Profil de protection d'un logiciel d'historian

Version 1.0 moyen-terme

GTCSI

1er juillet 2015

Avant-propos

Dans toute la suite de ce document, l'acronyme ToE (*Target of Evaluation*) désigne le composant qui est l'objet de l'évaluation.

Les passages en rouge sont ceux qui différent de la version de la cible à court terme.

1 Descriptif du produit

1.1 Descriptif général du produit

La ToE considérée dans ce profil de protection est un serveur d'historique, aussi appelé historian, est une base de données distante qui permet de stocker les différentes alarmes valeurs issues du système de supervision (SCADA) du processus industriel. Le serveur d'historique peut être local ou centralisé.

Un serveur d'historique local est souvent à proximité des équipements industriels dont il enregistre les données. La durée de rétention des informations est souvent limitée mais la granularité est très fine. Ce serveur permet aux opérateurs d'effectuer des analyses approfondies en cas d'incident ou d'anomalie du processus industriel.

Un serveur d'historique centralisé collecte souvent les informations de plusieurs systèmes de supervision (SCADA). La durée de rétention des informations est souvent importante. En contrepartie, la granularité est souvent moins fine que dans le cas du serveur d'historique local. Ce serveur d'historique est généralement utilisé pour des analyses de plus long terme. Il permet à des responsables d'unité ou d'usine d'avoir une vision d'ensemble de leurs installations.

1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

— **Stockage des données :** La ToE doit comporter un système de stockage, typiquement une base de données.

— **Interface avec le système de supervision :** La ToE doit comporter une ou plusieurs interfaces pour communiquer avec le système de supervision et récupérer ainsi les alarmes et valeurs issues du processus industriel.

— **Interface en lecture seule :** La ToE doit comporter une ou plusieurs interfaces pour permettre aux opérateurs d'accéder aux données stockées.

— **Fonctions d'administration :** La ToE comporte une ou plusieurs interfaces pour permettre son administration, notamment la gestion des utilisateurs et de la politique de droits.

— **Fonctions de configuration :** Le serveur comporte une ou plusieurs interfaces permettant d'assurer la mise à jour et le déploiement des données de configuration : données d'entrée/sortie, communication avec les équipements de terrain, conditions d'alarmes.

— **Fonctions de redondance :** La ToE peut permettre un fonctionnement en redondance pour assurer la haute disponibilité d'une ou plusieurs de ses fonctions.

— **Journalisation locale d'évènements :** La ToE permet de définir une politique de journalisation locale d'évènements notamment de sécurité et d'administration.
— **Journalisation distante d'évènements :** La ToE permet de définir une politique de journalisation distante d'évènements notamment de sécurité et d'administration.

1.3 Descriptif de l'utilisation du produit

La ToE sert à collecter des informations qui proviennent typiquement du système de supervision (SCADA) ou du système de gestion de la production (MES). En fonction des situations, la ToE pourra être à proximité des équipements dont il enregistre les données ou bien être plus éloigné.

Dans ce deuxième cas, la ToE peut éventuellement être localisé dans un système industriel de criticité inférieure, au sens du guide de l'ANSSI [1] au système industriel dont il enregistre les données. Si le système industriel monitoré est de classe 2 alors les flux doivent être unidirectionnels et l'unidirectionnalité doit être assurée à l'aide d'un pare-feu comme montré sur la figure 1.3. Si le réseau industriel monitoré est de classe 3 alors l'unidirectionnalité doit être assurée par une diode comme représenté sur la figure 1.3.

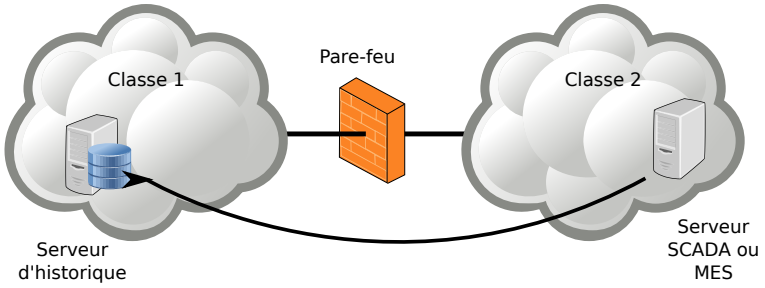

FIGURE 1 – Serveur d'historique derrière un pare-feu

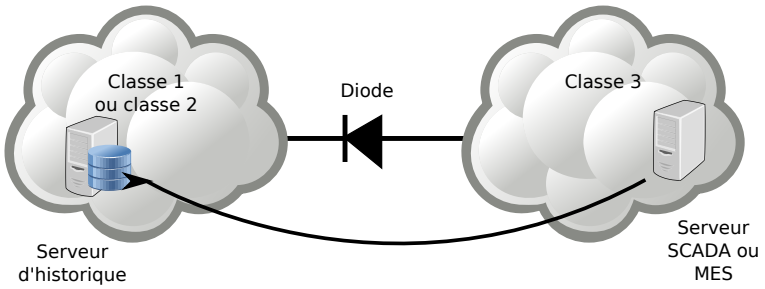

FIGURE 2 – Serveur d'historique derrière une diode

1.4 Descriptif des différents utilisateurs

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :
— **Consommateur :** Cet utilisateur a le droit de consulter une partie des données contenues dans la ToE mais ni de générer, ni de modifier ni de supprimer des informations.
— **Producteur :** Cet utilisateur produit des données qui seront stockées dans la ToE, il a donc le droit d'ajouter des données. En revanche, le producteur ne pourra pas modifier ou supprimer des données déjà existantes.
— **Correcteur :** Cet utilisateur peut ajouter des données dans la ToE mais peut également modifier ou supprimer des données existantes.

1. La cybersécurité des systèmes industriels : Méthode de classification et mesures principales, ANSSI, janvier 2014.

— **Administrateur :** Utilisateur ayant les droits de modifier une partie de la configuration de la ToE. Il ne peut cependant pas modifier les comptes des administrateurs.
— **Auditeur :** Utilisateur ayant le droit de consulter tout ou partie des journaux d'évènements produits par la ToE.
— **Super-administrateur :** Utilisateur ayant tous les droits sur la ToE, pouvant en particulier créer, modifier ou supprimer les comptes des administrateurs.

Note : Un utilisateur n'est pas forcément une personne physique et peut être un équipement ou un programme tiers. Par ailleurs, une même personne physique peut être titulaire de plusieurs comptes avec des profils d'utilisateur différents.

1.5 Hypothèses sur l'environnement

Les hypothèses suivantes sont formulées sur l'environnement et les conditions d'utilisation de la ToE :

— **Consultation des journaux :** Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.
— **Super-administrateurs :** Les super-administrateurs de la ToE sont compétents, formés et non hostiles.
— **Local :** La ToE doit se trouver dans un local sécurisé dont l'accès est restreint à des personnes autorisées considérées comme non hostiles. En particulier, l'attaquant n'aura pas accès aux ports physiques de la ToE.
En revanche, des équipements identiques à la ToE étant disponibles dans le commerce, l'attaquant peut acheter un tel équipement en vue d'y rechercher des vulnérabilités par tous les moyens à sa disposition pour attaquer la ToE.
— **Dimensionnement :** Il est supposé que la ToE est dimensionnée correctement pour les traitements qu'elle doit effectuer.
— **Serveurs d'authentification :** Le cas échéant, les serveurs d'authentification utilisés pour authentifier les utilisateurs sont considérés comme sains et configurés correctement.
— **Système d'exploitation sain :** Le système d'exploitation du système portant la ToE est considéré comme sain au début de l'évaluation et tout au long de l'évaluation sauf en cas de défaillance de la ToE.
— **Système d'exploitation durci :** Le système d'exploitation est supposé avoir été configuré et durci selon les recommandations du fabricant de la ToE.
En particulier, le système d'exploitation est supposé à jour.
— **Services non évalués désactivés par défaut :** L'ensemble des services présents dans la ToE mais hors de la cible de sécurité sont désactivés dans la configuration par défaut (parfois appelée configuration usine).
— **Documentation de securité :** La ToE est fournie avec une documentation détaillée sur l'utilisation sécurisée de l'équipement. En particulier, l'ensemble des secrets de connexion présents par défaut est listé pour permettre leur personnalisation.
L'ensemble des préconisations issues de cette documentation ont été appliquées en vue de l'évaluation.
— **Module externe :** Il supposé qu'aucun module externe [2] n'est installé sur la ToE sauf si celui-ci fait partie du périmètre d'évaluation.
— **Non-adhérence logicielle :** La ToE a été développée de telle sorte à ne pas être adhérente à une version donnée d'un composant externe [3] (système d'exploitation, logiciel, bibliothèque). En particulier, l'utilisateur doit avoir la possibilité d'appliquer les mises à jour de sécurité de tout composant externe.
Dans le cas contraire, ce composant doit être intégré à la ToE.

2. Un module externe est un élément logicel apportant de nouvelles fonctionnalités à la ToE mais qui n'est pas indispensable à son fonctionnement.
3. Un composant externe est un élément logiciel nécessaire au fonctionnement de la ToE.

2 Description des biens sensibles à protéger

2.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :

— **Données archivées :** La ToE doit être capable de stocker de manière intégre et authentifiée l'ensemble des valeurs archivées.

— **Capacité d'historisation :** La ToE doit être capable à tout moment d'appliquer la politique d'historisation définie.

— **Flux d'historisation et de consultation sécurisés :** Les flux entre la ToE et les producteurs, consommateurs ou correcteurs doivent pouvoir être protégés en intégrité et en authenticité.

Les besoins de sécurité pour les biens sensibles de l'environnement sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Données archivées			X	X
Capacité d'historisation	X			
Flux d'historisation et de consultation sécurisés			X	X
X : obligatoire (X) : optionnel				

2.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :

— **Logiciel(s) :** Afin d'assurer correctement ses fonctions, le logiciel doit être protégé en intégrité en toutes circonstances et en authenticité à l'installation ou la mise à jour.

— **Configuration :** La configuration de la ToE doit être confidentielle et intègre. L'attaquant ne doit pas pouvoir découvrir cette configuration autrement que par l'observation de l'activité de la ToE.

— **Mécanisme d'authentification des utilisateurs :** Ce mécanisme peut s'appuyer sur une base de données locale ou sur un connecteur avec un annuaire distant. Dans les deux cas, la ToE doit protéger l'intégrité et l'authenticité du mécanisme [4].

— **Secrets de connexion des utilisateurs :** Il peut s'agir de mots de passe, de certificats, etc. Ils peuvent être contenus dans la ToE ou être échangés avec un serveur distant. Dans tous les cas, la ToE doit garantir l'intégrité et la confidentialité de ces identifiants.

— **Politique de gestion des droits :** Cette politique peut être contenue en local sur la ToE ou être obtenue à partir d'un annuaire distant. Dans les deux cas, la ToE doit garantir l'intégrité de cette politique de gestion des droits.

— **Fonction de journalisation locale :** La ToE dispose d'une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle.

— **Fonction de journalisation distante :** La ToE dispose d'une fonction de journalisation distante qui, une fois configurée, doit rester opérationnelle.

— **Journaux d'évènements locaux :** Les journaux locaux générés par la ToE doivent être intègres.

— **Journaux d'évènements déportés :** Les journaux déportés émis par la ToE doivent être intègres et authentifiés. Un mécanisme doit également permettre au destinataire de détecter l'absence d'un message au sein d'une sequence de messages correctement reçus.

Les besoins de sécurité pour les biens sensibles de la ToE sont les suivants :

4. Tous les mécanismes d'authentification présents dans la ToE ne doivent pas nécessairement être présents dans la cible de sécurité. Néanmoins, il doit y en avoir au moins un et ceux qui ne sont pas inclus doivent être désactivés par défaut.

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Logiciel(s)			X	X
Configuration		X	X	
Mécanisme d'authentification des utilisateurs			X	X
Secrets de connexion des utilisateurs		X	X	
Politique de gestion des droits			X	
Fonction de journalisation locale	X			
Fonction de journalisation distante	X			
Journaux d'évènements locaux			X	X
Journaux d'évènements déportés			X	X
X : obligatoire (X) : optionnel				

3 Description des menaces

3.1 Description des agents menaçants

Les agents menaçants suivants ont été retenus :

— **Utilisateur malveillant :** L'attaquant a réussi à compremettre un compte sans privilèges d'administration et cherche à outrepasser les droits de son compte.

— **Attaquant avec les droits d'administration :** L'attaquant a réussi à compromettre le compte d'un administrateur. Ce compte peut avoir n'importe quel rôle à l'exception du super-administrateur.

— **Attaquant dans le système industriel :** Tout attaquant ayant pris le contrôle d'un composant du système industriel et cherchant à attaquer la ToE.

3.2 Menaces retenues

Les menaces suivantes ont été retenues :

— **Déni de service :** L'attaquant parvient à effectuer un déni de service sur la ToE en effectuant une action imprévue ou en exploitant une vulnérabilité (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu...). Ce déni de service peut concerner toute la ToE ou seulement certaines de ses fonctions.

— **Altération des flux :** L'attaquant parvient à modifier des échanges entre la ToE et un composant externe sans que cela ne soit détecté.

— **Corruption du logiciel :** L'attaquant parvient à modifier, de manière temporaire ou permanente le logiciel de la ToE. L'attaquant réussit à exécuter du code illégitime sur la ToE.

— **Corruption de la configuration :** L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la ToE.

— **Compromission de la configuration :** L'attaquant parvient à récupérer tout ou partie de la configuration de la ToE de manière illégitime.

— **Vol d'identifiants :** L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

— **Contournement de l'authentification :** L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.
— **Contournement de la politique de droits :** L'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus.
— **Corruption des journaux d'évènements locaux :** L'attaque parvient à supprimer ou modifier une entrée dans les journaux d'évènements locaux sans y avoir été autorisé par la politique de droits de la ToE.
— **Corruption des journaux d'évènements déportés :** L'attaquant parvient à modifier une entrée de journal distant émise par la ToE sans que le destinataire ne puisse s'en rendre compte. L'attaquant parvient à supprimer une émission de journalisation distante sans que le destinataire ne puisse s'en rendre compte.

4 Objectifs de sécurité

Les objectifs de sécurité retenus sont les suivants :
— **Gestion des entrées malformées :** La ToE a été développée de manière à gérer correctement les entrées malformées, en particulier en provenance du réseau.
— **Communications sécurisées :** La ToE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.
— **Connexion sécurisée avec le serveur d'authentification :** La ToE permet une connexion sécurisée avec le serveur d'authentification en assurant l'authenticité des deux extrémités, l'intégrité et la confidentialité des échanges, ainsi que le non-rejeu.
— **Stockage sécurisé des secrets :** Les secrets de connexion des utilisateurs sont stockés de manière sécurisée sur la ToE et la compromission d'un fichier ne permet pas de les récupérer.
— **Authentification sécurisée sur l'interface d'administration :** Les jetons de session sont protégés contre le vol et contre le rejeu. Les jetons de session ont une durée de vie limitée. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.
— **Politique de droits :** La politique de gestion des droits est gérée de manière extrêmement stricte. L'implémentation de cette politique permet en particulier de garantir l'authenticité des opérations critiques, c'est-à-dire pouvant porter atteinte aux biens sensibles identifiés.
— **Signature du logiciel :** Un mécanisme de signature est utilisé par la ToE pour permettre la vérification par l'administrateur de l'authenticité et de l'intégrité des composants logiciels lors de leur installation.
— **Intégrité et confidentialité de la configuration :** La politique de gestion des utilisateurs ne permet à une personne non autorisée, ni de consulter, ni de modifier tout ou partie de la configuration de la ToE.
— **Intégrité des journaux :** Les journaux d'événements générés par la ToE sont intégres et seul le super-adminstrateur peut les modifier.
— **Intégrité des journaux déportés :** La ToE permet de transmettre les journaux déportés à un équipement tiers de manière intègre, authentifiée, et sans rejeu des journaux générés avec détection des événements manquants.

A Couverture des biens par les menaces

	Données archivées	Capacité d'historisation	Flux d'historisation et de consultation sécurisés	Logiciel(s)	Configuration	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évènements locaux	Journaux d'évènements déportés
Déni de service		D							D	D		
Altération des flux	I A		I A									
Corruption du logiciel				I A								
Corruption de la configuration					I							
Compromission de la configuration					C							
Vol d'identifiants							C I					
Contournement de l'authentification						I A						
Contournement de la politique de droits	I A							I				
Corruption des journaux d'évènements locaux											I A	

D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité

	Données archivées	Capacité d'historisation	Flux d'historisation et de consultation sécurisés	Logiciel(s)	Configuration	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évènements locaux	Journaux d'évènements déportés
Corruption des journaux d'évènements déportés												I A
D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité												

B Couverture des menaces par les objectifs de sécurité

	Déni de service	Altération des flux	Corruption du logiciel	Corruption de la configuration	Compromission de la configuration	Vol d'identifiants	Contournement de l'authentification	Contournement de la politique de droits	Corruption des journaux d'évènements locaux	Corruption des journaux d'évènements déportés
Gestion des entrées malformées	X									
Communications sécurisées		X								
Connexion sécurisée avec le serveur d'authentification							X			
Stockage sécurisé des secrets						X				
Authentification sécurisée sur l'interface d'administration				X	X	X	X			
Politique de droits								X		
Signature du logiciel			X							
Intégrité et confidentialité de la configuration				X	X					
Intégrité des journaux									X	

	Déni de service	Altération des flux	Corruption du logiciel	Corruption de la configuration	Compromission de la configuration	Vol d'identifiants	Contournement de l'authentification	Contournement de la politique de droits	Corruption des journaux d'évènements locaux	Corruption des journaux d'évènements déportés
Intégrité des journaux déportés										X

C Liste des contributeurs

Ce profil de protection a été rédigé dans le cadre des travaux du groupe de travail sur la cybersécurité des systèmes industriels (GTCSI) sous l'égide de l'ANSSI.

Les sociétés et organismes suivants ont apporté leur concours à la rédaction de ce document :

— Amossys
— ARC Informatique
— Areal
— Codra
— DGA/MI
— EDF
— Gimelec
— Oppida
— Ordinal Software (représentant le club MES)
— RATP
— Schneider Electric
— Siemens
— Sogeti
— Stormshield
— Thales