RECOMMANDATIONS

Recommandations générales :

- Contrôle de l'efficacité des systèmes de protection / alarme / détection.
- Restriction des droits d'accès piéton / véhicule.
- Renforcement des contrôles sur les personnes extérieures amenées à pénétrer sur les sites.
- Recensement des fournisseurs réguliers ou occasionnels (liste à disposition du poste de garde).
- Surveillance renforcée des accès (parking, contrôles visiteurs et des équipes d'intervention).
- Vérification du contenu des véhicules.
- Vigilance pour la réception des colis (contrôle).
- Vérification des dispositifs / mesures d'évacuation rapide des bâtiments.
- Vérification des mesures de coordination avec les forces de l'ordre (N° d'appel, délai d'intervention, …).
- Accompagnement de toute livraison (véhicule ou à pied) non programmée.
- Suspension des manifestations ouvertes au public.
- Vigilance sur l'évolution du comportement de vos employés, mais aussi de ceux des prestataires

Recommandations Cyber :

- Remontée de tout incident affectant les systèmes d'information (classifiés, DR ou d'entreprise).
- Examen régulier des journaux de sécurité des systèmes d'information.
- Vérification de l'application de la politique de sécurité technique (paramétrages FW, contrôles d'accès, authentifiants).
- Cloisonnement entre activités professionnelles et personnelles sur les réseaux sociaux.
- Vigilance accrue concernant tout mail d'origine douteuse comportant des pièces jointes.
- Sensibilisation des utilisateurs et administrateurs (hygiène cybernétique de l'ANSSI).