DOCTRINE DE DÉTECTION POUR LES SYSTÈMES INDUSTRIELS

GUIDE ANSSI

ANSSI-PA-084
03/12/2020

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente la **« Doctrine de détection pour les systèmes industriels »**. Il est téléchargeable sur le site www.ssi.gouv.fr.
Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [8].
Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.
Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	03/12/2020	Version initiale

Table des matières

1
Introduction

1.1 Contexte

Les systèmes industriels, ou *Industrial Control Systems* (ICS), sont omniprésents dans un grand nombre de secteurs d'activité et d'infrastructures critiques, stratégiques ou non :

- raffinage, transport et distribution de pétrole et de gaz naturel ;
- production, transport et distribution d'électricité et de l'eau ;
- transport maritime, ferroviaire et urbain ;
- production de produits pharmaceutiques, alimentaires et manufacturés ;
- etc.

1.2 État de la menace

Depuis quelques années, les systèmes industriels sont informatisés et interconnectés, d'abord entre eux, puis avec le système d'information de l'entreprise. Certains systèmes peuvent, par conséquent, être accessibles directement ou indirectement depuis Internet.

Les cybermenaces qui pèsent sur ces systèmes sont réelles et croissantes, et le nombre d'incidents les impliquant est en forte augmentation.

Les conséquences de ces incidents peuvent être d'ordre opérationnel (arrêt de la production), mais aussi être à l'origine de dommages sur les installations (dégradation de la production ou destruction de matériel), environnementaux (effet néfaste sur une ressource naturelle avoisinante) et corporels (mise en danger des employés et du public en contact avec ces systèmes).

L'origine et les objectifs des cyberattaques sur des systèmes industriels sont divers, mais on peut citer principalement :

- les États ou groupes soutenus par des États, dont les motivations peuvent être d'ordre géopolitique ;
- les groupes criminels à la recherche d'un gain financier ;
- les hacktivistes soutenant une cause sociale, politique ou idéologique ;
- les initiés (p. ex. la menace interne : employés, sous-traitants, anciens employés) agissant par inadvertance ou de façon malintentionnée ;
- les opportunistes, à la recherche de cibles faiblement sécurisées, souhaitant en retirer un bénéfice personnel (ludique, financier).

1.3 De la nécessité de superviser les systèmes industriels d'un point de vue de la sécurité

Une supervision à partir de systèmes de contrôle et d'acquisition de données (*Supervisory Control And Data Acquisition*, SCADA) existe sur la majorité des installations industrielles. Elle permet notamment de piloter et de veiller au bon fonctionnement du procédé industriel.

En revanche, cette supervision n'est ni prévue ni adaptée pour la détection d'incidents de sécurité, notamment induits par l'ouverture de ces systèmes et par leur interconnexion avec des réseaux largement connectés.

Rappelons tout d'abord qu'il est essentiel de renforcer la sécurité informatique des systèmes industriels, afin de garantir la fiabilité, la disponibilité et la sécurité [1] de ceux-ci. L'objectif de ce renforcement de la sécurité informatique est de fiabiliser le pilotage des procédés industriels, par l'ajout de mécanismes visant à assurer le respect des propriétés de confidentialité, d'intégrité et de disponibilité des ressources et services sensibles (données, procédés industriels, systèmes de contrôle/commande, etc.).

Dans son rôle d'assistance technique aux organismes et industriels concernés, l'ANSSI met à disposition des éléments permettant de déployer, dans la durée, les bonnes pratiques en la matière (par exemple [3] et [4]).

Il est rappelé que les systèmes industriels identifiés en tant que système d'information d'importance vitale ou système d'information essentiel, doivent être respectivement conformes aux règles relatives à la détection, 7 de la loi de programmation militaire (LPM) et 18 de la directive NIS.

Sont concernées également, les activités de prestation de détection des incidents de sécurité. En effet, le référentiel d'exigences [7] prévoit que le prestataire puisse être capable d'opérer des sondes dédiées aux systèmes d'informations industriels .

L'objectif de ce document est de présenter une doctrine en matière de détection des attaques visant les systèmes industriels. Les mesures de détection présentées viendront renforcer et compléter les moyens de protection déjà mis en place. Ces mesures de détection peuvent également compenser l'impossibilité de mettre en œuvre certaines actions de sécurisation (incompatibles par exemple avec les exigences de sûreté de fonctionnement, durée du cycle de vie des équipements, etc.). Elles offriront une supervision de sécurité des éléments ne pouvant faire l'objet de mesures de protection (ces derniers seront l'objet des risques résiduels assumés en connaissance de cause par l'entreprise, mais néanmoins assumés).

Elles permettront également d'alimenter les informations nécessaires à la remédiation du système dans le cadre d'une réponse à incident.

1. Il s'agit de la sécurité industrielle (FDMS), introduite par la sûreté de fonctionnement, à ne pas confondre avec la sécurité informatique.

1.4 Organisation du document

Dans une première partie, ce document introduit les grands principes de la supervision de sécurité avant d'identifier les particularités des systèmes industriels en la matière.
Une deuxième partie présente, pour un système industriel considéré, comment définir les différentes zones partageant des caractéristiques permettant la déclinaison de moyens de défense communs.
Une troisième partie décrit la doctrine à proprement parler. Cette partie précise les sources de données disponibles, les techniques de détection appropriées et les capacités technologiques nécessaires en conséquence, selon les « profils d'activité [2] » au sein ou à la périphérie des zones considérées (cœur du système industriel, interfaces avec le système d'information de l'entreprise, etc.).
Un modèle de maturité est décrit dans une quatrième partie afin de hiérarchiser les mesures à mettre en œuvre.
Enfin, dans une dernière partie, la mise en œuvre à proprement parler du système de supervision de la sécurité est évoquée afin d'illustrer l'ensemble, par quelques cas concrets, et également d'attirer l'attention du lecteur sur les principaux écueils et bonnes pratiques en la matière.

1.5 Glossaire

Analyseur
: Fonction ayant pour but de traiter les informations transmises par un capteur pour caractériser une activité non autorisée ou non désirée, ou tout évènement d'intérêt du point de vue de la sécurité du système supervisé. Une fonction analyseur peut, dans les exemples les plus courants, être un module de reconnaissance de motifs réputés malveillants, un module de classification de protocoles réseau, un module d'analyse statique ou dynamique de fichiers, un module d'identification de comportements anormaux, etc.

API
: Automate programmable industriel. Il s'agit d'un équipement disposant d'un ensemble d'entrées/sorties électriques sur lesquelles sont raccordées des capteurs et actionneurs et qui exécute un programme de façon cyclique afin de piloter un procédé industriel.

APS
: Automate de sûreté. Il s'agit d'un API ou un composant automatisé assurant des fonctions de sécurité pour la protection des biens et des personnes selon des critères de fiabilité, disponibilité, de maintenabilité et de sécurité (il s'agit de la sécurité industrielle – FDMS – introduite par la sûreté de fonctionnement, à ne pas confondre avec la sécurité informatique).

Capteur du système de détection
: Fonction ayant pour but de capturer une « source de données », c'est-à-dire de discrétiser l'activité du système à superviser et de la transmettre à un analyseur. Une fonction capteur peut, dans les exemples les plus courants, être un tap, un agrégateur de flux, une bibliothèque logicielle de captation de flux au format pcap, un générateur de métadonnées réseau (NetFlow), un agent de collecte de journaux systèmes ou applicatifs, etc.

2. On entend par « profil d'activité » un ensemble représentatif de caractéristiques réseau, système et applicatives au sein ou à la périphérie d'une zone donnée ; en particulier, les protocoles réseau et les applications employés sont relatifs à des usages typiques de la zone considérée, et conditionnent fortement le choix des mesures adaptées en matière de supervision de sécurité.

C&C

Command and Control. Outillage utilisé par un attaquant pour administrer les ressources compromises du système ciblé et propager son attaque ; le C&C se caractérise notamment par l'infrastructure distante qui l'héberge (p. ex. un serveur sur Internet), par l'applicatif installé sur la ressource compromise et permettant les opérations à distance (p. ex. un maliciel), ou par le protocole de communication employé entre la ressource compromise et le serveur distant de commande et de contrôle (p. ex. un protocole sur mesure élaboré par l'attaque, l'usage détourné d'un protocole existant sur le système attaqué, etc.).

FDMS

Fiabilité, Disponibilité, Maintenabilité, Sécurité. Composantes de la sûreté de fonctionnement d'un système.

ERP

Enterprise Resource Planning. Système informatique permettant la gestion du process de planification, le suivi des fabrications, la gestion des stocks, etc.

Gestionnaire de détection

Fonction ayant pour but la gestion métier des différents composants du système de détection. Cela inclut notamment, le paramétrage technique des composants, tels que la configuration des capteurs et des analyseurs, la consolidation des alertes, le stockage des alertes, la notification à l'opérateur, le traitement par l'opérateur des alertes et autres données métier produites, etc. Une fonction gestionnaire peut, dans les exemples les plus courants, être une plateforme de maintien en condition opérationnelle du socle logiciel, un centre de configuration de règles de détection, un module d'enrichissement contextuel des alertes (p. ex. géolocalisation), une interface de visualisation et de traitement d'alertes, un outil de recherches d'antécédents, etc.

GMAO

Gestion de la Maintenance Assistée par Ordinateur. Logiciel de maintenance industrielle permettant la gestion des opérations de maintenance (préventive ou corrective) des équipements, la gestion des stocks, etc.

MES

Manufacturing Execution System. Système informatique permettant l'acquisition de données de production, la gestion des ressources, le contrôle de la qualité, la gestion de la maintenance, le cheminement des produits et des lots, la traçabilité du produit, etc.

Poste de maintenance

Élément permettant d'interagir avec le système SCADA et l'ensemble des automates afin de réaliser des opérations de maintenance et éventuellement de modifier la configuration des automates.

