

1. Exigences de sécurité des SI pour les systèmes de vidéoprotection

Réf	Règles
ID-ACT-1	<p><u>Cartographier les systèmes de vidéoprotection</u> Les documents suivants doivent être formalisés :</p> <ul style="list-style-type: none"> Document décrivant les composants logiciels ainsi que les flux de données entre ces composants ; Document répertoriant les périmètres et niveaux de privilèges des utilisateurs et des administrateurs ; Schéma représentant les zones à surveiller et leur niveau de protection attendu ; Schéma représentant le positionnement des dispositifs (caméras, systèmes de gestion, etc.) ; Schéma représentant le cloisonnement physique et logique des réseaux, les plages d'adresses IP, les fonctions de routage et de filtrage ; Document décrivant la liste complète des équipements physiques utilisés.
ARCH-SI-1	<p><u>Définir l'architecture cible.</u></p> <ul style="list-style-type: none"> Identifier le nombre de systèmes de vidéoprotection à mettre en place en fonction de la sensibilité des zones à traiter ; Déterminer l'emplacement du centre de gestion ; Déterminer le ou les réseaux fédérateurs qui véhiculeront les flux de vidéoprotection jusqu'au centre de gestion ; Déterminer les interconnexions nécessaires entre le centre de gestion et les autres SI de l'EFS ; Déterminer l'emplacement des stations de gestion.
ARCH-SI-2	<p><u>Privilégier l'utilisation de produits et services qualifiés/certifiés par l'ANSSI.</u> Lorsque c'est possible, il est recommandé que les matériels, les logiciels et services utilisés pour la vidéoprotection soient qualifiés par l'ANSSI¹ au niveau requis par les besoins de sécurité. À défaut, il est recommandé qu'ils disposent d'un autre Visa de sécurité délivré par l'ANSSI.</p>
ARCH-SI-3	<p><u>Cloisonner physiquement les SI de vidéoprotection.</u> Le SI de vidéoprotection doit être cloisonné des autres composantes du système d'information de l'établissement au travers d'un cloisonnement physique (câblage et équipements réseau dédiés voire serveur spécifique).</p>
ARCH-SI-4	<p><u>Protéger physiquement les liaisons filaires.</u> Les liaisons filaires ne doivent ni être apparentes, ni situées dans une zone non contrôlée et protégées physiquement (encastrées, bien enterrées, etc.).</p>
ARCH-SI-5	<p><u>Privilégier une connectivité filaire pour les dispositifs de vidéoprotection.</u> Pour les dispositifs de vidéoprotection la connectivité filaire doit être privilégiée à la connectivité sans-fil (comme par exemple : ZigBee², Wifi, téléphonie 3/4/5G) qui augmente l'exposition aux attaques logiques. Dans le cas où la connectivité filaire n'est pas possible, une solution proposant un deuxième chiffrement, en plus du chiffrement opéré par la liaison sans-fil doit être mise en place. Les flux doivent être authentifiés, et protégés en confidentialité et en intégrité. Les opérations de chiffrement et de déchiffrement doivent s'effectuer en zone contrôlée. La borne d'accès sans-fil doit être placée à l'intérieur de la zone contrôlée.</p>
ARCH-SI-6	<p><u>Cloisonner les dispositifs au sein du réseau support (local au site à protéger).</u> Un cloisonnement physique doit être prévu entre les dispositifs (entre vidéoprotection et reste du SI mais aussi entre dispositifs du même type : caméras, etc.). Notamment dans les cas où les dispositifs : n'ont pas besoin de communiquer entre eux ; sont associés à des zones de niveaux de protection différents, ont des spécificités particulières et leur exposition peuvent entraîner une atteinte à la confidentialité des flux, particulièrement les caméras placées à l'extérieur des zones contrôlées.</p>
ARCH-SI-7	<p><u>Ne pas laisser les points d'accès au réseau apparents.</u> Les points d'accès au réseau des dispositifs comme les caméras constituant une vulnérabilité, ils ne doivent être ni apparents ni accessibles facilement (par exemple : prise réseau murale pour le raccordement d'une caméra IP sur le réseau support).</p>

¹ Découvrir les solutions qualifiées | ANSSI

² Protocole de communication sans-fil à courte portée et faible consommation reposant sur la norme IEEE 802.15.4

