

Justification technique de la norme de fiabilité CIP-015-1

CIP-015-1 – Cybersécurité – Surveillance de sécurité de réseau interne

Introduction

Ce document présente la justification technique de la norme de fiabilité CIP-015-1 proposée. Il précise aussi, à l'intention des entités responsables, la notion de système de surveillance de sécurité de réseau interne (SSRI) ainsi que l'intention première de l'équipe de rédaction. Le présent document de justification technique n'est pas une norme de fiabilité et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Contexte

Le 19 janvier 2023, la Federal Energy Regulatory Commission (FERC) publiait son Ordonnance 887¹, dans laquelle elle demandait à la NERC d'intégrer aux *normes de fiabilité* portant sur la protection de l'infrastructure essentielle (normes CIP) des exigences SSRI pour tous les *systèmes électroniques BES* à impact élevé ainsi que pour les *systèmes électroniques BES* à impact moyen à *connectivité externe routable (ERC)* du *système de production-transport d'électricité (BES)*. La SSRI permet aux entités responsables de surveiller le trafic à l'intérieur d'une zone de confiance, notamment un *périmètre de sécurité électronique (ESP)*, afin de détecter toute intrusion ou activité malveillante. En particulier, l'Ordonnance 887 demande à la NERC d'élaborer des exigences à intégrer aux *normes de fiabilité* CIP, par ajout ou modification de normes, en fonction de trois objectifs de sécurité². Dans son Ordonnance 887, la FERC demande à la NERC de soumettre ces révisions pour approbation dans un délai de 15 mois suivant la date d'entrée en vigueur de la décision finale, soit le 9 juillet 2024.

Résumé

La surveillance de sécurité de réseau (SSR) recouvre un ensemble de pratiques et de processus mis en œuvre par les organisations pour surveiller et protéger leurs réseaux et systèmes internes contre de

1. *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*. Ordonnance 887, 182 FERC ¶ 61,021 (2023).

2. Toute norme de fiabilité CIP nouvelle ou modifiée doit répondre aux trois objectifs de sécurité suivants : 1) l'impératif pour les entités responsables d'établir des conditions de référence pour le trafic réseau à l'intérieur de leur environnement réseau CIP ; 2) l'impératif pour les entités responsables d'exercer une surveillance afin de détecter les activités, connexions, dispositifs et logiciels non autorisés à l'intérieur de leur environnement réseau CIP ; et 3) l'exigence pour les entités responsables de reconnaître toute activité anormale avec un niveau de confiance élevé par la journalisation du trafic réseau, la conservation de journaux et d'autres données collectées en rapport avec le trafic réseau, et la mise en place des mesures propres à empêcher le plus possible un assaillant d'effacer les traces de ses tactiques, techniques et procédures dans les dispositifs compromis. (*Idem*, page 5.)

potentielles menaces. La SSR nécessite une collecte et une analyse continues de communications réseau, de journaux d'application, de journaux de système d'exploitation, de journaux de dispositif, ainsi que d'autres journaux de sécurité liés à l'infrastructure et aux dispositifs de réseau interne de l'organisation.

La SSRI représente un sous-ensemble de la SSR ; elle concerne spécifiquement la collecte et l'analyse des communications réseau à l'intérieur d'une « zone de confiance », notamment un *ESP*. La SSRI porte sur les réseaux situés à l'intérieur des zones opérationnelles de l'entité responsable. Les entités responsables peuvent avoir recours à des systèmes SSR pour surveiller d'autres réseaux, comme des périmètres Internet d'entreprise, des intranets d'entreprise ou des réseaux de *systèmes de contrôle ou de surveillance des accès électroniques (EACMS)* et de *systèmes de contrôle des accès physiques (PACS)* associés ; toutefois, les présentes exigences s'appliquent uniquement aux communications réseau entre des dispositifs protégés par l'*ESP* de *systèmes électroniques BES* visés.

La norme de fiabilité CIP-015-1 exige des entités responsables qu'elles mettent en œuvre des systèmes et des processus SSRI. Les entités responsables doivent évaluer leurs réseaux situés à l'intérieur des *ESP* et déterminer quels flux de données réseau permettraient le mieux de détecter une activité anormale dans leurs configurations réseau particulières. Les entités responsables devront collecter et analyser les communications réseau anormales dans les réseaux visés, et y répondre adéquatement. Les entités responsables doivent évaluer et faire escalader au besoin les occurrences d'activité anormale en vue d'une enquête plus poussée. Une enquête subséquente pourrait enclencher l'escalade vers un processus de déclaration des *incidents de cybersécurité* et de planification des mesures d'intervention (selon la norme CIP-008) de l'entité responsable, si l'activité anormale sous enquête peut être liée à un *incident de cybersécurité* qui correspond à la définition de ce terme dans le glossaire de la NERC³.

Les entités responsables doivent aussi protéger adéquatement les données de communication réseau collectées par la SSRI afin de les soustraire à toute manipulation non autorisée et de les préserver de manière à faciliter toute enquête. La SSRI se présente comme un processus continu, possiblement itératif, permettant aux entités responsables de détecter, d'atténuer et de faire escalader activement les actions potentiellement menaçantes avant qu'elles ne puissent nuire à l'exploitation fiable du *BES*.

Généralités

Résumé

L'équipe de rédaction a envisagé plusieurs options pour l'intégration des exigences SSRI à la série de normes CIP : notamment l'ajout d'exigences SSRI à une norme existante, ou la création d'une toute nouvelle norme. Elle a principalement appuyé sa décision sur le texte de l'Ordonnance 887, sur les attentes relatives au calendrier ainsi que sur les principes fondamentaux de la SSR exposés dans des

3. [Glossaire de la NERC](#) (en anglais).

ouvrages comme celui de Richard Bejtlich, *The Practice of Network Security Monitoring*⁴ et celui de Chris Sanders et Jason Smith, *Applied Network Security Monitoring*⁵.

Création d'une nouvelle norme CIP-015

Au début du projet 2023-03 – Surveillance de sécurité de réseau interne, l'équipe de rédaction a tenu des discussions sur la possibilité de créer une nouvelle *norme de fiabilité* ou de modifier des *normes de fiabilité* existantes – en particulier les normes CIP-005, *Périmètres de sécurité électronique*, et CIP-007, *Gestion de la sécurité des systèmes*. Après mûre réflexion, l'équipe a conclu que la norme CIP-005 ne convenait pas vraiment, car son thème principal est l'établissement de l'ESP et les communications réseau entrantes et sortantes de l'ESP. En outre, le projet 2016-02 apportait des modifications à la norme CIP-005 afin de l'harmoniser avec le modèle à vérification systématique (Zero Trust).

Quant à la *norme de fiabilité* CIP-007, l'équipe de rédaction a noté certaines similitudes quant à la journalisation et aux alertes (voir l'exigence E4 de la norme CIP-007). Cependant, après la mise en ligne initiale et la réception des commentaires des parties prenantes, il est apparu que l'harmonisation entre la norme CIP-007 et les objectifs de l'équipe n'allait pas de soi. La norme CIP-007 concerne principalement les *systèmes électroniques BES* et les *EACMS*, *PACS* et *actifs électroniques protégés (PCA)* associés qui mettent en œuvre des mesures de sécurité, ce qui ne concorde pas parfaitement avec le thème de la SSRI, puisque l'équipe de rédaction s'intéresse ici aux données transmises à l'intérieur des réseaux contenant des *systèmes électroniques BES*.

Compte tenu des commentaires reçus lors de la mise en ligne initiale, et afin de ménager un maximum de souplesse en vue d'éventuelles modifications, l'équipe de rédaction a décidé de créer une nouvelle *norme de fiabilité*, numérotée CIP-015-1. Cette nouvelle norme servira plus efficacement l'objectif de détection et d'évaluation des activités réseau anormales.

SSRI des réseaux protégés par un ESP de l'entité responsable

Il faut souligner l'influence de l'Ordonnance 887 de la FERC, qui a joué un rôle important dans la rédaction de ces textes. L'Ordonnance 887 emploie spécifiquement le terme « environnement réseau CIP » (*CIP-networked environment*) quant à l'applicabilité aux *systèmes électroniques BES* à impact élevé ainsi qu'aux *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Il est cependant à noter que le sens du terme « environnement réseau CIP » n'est précisé ni dans l'Ordonnance 887, ni dans le glossaire de la NERC. En outre, la prescription de l'Ordonnance 887 ne mentionne pas explicitement les *EACMS* et les *PACS* associés, qui pourraient être situés à l'extérieur de l'ESP.