SCADA

Supervisory Control And Data Acquisition. Ensemble de moyens informatiques permettant aux opérateurs et techniciens la supervision fonctionnelle et le contrôle, à distance ou localement, des installations techniques d'un ou plusieurs sites.

SDI

Système de Détection d'Incendie.

SIS

Safety Instrumented System. Il s'agit du terme anglais désignant un automate programmable industriel de sûreté.

Source de données

Information brute utilisée par un système de détection pour détecter une activité non autorisée ou non désirée. Une source de données peut, dans les exemples les plus courants, être un flux réseau, un journal d'évènements système, un journal d'évènements applicatifs, etc.

Station d'Ingéniérie

Équipement permettant, entre autres fonctionnalités, la programmation du système SCADA et des automates industriels. Cet élément est fréquemment mutualisé (non recommandé) avec les fonctionnalités du poste de maintenance.

Système de détection

Ensemble des fonctions « capteur », « analyseur » et « gestionnaire », permettant à un opérateur, sur la base de « sources de données », de réaliser la supervision de sécurité du système considéré.

TAP

De l'anglais *TAP* signifiant « robinet ». Il s'agit d'un équipement physique placé sur un lien réseau (cuivre, fibre) permettant une recopie du flux transitant par ce lien, sans pour autant opérer une « coupure » au sens communément admis, c'est-à-dire par le biais d'opérations matérielles ou logicielles qui pourraient avoir un impact sur le flux de production. Cette recopie est réalisée bit-à-bit au niveau du signal électrique ou optique, le *tap* possède la capacité de rester « passant » pour le flux de production en cas de perte de son alimentation électrique (le seul impact étant la perte de la fonction de duplication de flux).

Zone

Groupement de biens logiques ou physiques reposant sur des critères de risque ou sur d'autres critères tel que les biens sensibles, les fonctions métiers, les aspects organisationnels, etc.

2
Supervision de sécurité

2.1 Grands principes de la supervision de sécurité

On entend par supervision de sécurité d'un système numérique considéré, la capacité à contrôler dans le temps le bon respect de ses propriétés de sécurité, afin de maintenir, voire d'améliorer, le niveau de cette dernière. Superviser la sécurité repose sur la capacité à se doter des moyens d'observer et d'analyser l'évolution du système, afin de détecter et d'initier le traitement des incidents de sécurité avant que leurs impacts ne deviennent trop importants.

Pour ce faire, l'emploi de systèmes de détection, constitués d'un ensemble de capteurs, d'analyseurs et de gestionnaires, est nécessaire, afin de permettre à un opérateur d'identifier et de contextualiser les activités non autorisées ou non désirées, ou tout autre événement d'intérêt du point de vue de la sécurité du système supervisé.

Superviser la sécurité d'un système suppose l'adoption d'une démarche globale cohérente, intégrant notamment sur le plan technique la prise en compte des éléments suivants :

- différents types de sources de données, provenant du réseau, des systèmes et des applications ;
- différentes méthodes de détection, dont les deux grandes approches reposent sur (1) une connaissance de ce qui est non autorisé ou non désiré et sur (2) une connaissance de ce qui est normal et autorisé. Par souci de simplification dans ce document, et parce que ce sont des notions communément admises, on associera le premier cas à la reconnaissance de signatures, qui pourront être plus ou moins complexes (p. ex. marqueurs techniques, scénarios), et le second cas à l'identification d'anomalies, qui consiste à caractériser une attaque par la détection d'une déviation du système supervisé par rapport à un comportement normal de référence ;
- différentes technologies, dont les trois principales reposent sur la captation et l'analyse (1) de flux réseau, (2) d'événements issus de journaux produits nativement par les différents composants du système considéré (postes de travail, serveurs, équipements d'infrastructure, équipements de sécurité, équipements industriels, etc.), et (3) de traces issues des systèmes d'exploitation ou des applicatifs générées par l'usage de composants dédiés à cet effet (c.-à-d. non produits nativement par ces systèmes et applicatifs, par exemple, par l'usage d'agents de collecte logiciels installés sur les systèmes) ;
- différents « profils d'activité » selon le périmètre considéré (intérieur du périmètre lui-même, interfaces avec d'autres périmètres), pouvant inclure par exemple de la navigation Web, de la messagerie électronique, de la bureautique, de l'hébergement Web, du contrôle/commande d'automates, de la télémaintenance, etc. ;
- les causes, les effets et les conséquences possibles d'une attaque, permettant une déclinaison de la stratégie de détection optimale.

Ces éléments sont complémentaires et concourent à l'efficacité du système de détection dans son ensemble. Aussi, pour un système considéré, en résulte un système de détection généralement constitué d'un ensemble de composants positionnés de façon adaptée, comportant chacun des fonctionnalités et un paramétrage adaptés, afin de répondre à l'objectif de détection des activités constituant des violations de la politique de sécurité.

2.2 Particularités des systèmes industriels

La supervision de sécurité des systèmes industriels doit prendre en compte certaines particularités, principalement liées aux raisons suivantes :

- la convergence croissante avec les systèmes d'information d'entreprise : d'une part, sur le plan des technologies (p. ex. protocoles réseau/transport), d'autre part, sur le plan organisationnel (p. ex. interconnexions avec le système d'information d'entreprise ou Internet, télémaintenance, etc.) ;
  - > en conséquence, un système de détection cohérent pour superviser un système industriel intégrera des fonctions spécifiques aux systèmes industriels (p. ex. dispositifs de détection au niveau des automates), mais aussi des fonctions communes avec les systèmes d'information d'entreprise ; en particulier, la mise en œuvre de dispositifs de détection réseau aux interfaces avec le système d'information d'entreprise ou Internet sera essentielle car c'est de ce dernier que proviennent la plupart des attaques sur les systèmes industriels (directement ou par rebond sur le système d'information d'entreprise) ;
- le caractère déterministe et parfois cyclique du fonctionnement des systèmes industriels (p. ex. répétition d'un même cycle d'actions, plages de valeurs maîtrisées, évolutions fonctionnelles peu fréquentes, etc.) ;
  - > en conséquence, il conviendra sur les systèmes industriels d'utiliser en premier lieu une approche par détection d'anomalies, complétée par une approche par détection de signatures plus classiquement utilisées dans les systèmes d'information d'entreprise où l'on considère généralement en premier lieu des approches par signatures (du fait de la difficulté de prévoir le comportement normal du système, et de la variété des caractéristiques techniques connues des modes opératoires d'attaques) ;
- dans certains cas, l'étendue géographique, la multiplicité de sous-systèmes ou la présence d'équipements sur l'espace public complexifie la maîtrise du contrôle des accès physiques ;
  - > en conséquence, un système de détection cohérent pour superviser un système industriel devra tenir particulièrement compte des opportunités d'accès non prévus dans le fonctionnement normal du système (p. ex. réseaux sans-fil, interconnexions peu sécurisées, opportunités d'accès à des composants du système industriel, etc.) ; cela appuiera notamment l'intérêt du positionnement de dispositifs de détection au cœur des systèmes industriels, en complément des solutions périmétriques ; à noter également que dans certains cas, augmenter le niveau de sécurité pourrait permettre de réduire le nombre de dispositifs de détection à déployer [3], ce qui pourra constituer une motivation supplémentaire à la sécurisation ;

3. Par exemple, dans certains cas, sur des liens d'interconnexion non (ou peu) maîtrisés entre deux sites géographiques, la mise en œuvre d'un VPN sécurisé de type IPsec, configuré selon les recommandations de l'ANSSI, pourra rendre moins prioritaire – voire optionnel – le déploiement de systèmes de détection à ces interconnexions.

- la durée de vie (pouvant atteindre 40 ans) et l'évolution parfois complexe des équipements et des systèmes industriels, pour des raisons, par exemple, de continuité d'activité ou d'homologation réglementaire des systèmes ou sous-systèmes ;
  - > en conséquence, il est parfois difficile d'appliquer certaines mesures de sécurité (ex. : mises à jour de sécurité) dans des délais pertinents ; dans de tels cas, la supervision de sécurité se révélera un complément indispensable, afin de pouvoir être alerté rapidement en cas d'attaque exploitant les faiblesses de sécurité concernées ;
  - > le déploiement de dispositifs de détection réseau s'appuyant sur des *taps* réseau passifs, pourra être envisagé pour ne pas porter atteinte à la disponibilité du système en cas de défaillance du dispositif ;
- des périmètres parfois extrêmement difficiles à définir et à maîtriser, de par leur complexité, leur hétérogénéité, leur étendue géographique, voire parfois leur caractère mobile (transport routier ou ferroviaire, énergie, etc.) ;
  - > en conséquence, le travail préliminaire d'identification à la bonne granularité des périmètres sera essentiel dans la détermination de mesures de défense pertinentes ;
- des objectifs de sécurité prioritairement portés sur l'intégrité (p. ex. des communications, des programmes, etc.), dans le but de garantir la fiabilité des procédés industriels, et selon les cas sur la disponibilité, pour offrir des garanties sur la continuité du service (une considération en moyenne moins importante et surtout une prise en compte [4] souvent différente de la confidentialité par rapport aux systèmes d'information de l'entreprise – hors système industriel) ;
- enfin, globalement, une maturité à développer en matière de sécurité du numérique, en lien notamment avec la genèse et l'évolution des systèmes industriels, où prédominent les compétences en automatisme et en sûreté de fonctionnement.

4. Dans les systèmes industriels, on accepte généralement qu'une information fournie par un composant d'un certain niveau de confiance puisse être transmise à un élément de niveau de confiance équivalent ou inférieur, mais pas à un élément de niveau de confiance supérieur.

3
Définition des périmètres de la détection

Des particularités présentées dans la section 2.2, il découle le besoin d'un découpage du système d'information industriel en un ou plusieurs sous-ensembles. En effet, plus la définition du périmètre considéré pour chaque sous-ensemble sera précise et plus il sera facile de mettre en place des solutions de détection pertinentes au sein même et aux interfaces de ces sous-ensembles, tant au niveau du dimensionnement que des fonctions nécessaires.