Réf	Règles
ARCH-SI-8.1	<p><u>Durcir les commutateurs réseau (switches).</u> Les commutateurs réseau doivent être durcis, notamment :</p> <ul style="list-style-type: none"> • Les ports inutilisés doivent être désactivés ; • Les mots de passe par défaut doivent être changés ; • Les accès aux ports réseau doivent être contrôlés par authentification (par exemple : en utilisant une authentification cryptographique des accès au réseau comme le protocole 802.1X ou à défaut par vérification des adresses MAC).
ARCH-SI-8.2	<p><u>Filtrer les flux entre les réseaux support.</u> Lorsqu'ils sont nécessaires, les flux en provenance et à destination des réseaux support (réseaux locaux aux sites à protéger) doivent être filtrés par un ou plusieurs pare-feux (firewall). Seuls les flux strictement nécessaires au fonctionnement du système doivent être autorisés, les autres sont bloqués par défaut.</p>
ARCH-SI-9	<p><u>Protéger les flux de vidéoprotection transitant par un réseau de transport non maîtrisé.</u> Si les flux de vidéoprotection en provenance de sites distants circulent sur un réseau non maîtrisé, ces flux doivent être chiffrés et authentifiés entre les deux réseaux (par exemple : au travers d'un tunnel IPsec).</p>
ARCH-SI-10	<p><u>Éviter l'externalisation des services de gestion chez un prestataire de services.</u> Il est recommandé d'éviter de recourir à l'externalisation des services de gestion de vidéoprotection, ainsi que leur télémaintenance, chez un prestataire de services pour éviter tout compromission d'éléments secrets ou de données confidentielles.</p>
ARCH-SI-11	<p><u>Éviter une interconnexion avec le SI de production de l'EFS ou tout autre système d'information.</u> Dans la mesure du possible, il est recommandé d'éviter d'interconnecter le système de vidéoprotection du site avec le SI de l'EFS ou tout autre système d'information. Dans le cas où une interconnexion est incontournable, il est recommandé de filtrer tous les accès entre le système de vidéoprotection et le SI de l'EFS et d'autoriser les seuls flux concernés par le besoin d'interconnexion.</p>
ARCH-SI-12	<p><u>Synchroniser les horloges des équipements sur une source de temps fiable.</u> Tous les équipements qui composent les systèmes d'information de vidéoprotection doivent être synchronisés (protocole NTP) depuis une source de temps fiable. Dans le cas où les informations issues de ces systèmes sont croisées avec celles d'autres systèmes de contrôle d'accès physique ou de vidéoprotection, les sources de temps de ces systèmes doivent être synchronisées.</p>
ARCH-SI-13	<p><u>Mettre en œuvre les mesures de sécurité d'administration des SI.</u> Comme tout SI à part entière, les systèmes de vidéoprotection doivent respecter les mesures de sécurité d'administration des SI. Notamment :</p> <ul style="list-style-type: none"> • Sécurisation des comptes d'administration (authentification, politique de mot de passe, gestion des comptes, journalisation, etc.) ; • Chiffrer et authentifier les flux d'administration technique et métier : station de gestion/serveur de gestion, serveurs de gestion/dispositifs administrés, postes d'administration technique/équipements du centre de gestion ; • Réaliser les tâches d'administration depuis un poste d'administration durci ; • Mettre en place un réseau d'administration dédié à l'administration technique des équipements du centre de gestion, dans la mesure du possible ; • Distinguer les rôles sur les ressources d'administration métier en attribuant des stations de gestion distinctes aux rôles suivants : administrateur applicatif, opérateur du centre de gestion... ; <p>Durcir les postes de travail avec un rôle particulier.</p>
SEC-SYS-VID-1	<p><u>Chiffrer et authentifier les flux émis et reçus par les caméras.</u> Les flux émis et reçus par les caméras (images, administration) doivent être chiffrés et authentifiés par des protocoles tels que TLS ou IPsec.</p>

