eBook Cisco IoT

CYBERSÉCURITÉ INDUSTRIELLE :

Surveillance et détection d'anomalies

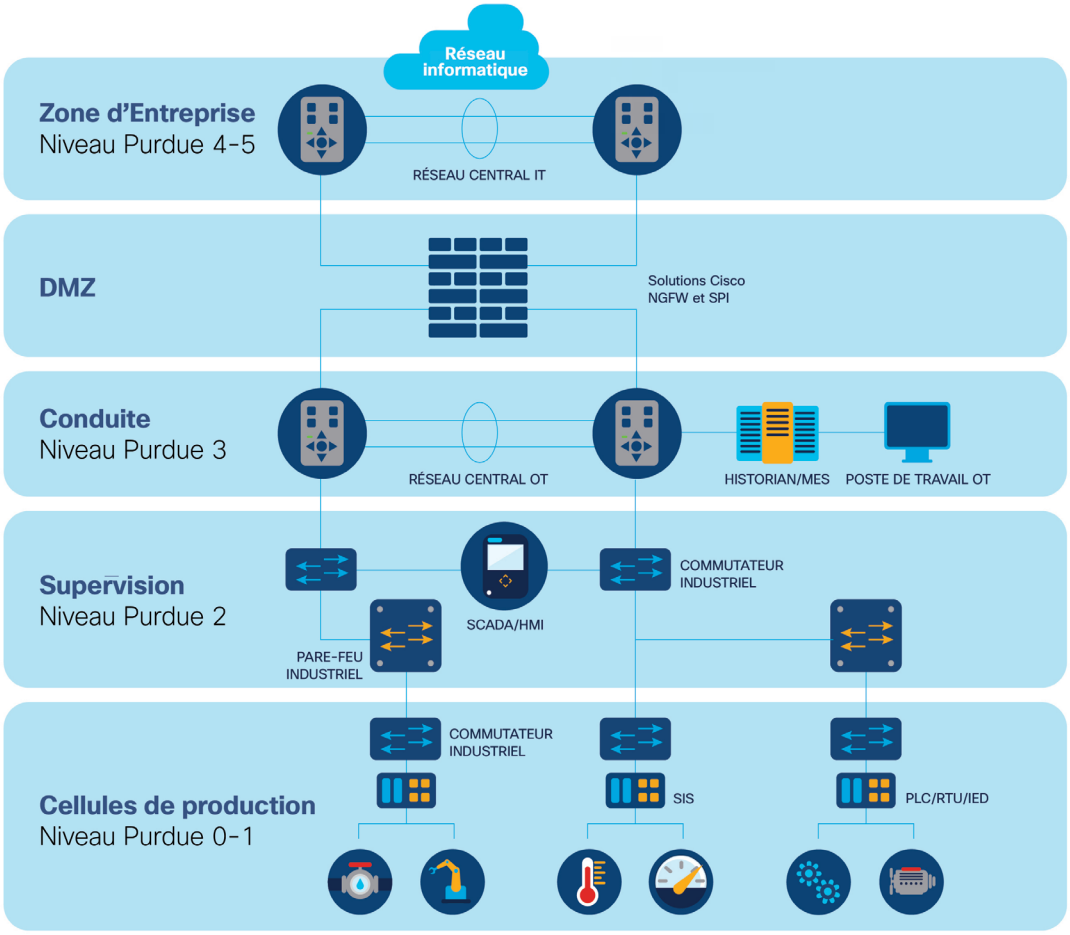
cisco

INTRODUCTION

Les systèmes industriels pilotent aujourd'hui de nombreuses installations critiques.

Ils sont créés et mis en œuvre par une industrie établie et structurée depuis des dizaines d'années. Ils suivent des normes internationales établies par des organismes transverses (ISA, IEC) ou sectoriels (IAEA dans le nucléaire, CENELEC dans le ferroviaire, etc.).