Pour réaliser un tel découpage, aucune méthode n'est encore universellement admise. Le but de ce chapitre est donc de préciser la méthode recommandée par l'ANSSI et adaptée aux systèmes d'information industriels.

3.1 Premier découpage des sous-ensembles

La méthode considérée repose sur un découpage initial identique à celui réalisé dans le cadre de [4], qui nécessite elle aussi de poser une limite clairement identifiable entre différents sous-systèmes (le principe de découpage de cette étude est également soutenue dans le référentiel IEC-62443 [1]).

Dans un premier temps, le système industriel est découpé suivant des fonctions prises de façon isolée les unes des autres. Ces fonctions peuvent être identifiées selon les besoins métier. Elles correspondent le plus souvent à celles considérées dans les études de sûreté de fonctionnement, par exemple dans les « AMDEC [5] fonctionnelles ».

Il convient ensuite de prendre en compte les relations fonctionnelles entre chaque sous-ensemble et retravailler le découpage jusqu'à ce que soit vérifié un des principes fondateurs de la méthode de classification des systèmes industriels [4] : il consiste à dire qu'une information fournie par un composant d'un certain niveau de confiance peut être transmise à un élément de niveau de confiance équivalent ou inférieur, mais qu'elle ne peut être transmise vers un composant de niveau de confiance supérieur.

Ces différences de niveaux de confiance doivent être prises en compte pour la supervision de sécurité. De ce fait, lorsque ce principe de dépendance unidirectionnelle ne peut être respecté, les deux sous-ensembles impliqués dans cette relation de dépendance peuvent être regroupés en un seul sous-ensemble. Les besoins de détection sont alors alignés sur le majorant des besoins de ces deux sous-ensembles.

Si d'un point de vue purement logique deux fonctions peuvent être considérées comme isolées, elles peuvent ne pas l'être du point de vue de la supervision de sécurité si elles sont hébergées sur

5. Analyse des méthodes de défaillance, de leurs effets et de leur criticité : il s'agit d'un des principaux outils d'analyse de risque utilisés dans le cadre de la sûreté de fonctionnement et de la gestion de la qualité.

un même équipement physique, par exemple un même automate programmable [6]. Dès lors, si la mise en place d'équipements dédiés n'est pas possible, les besoins de détection seront alors alignés sur le majorant des besoins de ces deux sous-ensembles.

3.2 Raffinement des sous-ensembles pour la détection

Lorsque le regroupement de fonctions a été réalisé, il est nécessaire de procéder à une déclinaison des sous-ensembles en utilisant le modèle Purdue [2]. En effet, ce modèle va permettre de déterminer le positionnement des points de détection.

3.2.1 Segmentation par zone

La segmentation proposée est basée sur le modèle Purdue. Ce modèle est architecturé selon six zones auxquelles il est ajouté une zone Externe.

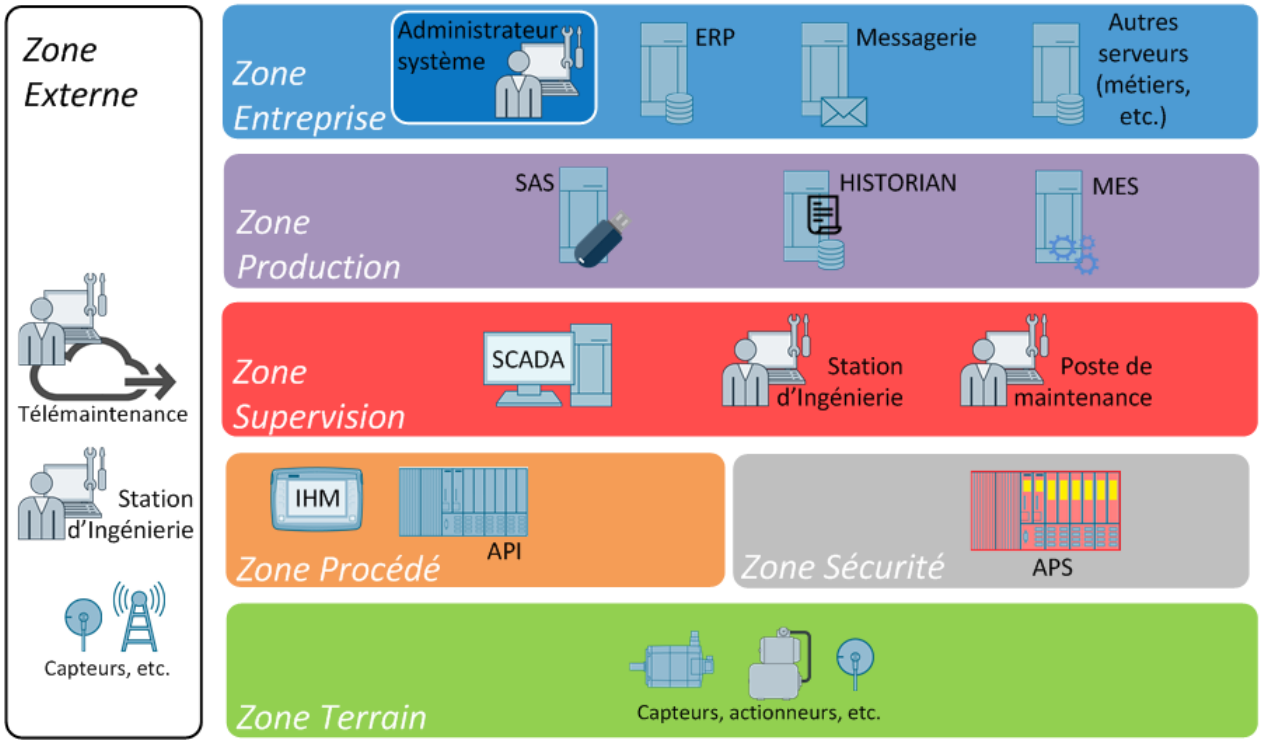

FIGURE 3.1 – Découpage des fonctions selon le modèle Purdue

Zone Entreprise

Il s'agit de la zone concernant la gestion des stocks, des commandes et de la facturation par exemple au travers de progiciel de gestion (ERP) de l'entreprise.

Zone Production

Il s'agit de la zone de contrôle des opérations du procédé industriel. Cette zone permet d'op-

6. Une telle mutualisation ne doit être envisagée que si la fonction de cloisonnement a fait l'objet d'une évaluation de sécurité au niveau attendu par les enjeux de sécurité du système (au travers d'un visa de sécurité de l'ANSSI par exemple).

timiser le procédé industriel selon les stocks et les commandes, mais également de récupérer des données du procédé à destination de la zone entreprise.

Zone Supervision (SCADA)
Il s'agit de la zone de supervision et de commande du procédé industriel.

Zone Procédé
Il s'agit de la zone comprenant l'ensemble des automates programmables industriels (API) et des pupitres (IHM locale). Cette zone permet de réaliser le traitement du procédé industriel.

Zone Sécurité
Il s'agit de la zone comprenant l'ensemble des automates programmables industriels de sûreté (APS). Cette zone permet de réaliser le traitement d'un procédé industriel critique.

Zone Terrain
Il s'agit de la zone qui regroupe les équipements d'acquisition « terrain » (capteurs) et les organes de commande (actionneurs).

Zone Externe
Il s'agit de la zone regroupant d'autres systèmes et équipements connectés au système industriel étudié et en particulier ceux non maîtrisés par l'opérateur de l'installation industrielle (télémaintenance ou programmation de l'installation par un tiers par exemple).

La déclinaison des sous-ensembles en modèle Purdue est logique, elle ne correspond pas nécessairement aux spécificités de l'architecture physique et la distinction des flux entre les différentes zones n'est pas prise en compte.

3.2.2 Segmentation topographique

Il est également important de prendre en compte la topographie des sites au sein d'un sous-ensemble et au sein d'une même zone du modèle Purdue (par exemple dans le cas d'une usine constituée de plusieurs ateliers ou unités de production distants). Les moyens de communication mis en œuvre entre des sites distants ont un impact direct sur l'exposition. Ces interconnexions doivent apparaître clairement dans la segmentation. Par exemple, si la zone Procédé est répartie sur plusieurs sites, il faudra en tenir compte en ajoutant une interconnexion comme énoncé dans la section 5.2.

3.2.3 Rassemblement par composant

Certains composants, comme les automates, portent plusieurs fonctions à la fois : une composante métier et une composante sécurité [7]. Dans ce cas, la détection doit porter sur l'ensemble des fonctions. En particulier, la détection réseau doit être réalisée sur l'ensemble des interconnexions et non uniquement sur l'interconnexion de sécurité [7].

3.2.4 Application au cas « tunnel »

La méthodologie présentée précédemment peut être appliquée à l'étude de cas « tunnel » (présentée dans les guides de l'ANSSI [5] et [6]) .

7. Il s'agit de la sécurité industrielle (FDMS), introduite par la sûreté de fonctionnement, à ne pas confondre avec la sécurité informatique.

Pour les besoins de cet exemple d'application de la méthodologie, une zone « Entreprise » a été ajoutée au cas du tunnel routier pour l'envoi d'informations en provenance de la supervision vers un serveur GMAO pour les applications de maintenance.

Comme énoncé dans la section 3.1, l'étude de classification (partie 1 du cas pratique) permet d'obtenir un regroupement en sous-ensembles des fonctions composant le système. Pour rappel, la conclusion de l'étude propose la configuration suivante : Classe C1 et association des classes C2 et C3 (C1, C2 + C3).

L'architecture correspondant au regroupement de classes issue de l'étude de cas « tunnel », ainsi que la mise en pratique de la méthodologie présentée aux paragraphes 3.2.1, 3.2.2 et 3.2.3, figurent ci-après. La figure 3.2 présente ainsi, pour chaque composant, l'identification des zones du modèle de Purdue sur le schéma d'architecture. La figure 3.3 présente une vision « redressée » du schéma d'architecture pour correspondre au modèle.