Réf	Règles
SEC-SYS-VID-2	<p><u>Durcir la configuration des caméras.</u> Au même titre que les postes de travail, les exigences de durcissement s'appliquent aux caméras et plus particulièrement :</p> <ul style="list-style-type: none"> • Les interfaces locales d'administration des caméras déployées, lorsque de telles interfaces existent, doivent être désactivées ; • Les mots de passe par défaut des caméras doivent être remplacés par des mots de passe spécifiques, robustes et dans la mesure du possible différents pour chaque équipement ; • Il est fortement recommandé de remplacer les certificats installés par défaut dans les équipements par des certificats générés par une infrastructure de gestion de clés maîtrisée par l'EFS, et dédiée au système de vidéoprotection ; • Les fonctions (par exemple réorientation de la caméra) qui ne sont pas utilisées dans le cadre du déploiement doivent être désactivées ; • La caméra doit être compatible avec les processus de changement de mot de passe par groupe de caméra depuis le serveur et par les mises à jour à distance automatiques. • La caméra doit pouvoir s'authentifier sur le réseau selon la norme 802.1x. • Le logiciel interne (firmware) doit être chiffré et signé pour éviter tout détournement du périphérique.
SEC-SYS-VID-3	<p><u>Utiliser un centre de gestion du système de vidéoprotection centralisé.</u> La mise en œuvre d'un système d'un centre de gestion du système de vidéoprotection centralisé (serveurs, analyse, administration des caméras) est nécessaire pour protéger un périmètre donné. Ce centre de gestion peut être situé au sein du poste de sécurité du site concerné.</p>
SEC-SYS-VID-4	<p><u>Sécuriser le système de vidéoprotection.</u> Le SI de vidéoprotection doit être considéré comme un SI à part entière. Il est nécessaire de sécuriser l'ensemble des éléments constituant ce SI. À ce titre, il doit respecter la PNSSI en vigueur. Notamment :</p> <ul style="list-style-type: none"> • l'authentification individuelle des utilisateurs sur la base de mécanismes robustes ; • accès aux données et aux interfaces de gestion du système cloisonnés par profil (aucun utilisateur ne peut accéder à des fonctionnalités ou des données non expressément autorisées par l'autorité contractante) ; • le chiffrement et l'authentification des flux (TLS ou IPsec) avec un niveau de sécurité similaire à AES256 ; • l'utilisation d'un réseau d'administration, si les équipements du centre de gestion sont administrés par le réseau ; • le stockage sécurisé des données vidéos ; • le suivi des versions et la mise à jour des composants matériels et logiciels ; • le strict contrôle des branchements de périphériques amovibles ; • la journalisation des opérations, notamment celles portant sur l'administration du parc de caméras et des serveurs de collecte des flux, et au contrôle régulier de ces journaux.
SEC-SYS-VID-5	<p><u>Etudier le niveau de risque des nouvelles technologies intégrées au système de vidéoprotection.</u> L'usage de fonctionnalités basées sur des nouvelles technologie (par exemple : analyse vidéo basée sur l'Intelligence Artificielle) sont à désactiver/bloquer par défaut. Leur déploiement nécessite une étude préalable et une analyse de risques de sécurité numériques préalable et une validation de l'équipe RNSSI et de la direction juridique.</p>
MAINT-EXP-1	<p><u>Faire appel à des intervenants certifiés.</u> Dans la mesure du possible faire appel à des prestataires certifiés dans les domaines de la vidéoprotection notamment sur les thématiques de sûreté et de cybersécurité. Seules les personnes dûment habilitées au titre de la protection des sites sensibles sont autorisées à intervenir sur le site. Le prestataire transmet la liste nominative des intervenants avec copie des habilitations avant toute opération. Les personnels ne figurant pas sur la liste, ne seront pas autorisés à pénétrer dans le site.</p>
MAINT-EXP-2	<p><u>Disposer de matériel de rechange.</u> Afin de minimiser les délais d'intervention en cas de panne matérielle, il est essentiel de disposer de matériels de rechange (caméras...). Ces matériels de rechange doivent être entreposés dans des locaux sécurisés, dont l'accès n'est autorisé qu'aux personnes habilitées.</p>
MAINT-EXP-3	<p><u>Effectuer des sauvegardes régulières.</u> Les systèmes de gestion doivent être sauvegardés au même titre que le reste des systèmes d'information et doit donc respecter la politique nationale en la matière.</p>

Réf	Règles
MAINT-EXP-4	<p><u>Assurer le maintien en condition de sécurité.</u></p> <p>Il est impératif d'assurer un maintien en condition de sécurité pour les systèmes de vidéoprotection, au même titre que pour tout autre système d'information. Particulièrement, les mainteneurs doivent :</p> <ul style="list-style-type: none"> • notifier la présence de vulnérabilités sur leurs produits, • proposer la mise en place de mesures de remédiation et un plan de déploiement des correctifs, détailler les risques encourus dès lors que les versions déployées ne sont pas les plus récentes ou que les correctifs de sécurité ne sont pas tous installés.
MAINT-EXP-5	<ul style="list-style-type: none"> • Mettre en place une procédure en cas de panne d'une caméra.
MAINT-EXP-6	Mettre en place une procédure en cas de panne du système de gestion.