Leur structure est représentée par le schéma suivant, défini par le standard ISA 95 :



Industriel - Niveau 0 - TERRAIN : Capteurs, actionneurs, moteurs

Industriel - Niveau 1 - PROCESS : Dispositifs d'automatisation, systèmes de sécurité, contrôleurs

Industriel - Niveau 2 - SUPERIVSION : Stations SCADA, poste opérateur DCS, stations d'ingénierie

Industriel - Niveau 3 - CONDUITE : MES, LIMS

Informatique - Niveau 4 et 5 - ENTREPRISE : Bureaux, PC, messagerie, intranet

Il est parfois délicat de catégoriser certains réseaux pouvant être considérés comme IT selon certaines de leurs caractéristiques techniques. Il est vrai que depuis les années 2000, les systèmes industriels intègrent les briques classiques d'un système IT (Microsoft Windows, Ethernet, protocole TCP/IP, etc). Il est néanmoins possible de définir précisément un réseau de contrôle industriel.
Si au moins 4 des 5 caractéristiques ci-dessous sont réunies, alors il s'agit d'un réseau de contrôle industriel :

- Il a pour objectif de piloter et de superviser un processus physique
- Il est déployé dans un environnement nécessitant une résistance matérielle spécifique (ex : jusqu'à 70° C, alimentation courant continu 12V ou 24V, résistance à la poussière, avec un niveau IP compris entre 20 et 80 etc.)
- Il utilise des protocoles de communications standardisés par l'IEC ou des protocoles propriétaires issus de constructeurs reconnus (voir encart ci-dessous)
- Il est composé majoritairement de communications « Machine to Machine » à faible bande passante (10 – 100 Mb/s réseaux locaux, 512 kb/s pour réseaux distants)
- L'usage des technologies IT (protocole HTTP par exemple) est réservé à des opérations de management : administration web, surveillance SNMP ou ICMP. À l'inverse, il n'y a pas de communications « utilisateur » (surf web, messagerie, etc.)

LISTE DES CONSTRUCTEURS

ABB - Ansaldo - Bombardier - Beckhoff - Belden et ses acquisitions (Tofino, Hirshmann) - Emerson - General Electric - Honeywell - Moxa - Pilz - Schneider et ses filiales (Invensys, Foxboro, Telemecanique, Modicon) - Siemens - Yokogawa - Wago ...

DES RISQUES SPÉCIFIQUES

Dans le monde informatique (appelé « IT ») traditionnel, la nature du risque est de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes. L'impact est majoritairement financier comme en cas d'extorsion (virus de type cryptolocker), de fraudes bancaires ou de déni de service distribué sur des serveurs web utilisés par les sites de e-commerce.

Les systèmes de contrôle industriels quant à eux pilotent le monde physique. Le risque est de porter atteinte à la sûreté de fonctionnement (sécurité physique des biens et des personnes, impact environnemental), à la disponibilité voire à l'intégrité physique de l'outil de production. Le vol de données industrielles critiques est aussi redouté. Les impacts sont économiques mais aussi sociaux ; la responsabilité civile et pénale du chef d'établissement est engagée.

DES VECTEURS DE COMPROMISSION SPÉCIFIQUES ET IDENTIFIÉS

Le vecteur de menace principal n'est pas l'intrusion au travers d'un réseau grand public comme Internet mais de multiples vecteurs spécifiques. Ainsi, craint-on l'insertion de programmes malveillants **au travers de clés USB** ou encore le déplacement latéral d'un programme malveillant (malware) jusqu'aux stations pilotant les réseaux industriels.

Le télédiagnostic et la télémaintenance nécessitent un accès distant aux réseaux de contrôle industriels. Ce sont aussi des vecteurs de menaces à prendre en compte d'autant plus qu'il s'agit d'interconnexions entre des réseaux de différentes criticités et appartenant à des tiers. Enfin, il existe pour des raisons opérationnelles et économiques, de multiples postes de travail non maîtrisés par les opérateurs, opérés par des tiers (sous-traitants, prestataires extérieurs). Il n'est pas possible d'accorder à ces tiers une confiance importante.

Ces postes vont pourtant se connecter au cœur des systèmes industriels critiques pour des opérations impactant potentiellement le système cible (mise à jour de programmes, etc.). Elles ne peuvent être simplement interdites **mais elles doivent être contrôlées par des mécanismes de surveillance efficaces.**

L'ensemble de ces vecteurs sont pour la plupart spécifiques au monde industriel. Les mesures de sécurité à mettre en œuvre dans les systèmes de contrôle industriels doivent prendre en compte la réalité opérationnelle, et ne peuvent pas uniquement reposer sur le contrôle d'accès et les mesures organisationnelles.

DES SYSTÈMES NON CONÇUS POUR LUTTER CONTRE LA MALVEILLANCE

Par ailleurs les systèmes de contrôle industriels n'ont jamais été conçus pour faire face à des menaces liées à la cybersécurité. Ils sont conçus avec l'objectif d'assurer la sûreté de fonctionnement et la continuité des opérations et ne prennent généralement pas en compte la possibilité qu'une personne malveillante s'introduise via leurs interfaces numériques.