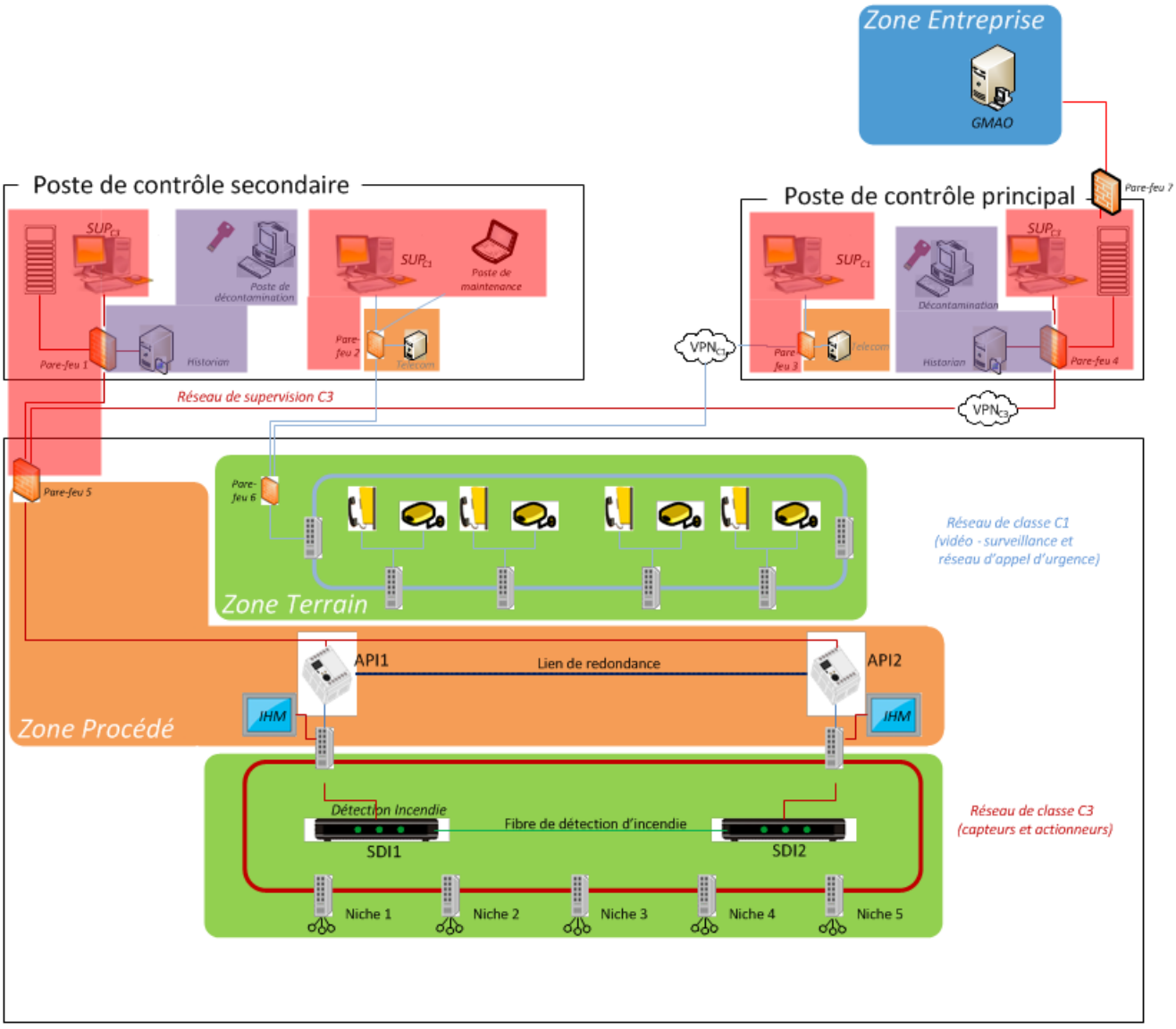

FIGURE 3.2 – Identification des zones pour l'architecture « C1, C2 + C3 »

La segmentation par zone permet d'identifier :

- le serveur de GMAO au sein de la zone « Entreprise » représentée en bleu sur le schéma d'architecture ;
- les postes de décontamination et les serveurs de journalisation au sein de la zone « Production » représentée en violet sur le schéma d'architecture ;
- les serveurs et clients de supervision ainsi que le poste d'administration au sein de la zone « Supervision » représentée en rouge sur le schéma d'architecture ;
- le réseau « automates », les serveurs « Télécom » et le poste d'administration au sein de la zone « Procédé » représentée en orange sur le schéma d'architecture ;
- le réseau de vidéosurveillance et le réseau de capteurs/actionneurs au sein de la zone « Terrain » représentée en vert sur le schéma d'architecture.

Ainsi, les sous-ensembles et les interconnexions associées peuvent être représentés schématiquement de la façon suivante :

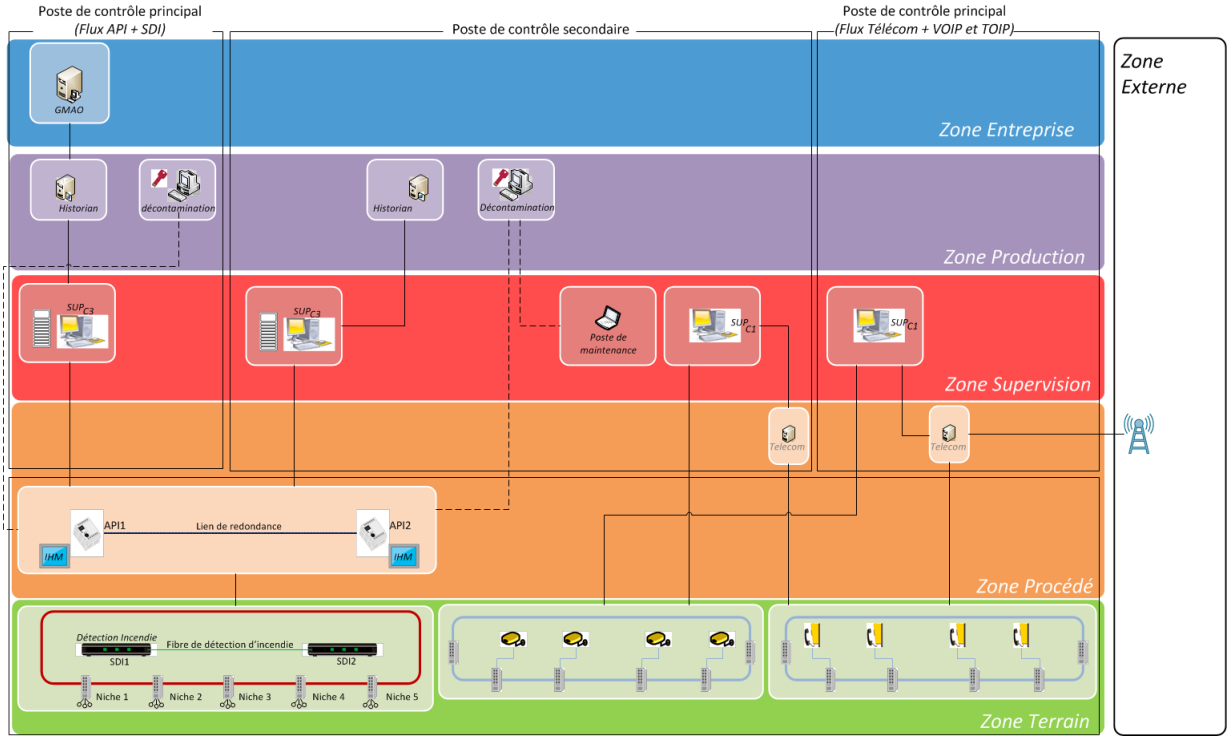

FIGURE 3.3 – Architecture « C1, C2 + C3 » selon le modèle Purdue

Le présent chapitre permet de définir des zones pour l'étude des points et moyens de détection à mettre en œuvre pour le système considéré. Lorsque ce travail de définition est réalisé, il est possible d'y associer les moyens de détection adaptés à la zone Purdue concernée, comme cela est décrit au chapitre suivant.

4
Principes généraux de détection

L'objectif de ce chapitre est de présenter la doctrine à adopter, en considérant tour à tour les différentes zones définies précédemment.

Pour une zone considérée, pour déterminer les moyens de détection qu'il est techniquement possible de mettre en œuvre, il est nécessaire de prendre en compte ses « profils d'activité » (usages, types de protocoles, fonctionnement normalement prévu, etc.) et les sources de données disponibles.

Pour ce faire, il faut distinguer ce qui est externe et ce qui est interne à cette zone.

Dans un premier temps, il faut s'intéresser à la **périphérie de la zone**, en considérant ses connexions (existantes ou potentielles) avec d'autres zones :

- interconnexions véhiculant des flux de « profil d'activité » (la définition du terme « profil d'activité » est donnée à la section 1.4) des systèmes d'information de l'entreprise (flux non spécifiques aux systèmes industriels, protocoles classiques bureautique et Internet) ;
- interconnexions véhiculant des flux de « profil d'activité » des systèmes industriels [8] (envoi de commandes, de consignes, réception de mesures, etc.) ;
- opportunités d'accès (flux correspondant à des dispositifs connectés de façon temporaire, équipements laissant l'opportunité à un attaquant de se connecter).

Dans un second temps, on s'intéresse **à la zone elle-même**, c'est-à-dire les différents équipements qui la composent :

- postes et serveurs ;
- équipements d'infrastructure (commutateurs, routeurs, pare-feu, etc.) ;
- équipements industriels (automates et équipements métiers, GTB/GTC, etc.).

