour ses questions intrusives. De plus, pendant toute la durée du salon, la jeune femme s'est distinguée par un comportement réservé, se tenant à l'écart des moments de cohésion avec ses collègues. En revanche, elle s'est montrée particulièrement intéressée par les caractéristiques techniques de certains matériels exposés en faisant montre d'une connaissance inattendue des systèmes exposés.

Conséquences : intrigués par son comportement, des collaborateurs de l'entreprise exposante présents sur le stand ont fait part de leur étonnement au numéro d'astreinte de la DRSD. Après investigations par le Service, il a été établi qu'elle avait effectué plusieurs voyages en Russie au cours des mois précédant son embauche. Ces éléments ont permis d'entamer une enquête toujours en cours sur le ciblage potentiel de plusieurs matériels exposés lors du salon.

La détection « à temps » des atteintes visant vos savoir-faire repose sur notre vigilance commune, le partage des alertes et notre capacité à vous conseiller.
C'est la traduction d'une confiance réciproque.
Vous pouvez compter sur la DRSD et ses agents déployés à vos côtés.

CONTACT DRSD SUR LE SALON : 01 46 73 56 65 / 06 33 71 01 07

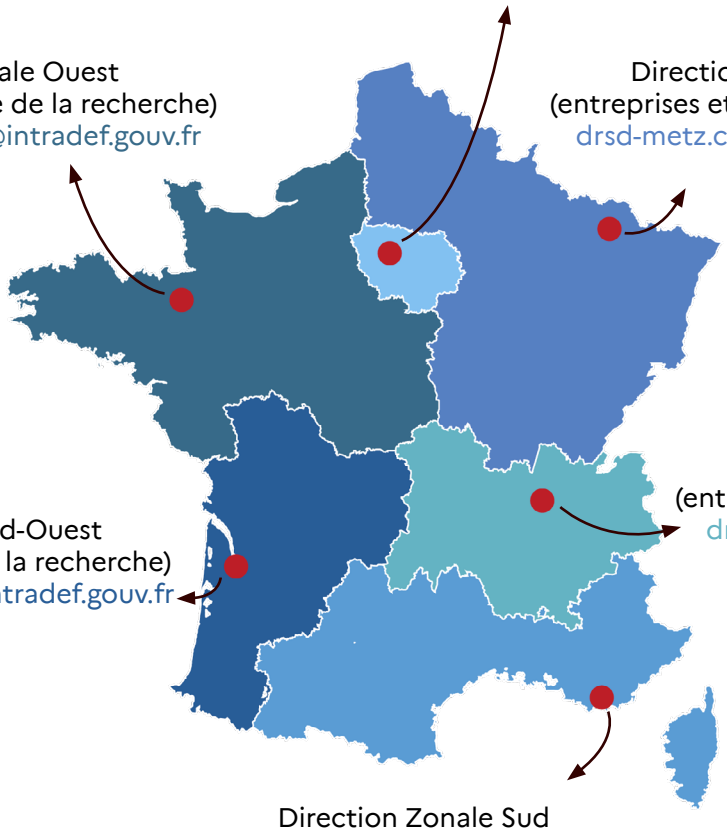
Gardons le contact

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