Voilà pourquoi les produits d'automatisme ou de contrôle commande numérique ne comportent jusqu'à aujourd'hui que peu de fonctions de cybersécurité. De plus, dans la plupart des cas les fonctions de cybersécurité disponibles ne sont pas activées par les opérateurs industriels.

DES PROTOCOLES PROPRIÉTAIRES

Les systèmes industriels sont bâtis sur un ensemble de protocoles permettant l'échange entre les composants sur les réseaux. Si certains standards existent comme MODBUS ou PROFINET, **les protocoles permettant de reprogrammer ou de modifier le système de contrôle commande sont la plupart du temps propriétaires et fermés.** La majorité d'entre eux (Siemens, Schneider, ABB, Rockwell Automation, etc) n'ont en aucun cas prévu d'ouvrir ces protocoles pour des raisons de propriété intellectuelle légitimes.

Par conséquent, il n'est pas envisageable d'appliquer des techniques IT comme le contrôle de conformité protocolaire (vérification syntaxique ou sémantique du respect d'une norme ou d'un standard) sur l'ensemble des messages. Celui-ci reste utile sur une partie des messages (entêtes protocolaires) qui respectent des standards ouverts (MODBUS par exemple).

DES ÉVÉNEMENTS OPÉRATIONNELS À QUALIFIER

Plus encore, du point de vue du réseau, un ordre d'arrêt d'un automate programmable (ie. ordre « STOP ») qui aurait été vu par un système de détection n'est en soi, ni malveillant ni légitime. **Il peut s'agir d'une opération de maintenance ou d'un malware.** En aucun cas, cet ordre ne peut constituer une « signature d'attaque » comme un IDS classique qui fonctionnerait avec une liste noire le qualifierait. L'ordre « STOP » doit donc générer un événement de sécurité qui doit être ensuite contextualisé dans une solution qui les centralise et les replace dans leur contexte et leur historique (« qui fait quoi, à quel moment / récurrence »).

COMPRENDRE LES TACTIQUES D'ATTAQUE ICS

Afin de mettre en place une stratégie de cybersécurité ICS efficace, il est essentiel d'identifier les événements de sécurité les plus susceptibles de se produire. Vous pourrez ainsi vous focaliser sur le déploiement des mesures appropriées à la protection des biens les plus susceptibles d'être visés et améliorer la sécurité des biens sensibles qu'un agresseur pourrait utiliser pour s'introduire dans votre ICS.

DES ÉVÉNEMENTS REDOUTÉS

En matière de cybersécurité industrielle, un événement redouté correspond à une situation de cyberattaque sur un système d'information industriel dont les impacts sur le bon fonctionnement de l'entreprise, ses outils de production, sa production, voire sur ses employés ou clients créeraient des préjudices importants. Ces événements auront un impact matériel dans le monde physique. Et certains relèvent de la responsabilité pénale du chef d'entreprise.

Dans la suite du document, trois événements redoutés sont décrits. Chaque événement est développé en trois rubriques :

CATÉGORISATION	but, cible, impact et moyens techniques de l'attaquant
DESCRIPTION	motivations et procédés de l'attaquant
DÉROULEMENT	scénario d'attaque étape par étape

cisco

CYBER KILL CHAIN

Pour codifier les scénarios d'attaque et détailler leurs différentes phases, on utilise le concept de Cyber Kill Chain. Ce concept permet de décrire en détail la structure d'une tentative d'intrusion complexe, typique des nouvelles attaques.

Les différentes étapes de la Cyber Kill Chain sont les suivantes :
Reconnaissance, armement, dissémination, exploitation, installation, prise de contrôle, actions sur un objectif. Dans le cas des événements redoutés développés dans ce document, on considère qu'un attaquant est déjà « connecté » au réseau de contrôle industriel. Il a réussi avec succès les étapes jusqu'à l'installation. Il peut s'agir d'un programme malveillant qui s'est déplacé jusqu'à une station industrielle ou quelqu'un qui a obtenu un accès physique.

Par conséquent, les étapes suivantes, jugées comme acquises, ne seront pas considérées :

- Reconnaissance humaine et technique de l'organisation cible (réseaux sociaux, appels d'offres publiques, publications de l'organisation),
- Armement & dissémination via la création d'un malware (fichier MS Office ou PDF infecté, jeux vidéos piégés, site web de type water hole) envoyé par le web ou par email,
- Installation via un déplacement latéral vers le réseau industriel ou insertion dans le réseau de contrôle industriel et plus particulièrement celui qui contient les stations d'ingénierie.

IDENTIFIER VOS VULNÉRABILITÉS

Il est particulièrement important de noter comment l'attaquant va s'insérer dans le réseau industriel de sa cible. Ses points d'insertion seront autant de points sensibles à considérer dans une démarche de surveillance. Ils sont classés par vraisemblance : ils sont classés par ordre de probabilité :

1

Prise de contrôle d'une station industrielle

L'attaquant utilise des mécanismes de propagation d'attaque ciblée IT (ie malware connecté à un serveur « Command & Control ») pour se propager dans les réseaux de sa cible jusqu'à atteindre un poste du domaine industriel. Les cibles principales sont les stations SCADA et les stations d'ingénierie car elles contiennent des informations importantes sur le processus (point de consignes, variables utilisées dans la programmation, etc.).

2

Usurpation d'un accès à distance autorisé pour un tiers

L'attaquant tire parti d'un accès distant autorisé pour un tiers, tel un sous-traitant. Il peut s'agir d'une connexion de type ADSL ou VPN laissée ouverte, ou uniquement utilisée depuis des adresses IP particulières. Ces accès distants sont souvent autorisés à pénétrer dans le cœur de l'installation industrielle, offrant un point d'entrée « de qualité » à l'assaillant.

3

Détournement d'une liaison sans fil

L'attaquant utilise une vulnérabilité dans les liaisons sans fil utilisées (attaques connues sur WEP ou WPA). Par ce biais, il peut se connecter au réseau de contrôle industriel. Il a alors un accès direct au coeur du système au niveau des stations d'ingénierie, SCADA et des automates.

4

Accès au réseau de terrain de l'installation

L'assaillant dispose pour son attaque d'un accès physique direct au réseau de terrain de l'installation, par exemple en ayant accès à une armoire informatique le long d'un axe de distribution (un pipeline, un égout ou le long d'une conduite). Le réseau de terrain donne un accès direct aux automates qui y sont connectés pour piloter les modules d'entrée/sortie. Cela est particulièrement critiques dans les activités de transport.

5

Installation d'un composant physique étranger permettant de modifier le réseau à distance

Pour tirer parti de son accès physique sans pour autant être contraint à être physiquement sur site en permanence, l'attaquant va installer dans le réseau industriel un module de prise de contrôle à distance : par exemple une carte miniaturisée de type Raspberry Pi avec une batterie et un modem 4G lui permettant une prise de contrôle à distance.

Événement redouté A : vol de propriété intellectuelle

CATÉGORISATION

- **But de l'attaquant :** voler un procédé ou des données industrielles
- **Type d'installation :** process manufacturier (discret), non distribué
- **Impact :** porte atteinte à la confidentialité des données
- **Moyen technique :** téléchargement des programmes des automates de l'installation

DESCRIPTION

Une attaque sur un système de contrôle industriel ayant pour but de voler un procédé ou des données industrielles ayant une valeur pour l'attaquant. **Les motivations de l'attaquant peuvent être de nature :**

- **économique :** voler un secret de fabrication à un concurrent pour pouvoir dupliquer ses produits ou rétroconcevoir son mode de fabrication.
- **patriotique :** voler les plans d'un produit souverain pour le répliquer, comme par exemple un avion ou un produit de défense (ex: frégate, sous-marin).

Le but ultime de l'attaquant est d'exfiltrer les données voulues en s'échappant en toute détection, pour que la cible ne mette pas en place des contre-mesures. Il ne va pas chercher à agir sur le procédé en lui-même, il s'agit uniquement de porter atteinte à la confidentialité du système.

L'attaque se place dans un contexte temporel à long terme : l'attaquant voudra conserver son accès le plus longtemps possible, ou du moins tant qu'il n'a pas réussi à exfiltrer toutes les données recherchées. Si l'attaquant n'a pas d'accès physique direct, il lui sera nécessaire de maintenir une connexion de « contrôle » entre son malware installé sur le réseau de contrôle industriel et son serveur C&C (Command & Control).

DÉROULEMENT

1. Connexion aux automates programmables : extraction des programmes, extraction des variables
2. Extraction depuis les stations de supervision de données sensibles (programmes, synoptiques, consignes, seuil d'alarmes)
3. Exfiltration des programmes des automates depuis les stations d'ingénierie
4. Extraction des informations stockées en base de données (Historian)
5. Enfin, une fois les données acquises, il faut les exfiltrer par Internet ou par média amovible de la façon la plus discrète possible, ce qui peut être compliqué si elles sont volumineuses.

Événement redouté B : sabotage industriel

CATÉGORISATION

- **But de l'attaquant :** modifier furtivement un procédé industriel
- **Type d'installation :** process manufacturier (discret ou continu)
- **Impact :** porte atteinte à l'intégrité du process industriel
- **Moyen technique :** modification du programme d'un ou plusieurs automates, leurre des supervisions SCADA

DESCRIPTION

Ce scénario décrit une atteinte à un système industriel manufacturier qui a pour conséquence le sabotage de l'outil. Les motivations de l'attaquant peuvent relever du cyberterrorisme, être d'ordre concurrentiel ou même d'un acte de guerre entre deux nations.

L'attaquant cherche alors à agir sur le procédé industriel en s'échappant en toute détection, l'exfiltration de données n'est pas un but en soi. Ce scénario vise à modifier de manière persistante et indétectable un processus industriel pour qu'il ne fonctionne plus dans ses conditions nominales et produise des pièces non conformes. **Pour ce faire, l'assaillant va chercher à :**

- obtenir une connaissance la plus détaillée possible du procédé industriel et de son système de contrôle-commande numérique, pour pouvoir le modifier. Il est question ici de données relevant de l'architecture (plans des réseaux, configurations, etc.) mais aussi de données purement industrielles, par exemple des valeurs de pression, de température, de vitesse de rotation, etc. L'attaquant doit se procurer les valeurs nominales de ces données ainsi que les seuils d'alerte associés pour pouvoir les modifier de façon indétectable.
- Une fois qu'il a une vision détaillée du procédé industriel, il peut modifier les programmes de certains automates afin d'agir sur le procédé industriel. Pour éviter que la modification soit apparente, il doit aussi potentiellement prendre le contrôle des stations SCADA pour présenter de fausses informations, ou modifier les seuils d'alarme.

DÉROULEMENT

Ce scénario est en quelque sorte la suite logique du scénario A : il commence par les mêmes étapes d'attaque. La différence se situe sur les étapes supplémentaires qui rendent le scénario beaucoup plus complexe.

Une fois qu'il a mené à bien l'exfiltration des programmes des automates, l'attaquant modifie les programmes et les réinjecte dans les automates pour agir sur le procédé industriel. Il doit au passage s'assurer de faire la modification discrètement, en leurrant si possible la supervision en place.

C'est la trame de l'attaque Stuxnet, qui avait pour but de modifier la vitesse de rotation de centrifugeuses, bien qu'il ne soit pas confirmé si l'attaque a modifié les programmes, ou altéré les couches basses du système d'exploitation (ie. Drivers, OS).

Ici l'attaque vise à modifier le programme chargé directement sur l'automate (ce qui est potentiellement visible), mais on pourrait aussi agir directement sur les valeurs des variables, ou en modifiant des logiciels qui interagissent avec les équipements industriels (dont par exemple le logiciel de supervision).

Événement redouté C : déni de service sur installation industrielle

CATÉGORISATION

- **But de l'attaquant :** provoquer un arrêt de production
- **Type d'installation :** process continu (raffinerie, eau ou gaz) distribué
- **Impact :** porte atteinte à la disponibilité du process industriel
- **Moyen technique :** mise hors service des automates

DESCRIPTION

Ce scénario est plus directement orienté vers le déni de service industriel : **il concerne l'arrêt de production d'une installation industrielle à processus continu,** comme une raffinerie, une usine de traitement de l'eau ou un réseau de distribution de gaz.

L'attaquant va alors prendre le contrôle d'une partie de l'infrastructure pour la rendre inopérante, et éventuellement causer des dommages physiques à l'outil de production afin de compliquer sa remise en service. L'arrêt de production d'une installation de ce type impacte directement tous les utilisateurs qui en dépendent, ce qui peut avoir des conséquences humaines importantes.

Ce type d'installation est aussi souvent distribué : il est réparti géographiquement sur une zone assez large, ce qui offre des possibilités à un attaquant pour une prise de contrôle physique, sans passer par Internet.

DÉROULEMENT

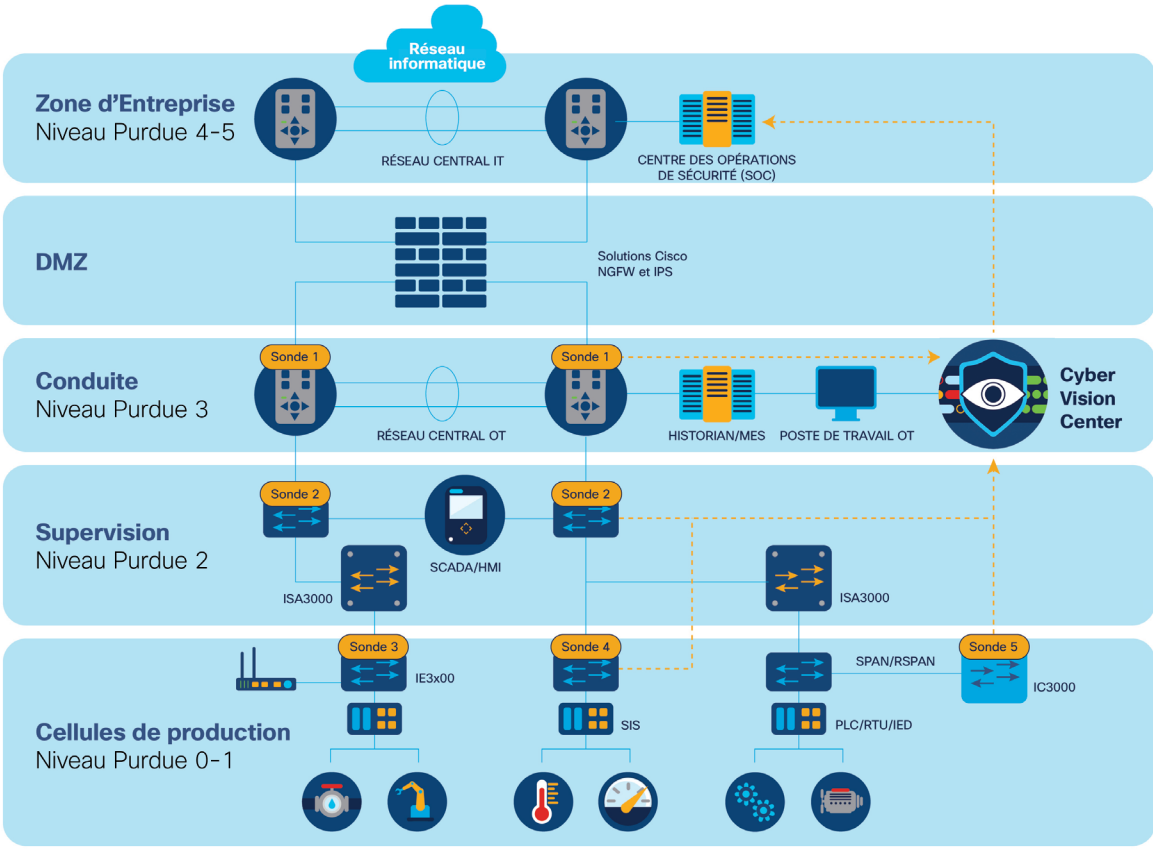
Dans le cadre de ce scénario, le déni de service consiste à la mise hors service de tout ou partie des automates accessibles par l'attaquant. Ce dernier peut utiliser des moyens techniques variables, par exemple :

- **déni de service par saturation réseau :** générer un trafic trop important pour que l'automate ne puisse plus répondre et ne remplisse plus la fonction pour laquelle il a été programmé. Cette technique se rapproche d'un déni de service connu du monde IT.
- **déni de service par reprogrammation :** l'attaquant tire alors parti de son accès direct au réseau de l'installation pour installer un programme non fonctionnel sur les automates.

SYSTÈME DE SURVEILLANCE ET DÉTECTION D'ANOMALIES

Étant donné que les réseaux de contrôle industriels sont géographiquement étendus et constitués d'une agrégation de « petits réseaux » de quelques équipements, le système de détection est très souvent découpé entre :

- des sondes proches du procédé qui vont extraire les données des communications entre les équipements
- un serveur central qui va collecter, analyser et stocker les données recueillies au travers des sondes



Le placement des sondes doit permettre de suivre les différents points d'insertion dans le système industriel :

SONDE 1 : Interconnexion entre le réseau tiers de type IT et le réseau OT (flux historian, statistiques, conduite)

SONDE 2 : Réseau de procédé, entre les automates programmables et les machines Windows (flux supervision et contrôle-commande, station SCADA, ingénierie)

SONDE 3 : Interconnexion sans fil ou télémaintenance (routeur DSL ou MPLS)

SONDE 4 : Contrôle des flux entre les systèmes de pilotage et entre les systèmes de pilotage et les systèmes de sécurité

SONDE 5 : Réseau de terrain physiquement ouvert.

Afin de couvrir les risques énoncés plus haut, le système de détection s'appuie sur les propriétés des composants, sur les messages de contrôle et sur différents marqueurs :

- **Propriétés d'identification :** adresse MAC, ID de protocole, port TCP, port UDP.
- **Propriétés d'inventaire :** fabricant, nom de PLC, nom de projet, version de projet, nom de modèle, version logicielle, version matérielle, numéro de série, emplacement/slot du module, code produit, rôle du composant (SCADA, ingénierie).
- **Contrôle simple des automates / PLC :** téléchargement de programme depuis/vers l'automate, ordre d'arrêt / démarrage, changement des horloges, mise à jour de firmware.
- **Contrôle avancé des automates / PLC :** suivi du contenu des programmes automates, métadonnées des programmes (liste des blocs de programmations, horodatage, taille), données d'authentification (identifiant et mot de passe), changement des bases de données résiduelles, effacement mémoire, passage en mode maintenance, passage en mode diagnostique.
- **Contrôle du procédé :** commande d'écriture et de lecture, liste des variables/registres.
- **Indicateur de compromission :** requêtes DNS faites par les stations industrielles, métadonnées HTTP ou FTP ; ces IoC permettent de détecter les activités d'un serveur « Command & Control » pilotant des malwares installés sur les stations industrielles.

Il est important de comprendre qu'à ce jour, d'un point de vue de la détection, ce sont les commandes dites « Contrôle simple des automates » qui offrent beaucoup de possibilités à l'attaquant et qu'il convient de savoir détecter sur le réseau. En termes de détection, il est nécessaire de savoir comment déceler ces commandes sur le réseau.

Afin d'extraire les informations nécessaires à la surveillance de la cybersécurité du système industriel, la plateforme doit décoder les flux d'applications collectés sur le réseau industriel. **En matière de réseaux de contrôle industriel, il existe plusieurs types de protocoles réseau :**

- les protocoles ouverts, dont la spécification est connue et disponible. Ces protocoles ont été normalisés par des organismes internationaux,
- les extensions propriétaires dans les protocoles ouverts. Ces extensions utilisent une zone de données ouvertes et y intègrent des structures de données propriétaires, non documentées,
- les protocoles propriétaires, dont les spécifications ne sont publiques.

Malheureusement les protocoles de contrôle commande qui permettent d'avoir un impact système (changement de programme ou de paramétrage) sont propriétaires.

CYBERSÉCURITÉ INDUSTRIELLE :

Surveillance et détection des anomalies

DÉMARREZ VOTRE PROJET DE CYBERSÉCURITÉ INDUSTRIELLE

Que vous ayez besoin d'une vision précise de l'inventaire de vos équipements industriels pour pouvoir segmenter votre réseau, ou d'une surveillance en temps réel des flux d'applications ICS pour détecter les intrusions et les comportements anormaux, Cisco® Cyber Vision peut vous aider à tracer votre voie et à étendre vos politiques de cybersécurité au domaine des technologies opérationnelles.

Cisco Cyber Vision a été spécialement conçu pour les organisations industrielles afin d'obtenir une pleine visibilité sur leurs réseaux industriels, afin de garantir l'intégrité des processus, de construire des infrastructures sécurisées, d'assurer la conformité réglementaire et d'appliquer des politiques de sécurité pour contrôler les risques.

Combinant une architecture de surveillance Edge unique et une intégration complète avec les outils de sécurité de Cisco, Cisco Cyber Vision peut être facilement déployé à grande échelle afin que vous puissiez assurer la continuité, la résilience et la sécurité de vos opérations industrielles.

Pour en savoir plus, visitez cisco.com/go/cybervision ou contacter votre représentant Cisco ici.

Cisco-IoT-CyberVision-EB-02202020