Information

Un équipement ou une interconnexion peut être associé à plusieurs des catégories ci-dessus (catégorie du type de connexion de la zone et catégorie du type de composant de la zone). Par exemple, un commutateur réseau, qui est un équipement d'infrastructure, peut aussi constituer une opportunité d'accès par les ports réseau qu'il expose physiquement. De même, une caméra IP est un équipement industriel qui peut constituer une opportunité d'accès par l'interface réseau qu'elle est susceptible d'exposer dans un espace public ou peu maîtrisé.

8. Au sens physique du terme, une interconnexion peut véhiculer à la fois des flux de « profil d'activité » des systèmes d'information et des flux de « profil d'activité » des systèmes industriels. Dans un tel cas, on considérera simplement ces deux types d'interconnexion au sens logique, et on appliquera la doctrine sur chacune d'entre elles.

Pour toutes ces catégories, plusieurs sources de données utiles pour la détection sont disponibles, parmi les trois grandes familles suivantes :

- des flux réseau, qui peuvent être captés par le biais d'équipements de duplication de trafic ;
- des événements issus de journaux générés nativement par les systèmes d'exploitation des postes, serveurs, équipements industriels ou d'infrastructure, ainsi que par les applications qu'ils hébergent ;
- des traces et indicateurs issus d'agents de collecte dédiés, déployés sur des postes, serveurs ou équipements industriels ou d'infrastructure.

Ces trois grandes familles de données sont complémentaires dans la nature et la granularité des informations qu'elles apportent. Par ailleurs, dans le cas de flux chiffrés [9] ainsi qu'en présence de protocoles réseau propriétaires [10], les deux dernières familles se révéleront d'autant plus indispensables pour pallier les limitations de l'approche réseau.

L'enjeu consiste à mettre en œuvre et à opérer les fonctions adaptées de captation et d'analyse de telles sources de données, dans le but d'identifier des événements de sécurité redoutés, dont certains pourront constituer des incidents de sécurité pour le système considéré.

4.1 Captation

Les principales sources de captation sont les flux réseau, les événements générés nativement et les traces et indicateurs issus d'agents de collecte dédiés.

4.1.1 Flux réseau

Les informations intéressantes à des fins de supervision de sécurité dans les flux réseau peuvent être captées à l'aide de dispositifs généralement en dérivation, par la mise en place des fonctions suivantes :

Captation des flux réseau bruts : il s'agit de réaliser une duplication des flux réseau bruts, généralement à l'aide d'un dispositif de type *tap* [11], qui procède par recopie bit-à-bit des flux à superviser ;

Normalisation : il s'agit de classifier et structurer les données véhiculées dans les flux bruts, afin de les rendre exploitables par des fonctions d'analyse ; cette fonction intègre principalement la reconnaissance et le décodage des protocoles ;

Reconnaissance [12] et extraction de fichiers : il s'agit d'extraire les fichiers véhiculés au sein des protocoles afin d'accroître la capacité d'analyse ;

9. Attention, cela ne signifie pas qu'il faut exclure l'analyse des flux réseau lorsque ceux-ci sont chiffrés ou propriétaires ; en effet, les métadonnées associées (comme les adresses IP, les ports, les volumes de données échangés, etc.) ainsi que certaines informations parfois en clair (comme les certificats) peuvent se révéler très utiles pour la détection.

10. La difficulté intervient principalement dans le cas de protocoles dont les spécifications ne sont pas partagées par l'éditeur, ce qui peut rendre complexe voire impossible le décodage des informations véhiculées par ces protocoles.

11. D'autres solutions existent mais elles sont généralement moins sécurisées ; par exemple, l'emploi d'un port miroir sur un équipement réseau (commutateur, routeur) est une alternative non recommandée par l'ANSSI, car offrant moins de garantie quant à l'intégrité et la disponibilité des flux à superviser ; aussi, on préférera l'usage d'équipements dédiés comme les taps (qui peuvent par ailleurs offrir des fonctions d'isolation entre le système d'information supervisé et le système d'information de supervision).

12. On entend par « reconnaissance de fichiers » la capacité à reconnaître son format, afin de pouvoir en réaliser une analyse adaptée. En effet, le format réel d'un fichier n'est pas nécessairement celui indiqué par son extension. De plus, de nombreux formats de fichiers peuvent être inclus dans d'autres formats (p. ex. image JPG incluse dans un document PDF, lui-même inclus dans une archive ZIP). Reconnaître le format réel et la possible encapsulation de formats dans des fichiers requiert donc une analyse approfondie de la structure d'un fichier, comparable au traitement qui peut être fait sur un protocole réseau.

Journalisation : il s'agit de stocker dans des journaux d'événements des informations issues des flux réseau (généralement, des métadonnées), notamment dans un objectif de qualification des incidents (éléments de contexte) et de détection *a posteriori* (ex. : recherches d'antécédents sur la base de marqueurs caractéristiques d'un mode opératoire).

Protocoles industriels

Dans les systèmes industriels, les protocoles « réseau » reposent souvent sur des couches réseau et transport communes à celles des systèmes d'information (IP, TCP/UDP), les spécificités apparaissant essentiellement au niveau des couches applicatives (Modbus, OPC UA, etc.). Concernant les fichiers échangés, il s'agira, le plus souvent, de programmes (*firmwares*, programmes utilisateur) et de fichiers de configuration.

4.1.2 Événements générés nativement

De nombreux éléments (logiciels ou matériels) disposent de capacités de journalisation, permettant la conservation des principaux événements relatifs à leur fonctionnement. Ces événements peuvent être captés à l'aide de dispositifs externes aux équipements qui les génèrent, par la mise en place des fonctions suivantes :

Captation d'événements natifs : il s'agit de collecter les événements intéressants pour la supervision de sécurité selon différentes technologies et méthodes de collecte à adapter au contexte ; par exemple, cela peut être réalisé à l'aide de collecteurs Syslog sous Linux ou le mécanisme WinRM sous Windows.

Normalisation : il s'agit de classifier et structurer les données, provenant de nombreuses sources hétérogènes, afin de les rendre exploitables par des fonctions d'analyse ; cette fonction peut par exemple intégrer la normalisation des horodatages, afin que l'analyse temporelle des événements dans leur ensemble soit cohérente.

Journalisation : il s'agit de stocker dans des journaux d'événements[13] des informations issues des événements collectés (généralement, des métadonnées), notamment dans un objectif de qualification des incidents (éléments de contexte) et de détection *a posteriori* (ex. : recherches d'antécédents sur la base de marqueurs caractéristiques d'un mode opératoire d'attaque).

Journaux

Dans les systèmes industriels, les journaux pourront reposer tant sur le fonctionnement général des systèmes (p. ex. automates, commutateurs) que sur le fonctionnement du procédé industriel lui-même. Dans le premier cas, les événements concerneront notamment les arrêt/démarrage de l'équipement concerné, les erreurs de fonctionnement du système d'exploitation, les tentatives d'accès ou les accès aux fonctions d'administration (mise à jour du *firmware*, téléchargement d'un programme utilisateur, etc.), etc. Dans le second cas, les événements seront plutôt relatifs aux consignes envoyées aux actionneurs ou aux valeurs remontées par les capteurs, aux changements de programme, aux acquittements d'alertes de fonctionnement depuis les IHM, etc.

13. Il est possible de distinguer les événements bruts, qui sont archivés tels que collectés, et qui peuvent avoir une valeur judiciaire, et les événements issus de la phase de normalisation, qui sont mis en forme pour permettre l'analyse.

4.1.3 Traces et indicateurs issus d'agents de collecte dédiés

En plus des événements disponibles nativement, il est parfois possible de générer des informations complémentaires pour l'analyse, le plus souvent à l'aide d'agents logiciels déployés *in situ*, par la mise en place des fonctions suivantes :

Captation de traces système et réseau : il s'agit de mettre en œuvre des agents logiciels ou matériels dédiés sur les équipements considérés, afin de permettre la collecte d'informations générées *in situ*.

Normalisation : il s'agit de classifier et structurer les données, provenant de nombreuses sources hétérogènes, afin de les rendre exploitables par des fonctions d'analyse.

Reconnaissance et extraction de fichiers : il s'agit de permettre la collecte de fichiers présents sur les équipements considérés, afin d'accroître la capacité d'analyse.

Journalisation : il s'agit de stocker dans des journaux d'événements des informations issues des traces générées (généralement, des métadonnées), notamment dans un objectif de qualification des incidents (éléments de contexte) et de détection *a posteriori* (ex. : recherches d'antécédents sur la base de marqueurs caractéristiques d'un mode opératoire).

Information

Certains équipements industriels ne permettent pas le déploiement d'agent. Cette fonction est cependant envisageable sur certains équipements, notamment ceux qui s'appuient sur des systèmes d'exploitation « grand public » (Microsoft Windows, Linux, etc.).

4.2 Analyse

Les principales fonctions d'analyse se répartissent selon les deux grandes approches complémentaires de détection présentées en introduction, « ce qui est non autorisé ou non désiré » et « ce qui est normal et autorisé ».

4.2.1 Connaissance de ce qui est non autorisé ou non désiré

Méthode dite « par signature simple » La notion de signature « simple » est assimilable à la reconnaissance de marqueurs techniques d'attaques (p. ex. adresses IP, noms de domaines, condensats de micrologiciels, portion d'URL, etc.). Des fonctions de reconnaissance de signatures simples seront nécessaires (p. ex. listes noires, expressions rationnelles).

Méthode dite « par signature complexe » La notion de signature « complexe » est assimilable à la reconnaissance de scénarios techniques d'attaques, à l'usage d'heuristique, ou encore d'opérations complexes sur les données analysées (algorithmiques, statistiques, etc.), dans l'objectif de reconnaître un comportement suspect ou malveillant. Des fonctions de reconnaissance de signatures complexes seront nécessaires. Elles reposeront le plus souvent sur des langages de règles, la capacité d'écrire des scripts sur la base des événements captés, etc. L'application de certaines techniques issues de l'intelligence artificielle peut entrer dans cette catégorie, notamment par leur capacité à permettre l'acquisition de signatures dites « complexes » (p. ex. construction de modèles de comportements malveillants par l'usage de technique d'apprentissage supervisé ou non).