Dans la version initiale mise en ligne, l'équipe de rédaction avait cherché à préciser dans les exigences SSRI certains types de données réseau, en incluant les *EACMS* et les *PACS* associés aux *systèmes électroniques BES* visés qui sont situés à l'extérieur de l'ESP. Cependant, après mûre réflexion, elle a décidé à l'unanimité de se raviser et d'appliquer les exigences SSRI aux réseaux protégés par les ESP des

4. Bejtlich, Richard. *The Practice of Network Security Monitoring*. No Starch Press, 15 juin 2013.

5. Sanders, C. et J. Smith. *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Syngress Publishing, décembre 2013.

systèmes électroniques BES à impact élevé et des systèmes électroniques BES à impact moyen à connectivité externe routable de l'entité responsable.

Cette réorientation découle de plusieurs facteurs importants. Premièrement, l'ambiguïté liée à l'absence de définition claire du terme « environnement réseau CIP » et à l'absence de précision dans l'Ordonnance 887 quant à l'inclusion ou non des *EACMS* et des *PACS* situés à l'extérieur de l'*ESP*. Deuxièmement, d'après les commentaires reçus lors de la période initiale de consultation, l'interprétation très majoritaire par l'industrie de l'Ordonnance 887 était que les *EACMS* et les *PACS* situés à l'extérieur de l'*ESP* n'étaient pas visés. Enfin, rappelons que la *norme de fiabilité* CIP-002 désigne les *systèmes électroniques BES* comme des systèmes pouvant avoir un effet nuisible sur la fiabilité du *BES* dans un délai de 15 minutes, et que les exigences actuelles de la *norme de fiabilité* CIP-005 couvrent déjà la détection des communications malveillantes avérées ou présumées, en entrée ou en sortie, passant par les *points d'accès électroniques (EAP)* de l'*ESP*. En outre, l'équipe de rédaction reconnaît la validité des commentaires indiquant qu'il est plus avantageux pour la fiabilité du *BES* de se limiter aux flux de données réseau à l'intérieur de l'*ESP*, et que le fait de vouloir inclure les *EACMS* et les *PACS* situés à l'extérieur de l'*ESP* pourrait mener à écarter des solutions à coût abordable pour la protection de la fiabilité. Ainsi, considérant l'ensemble de ces facteurs, l'équipe considère que son approche révisée répond adéquatement aux risques essentiels énoncés dans l'Ordonnance 887 de la FERC en rapport avec le *BES*.

Catégorisation du système

Il convient de se référer aux processus existants de l'entité responsable afin de déterminer si le système SSRI et ses éléments correspondent à des *PCA* ou à des *EACMS*, ou s'ils sont exemptés de l'application de protections autres que celles requises pour la protection de l'*information de système électronique BES (BCSI)*.

Surveillance de sécurité de réseau interne (SSRI)

La SSRI a pour objet de détecter les activités malveillantes. Les technologies de SSRI ont le maximum de pertinence et d'efficacité lorsqu'elles sont conçues en fonction des protocoles de systèmes de commande industrielle (SCI), de manière à détecter les activités réseau susceptibles de nuire à un procédé industriel. La SSRI est habituellement utilisée comme mesure de détection (dans un rôle passif), pour aider à déceler puis à contrer les activités hostiles, plutôt que comme mesure de prévention chargée de bloquer toute activité suspecte. Les systèmes SSRI peuvent être combinés à d'autres mesures de détection, et aussi s'intégrer avec des mesures de prévention, comme la détection et réponse des points terminaux (EDR). En elle-même, la SSRI n'est pas censée bloquer les activités de réseau ou de point terminal, et de nombreux produits courants sont conçus expressément pour exercer une surveillance passive de manière à éliminer presque toute possibilité d'impact négatif sur des systèmes opérationnels. Bien qu'une entité responsable puisse choisir de mettre en place des mesures de prévention active dans un système SSRI ou encore d'avoir un réseau défini par logiciel (*software defined*

network, ou SDN) assurant une telle fonctionnalité, la prévention ne fait pas partie des exigences de la norme de fiabilité CIP-015-1.

Justification de l'exigence E1

Exigence :

Chaque entité responsable doit mettre en œuvre un ou des processus documentés, pour la surveillance de sécurité de réseau interne des réseaux protégés par les *périmètres de sécurité électronique* de ses *systèmes électroniques BES* à impact élevé et de ses *systèmes électroniques BES* à impact moyen à *connectivité externe routable*, permettant d'établir des méthodes pour la détection de toute activité réseau anormale et son évaluation.

Résumé

À maturité, les programmes de surveillance de sécurité ont habituellement une fonctionnalité de surveillance du trafic réseau ; celle-ci offre une couche de visibilité supplémentaire par rapport à l'exploitation des journaux de point terminal et autres journaux de dispositifs. L'exigence E1 demande aux entités responsables de collecter et de surveiller les communications réseau à l'intérieur des environnements *ESP*.

L'exigence E1 et ses alinéas 1.1, 1.2 et 1.3 spécifient que les entités responsables doivent créer un processus documenté pour la collecte et l'analyse du trafic réseau. Ce processus amène à mettre en place un système SSRI et des processus connexes qui seront utilisés par l'entité responsable pour la surveillance réseau.

Justification de l'alinéa 1.1 de l'exigence E1

Alinéa 1.1 de l'exigence E1 : « mettre en œuvre, à partir d'une démarche axée sur les risques, une collecte d'un ou de plusieurs flux de données réseau afin de surveiller l'activité réseau, en spécifiant les connexions, les dispositifs et les communications réseau ; »

Comme l'explique l'ouvrage de Richard Bejtlich, *The Practice of Network Security Monitoring*, la surveillance a le maximum d'efficacité lorsque la collecte se fait à des points stratégiques dans le réseau (chapitre 2) et utilise un éventail de méthodes (chapitres 9 à 11). Dans l'ouvrage *Applied Network Security Monitoring* (Chris Sanders et Jason Smith), un modèle de collecte appelé *Applied Collection Framework* consiste pour les entités responsables à désigner d'abord de larges flux de données, puis à restreindre la collecte aux données jugées les plus avantageuses. L'alinéa 1.1 de l'exigence E1 stipule que l'entité responsable doit déterminer de possibles points de collecte de données dans le réseau, puis restreindre la collecte de données aux flux qui contiennent les données les plus rentables et les plus pertinentes pour la surveillance de la cybersécurité.

Une démarche axée sur les risques permettant d'exclure de la collecte certaines données peut faire appel à toute méthode de priorisation des flux de données, notamment : une analyse des risques, une analyse des impacts, une analyse des techniques malveillantes courantes, etc. En plus de l'analyse des risques, l'entité responsable pourrait évaluer le trafic réseau et exclure certains flux de données afin de réduire la duplication des données réseau collectées, ou encore restreindre la collecte aux données réseau les plus pertinentes pour la cybersécurité, en écartant le trafic réseau de faible valeur comme celui des sauvegardes.

L'équipe de rédaction a jugé qu'il serait déraisonnable d'établir des exigences détaillées et spécifiques couvrant la collecte de données pour la totalité des réseaux et des technologies en usage. C'est pourquoi l'alinéa 1.1 de l'exigence E1 demande aux entités responsables d'évaluer leurs réseaux *ESP* et de désigner, dans chaque *ESP*, un ou plusieurs flux de données réseau pour la SSRI. Ces flux de données sont la source des données sur lesquelles porteront les alinéas 1.2 et 1.3 de l'exigence E1. L'alinéa 1.1 de l'exigence E1 accorde à l'entité responsable la latitude voulue pour sélectionner les flux de données réseau jugés utiles d'après une évaluation par l'entité responsable du risque de cybersécurité dans ses réseaux internes.

Flux de données réseau

Un flux de données réseau est caractérisé par la combinaison d'un point de collecte de données et d'une méthode de collecte. Les méthodes de collecte sont des technologies qui rendent les données réseau visibles pour un système SSRI (voir les exemples ci-après). Dans le contexte de la *norme de fiabilité* CIP-015-1, les points de collecte correspondent aux dispositifs physiques ou virtuels qui déplacent les données dans le réseau : notamment les commutateurs (physiques ou virtuels), les coupe-feu, les routeurs, les interfaces réseau et autres dispositifs semblables.

Points de collecte de données

Les points de collecte de données réseau peuvent correspondre à une réalité physique ou logique. Dans un contexte physique, les points de collecte désignent des dispositifs qui acheminent les données dans et entre les réseaux (commutateurs, routeurs, coupe-feu, etc.). Un point de collecte physique peut aussi être un port réseau ou un câble. Un point de collecte logique peut être un réseau local virtuel (VLAN), un commutateur virtuel, un réseau privé virtuel routé, ou tout concept semblable dans un SDN.

Un exemple de point de collecte est un commutateur (entité physique) utilisant des VLAN (entités logiques) pour la segmentation du réseau. L'entité responsable pourrait établir la connexion à un port physique du commutateur et configurer ce dernier pour diriger une copie du trafic provenant de tous les VLAN, ou de certains d'entre eux, vers un collecteur. L'entité responsable peut désigner un commutateur central comme point de collecte physique idéal, pour ensuite restreindre la collecte en excluant le trafic VLAN jugé de faible valeur pour la surveillance de cybersécurité. Dans un autre exemple, l'entité responsable peut désigner le trafic physique entrant et sortant d'un hôte opérationnel particulier, comme une interface personne-machine (IPM), puis en filtrer le trafic de sauvegarde, de

sorte que les analystes puissent focaliser la surveillance sur les communications au protocole SCI entre l'IPM et d'autres réseaux opérationnels.

Méthodes de collecte de données

Le tableau suivant commente certaines méthodes de collecte de données couramment utilisées.

Méthode	Commentaires
Points d'accès de test (TAP) dans le réseau (dispositifs physiques)	<p>Matériel supplémentaire requis.</p> <p>Scénarios de défaillance de dispositif inconnus chez certains fournisseurs.</p> <p>Interruption de service généralement nécessaire pour le déploiement.</p> <p>Capacité de collecte de 100 % des paquets.</p> <p>Bon choix pour un environnement centralisé.</p> <p>Collecte des communications de couches 2 et 3.</p> <p>ERC probablement non nécessaire.</p>
<p>Ports miroirs</p> <p>Ports SPAN (analyseur de port commuté)</p> <p>Ports miroirs virtuels (dans un hyperviseur)</p>	<p>Peu de matériel requis (l'entité responsable voudra probablement installer quand même des agrégateurs de réseau).</p> <p>Activation sans interruption de service.</p> <p>Degré d'expérience et de soutien variables selon le fournisseur.</p> <p>Bon choix pour un environnement centralisé.</p> <p>Utilisation accrue du processeur pour les commutateurs de couche 2.</p> <p>Perte (minime) de paquets à prévoir.</p> <p>Collecte des communications de couches 2 et 3.</p> <p>La plupart des ports miroirs ou SPAN transmettent les données sans ERC ; le franchissement d'un <i>point d'accès électronique (EAP)</i> peut donc ne pas être nécessaire.</p>

Méthode	Commentaires
Surveillance des flux réseau (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	<p>Pas de coûts de matériel pour le transfert.</p> <p>Bon choix pour un environnement centralisé.</p> <p>Bon choix pour un environnement à faible bande passante.</p> <p>Protocoles exclusifs variant selon le fournisseur.</p> <p>Fonctionnalités de collecte de couche 2 variant selon le fournisseur.</p> <p>Collecte des communications de couche 3.</p> <p>Option possible : échantillonnage de flux (Sampled NetFlow).</p> <p>Données utiles non incluses.</p> <p>Prise en charge possible par les commutateurs, les routeurs et les coupe-feu.</p> <p>ERC probablement nécessaire.</p>
RSPAN (SPAN à distance)	<p>Semblable à la surveillance des flux réseau pour la collecte.</p> <p>Besoin d'une plus large bande passante.</p> <p>Collecte du trafic de couche 2.</p> <p>Données utiles incluses.</p> <p>ERC probablement nécessaire.</p>
Déploiement et gestion de capteurs	<p>Dispositifs TAP ou ports miroirs ou SPAN habituellement nécessaires.</p> <p>Technologie externe de collecte de données nécessaire pour la plupart des capteurs.</p> <p>Besoin de matériel coûteux.</p> <p>Déploiement assez rapide dans un environnement centralisé.</p> <p>Coût élevé dans un environnement décentralisé.</p> <p>Coût de gestion des capteurs possiblement élevé.</p>
Réseaux définis par logiciel (SDN)	<p>Fonctionnalité d'administration centralisée souvent intégrée.</p> <p>Capacité de bloquer le trafic non autorisé sur la couche 2.</p> <p>Technologie prometteuse, mais non largement déployée.</p>
Bump-in-the-wire (BITW)	<p>Certains systèmes, comme les coupe-feu, ont une capacité de surveillance des données réseau semblable à celle des TAP.</p>
Agents de point terminal	<p>Certains systèmes permettent la collecte de données réseau au moyen d'un logiciel de point terminal.</p>
Autres technologies	<p>Il existe d'autres technologies qu'on peut utiliser pour assurer la visibilité des données réseau.</p>

Critères de sélection des flux de données réseau

Les critères présentés ci-après pourront guider la sélection des flux de données réseau en vue de la collecte de données.

Analyse des moyens malveillants

L'entité responsable pourrait passer en revue les différentes tactiques, techniques et procédures malveillantes utilisées dans des attaques antérieurement documentées. Cette analyse pourrait aider à déterminer les flux de données réseau associées à des cas d'utilisation précis.

Protocoles de système de commande industrielle (SCI)

Les flux de données réseau, ainsi que les outils d'analyse utilisés pour la SSRI, devraient être évalués quant à la possibilité de traitement et d'analyse des protocoles spécifiques aux SCI.

Types de données

La méthodologie ATT&CK de la société MITRE décrit trois sources de données de trafic réseau qui conviennent pour la SSRI :

1. création de contenu réseau ;
2. contenu du trafic réseau ;
3. flux de trafic réseau.

Dans sa sélection de flux de données réseau, l'entité responsable peut aussi restreindre la collecte aux types de données qui correspondent à des cas d'utilisation ou à des détections spécifiques.

Duplication de trafic

La collecte de données réseau peut entraîner une duplication des données lorsque celles-ci sont collectées à partir de plusieurs commutateurs. Dans certaines topologies de réseau, un même paquet Ethernet pourrait être collecté plusieurs fois par le système SSRI. Une telle surcollecte entraîne un gaspillage de ressources et dégrade la performance du système SSRI, et il convient de s'en préoccuper lorsqu'on sélectionne les flux de données réseau. Le critère de duplication de trafic peut contribuer à justifier la stratégie d'inclusion ou d'exclusion des flux de données réseau pour la collecte.

Systèmes de surveillance complémentaires

Souvent, l'entité responsable dispose déjà de systèmes de gestion de l'information des événements de sécurité (GIES) capables de détecter diverses tactiques d'attaque (reconnaissance, accès initial, exécution, persistance, évocation des défenses, accès aux identifiants, découverte, mouvement latéral, collecte, commande et contrôle, exfiltration, etc.). La prise en compte des moyens de détection d'autres systèmes déjà en place permet de restreindre la collecte des flux de données réseau.

Les entités responsables équipées de systèmes matures pour la collecte et la détection des points terminaux qui assurent notamment la journalisation de la mémoire et des processus peuvent invoquer cette fonctionnalité pour justifier l'inclusion ou l'exclusion des flux de données réseau.

Une entité responsable peut choisir d'inclure des journaux de coupe-feu pour étoffer la collecte de données SSRI.

Coordination de la collecte et de la surveillance avec l'exploitation

Des changements opérationnels pourraient nécessiter une suspension momentanée ou prolongée de la collecte par le système SSRI à certains emplacements. La capacité d'activer ou de désactiver les alertes en coordination avec les activités d'exploitation est un signe de maturité pour un système SSRI et, selon l'avis de l'équipe de rédaction, ne constitue pas un motif de non-conformité avec les alinéas 1.2 ou 1.3 de l'exigence E1. Par exemple, pendant la maintenance de turbines ou la mise à niveau d'un système de commande dans une centrale, l'entité responsable pourrait désactiver une partie ou la totalité des composants et des alertes du système SSRI afin d'éliminer les fausses notifications résultant des activités de maintenance.

Les événements climatiques, les pannes de réseau et diverses perturbations opérationnelles peuvent entraîner un nombre important d'alertes dans certains systèmes SSRI. La désactivation des alarmes ou de la collecte de données peut être justifiée dans certaines situations, même s'il ne s'agit pas de *circonstances CIP exceptionnelles*.

Limitations à la collecte

Les limitations connues et prévisibles des systèmes SSRI sont notamment les suivantes :

1. une capacité limitée d'analyse du trafic chiffré ;
2. un nombre élevé de fausses alertes pendant la période d'ajustement du système ;
3. un volume de trafic réseau trop abondant pour la technologie d'analyse SSRI. Dans certaines situations, la visibilité du trafic réseau s'en trouve amoindrie ; il s'ensuit de courtes périodes de visibilité réduite, ce qui est considéré comme une limitation connue des systèmes SSRI. L'équipe de rédaction est d'avis que ces situations somme toute courantes ne justifieraient pas un constat de non-conformité, surtout si d'autres moyens de surveillance de cybersécurité sont en place.

Réseaux partenaires

Les *exploitants de réseau de transport* ont des liaisons avec des réseaux partenaires pour l'échange de données ICCP (Inter-Control Center Communications Protocol). De leur côté, certains *exploitants d'installation de production* ont des liaisons avec des partenaires externes pour leurs systèmes de surveillance des turbines. Les communications dans les deux sens avec des réseaux partenaires transitent fréquemment par un *EAP* et sont visibles dans les réseaux *ESP*. La collecte des flux de données échangés avec ces partenaires présente une valeur élevée pour les systèmes SSRI.

Résilience

Bien que la collecte des données dans les dispositifs existants par le système SSRI nécessite habituellement un certain degré de recours à des ressources additionnelles, il convient de prendre en compte les modes de défaillance des dispositifs de collecte. Par exemple, certains systèmes de commande peuvent comporter de petits réseaux reliés directement à un *EAP*, à un routeur ou à un coupe-feu, sans passer par un commutateur. Si la collecte du trafic SSRI sur la couche 2 nécessite l'ajout d'un commutateur en l'absence d'un tel dispositif, ou si un très faible trafic de couche 2 est visible, une stratégie mieux ciblée pourrait consister à exploiter les journaux de coupe-feu ou à collecter les données réseau plus en amont, plutôt que de créer des points de défaillance supplémentaires dans le système

SCI. L'alinéa 1.1 de l'exigence E1 autorise un large éventail de moyens de collecte de données, y compris des dispositifs TAP, les données sur les flux réseau et d'autres méthodes qui n'affaiblissent pas la fiabilité du SCI.

Réseautique définie par logiciel (SDN)

L'utilisation de technologies modernes, comme la SDN, peut permettre d'obtenir des données pertinentes dans le cadre d'un système de collecte de données SSRI.

Filtrage des données

Un système de collecte SSRI bien ciblé assure le filtrage ou l'élimination du trafic ayant une faible valeur de cybersécurité (sauvegardes, réplication, migration de machine virtuelle, réseau de stockage virtuel, protocoles de stockage réseau, contenus vidéo, trafic chiffré, etc.).

Le filtrage de ces types de données améliore la capacité du système SSRI d'analyser le trafic, et entraîne généralement un meilleur rapport signal/bruit et une meilleure performance de détection.

Types de données non visés par la norme

L'alinéa 1.1 de l'exigence E1 n'impose pas la collecte de certains types de données, notamment :

- les communications série ;
- les circuits de 4-20 mA ;
- les circuits de réseau étendu, comme les circuits MPLS (commutation multiprotocole par étiquette) (bien que le protocole MPLS et les technologies semblables puissent être un moyen efficace de collecter des données SSRI, ce qui est permis).

Contraintes liées aux fournisseurs et aux fonctionnalités de leurs systèmes

Dans le passé, certains fournisseurs de SCI ont indiqué que leurs systèmes ne prennent pas en charge la surveillance de cybersécurité, que ce soit par collecte de données SSRI ou par collecte des journaux de point terminal. Plutôt que d'ajouter une exclusion comme « selon les fonctionnalités du système », l'alinéa 1.1 de l'exigence E1 accorde une grande latitude à chaque entité responsable pour déterminer les flux de données réseau SSRI appropriés pour ses réseaux *ESP*.

Certains réseaux peuvent ne pas avoir de fonctionnalité ou de capacité pour fournir des données de surveillance réseau à un système SSRI. Dans un tel cas, l'entité responsable dispose de diverses solutions de rechange, notamment :

- la mise en place d'une telle fonctionnalité par mise à niveau matérielle ou logicielle ;
- l'installation de dispositifs TAP pour la collecte des données réseau ;
- la collecte de données sur les flux ;
- la collecte de flux de données à partir d'autres réseaux internes adjacents à un réseau dépourvu de fonctionnalités ou de capacités modernes ;

- en complément des flux de données réseau, la collecte d'autres flux de données pertinents, comme des journaux de point terminal ou de coupe-feu ;
- la sélection des flux de données réseau ayant la valeur la plus élevée à partir de ports réseau judicieusement ciblés, de telle sorte que le système n'éprouve pas de problèmes de capacité découlant de la surveillance de la totalité des ports d'un dispositif donné.

Il est à noter que dans le cas des *ESP* pour *systèmes électroniques BES* à impact élevé ou moyen, il serait nettement plus probable que l'entité responsable choisisse des options qui donnent accès à des flux de données réseau, notamment une mise à niveau matérielle. Les critères qui guident le choix de l'emplacement des ports de surveillance sont exposés au chapitre 2 de l'ouvrage *The Practice of Network Security Monitoring*⁶.

Architecture de référence

Un exemple d'architecture de référence pour la collecte de données SSRI est présenté ci-dessous. Ce schéma vise à illustrer une grande variété de méthodes de collecte possibles. Il ne s'agit pas pour les entités responsables de mettre en place toutes ces solutions, mais plutôt de sélectionner et de collecter les flux de données réseau jugés les plus avantageux, d'après la démarche axée sur les risques spécifiée à l'alinéa 1.1 de l'exigence E1.

6. Bejtlich, Richard. *The Practice of Network Security Monitoring*. No Starch Press, 15 juin 2013.

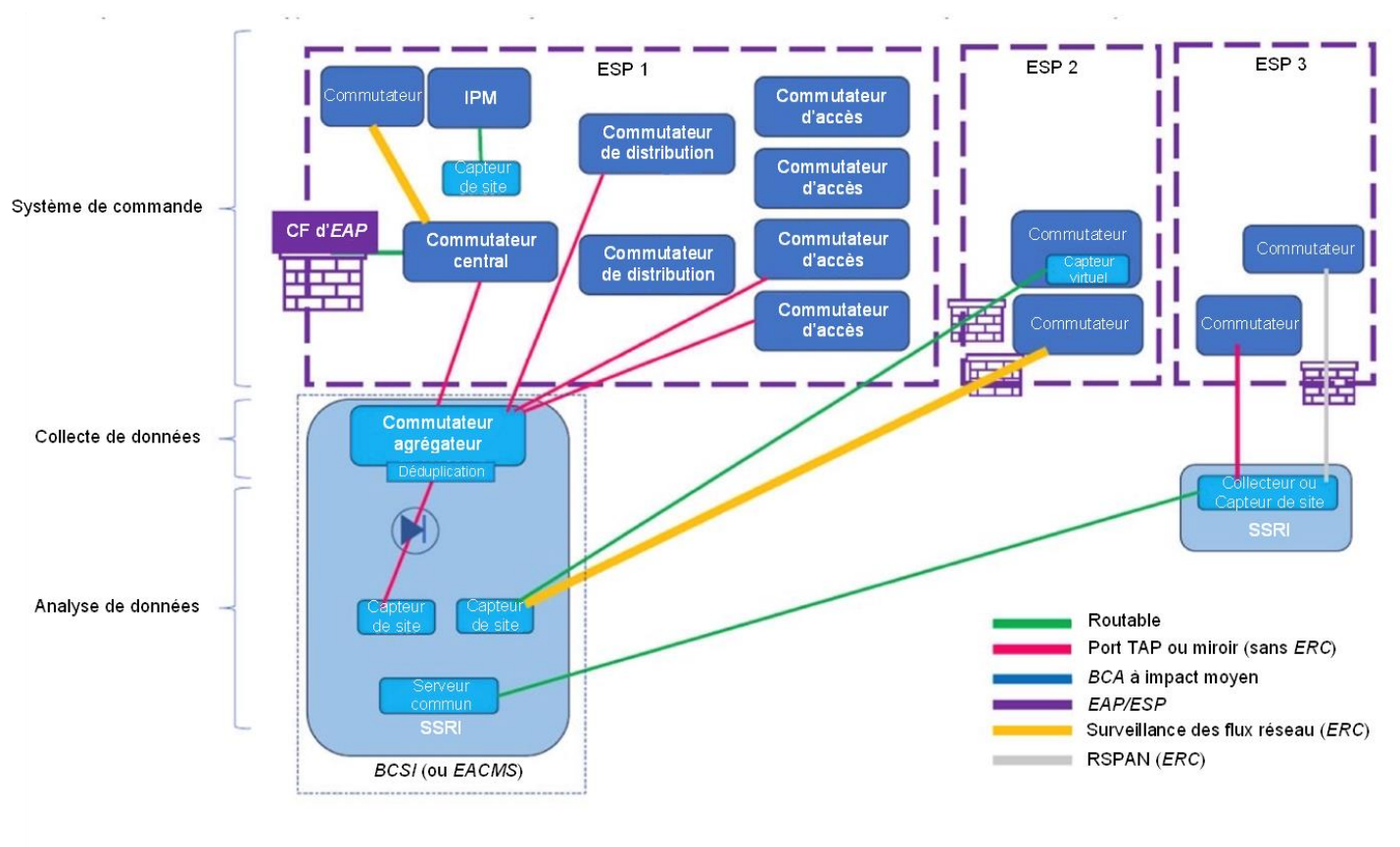


Figure 1

L'architecture de référence de la Figure 1 présente les caractéristiques suivantes :

ESP 1

- Le niveau de la collecte de données est indépendant de celui de l'analyse, ce qui permet d'éviter la dépendance envers un fournisseur unique.
- Le niveau de la collecte de données n'est pas relié aux systèmes applicables par ERC, ce qui assure une visibilité à très faible risque.
- Des ports miroirs sont situés aux endroits appropriés pour collecter les données.
- Une diode réseau (facultative) est insérée entre le niveau de l'analyse et celui de la collecte afin d'assurer une très forte segmentation.

ESP 2

- Un capteur virtuel est installé dans un commutateur sous la forme d'une machine virtuelle.
- Les données sur les flux réseau sont envoyées ailleurs pour analyse.

ESP 3

- Le SPAN distant (RSPAN) est configuré pour transmettre les données sur une liaison à bande passante élevée.
- Un port TAP ou SPAN réseau transmet les données à un dispositif de collecte de données local.

Technologies émergentes

Dans son Ordonnance 887, la FERC demande aussi à la NERC que les *normes de fiabilité* nouvelles ou modifiées à élaborer soient ouvertes sur l'avenir. En conséquence, l'équipe de rédaction s'est efforcée de rédiger des exigences qui présentent aux entités responsables des objectifs à satisfaire, sans spécifier les technologies ou les méthodes à utiliser à cette fin. Le paysage technologique actuel compte divers fournisseurs qui, dans bien des cas, ont élaboré des méthodes exclusives pour détecter des comportements réseau anormaux. Au fur et à mesure des avancées technologiques, de nouveaux produits de détection d'anomalies seront commercialisés, et l'équipe de rédaction veut éviter de restreindre les choix technologiques des entités responsables. Le but visé est que les entités responsables soient en mesure de détecter les activités malveillantes dans leurs réseaux *ESP*. Les alinéas 1.2 et 1.3 de l'exigence E1 portent sur le choix, par chaque entité responsable, des méthodes utilisées pour la collecte de données et la détection des anomalies.

Justification de l'alinéa 1.2 de l'exigence E1

Alinéa 1.2 de l'exigence E1 : « mettre en œuvre une ou des méthodes pour détecter toute activité réseau anormale, à partir des flux de données réseau spécifiés à l'alinéa 1.1 ; »

Résumé

La conformité avec l'alinéa 1.2 de l'exigence E1 nécessite en principe plusieurs étapes. La détection d'une activité réseau anormale comprend le traitement des données collectées, l'analyse de ces données au moyen d'une ou de plusieurs techniques d'analyse, puis l'envoi de notifications concernant le trafic ou les événements d'intérêt en vue d'une évaluation selon l'alinéa 1.3 de l'exigence E1.

« Anormal »

Tel qu'il est utilisé dans le présent document ainsi que dans l'exigence E1 et son alinéa 1.2, le mot « anormal » désigne un trafic réseau imprévu, intempestif, inhabituel ou indéterminé. Sauf indication particulière, l'utilisation des mots « anormal » et « anomalie » dans le présent document et dans la *norme de fiabilité* CIP-015-1 ne fait référence à aucune technologie exclusive dite de « détection d'anomalies. » Un trafic anormal n'indique pas nécessairement une activité malveillante dans un réseau ; toutefois, après une analyse et compte tenu du contexte tiré de données de journalisation et autres, l'entité responsable pourra caractériser le trafic analysé comme bénin, suspect ou autre qualificatif semblable à l'étape de l'alinéa 1.3 de l'exigence E1. Le processus de repérage, dans le trafic réseau, de certaines données réseau à soumettre à une évaluation est illustré à la Figure 2.

L'alinéa 1.1 demande aux entités de mettre en œuvre, à partir d'une démarche axée sur les risques, une collecte d'un ou de plusieurs flux de données réseau afin de surveiller l'activité réseau, en spécifiant les connexions, les dispositifs et les communications réseau.

L'alinéa 1.2 demande aux entités de détecter toute activité réseau anormale.

L'exigence E2 demande aux entités de protéger les données collectées contre toute suppression ou modification non autorisée.

L'exigence E3 demande aux entités de conserver les données relatives à une activité anormale en vue d'une évaluation selon l'alinéa 1.3, et pour répondre éventuellement aux exigences de la norme CIP-008 si l'activité anormale est liée à un incident de cybersécurité ou à une tentative de compromission.

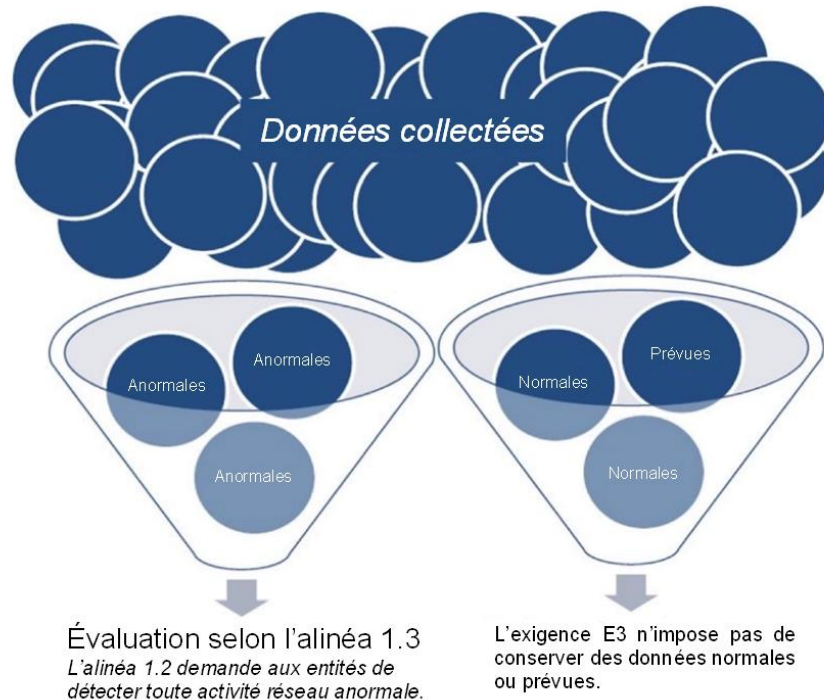


Figure 2

Méthodes de détection

Détection d'anomalies (terme en usage chez les fournisseurs pour désigner diverses technologies spécifiques)

Bien des fournisseurs utilisent le terme « détection d'anomalies » pour désigner une technologie ou des algorithmes spécifiques utilisés par leur logiciel pour établir une représentation du trafic normal prévisible dans le réseau de l'entité responsable ; cette représentation devient la « référence » de comportement prévu du réseau. Par la suite, le trafic collecté est comparé à cette référence, et les structures de trafic qui présentent une déviation statistique par rapport au trafic de référence sont signalés. La détection d'anomalies peut aussi être désignée par d'autres termes ; on parle parfois de « modélisation ». Certains outils de détection d'anomalies font appel à des algorithmes d'apprentissage machine ou à d'autres technologies pour réduire le nombre de notifications.

Sans égard à l'algorithme ou à la terminologie du fournisseur, un système SSRI comportant une fonctionnalité de détection d'anomalies est une méthode valide pour la conformité avec l'alinéa 1.2 de l'exigence E1.

Détection par signature

La détection par signature est une technique utilisée par les systèmes de détection d'intrusion, les fonctions d'inspection poussée des paquets et autres outils apparentés. Ces outils et techniques ont un long historique et ont atteint un haut niveau de maturité.

Lorsqu'on évalue des méthodes de détection par signature en vue de la mise en conformité avec l'alinéa 1.2 de l'exigence E1, il convient de porter attention aux signatures associées aux protocoles SCI à traiter, et au besoin de conserver les données selon l'exigence E2.

Détection comportementale

Certains comportements réseau sont détectés aisément par les systèmes SSRI. Par exemple, la découverte d'information de système distant (*remote system information discovery*)⁷ est une technique qui permet d'obtenir des renseignements détaillés sur un système distant. Les systèmes SSRI sont souvent en mesure de détecter de telles activités, surtout si elles ont été repérées lors d'attaques de SCI antérieures.

Recherche d'indicateurs de compromission (IdC)

Après la détection d'un auteur de menace, il est d'usage que l'équipe d'intervention diffuse les IdC pertinents dans le cadre d'un programme de mise en commun de l'industrie. Les outils SSRI ont souvent la capacité de scruter l'historique de trafic réseau ainsi que certains éléments de trafic comme des fichiers extraits afin de détecter des activités semblables dans l'environnement du réseau analysé.

Contrôles de configuration

Les systèmes SSRI offrent souvent des fonctions qui analysent certains protocoles afin de détecter une mauvaise utilisation ou une configuration incorrecte du protocole. Par exemple, un système SSRI pourrait analyser les messages DNS (système de noms de domaine), les chaînes d'agent utilisateur ou les certificats x.509 à la recherche d'activités suspectes. Lorsqu'on évalue une méthode de contrôle de configuration, porter une attention particulière aux protocoles comme Modbus, DNP3, EGD, ICCP et autres protocoles SCI utilisés dans le SCI surveillé.

Combinaison de diverses méthodes

Certains systèmes SSRI combinent plusieurs des méthodes décrites précédemment pour détecter tout trafic malveillant.

Autres méthodes

Au moment de publier le présent document, on peut recenser de nombreuses méthodes acceptables pour détecter une activité réseau anormale, notamment :

- la détection des lacunes d'hygiène (analyse de protocole, analyse de certificat, détection de chiffrement faible, utilisation de protocoles vulnérables connus comme SMBv1 et NTLMv1, détection de serveurs DNS non autorisés, etc.) ;

7. <https://attack.mitre.org/techniques/T0888/>

- la détection comportementale (délais de connexion inhabituels, erreurs de protocole, volume ou données utiles de protocole imprévus, etc.) ;
- diverses méthodes de détection exclusives.

Le présent document ne saurait présenter une liste exhaustive de toutes les méthodes de détection possibles. Il revient à l'entité responsable d'adopter des méthodes de détection qui, dans le cadre général du programme SSRI, fourniront aux analystes les données nécessaires pour détecter les activités anormales avec un haut niveau de confiance.

Ajustements

Les systèmes de détection de cybersécurité, y compris les systèmes SSRI, nécessitent un ajustement permanent des notifications et des alertes. Ce processus d'ajustement pourrait faire en sorte que des notifications et des alertes soient supprimées ou ignorées pendant des opérations de maintenance ou pendant l'ajustement des signatures visant à améliorer le rapport signal/bruit. Cette activité normale d'ajustement fait partie intégrante d'un programme SSRI à maturité.

Justification de l'alinéa 1.3 de l'exigence E1

Alinéa 1.3 de l'exigence E1 : « mettre en œuvre une ou des méthodes permettant d'évaluer toute activité réseau anormale détectée selon l'alinéa 1.2 afin de déterminer les mesures à prendre. »

L'évaluation des activités détectées selon l'alinéa 1.2 de l'exigence E1 correspond à l'étape d'« analyse » décrite dans l'ouvrage de Bejtlich⁸. L'analyse des données fait partie intégrante des opérations de cybersécurité.

Évaluation

L'évaluation d'une activité anormale détectée consiste à suivre les étapes d'une procédure d'analyse préétablie, à consulter le personnel d'exploitation ou à effectuer des démarches semblables documentées par une entité responsable dans le cadre de son ou ses processus SSRI établis selon l'exigence E1.

Actions potentielles

Le processus d'évaluation peut entraîner, notamment :

- une procédure d'escalade, suivant le plan d'intervention en cas d'*incident de cybersécurité* de l'entité responsable (conformément à la *norme de fiabilité* CIP-008) ;
- la décision de ne rien faire ;
- une enquête plus approfondie ;
- des ajustements au système SSRI visant à réduire les fausses notifications ou à modifier le niveau de gravité ;

8. Bejtlich, Richard. *The Practice of Network Security Monitoring* (chapitres 3 à 8). No Starch Press, 15 juin 2013.

- toute autre action, selon l'évaluation de l'entité responsable.

Justification de l'exigence E2

Exigence E2 : « Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés en vue de conserver les données de surveillance de sécurité de réseau interne associées à une activité réseau jugée anormale par l'entité responsable, au moins jusqu'à ce que les mesures pertinentes prévues à l'alinéa 1.3 de l'exigence E1 aient été prises. »

Remarque : L'entité responsable n'est pas tenue de conserver des données de surveillance de sécurité de réseau interne qui ne sont pas pertinentes à une activité réseau anormale détectée selon l'alinéa 1.2 de l'exigence E1.

L'exigence E2 laisse à l'entité responsable le soin de choisir quelles données et quels types de données celle-ci peut rejeter rapidement, quels types de données doivent être stockés pendant une courte période, et quels types doivent l'être plus longtemps. Le processus de conservation des données de l'entité responsable devra spécifier des durées de conservation plus longues pour les données ayant une valeur de cybersécurité plus élevée ; quant aux données dont la valeur de cybersécurité est faible, elles seront conservées moins longtemps, voire pas du tout. Quel que soit le processus mis en place pour la conservation des données, il doit viser à conserver les données susceptibles d'alimenter l'analyse spécifiée à l'alinéa 1.3 de l'exigence E1, et à produire les pièces justificatives nécessaires pour répondre à l'exigence E2 de la norme CIP-008-6 quant à la conservation des données liées à un *incident de cybersécurité* avéré ou à une tentative de compromission.

L'exemple de tableau de conservation des données suivant résume les points à prendre en compte.

Type de données de communications réseau	Valeur de cybersécurité en fonction du temps	Coût de conservation	Durée de conservation ou nombre d'événements à conserver
Trafic réseau : Capture de paquets (PCAP) intégrale (données utiles) ; enregistrement de toutes ou de la plupart des données dans le réseau	La valeur diminue rapidement avec le temps Les données utiles chiffrées ont une faible valeur de conservation	Élevé	À déterminer par l'entité responsable
PCAP ciblée (données utiles) dans le cadre d'une analyse ou d'une enquête PCAP ciblée (données utiles) en lien avec une alerte, une notification ou tout autre événement d'intérêt Enregistrements de trafic réseau conservés dans le cadre d'une analyse ou d'une enquête	La valeur diminue lentement avec le temps	Faible	À déterminer par l'entité responsable
Métadonnées de réseau : Données de connexion au réseau obtenues par PCAP Données sur les flux réseau Information de connexion et de session	La valeur diminue lentement avec le temps	Faible	À déterminer par l'entité responsable
Extractions à partir de fichiers PCAP	Valeur élevée pour les fichiers malveillants ; valeur quasi nulle pour les autres fichiers	Moyen	À déterminer par l'entité responsable
Hachages d'extractions à partir de fichiers PCAP	Valeur élevée maintenue dans le temps	Faible	À déterminer par l'entité responsable

La conservation des données est normalement spécifiée d'après le nombre d'événements ou d'enregistrements de communications réseau stockés dans le système SSRI, ou selon le nombre de jours

de conservation des données. L'entité responsable pourrait choisir d'augmenter temporairement le volume de collecte de données, ce qui pourrait nécessiter une réduction du volume de données conservées dans le système SSRI.

Justification de l'exigence E3

Exigence E3 : « Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés visant à protéger les données de surveillance de sécurité de réseau interne collectées aux fins de l'exigence E1, ainsi que les données conservées aux fins de l'exigence E2, contre les risques de modification ou de suppression non autorisée. »

Une technique malveillante très répandue est la « suppression d'indicateur » (T1070⁹). L'exigence E3 a pour objet de protéger les données SSRI collectées contre toute modification ou suppression par un attaquant.

La conformité avec cette exigence nécessite notamment des mesures de protection et de détection. Voici quelques exemples de mesures qu'on peut envisager pour préserver les données SSRI :

- restreindre au personnel autorisé l'accès électronique et physique au système SSRI ;
- incorporer au système SSRI des mécanismes qui garantissent l'intégrité des données stockées ;
- confiner le système SSRI dans un réseau isolé par rapport au *système électronique BES* surveillé ;
- établir pour les mécanismes d'authentification et d'autorisation utilisés pour le système SSRI un degré de rigueur plus élevé que pour les systèmes d'authentification généraux de l'entreprise, ou encore les dissocier de ces systèmes ;
- établir une authentification à deux facteurs pour l'accès au système SSRI ;
- adopter d'autres méthodes communément acceptées pour préserver les données journalisées.

Considérations supplémentaires

Partage d'information

Il est à noter que rien, dans la *norme de fiabilité* CIP-015-1, y compris son exigence E3, ne vise à limiter le partage d'information. L'exigence E3 concerne uniquement la disponibilité et l'intégrité des données. Le partage d'indicateurs de compromission, de renseignements sur les menaces, ainsi que de diverses informations pertinentes sur les tactiques, techniques et procédures malveillantes, fait partie d'un programme de cybersécurité bien rodé. Les organismes gouvernementaux invitent d'ailleurs les entités responsables à mettre en commun les informations collectées par leurs systèmes SSRI (voir le guide SP 800-150 du NIST-150¹⁰, le guide de partage d'information de la CISA¹¹, et la *Cybersecurity Information*

9. <https://attack.mitre.org/techniques/T1070/>

10. <https://csrc.nist.gov/pubs/sp/800/150/final>

11. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing>

*Sharing Act of 2015*¹²). Le guide de l'ERO sur les pratiques de surveillance de la conformité et d'application des normes (CMEP), intitulé *Network Monitoring Sensors, Centralized Collectors, and Information Sharing*¹³ indique que le processus spécifié à l'alinéa 1.2 de l'exigence E1 de la norme CIP-011 « devra encadrer la manière dont l'entité responsable gère la transmission des BCSI aux tiers fournisseurs et autres destinataires. » Après la mise en place du système SSRI, il y aurait lieu pour l'entité responsable d'examiner le processus en question afin de s'assurer qu'il précise les modalités de partage des données SSRI avec les tiers fournisseurs, les organismes gouvernementaux (y compris la CISA et les services policiers) et les organismes de partage et d'analyse d'information comme l'E-ISAC, conformément au guide CMEP précité.

12. <https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance>

13. <https://www.nerc.com/pa/comp/guidance/CMEPPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf> (voir page 8)

Annexe 1 – Exemple de sélection de flux de données réseau

L'annexe 1 expose un certain nombre de facteurs que l'entité responsable pourrait vouloir prendre en compte pour déterminer quels flux de données réseau seront sélectionnés fins de l'alinéa 1.1 de l'exigence E1.

Le tableau ci-dessous fait référence au schéma simplifié de la Figure 3, qui représente un réseau à impact élevé.

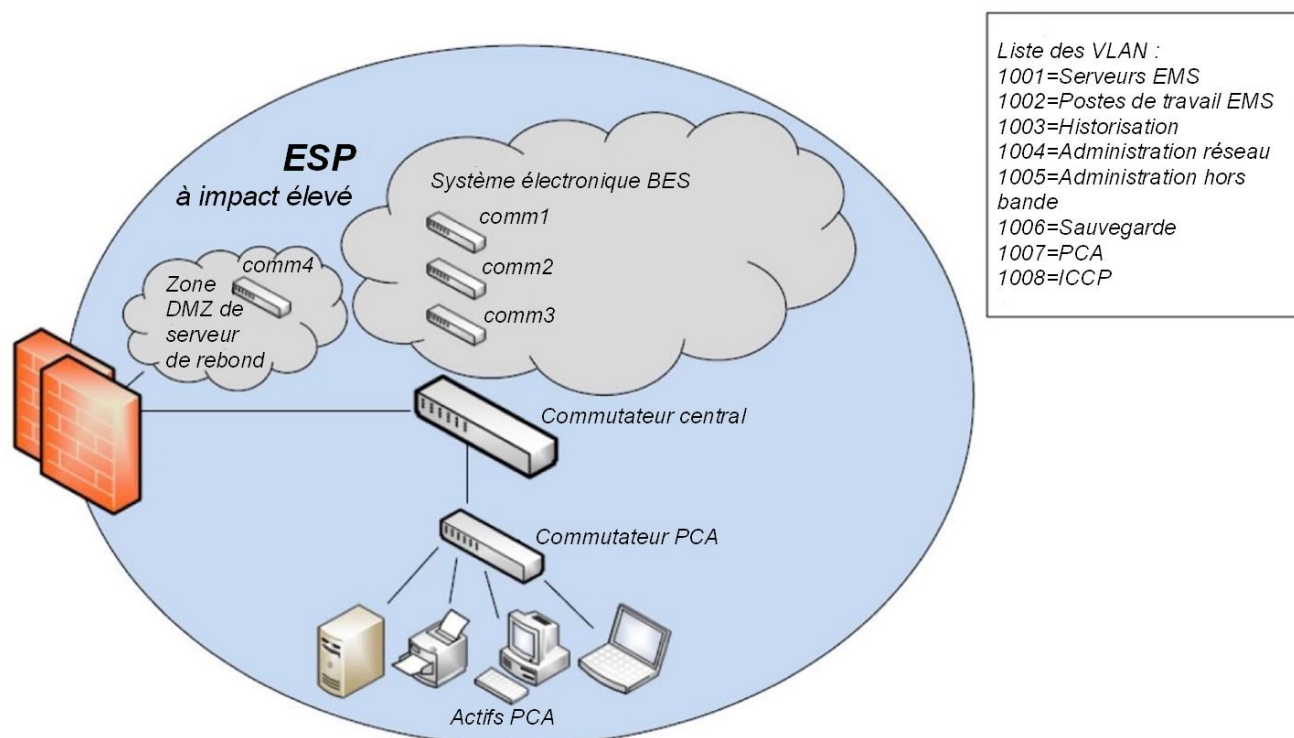


Figure 3

Exemple de sélection de flux de données :

Flux de données réseau	Sélection pour collecte	Emplacement dans le réseau	Méthode de collecte	Explication
PCAP central	Oui	Commutateur central	Écriture miroir de VLAN vers un port physique	<p>Presque toutes les données traversent ce commutateur. Une collecte au commutateur central permet de capter toutes les données entre les dispositifs de <i>système électronique BES</i> et les <i>PCA</i>.</p> <p>La collecte axée sur les VLAN permet d'exclure le trafic de sauvegarde.</p>
PCAP comm1	Oui	comm1 (commutateur d'accès de serveur EMS)	Écriture miroir de VLAN vers un port physique	<p>Les serveurs de système de gestion d'énergie (EMS) communiquent fréquemment entre eux et le trafic intra-VLAN peut ne pas transiter par le commutateur central.</p> <p>Un accès distant à ces serveurs est permis.</p>
	Non	comm2 (commutateur d'accès de poste de travail EMS)		<p>Tous les dispositifs reliés à ce commutateur sont des postes de travail EMS qui normalement ne communiquent pas entre eux.</p> <p>Tous les postes de travail EMS ont un niveau élevé de journalisation des points terminaux, notamment des journaux EDR (niveaux mémoire et processus).</p> <p>L'accès distant à ces postes de travail n'est pas autorisé.</p> <p>Tout le trafic prévu sera capté dans le flux de données du PCAP central.</p> <p>Les connexions non autorisées sont journalisées dans un coupe-feu local activé sur chaque poste de travail.</p>

Flux de données réseau	Sélection pour collecte	Emplacement dans le réseau	Méthode de collecte	Explication
	Non	comm3 (commutateur d'accès DNP3)		<p>Tout le trafic entre ces processeurs frontaux DNP3 transite par le commutateur central.</p> <p>Une collecte supplémentaire à partir de ce commutateur entraînerait une duplication intégrale du trafic.</p>
PCAP comm4	Oui	comm4 (commutateur d'accès)	Copie miroir des ports sources vers un port physique	<i>L'accès distant interactif (IRA)</i> au serveur de rebond est un vecteur d'attaque plausible.
	Non	Commutateur PCA		<p>Les communications entrantes et sortantes de tous les <i>actifs électroniques protégés (PCA)</i> transitent par le commutateur central et seront collectées. Il est entendu que le trafic intra-VLAN qui ne passe pas dans le commutateur central ne sera pas collecté.</p> <p>Une surveillance complémentaire des PCA est assurée par le système GIES qui surveille les journaux de points terminaux de tous les dispositifs, y compris si possible les journaux de mémoire et de processus.</p> <p>Un renforcement supplémentaire ainsi que des contrôles de points terminaux pour tous les PCA sont mis en place.</p> <p>La collecte des données réseau dans le commutateur PCA entraînerait une duplication de données sans véritable amélioration de la surveillance.</p>
PCAP central	Oui	VLAN 1001 – Serveurs EMS	Source du VLAN	Ce VLAN est essentiel pour le fonctionnement de l'EMS.
PCAP central	Oui	VLAN 1002 – Postes de travail EMS	Source du VLAN	Le VLAN collecte toutes les communications entre le VLAN 1002 et les autres dispositifs.

Flux de données réseau	Sélection pour collecte	Emplacement dans le réseau	Méthode de collecte	Explication
PCAP central	Oui	VLAN 1003 – Historisation	Source du VLAN	<p>L'historisation a été ciblée par des attaquants ayant ciblé d'autres entreprises d'électricité.</p> <p>La veille sur les menaces a permis de définir plusieurs cas d'utilisation qui nécessitent ces données.</p>
PCAP central	Oui	VLAN 1004 – Administration réseau	Source du VLAN	<p>Il arrive que des ports d'administration soient ciblés dans des attaques sur des systèmes de commande industrielle. Le système SSRI dispose de plusieurs cas d'utilisation qui alerteront en cas d'utilisation suspecte de connexions d'administration.</p>
PCAP central	Oui	VLAN 1005 – Administration hors bande (iDrac, iLO)	Source du VLAN	<p>Ces ports assurent un accès de niveau élevé, et pourraient donc être ciblés par un attaquant interne.</p> <p>Les cartes OOB (hors bande) actuellement en service n'offrent pas de fonctionnalités coupe-feu ; des mesures de détection SSRI sont donc ajoutées pour augmenter la visibilité de ces ports..</p>
	Non	VLAN 1006 – Sauvegarde		<p>Le trafic de sauvegarde occupe un fort volume et sa valeur de cybersécurité est minime ; il augmenterait le bruit dans la collecte de données.</p>
PCAP central	Oui	VLAN 1007 – PCA	Source du VLAN	<p>Certains PCA communiquent avec un hôte externe pour le téléchargement de correctifs logiciels. Ces flux transitent par le commutateur central et seront surveillés.</p>

Flux de données réseau	Sélection pour collecte	Emplacement dans le réseau	Méthode de collecte	Explication
PCAP central	Oui	VLAN 1008 – ICCP	Source du VLAN	Bien que des données ICCP légitimes soient déjà collectées sur le VLAN 1001 (serveurs EMS), une collecte sur ce VLAN assure la journalisation de toute demande imprévue provenant du réseau partenaire.
Données de journal de coupe-feu	Oui	Coupe-feu	API	L'outil SSRI comprend une intégration au coupe-feu qui informe sur les tentatives de connexion bloquées.

Cet exemple montre différents facteurs à prendre en compte lors de la sélection des flux de données réseau à collecter. L'exemple présenté n'est nullement exhaustif, mais sert principalement à expliquer un certain nombre d'éléments de décision qui interviennent dans le choix des flux de données réseau par l'entité responsable.

La collecte des flux de données réseau mise en œuvre dans le cadre de cet exemple est illustrée à la Figure 4.

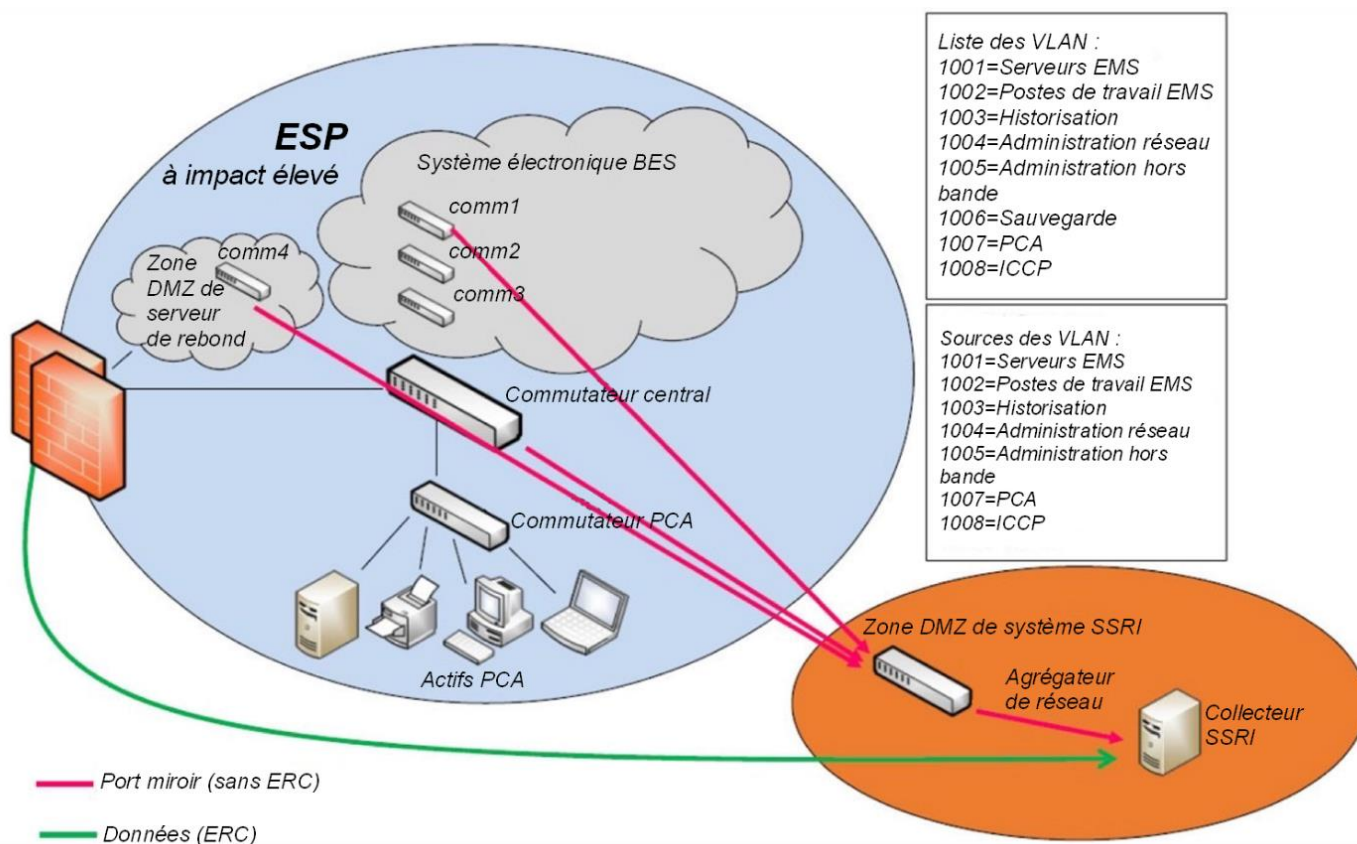


Figure 4

Historique des révisions

Révision	Date	Détails
V0.1	22 février 2024	Version initiale
V0.2	26 mars 2024	Changements découlant de commentaires formulés par l'industrie.
V0.3	24 avril 2024	Changements découlant de commentaires formulés par l'industrie.