4.2.2 Connaissance de ce qui est normal et autorisé

Méthode dite « par anomalie » L'approche par anomalie pourra s'appuyer sur de nombreuses techniques, que l'on regroupera sous la fonction d'identification d'anomalies. Cela va, par exemple, de la comparaison avec des listes blanches (p. ex. adresses IP ou nom de domaines normalement connus pour communiquer avec une zone considérée) aux méthodes plus complexes issues de l'intelligence artificielle (apprentissage supervisé ou non, réseaux de neurones, etc.), en passant par des applications de la statistique (distributions, séries temporelles, etc.) ou encore des méthodes heuristiques.

4.2.3 Utilisation des méthodes d'analyse

Plusieurs techniques d'analyse sont possibles pour appliquer ces méthodes de détection, dont les deux grandes familles suivantes :

Analyse statique L'analyse statique permettra, avec un haut niveau de performance, de reconnaître des signatures simples ou complexes, ainsi que d'identifier des anomalies, notamment dans les formats de fichiers et de protocoles (p. ex. structure anormale, éléments cachés, traces d'obscurcissement, etc.) comme dans le contenu (p. ex. présence d'appels à des fonctions connues comme dangereuses, de code d'exploitation de vulnérabilités, de code exécutable, etc.).

Analyse dynamique L'analyse dynamique permettra, par du rejeu dans un environnement supervisé (p. ex. fichiers, sessions réseau, etc.), l'observation de comportements (système, réseau, applicatif), qui constitueront de nouvelles sources d'information pour les méthodes de détection par signature et par anomalie.

Ces techniques se révèleront également complémentaires pour opérer une détection optimale.

4.3 Principes généraux de mise en œuvre

Pour être efficace, la détection devra offrir une couverture globale cohérente des différentes catégories présentées au début du chapitre 4 (catégorie des types de connexion de la zone et catégorie du type de composants de la zone), en s'appuyant sur les différentes sources de données disponibles.

De façon générale, la mise en œuvre sera orientée par l'analyse de risque (biens sensibles, exposition, impact, etc.) Les éléments prioritaires seront ceux pour lesquels une compromission du système supervisé aurait des conséquences importantes, et ceux pour lesquels les risques et l'exposition sont élevés [14].

En premier lieu, on considérera la plupart du temps les interfaces avec le système d'information de l'entreprise (hors système industriel), notamment avec Internet, qui constituent le plus souvent un point d'entrée privilégié par l'attaquant [15], renforcé par la tendance au « tout interconnecté ». Par

14. Une attaque étant souvent réalisée en plusieurs phases, il est important de considérer dans l'analyse de risque le fait qu'un équipement plus exposé puisse servir de rebond vers un autre équipement plus sensible (attaque par rebond).

ailleurs, l'accessibilité des technologies employées les rend plus faciles à comprendre et à utiliser dans l'objectif d'une attaque.

En second lieu, on considérera généralement les autres interfaces, qui constituent d'autres possibles points d'entrée externes à la zone pour un attaquant. Parmi ces interfaces, on s'intéressera prioritairement à celles qui sont les plus exposées sur le plan physique (p. ex. liaisons sur des voies de train ou vers des éoliennes, réseaux sans-fil, etc.).

Enfin, on considérera le périmètre interne de la zone, afin de prendre en compte la menace interne à celle-ci. C'est à l'intérieur même de la zone qu'on pourra être en mesure de détecter les conséquences d'une attaque réussie sur celui-ci (p. ex. modification d'un procédé industriel), ce qui s'inscrit pleinement dans la logique de complémentarité de la détection (ici, détecter au moins les manifestations d'une attaque réussie, si l'on a échoué à détecter l'attaque elle-même).

Plusieurs caractéristiques des équipements peuvent par ailleurs influer sur le niveau de risque et sont en conséquence à prendre en compte dans la priorisation des mesures mises en œuvre en matière de supervision de sécurité :

la maîtrise des équipements : autant que possible, les équipements doivent être dédiés, déployés et maintenus en interne par l'opérateur ; d'éventuels équipements qu'il ne maîtriserait pas (p. ex. station d'ingénierie ou poste de maintenance d'un sous-traitant) devront faire l'objet d'une prise en compte adaptée ;

le caractère permanent ou non des équipements : autant que possible, les équipements doivent être déployés de façon permanente ; s'il existe des cas où cela n'est soit pas possible (p. ex. poste de maintenance, déployé spécifiquement pour la durée d'une intervention) soit non recommandé (p. ex. stations d'ingénierie, qu'il est recommandé de ne raccorder qu'en cas de besoin), les équipements concernés devront faire l'objet d'une prise en compte adaptée ;

l'exposition par le biais d'interfaces réseau sans fil (p. ex. Wi-Fi, GSM/2G/3G/4G) : autant que possible, les points d'accès sans-fil et les équipements comportant des interfaces réseau sans-fil doivent être évités, du fait des opportunités d'accès offertes à un potentiel attaquant (accès trivial au canal physique de communication, possibles tentatives d'exploitation de vulnérabilités) ; d'éventuels équipements comportant des interfaces sans-fil, activées ou non, devront faire l'objet d'une prise en compte adaptée.

Afin de mettre en application ces grands principes, le chapitre 5 vise à présenter plus concrètement les moyens de détection adaptés selon les interconnexions et les équipements qui composent les zones considérées.

15. Cf. « Fiches incidents cybersécurité des systèmes industriels », CLUSIF - Groupe de travail SCADA, avril 2017.

5
Définition des points de détection

Pour chacune des zones d'un système industriel telles qu'identifiées dans la section 3.2, les points de détection se situent au niveau :

- de ses interconnexions de « profil d'activité » des systèmes d'information (hors système industriel) ;
- de ses interconnexions de « profil d'activité » des systèmes industriels ;
- de ses opportunités d'accès ;
- de ses postes et de ses serveurs ;
- de ses équipements d'infrastructure ;
- de ses équipements industriels.

Les sections de ce chapitre détaillent chacune de ces catégories.

5.1 Interconnexions de « profil d'activité » des systèmes d'information de l'entreprise

Les interconnexions présentant un « profil d'activité » des systèmes d'information correspondent notamment, aux usages suivants :

- navigation Web et messagerie électronique ;
- bureautique et transfert de fichiers ;
- échange de données de gestion via le réseau d'entreprise (p. ex. ERP – *Entreprise Resource Planning* – ou PGI – Progiciel de gestion intégré) ;
- accès distant aux équipements industriels par un sous-traitant (p. ex. télémaintenance) ;
- etc.

Parmi les attaques que l'on peut recenser, on trouve notamment :

- la propagation de maliciels ne ciblant pas spécifiquement le système industriel (p. ex. virus, rançongiciel), avec des conséquences plus ou moins importantes sur la production, pouvant aller jusqu'au blocage du procédé industriel ;
- l'exploitation de vulnérabilités par des maliciels (points d'eau [16], pièces jointes de courriels, etc.), visant par exemple les systèmes de gestion de commandes (ERP) ou la supervision (SCADA), dans le but d'espionner voire d'attenter à l'intégrité de la production ou des équipements ;

16. Un point d'eau est une ressource légitime (p. ex. site Web) détournée par un attaquant, dans le but d'attirer une potentielle victime, par exemple pour lui faire télécharger un maliciel.

- la mise en œuvre de moyens de rebond dans l'objectif d'attaquer le système industriel en son cœur, par exemple à des fins de sabotage.

Les moyens de détection pertinents reposent sur l'analyse des flux réseau qui transitent par ces interconnexions. Ils doivent donc être adaptés aux protocoles des flux réseau des systèmes d'information de l'entreprise (HTTP, SMTP, DNS, etc.). Les méthodes par signature seront prioritairement employées avant de les compléter par des méthodes par anomalie. En effet, le fonctionnement normal dans des systèmes d'information étant complexe à modéliser, ces dernières sont généralement beaucoup plus compliquées à mettre en œuvre. À l'opposé, les méthodes par signature sont relativement simples à mettre en œuvre et de nombreuses bases de connaissance (signatures notamment) sont disponibles sur les modes opératoires d'attaque.

Concernant les interconnexions véhiculant des flux de « profil d'activité » des systèmes d'information de l'entreprise (hors système industriel), l'analyse reposera donc en priorité sur :

1. la reconnaissance de signatures simples ;
2. la reconnaissance de signatures complexes ;
3. l'identification d'anomalies.

Information

Cette analyse est à compléter par l'exploitation des éléments issus des équipements d'infrastructure positionnés aux interconnexions, et cités dans la section 5.5.

Le tableau ci-après vise à présenter, du plus important au moins important, les moyens pertinents de détection sur les interconnexions de « profil d'activité » des systèmes d'information et à illustrer ceux-ci par des exemples concrets (liste non exhaustive) :

Sources de données	Méthodes de détection	Exemples de règles de détection
Flux réseau	Signatures simples	- Reconnaissance d'un serveur malveillant par son adresse IP ou son domaine - Reconnaissance d'un protocole de C&C par un motif spécifique ou une expression rationnelle dans un protocole applicatif - Reconnaissance d'un maliciel par son condensat
Flux réseau	Signatures complexes	- Reconnaissance d'une requête DNS suivie d'une requête HTTP réussie pour un domaine malveillant - Reconnaissance d'un algorithme de construction de nom de domaines (DGA) - Décodeur de protocole C&C
Fichiers extraits des flux réseau	Signatures simples ou complexes	- Reconnaissance de fichiers contenant du code d'exploitation de vulnérabilités - Reconnaissance de fichiers accédant à des ressources critiques du système d'exploitation
Flux réseau	Anomalies	- Identification d'une distribution anormale de caractères dans des noms de domaines - Identification de pics de trafic anormaux, de connexions hors des heures autorisées

Sources de données (suite)	Méthodes de détection	Exemples de règles de détection
Fichiers extraits des flux réseau	Anomalies	- Identification de fichiers présentant des comportements système ou réseau anormaux lors de leur traitement en environnement supervisé (sandbox) - Identification de fichiers anormaux par comparaison à un jeu de fichiers sains à l'aide de méthodes d'apprentissage supervisé

5.2 Interconnexions de « profil d'activité » des systèmes industriels

Les interconnexions présentant un « profil d'activité » des systèmes industriels correspondent notamment, aux usages suivants (liste non exhaustive) :

- commandes et remontées d'informations depuis et vers la supervision (SCADA) ;
- commandes issues d'automates vers les actionneurs ou d'autres automates depuis les automates, et remontées d'informations depuis les capteurs ou d'autres automates ;
- télémaintenance.

Parmi les attaques que l'on peut recenser, on trouve notamment :

- la propagation de maliciels pouvant ou non cibler spécifiquement le système industriel par l'usage de postes de maintenance non maîtrisés (c.-à-d. hors du périmètre de responsabilité du propriétaire du système industriel, non dédiés, non sécurisés, etc.), avec des conséquences plus ou moins importantes sur la production, pouvant aller jusqu'à son blocage complet ;
- l'exploitation de l'absence de sécurité des moyens de mise à jour des logiciels embarqués (*firmware*), programmes utilisateurs ou de configuration (ex. : absence d'authentification, de contrôle d'intégrité), par exemple à des fins de sabotage ;
- l'exploitation de l'absence de sécurité des protocoles permettant la modification des commandes du procédé industriel (ex. : absence d'authentification, de chiffrement), par exemple à des fins de sabotage.

Les moyens de détection pertinents reposent sur l'analyse des flux réseau qui transitent par ces interconnexions. Ils doivent donc être adaptés aux protocoles des flux réseau des systèmes industriels (Modbus, OPC-UA, etc.). Les méthodes par anomalie seront prioritairement employées avant de les compléter par des méthodes par signature. En effet, le fonctionnement normal des systèmes industriels étant souvent cyclique et déterministe, il est généralement possible d'établir des profils de comportements connus comme légitimes, afin d'identifier des attaques sur la base de déviations par rapport au comportement de référence (p. ex. plages de valeurs non respectées, activité à des heures inhabituelles). Néanmoins, l'approche par signature aux interconnexions peut se révéler très pertinente dans certains cas (p. ex. détection de maliciels).

Concernant les interconnexions véhiculant des flux de « profil d'activité » des systèmes industriels, l'analyse reposera donc en priorité sur :

1. l'identification d'anomalies ;
2. la reconnaissance de signatures simples ;
3. la reconnaissance de signatures complexes.

Le tableau ci-après vise à présenter, du plus important au moins important, les moyens de détection pertinents sur les interconnexions de « profil d'activité » des systèmes industriels et à illustrer ceux-ci par des exemples concrets (liste non exhaustive) :

Sources de données	Méthodes de détection	Exemples de règles de détection
Flux réseau	Anomalies	- Identification de valeurs de commandes en dehors des plages habituelles - Identification d'actions d'administration en dehors d'une plage de maintenance planifiée - Identification d'une mise à jour non conforme d'un programme d'automate ou du *firmware* - Identification d'un canal de C&C entre un automate et le SCADA par des caractéristiques temporelles anormales dans les paquets réseau - Identification d'anomalies dans le séquencement temporel des commandes ou dans les plages de valeurs entre un automate et des actionneurs
Flux réseau	Signatures simples	- Reconnaissance d'une adresse IP de C&C
Fichiers extraits des flux réseau	Signatures simples ou complexes	- Reconnaissance d'un maliciel pouvant affecter un équipement industriel par son condensat (statique) ou par une signature système ou réseau (dynamique)
Flux réseau	Signatures complexes	- Décodeur de protocole de C&C encapsulé dans un protocole industriel

5.3 Opportunités d'accès

On entend par opportunités d'accès les possibilités qui peuvent s'offrir à un attaquant d'accéder de façon opportuniste au système, sans passer par les interfaces normales du système (c.-à-d. conforme au mode de fonctionnement permanent du système). On retrouve notamment dans cette catégorie les éléments suivants (liste non exhaustive) :

- utilisation de ports Ethernet exposés sur des équipements réseau ;
- détournement du lien Ethernet d'un équipement industriel ;
- détournement de lien réseau sans-fil ;
- détournement de ports exposés : ports USB, ports pour carte SD, etc.

Parmi les attaques que l'on peut recenser, on trouve notamment :

- la propagation de maliciels, par le biais de dispositifs de stockage amovibles, pouvant ou non cibler spécifiquement le système industriel, avec des conséquences plus ou moins importantes

sur la production, pouvant aller jusqu'à son blocage ;

- la mise à jour du programme utilisateur d'un automate par la substitution de la carte SD ou par le biais du connecteur USB par exemple à des fins de sabotage ;
- la compromission d'une zone du système industriel (p. ex. système vidéo), dans une logique de rebond vers des ressources critiques du système, par exemple à des fins de sabotage ou d'espionnage.

Les moyens de détection pertinents reposent en premier lieu sur l'analyse de journaux d'événements judicieusement sélectionnés, notamment issus des équipements susceptibles d'être accédés, car ce sont les plus à même de révéler les traces nécessaires à la caractérisation des incidents de ce type. En second lieu, on pourra considérer l'analyse des flux réseau au sein de la zone considérée. En particulier, on s'intéressera à tout ce qui peut permettre d'identifier la présence de nouveaux équipements, au niveau des systèmes comme au niveau du réseau, par exemple à l'aide de listes blanches caractérisant les équipements légitimes, ou encore à l'aide de méthodes de détection statistiques (ex. : séries temporelles).

Concernant les opportunités d'accès, l'analyse reposera donc avant tout sur l'identification d'anomalies, par rapport à un comportement de référence réputé normal (listes blanches d'adresses MAC, de systèmes d'exploitation ou d'applications, caractéristiques temporelles de « profil d'activité » normaux, etc.).

Le tableau ci-après vise à présenter, du plus important au moins important, les moyens de détection pertinents concernant les opportunités d'accès et à illustrer ceux-ci par des exemples concrets (liste non exhaustive) :

Sources de données	Méthodes de détection	Exemples de règles de détection
Journaux d'événements	Anomalies	- Identification d'adresses MAC inconnues dans des journaux réseau, de « *User-Agents* » inhabituels dans des journaux de serveurs mandataires, etc. - Identification d'événements associés au branchement de nouveaux dispositifs USB inconnus (liste blanche) ou inhabituels dans des journaux système - Identification d'événements associés au changement d'état d'un port réseau
Flux réseau	Anomalies	- Identification d'adresses MAC inconnues (liste blanche), d'empreintes d'OS anormales, de « *User-Agents* » inhabituels, etc.

5.4 Postes et serveurs

Les différents postes et serveurs que comporte chaque zone considérée peuvent notamment permettre les usages suivants :

- gestion des commandes et de la comptabilité (p. ex. serveur ERP) ;
- gestion des données de production (p. ex. serveur MES, *Manufacturing Execution System*) ou gestion des processus industriels ;

- bureautique, messagerie, échange de fichiers, impression de documents (p. ex. postes clients, serveurs applicatifs) ;
- développement des programmes utilisateur automates, SCADA, et des interfaces Homme-Machine (p. ex. stations d'ingénierie) ;
- supervision du procédé industriel (p. ex. clients SCADA) ;
- stockage des données métier (p. ex. serveurs *Historian*) ;
- contrôle des fichiers importés (p. ex. sas d'analyse) ;
- maintien en conditions opérationnelles (p. ex. postes de maintenance) ;
- gestion des identités et des accès (p. ex. contrôleur de domaine) ;
- etc.

Parmi les attaques que l'on peut recenser, on trouve notamment :

- la compromission d'un poste ou d'un serveur à des fins de rebond vers des ressources ciblées par un attaquant ;
- la compromission d'une station d'ingénierie ou de maintenance à des fins d'espionnage ;
- la compromission d'un contrôleur de domaine afin de prendre la main sur l'ensemble du système.

Les moyens de détection pertinents reposent en premier lieu sur l'analyse des événements générés nativement par les systèmes d'exploitation et les applications des postes et serveurs concernés. Des agents dédiés de collecte peuvent en second lieu être installés localement sur les équipements, lorsque les contraintes de sécurité et de production l'autorisent.

Le choix de méthodes par signature ou par anomalie se fera au cas par cas, selon la nature des équipements (métier ou non). Dans la plupart des cas, ces équipements reposent sur des systèmes d'exploitation classiques des systèmes d'information. En conséquence, la mise en œuvre de méthodes par signature sera souvent préférable dans un premier temps, afin de pouvoir s'appuyer sur les nombreuses bases de connaissance existantes. Au niveau du système, il sera parfois possible de décrire certaines caractéristiques d'un comportement normal, par exemple par la définition de listes blanches de processus, ce qui constituera une piste intéressante pour compléter l'approche par la détection d'anomalies.

Concernant les postes et serveurs, l'analyse reposera sur : (1) la reconnaissance de signatures simples, (2) la reconnaissance de signatures complexes, (3) l'identification d'anomalies.

Le tableau ci-après vise à présenter, du plus important au moins important, les moyens de détection pertinents concernant les postes et serveurs et à illustrer ceux-ci par des exemples concrets (liste non exhaustive) :

Sources de données	Méthodes de détection	Exemples de règles de détection
Journaux d'événements	Signatures simples	- Reconnaissance d'un serveur malveillant par son adresse IP dans les journaux d'un pare-feu - Reconnaissance d'un lien Web associé à un point d'eau dans les journaux d'un serveur mandataire - Reconnaissance d'un nom de processus associé à un mode opératoire d'attaque dans des journaux systèmes d'un poste ou d'un serveur
Journaux d'événements	Signatures complexes	- Reconnaissance d'une résolution de domaine malveillant dans des journaux DNS, suivie d'un accès à l'adresse IP correspondante dans des journaux de pare-feu ou de serveur mandataire
Journaux d'événements	Anomalies	- Identification d'un client SCADA non légitime - Identification d'un comportement anormal du procédé industriel dans les journaux du serveur *Historian* - Identification de l'usage d'un compte privilégié depuis un poste normalement prévu pour des usages non privilégiés
Traces issues d'agents dédiés	Signatures simples	- Reconnaissance d'une clé de registre typiquement créée par un mode opératoire d'attaque, par exemple pour permettre le lancement d'un maliciel au démarrage du système - Reconnaissance dans la mémoire vive d'un système d'un domaine malveillant ou d'un nom de processus malveillant
Traces issues d'agents dédiés	Signatures complexes	- Reconnaissance dans la mémoire vive d'un système d'une exploitation de vulnérabilité
Traces issues d'agents dédiés	Anomalies	- Identification d'un processus ayant déclenché une séquence anormale d'appels système à l'aide de méthodes d'apprentissage

5.5 Équipements d'infrastructure

Les différents équipements d'infrastructure que comporte chaque zone considérée peuvent notamment permettre les usages suivants :

- transport des flux réseau au travers de commutateurs, de routeurs ou de points d'accès sans-fil ;
- protection périmétrique via l'usage de pare-feu réseau ;
- protection des flux par authentification et chiffrement à l'aide de passerelles VPN ;
- etc.

Parmi les attaques que l'on peut recenser, on trouve notamment :

- la compromission d'un équipement par un maliciel ne ciblant pas spécifiquement le système industriel (p. ex. virus, rançongiciel), avec des conséquences plus ou moins importantes sur la production, pouvant aller jusqu'à son blocage ;

- l'exploitation de faille de sécurité dans les mécanismes cryptographiques associés à l'authentification et au chiffrement (filaires ou sans-fil), par exemple dans un but d'espionnage (ex. : attaque de l'homme du milieu ou *man-in-the-middle attack* en anglais) ;
- la compromission d'un équipement réseau (commutateur, routeur, pare-feu, etc.) par un maliciel ciblé, dans le but d'espionner ou modifier les flux réseau à la volée à des fins de sabotage.

Les moyens de détection pertinents reposent en premier lieu sur l'analyse des événements générés nativement par les équipements considérés. Dans certains cas, des agents de collecte dédiés peuvent en second lieu être installés localement sur les équipements, lorsque des technologies existent et lorsque les contraintes de sécurité et de production l'autorisent. Dans un tel cas, ces agents peuvent permettre l'analyse de traces complémentaires au niveau du système, du réseau ou encore des applications, le cas échéant. Le choix de méthodes par signature ou par anomalie se fera au cas par cas, selon la nature des équipements.

Concernant les équipements d'infrastructure, l'analyse reposera sur : (1) la reconnaissance de signatures simples, (2) la reconnaissance de signatures complexes, (3) l'identification d'anomalies.

Le tableau ci-après vise à présenter, du plus important au moins important, les moyens de détection pertinents concernant les équipements d'infrastructure et à illustrer ceux-ci par des exemples concrets (liste non exhaustive) :

Sources de données	Méthodes de détection	Exemples de règles de détection
Journaux d'événements	Signatures simples	- Reconnaissance d'un accès à une interface d'administration depuis une adresse IP connue comme malveillante - Reconnaissance par son condensat d'une mise à jour logicielle malveillante (p. ex. *firmware*)
Journaux d'événements	Signatures complexes	- Reconnaissance de séquences de paquets réseau répondant à une construction spécifique à un mode opératoire d'attaque - Décodeur de protocole C&C dans le flux d'événements
Journaux d'événements	Anomalies	- Identification d'un accès à une interface d'administration par une adresse IP non connue comme légitime - Identification d'une modification de configuration par accès physique à l'équipement - Identification de comportements réseau inhabituels sur la base de séries temporelles
Traces issues d'agents dédiés	Signatures simples	- Reconnaissance d'un *firmware* malveillant par son condensat
Traces issues d'agents dédiés	Signatures complexes	- Reconnaissance d'une séquence d'événements système caractéristiques d'un code malveillant connu
Traces issues d'agents dédiés	Anomalies	- Identification d'anomalies sur les suites cryptographiques utilisées par une passerelle VPN - Identification de comportements inhabituels au niveau de zones spécifiques de la mémoire (p. ex. destinée au *firmware*, à des clés de chiffrement, etc.)

5.6 Équipements industriels

Les différents équipements industriels que comporte la zone considérée peuvent notamment permettre les usages suivants :

- gestion du procédé industriel par les automates ;
- numérisation d'une mesure physique à partir des capteurs ou modification du procédé industriel grâce aux actionneurs ;
- supervision locale ou à distance d'un procédé industriel à l'aide d'une IHM ou d'un SCADA ;
- protection d'un procédé industriel à l'aide d'un automate programmable de sécurité (ou *Safety Instrumented System* en anglais) ;
- importation de fichiers externes ;
- maintien en conditions opérationnelles ;
- gestion des identités et des accès ;
- etc.

Parmi les attaques que l'on peut recenser, on trouve notamment :

- la compromission par un maliciel ne ciblant pas spécifiquement le système industriel (p. ex. virus, rançongiciel), avec des conséquences plus ou moins importantes sur la production, pouvant aller jusqu'à son blocage ;
- la compromission d'un SCADA ou d'une IHM, par exemple dans le but d'espionner ou de leurrer la supervision par rapport à une attaque en cours sur le procédé industriel ;
- la compromission d'un automate ou d'un système instrumenté de sécurité, par exemple à des fins de sabotage.

La majorité des automates ne produisent pas ou peu de journaux d'événements de sécurité, et leurs flux métier et d'administration ne sont pas ou sont peu sécurisés. Dans ce contexte, les moyens de détection pertinents reposent en premier lieu sur l'analyse des flux réseau, plus particulièrement au cœur des systèmes industriels. Toutefois, l'existence d'une génération d'événements métier (notamment remontés vers les serveurs *Historian*), ainsi que des évolutions technologiques récentes sur la génération d'événements de sécurité, rendent possible l'analyse de journaux d'événements, qui sera d'autant plus utile en présence de flux réseau chiffrés. En général, compte tenu du caractère déterministe des procédés industriels, l'approche par anomalie est souvent privilégiée. Néanmoins, au fil des incidents rencontrés sur les systèmes industriels, la connaissance sur la menace s'accroît progressivement au fur et à mesure que celle-ci se dévoile. Ainsi, la détection par signature se révèle nécessaire en complément pour maximiser les chances de détecter des attaques déjà connues, ainsi que pour faciliter le travail de qualification d'incidents.

Concernant les équipements industriels, l'analyse reposera sur : (1) l'identification d'anomalies, (2) la reconnaissance de signatures simples, (3) la reconnaissance de signatures complexes.

Le tableau ci-après vise à présenter, du plus important au moins important, les moyens de détection pertinents concernant les équipements industriels et à illustrer ceux-ci par des exemples concrets (liste non exhaustive) :

Sources de données	Méthodes de détection	Exemples de règles de détection
Flux réseau	Anomalies	- Identification de valeurs anormales issues d'automates ou de capteur (vitesses, température, etc.) - Identification d'une communication anormale entre un automate et une adresse IP non connue
Fichiers extraits des flux réseau	Anomalies	- Identification de mises à jour logicielles non prévues ou anormales par rapport à une liste blanche de condensats de fichiers
Flux réseau	Signatures simples	- Reconnaissance d'une communication entre un automate et une adresse IP connue comme malveillante
Flux réseau	Signatures complexes	- Reconnaissance d'une séquence d'événements réseau réputée comme appartenant à un mode opératoire d'attaque donné
Fichiers extraits des flux réseau	Signatures simples	- Reconnaissance de mises à jour logicielles connues comme malveillantes par comparaison à une liste noire de condensats de fichiers
Journaux d'événements	Anomalies	- Identification de connexions anormales à l'interface Web de gestion de l'automate, par comparaison avec une liste blanche d'adresses IP ou par rapport à des caractéristiques temporelles des accès normalement prévus - Identification de valeurs anormales transmises à un actionneur ou reçues d'un capteur - Identification de modifications anormales de programmes utilisateur par rapport à des caractéristiques temporelles
Journaux d'événements	Signatures simples	- Reconnaissance d'une communication entre un équipement industriel et une adresse IP connue comme malveillante
Journaux d'événements	Signatures complexes	- Reconnaissance d'un protocole de C&C par des caractéristiques temporelles connues des connexions réalisées avec un automate
Fichiers extraits des flux réseau	Signatures complexes	- Reconnaissance de caractéristiques connues comme malveillantes dans un fichier par une analyse statique (p. ex. fonctions de communication, fonctions d'exécution de code)

Bibliographie

[1] *IEC-62443 : Cybersécurité des installations industrielles*.
Référentiel normatif, ISA.
https://www.isa.org.

[2] *Purdue Reference Model (ISA95)*.
Page web, PERA, Juin 1990.
https://www.pera.net.

[3] *La cybersécurité des systèmes industriels - Mesures détaillées*.
Guide Version 1.0, ANSSI, janvier 2014.
https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels.

[4] *La cybersécurité des systèmes industriels - Méthode de classification et mesures principales*.
Guide Version 1.0, ANSSI, janvier 2014.
https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels.

[5] *La cybersécurité des systèmes industriels - Cas pratique d'un tunnel routier - Partie 1 : classification*.
Guide Version 1.0, ANSSI, octobre 2016.
https://www.ssi.gouv.fr/etude-tunnel.

[6] *La cybersécurité des systèmes industriels - Cas pratique d'un tunnel routier - Partie 2 : mesures*.
Guide Version 1.0, ANSSI, octobre 2016.
https://www.ssi.gouv.fr/etude-tunnel.

[7] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf.

[8] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-PA-084
Version 1.0 - 03/12/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN