BTS SIO 2020 - Préfiguration d’un sujet de l’épreuve écrite E6 – option SISR

Afin d’illustrer les recommandations pour la conception de sujet de l’épreuve, la proposition ci-dessous constitue un exemple de problématique, de contexte, de questionnement et de documents permettant d’évaluer les compétences du bloc 3 « Cybersécurité des services informatiques » pour l’option SISR dans le cadre d’une épreuve écrite. Les critères d’évaluation de ce sujet correspondent aux critères de performance cités dans le référentiel.

Ce sujet a été élaboré sur la base d’un sujet réel, déjà bien abouti, proposé pour une session antérieure. Il a été adapté pour tenir compte des spécificités de la nouvelle épreuve.

S’il est largement admis qu’un questionnement orienté sécurité était déjà naturellement présent dans les sujets de l’épreuve E5 du précédent référentiel du BTS SIO, et que l’effort à fournir pour passer à la version du BTS révisé n’est pas trop important, il serait imprudent de sous-estimer les changements dans la nature de cette épreuve. Nous allons expliciter ces changements à l’aide du sujet proposé ci-après.

À propos de la structure du sujet

Conformément aux recommandations, le sujet est ainsi structuré :

* il débute par la présentation d’un contexte qui donne un cadre de travail inspiré d’une situation d’entreprise réelle **invitant les candidates et les candidats à contribuer à identifier et résoudre des problèmes de cybersécurité ;**
* il comporte des dossiers qui traitent chacun d’un aspect de la problématique du sujet ;
* chaque dossier contient des missions qui précisent un objectif à atteindre ;
* une mission requiert des réalisations qui font l’objet des demandes ou des questions soumises aux candidates et aux candidats.

L’ensemble s’appuie sur un dossier documentaire qui fournit tous les éléments permettant de mener à bien les missions.

À propos du choix de l’organisation et du contexte

Le secteur de l'énergie est devenu l'un des plus sensibles en matière de cybersécurité. Plonger un territoire dans le noir par une coupure des réseaux d’électricité est possible par une cyberattaque sur les systèmes informatiques qui gèrent le réseau de fourniture d’électricité (ce fut le cas par exemple fin 2015 en Ukraine). Cette menace est prise très au sérieux par les États et les entreprises du secteur de l’énergie. En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) suit de près une vingtaine d'entreprises du secteur qui sont qualifiées d' « opérateurs d'importance vitale » et effectuent régulièrement des tests et exercices.

Dans le sujet proposé, la société d’économie mixte Poitourégie, qui assure un service de distribution d’électricité et de gaz, peut être considérée comme un opérateur d’importance vitale puisque qu’elle assure la fourniture d’énergie pour des milliers de foyers.

**Nous trouvons là une première caractéristique du sujet proposé : il fait référence à une organisation, un métier dont on peut percevoir le caractère sensible vis-à-vis d’une cyberattaque.**

Les sujets ne porteront cependant pas toujours nécessairement sur des organisations importantes susceptibles d’être les cibles de cyberattaques. On peut constater que toutes les entreprises sont susceptibles aujourd’hui d’être l’objet de ce type d’attaques.

À propos du questionnement proposé dans le sujet

Les missions du sujet font référence à des préoccupations de sûreté et de sécurité qui sont emblématiques du métier d’informaticien en charge d'une infrastructure système et réseau. Ces missions sont donc transposables à d’autres contextes.

**Dans ce sujet on ne recherche pas une expertise en cybersécurité, on évalue les compétences de techniciens supérieurs, qui dans leurs pratiques, intègrent à tous les stades (anticipation, prévention, réaction) une préoccupation de sécurisation.**

Les pistes de questionnement explorées par ce sujet sont loin d’être exhaustives.

Les compétences évaluées sollicitent nécessairement des savoirs communs avec d’autres blocs professionnels du référentiel. Il est en effet impossible, par exemple, de sécuriser un réseau vis à vis d’attaques en provenance d’internet sans connaître les protocoles réseau.

À propos des dossiers

**Dossier A**

Ce dossier est plus particulièrement orienté vers des problématiques de sécurité qui sont intégrées dans le quotidien du métier d’informaticien.

**Le sujet évalue les compétences cybersécurité à un niveau d’exigence qui correspond à celui d’un technicien supérieur à bac + 2.**

Le dossier est composé de trois missions :

**La mission A1** est orientée sécurité puisqu'elle consiste à prévenir donc à anticiper une possible malveillance. Elle est ancrée dans la réalité du métier car il s’agit de prendre en compte un avis de sécurité provenant d’un organisme gouvernemental.

La candidate ou le candidat est amené à évaluer les risques techniques et leurs conséquences, y compris juridiques et économiques. Que peut-on faire techniquement si on exploite cette vulnérabilité ? Sur quels équipements ? Quelles seraient les conséquences si la menace se réalise ?

On attend des solutions pour supprimer la faille et limiter les impacts.

Ce type de questionnement est très significatif du métier et des compétences qu’il requiert ; il peut être décliné dans de nombreux scénarios différents.

On constate aussi que des savoirs économiques, juridiques et managériaux sont requis pour accomplir la mission de façon satisfaisante.

**Le sujet sollicite explicitement ou implicitement les savoirs économiques, juridiques et managériaux du bloc sans en faire pour autant des questions de cours. Pour obtenir tous les points associés à une question il sera nécessaire de fournir une réponse comportant des éléments techniques mais également, en tant que de besoin, des éléments économiques, juridiques ou managériaux.**

**La mission A2** est également orientée sécurité et prévention. Il s’agit de prévenir l’installation d’un ver informatique connu en installant un dispositif de prévention.

En poursuivant un objectif de sécurité, on mobilise des compétences métiers : Quels sont les systèmes cibles les plus vulnérables ? Où situer le dispositif dans l'infrastructure pour qu’il soit efficace ?

**Dans le sujet comme dans le métier, vérifier une infrastructure système et réseau peut amener à auditer l’existant puis à proposer des modifications ou des ajouts directement liés à un besoin de cybersécurité.**

Ensuite l’étude d’un tableau d’indicateurs de compromission (*IOC*) nécessite des connaissances précises. il s’agit ensuite d’écrire concrètement des règles de filtrage.

On constate ici la présence d’éléments nouveaux, axés sécurité, ils sont associés aux compétences métier “classiques” que sont l’analyse d’un schéma réseau et l’écriture de règles de filtrage. Ces éléments nouveaux sont documentés en annexe.

**Le sujet poursuit un objectif de sécurité toujours clairement motivé par une problématique de cybersécurité.**

**La mission A3** propose de réagir à une attaque. Il s’agit, en étudiant un journal d’évènements, d’identifier le type d’attaque et de déterminer ses conséquences probables.

On s’appuie encore une fois sur des compétences précises d’administration réseau : échanges protocolaires, protocole sécurisé, bonnes pratiques de gestion des mots de passe.

La dernière question de la mission est toujours située dans le contexte de l’attaque étudiée, elle évalue la capacité de la candidate ou du candidat à prendre en charge une action réglementaire en référence au RGPD, ce qui nécessite des savoirs économiques, juridiques et managériaux.

**Le questionnement est toujours cohérent avec la problématique du sujet et avec l’accomplissement de la mission confiée à la candidate ou au candidat. Il est ancré dans la réalité du métier, il sollicite certaines compétences et requiert les savoirs associés.**

**Dossier B**

Le dossier B est un dossier orienté à la fois sûreté (capacité à surmonter une panne) et sécurité (capacité à résister à une attaque).

Dans le référentiel du diplôme, on considère qu’une infrastructure réseau sécurisée, mise en œuvre en respectant les bonnes pratiques, doit être capable de résister à une attaque (elle est dite “résiliente”). Si la sécurisation d’une infrastructure est prise en charge par les compétences du bloc 2, la sécurité en place est vérifiée à l’aide des compétences du bloc 3. C’est là ce que le dossier B se propose notamment de faire.

**Il ne faut pas en conclure que dans les sujets il y aura nécessairement un dossier orienté sûreté et un dossier orienté sécurité, ces deux approches peuvent être présentes conjointement au sein d’un même dossier, comme c’est le cas ici. On pourra également trouver des missions plutôt axées sûreté et d’autres qui étudient à la fois les aspects sûreté et sécurité.**

**La mission B1** vise à vérifier la tolérance de panne sur l'établissement d’un circuit de réseau privé virtuel (*VPN*). On est ici clairement dans la validation d'éléments déjà en place car on élabore un scénario de panne pour vérifier la résilience de l'infrastructure.

Les deux premières questions de la mission évaluent la tolérance à la coupure d’un lien. On trouve ici un protocole déjà exploité (*VRRP*) et on étudie précisément la chaîne de liaison, les matériels traversés et l’établissement d’un circuit alternatif. Les compétences métiers mobilisées ici sont particulièrement significatives d’un exercice d’anticipation à partir de risques identifiés comme pouvant se réaliser.

La dernière question étudie la criticité d’un dispositif d'accès et demande une solution.

**Le sujet amène à vérifier la sûreté des équipements afin d’identifier des risques puis proposer des solutions.**

**La mission B2** étudie le remplacement d’un matériel obsolète en prenant en compte des critères de sécurité dans le choix du nouveau matériel. On trouve ici les deux problématiques : sûreté et sécurité.

On est encore une fois dans le cœur de métier : remplacement des commutateurs, établissement d’un cahier des charges, dépouillement d’un appel d’offre en vérifiant les éléments du cahier des charges en les évaluant par une note argumentée prenant en compte la sécurité.

**C’est là une mission habituelle dans les sujets de l’option SISR mais elle est ici clairement contextualisée dans la nouvelle approche cybersécurité.**

**Les documents**

La lecture des documents annexés au sujet représente un part non négligeable des quatre heures que les candidats peuvent consacrer à l’épreuve. Afin de bien comprendre le sujet, cette lecture sollicite beaucoup les savoirs du référentiel, on peut considérer qu’elle participe directement à l’évaluation des candidats avant même qu’elles ou ils aient répondu à la première question.

La capacité à identifier le ou les documents utiles pour répondre à telle ou telle question est aussi sollicitée.

**Le sujet fournit toute la documentation nécessaire à la compréhension du sujet. Ne peuvent être considérés comme acquis par les candidats que les savoirs fondamentaux et les technologies dont il est admis qu’ils sont communément enseignés dans les sections qui préparent au BTS SIO.**

***Les compétences évaluées dans le sujet proposé sont les suivantes :***

**Mission A1 – Limitation de la surface d’attaque**

Sécuriser les équipements et les usages des utilisateurs

* Identifier les menaces et mettre en œuvre les défenses appropriées

Garantir la disponibilité, l’intégrité et la confidentialité des services informatiques et des données de l’organisation face à̀ des cyberattaques

* Caractériser les risques liés à̀ l’utilisation malveillante d’un service informatique
* Recenser les conséquences d’une perte de disponibilité́, d’intégrité́ ou de confidentialité

Assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

* Prévenir les attaques

**Mission A2 – Mise en place d’un outil de détection d’intrusion (IDS/IPS)**

Sécuriser les équipements et les usages des utilisateurs

* Identifier les menaces et mettre en œuvre les défenses appropriées

Assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

* Mettre en œuvre et vérifier la conformité d’une infrastructure à un référentiel, une norme ou un standard de sécurité
* Prévenir les attaques
* Détecter les actions malveillantes

**Mission A3 - Résolution d’un problème de sécurité**

Garantir la disponibilité, l’intégrité et la confidentialité́ des services informatiques et des données de l’organisation face à des cyberattaques

* Identifier les obligations légales qui s’imposent en matière d’archivage et de protection des données de l’organisation
* Appliquer les procédures garantissant le respect des obligations légales

Assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

* Détecter les actions malveillantes
* Analyser les incidents de sécurité́, proposer et mettre en œuvre des contre-mesures

**Mission B1 - Étude de la tolérance de pannes de l’infrastructure du siège**

Assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

* Participer à la vérification des éléments contribuant à la sûreté d’une infrastructure informatique
* Mettre en œuvre et vérifier la conformité d’une infrastructure à un référentiel, une norme ou un standard de sécurité
* Détecter les actions malveillantes
* Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures

**Mission B2 - Renforcement de la sûreté et la sécurité de l’infrastructure réseau**

Assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

* Participer à la vérification des éléments contribuant à la sûreté d’une infrastructure informatique
* Prendre en compte la sécurité dans un projet de mise en œuvre d’une solution d’infrastructure
* Mettre en œuvre et vérifier la conformité d’une infrastructure à un référentiel, une norme ou un standard de sécurité

BTS SIO – ÉPREUVE E6 SISR - SUJET ZÉRO

CAS POITOURÉGIE

**Dossier documentaire**

[Documents associés au dossier A 14](#_Toc38702415)

[Document A1 : Schéma simplifié du réseau de distribution d’électricité 14](#_Toc38702416)

[Document A2 : Extrait (traduit) du bulletin de sécurité SCADA Siemens SSA-697412 15](#_Toc38702417)

[Document A3 : Fonctionnement des réseaux d’ordinateurs zombies (botnets) et des serveurs de commande et de contrôle 16](#_Toc38702418)

[Document A4 : Industroyer - Extrait des indicateurs de compromission (IOC) 17](#_Toc38702419)

[Document A5 : IDS, IPS et contraintes des systèmes industriels 18](#_Toc38702420)

[Document A6 : Logiciel Suricata et règles de détection 19](#_Toc38702421)

[Document A7 : Alerte de l’attaque et extrait des journaux d’événements 19](#_Toc38702422)

[Documents associés au dossier B 20](#_Toc38702423)

[Document B1 : Schéma général actuel du réseau de Poitourégie 20](#_Toc38702424)

[Document B2 : Architecture actuelle de l’infrastructure du siège 21](#_Toc38702425)

[Document B3 : Extrait d’un rapport de M. Jason, responsable infrastructure réseau 22](#_Toc38702426)

[Document B4 : Organisation des 3 clusters VMware ESX 22](#_Toc38702427)

[Document B5 : Extrait du plan d’adressage des réseaux de Poitourégie 22](#_Toc38702428)

[Document B6 : Extrait du cahier des charges "Solution réseau - Poitourégie" 23](#_Toc38702429)

[Document B7 : Tableau comparatif des offres des prestataires A et B 25](#_Toc38702430)

[Document B8 : Offres des prestataires A et B – Représentation schématique 26](#_Toc38702431)

**Présentation du contexte**

Poitourégie est une société d’économie mixte, elle assure depuis 1991 le service de distribution d’électricité et de gaz auprès de 265 communes adhérentes du syndicat intercommunal ENERGIES86. Ces communes sont principalement situées dans le département de la Vienne mais également dans trois départements limitrophes. Poitourégie compte aujourd’hui 155 000 clients et entretient en parallèle 55 000 points d’éclairage public.

En 2001, la société ERGIE est créée au sein du syndicat ENERGIES86. Elle a pour mission de construire et d’exploiter des unités de production d’énergie renouvelable comme par exemple des parcs éoliens, des centrales photovoltaïques ou des unités de méthanisation. ERGIE permet d’injecter 15 % d’énergie renouvelable dans le mix énergétique des communes du syndicat ENERGIES86, avec une ambition de 45 % d’ici 2025.

En 2008, la loi impose la séparation des activités de transport d’énergie d’une part et de fourniture d’énergie d’autre part. Cette nouvelle législation a fait naître la société SRD qui construit, exploite, entretient, sécurise, dépanne et pérennise les réseaux électriques.

La direction des systèmes d’information (DSI) de Poitourégie gère aujourd’hui l’ensemble du système d’information (SI) du syndicat ENERGIES86, elle facture ses services aux différentes entités du syndicat.

Une entreprise fournisseuse d’énergie est soumise à de très fortes contraintes. En effet, un réseau électrique doit distribuer de manière ininterrompue l’énergie tout en s’assurant de la sécurité des personnes et des équipements.

Compte tenu des très graves conséquences que provoquerait une cyberattaque sur le système informatique qui gère le réseau électrique d’un pays, celui-ci est devenu l'un des plus sensibles en matière de cybersécurité.

La DSI de Poitourégie est composée de 35 personnes et dispose d’un budget d’investissement de 1,2 million d’euros et d’un budget de fonctionnement de 1,7 million d’euros.

Vous travaillez au sein de cette équipe conséquente, vous aurez pour mission d’assister la DSI dans les missions suivantes :

* Sécuriser le réseau informatique associé à la distribution électrique ;
* Réaliser un audit permettant de s’assurer de la disponibilité du système informatique et de participer au choix des mesures qui en découlent.

Le système informatique, architecturé autour d’un réseau MPLS[[1]](#footnote-1), comporte actuellement :

* 30 sites techniques de gestion du réseau électrique et 16 agences ;
* 200 serveurs et 250 clients légers ;
* 450 utilisateurs.

**Vous vous appuierez sur les dossiers documentaires mis à votre disposition.**

|  |
| --- |
| **Dossier A - Sécurisation du réseau** |

Dans le cadre de sa mission de fournisseur d’énergie, Poitourégie doit prendre en compte la sécurité de ses réseaux de distribution et de gestion. M. SUTTER, l’adjoint à la DSI, a la responsabilité de la sécurité des systèmes d’information (RSSI).

**Mission A1 – Limitation de la surface d’attaque**

Abonné aux alertes du site du centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques (CERT-FR), l’avis du 14 mai 2019 concernant notamment trois vulnérabilités publiquement connues (CVE[[2]](#footnote-2)) a attiré son attention. Ces vulnérabilités décrivent plusieurs failles de sécurité découvertes dans le logiciel utilisé dans le réseau de distribution d’électricité (ICS[[3]](#footnote-3)) de Poitourégie, à savoir le logiciel SIMATIC WinCC. Le détail de cette alerte est fourni dans le document A2.

Le RSSI souhaite faire un état des lieux concernant ce risque et mettre en place, le cas échéant, les contre-mesures adéquates. Il vous demande de préciser un certain nombre de points qui feront l’objet d’une note de synthèse.

|  |
| --- |
| **Question A1.1**  a) Relever et expliquer les risques techniques engendrés par les failles de sécurité ayant fait l’objet d’une alerte du CERT-FR.  b) Identifier, sur les trois réseaux, quelles pourraient être les conséquences techniques, juridiques et économiques de ces failles pour Poitourégie au cas où elles seraient exploitées par un tiers malveillant. |

En plus des solutions spécifiquement proposées pour ces failles, l’éditeur du logiciel, la société Siemens, recommande fortement de protéger l'accès réseau aux produits industriels par des mécanismes appropriés.

|  |
| --- |
| **Question A1.2**  Proposer trois solutions concrètes à mettre en œuvre afin de limiter les risques d’attaques. |

**Mission A2 – Mise en place d’un outil de détection d’intrusion (*IDS*/*IPS*)**

Le RSSI souhaite améliorer la protection du réseau de distribution en préservant l’infrastructure de distribution électrique de l’intrusion de vers de type *stuxnet* et notamment du ver "Industroyer / CrashOverride" qui ciblent particulièrement les réseaux électriques.

Ce ver a fait parler de lui en mettant hors service une centrale électrique en Ukraine en décembre 2015. Il permet à des pirates de prendre le contrôle à distance de transformateurs et de couper des parties du réseau électrique pour le déstabiliser et provoquer des coupures d’électricité géantes. Pour communiquer avec ses serveurs de commande et de contrôle (C&C), le logiciel malveillant utilise le réseau anonyme Tor et n’est actif qu’en dehors des heures de bureau afin de rester discret.

Après avoir étudié le fonctionnement des réseaux d’ordinateurs zombies (*botnets)* et des serveurs de commande et de contrôle, M. SUTTER vous charge de faire une première étude en vous aidant d’un tableau d’indicateurs de compromission (*Indicator of Comprise -* IoC).

|  |
| --- |
| **Question A2.1**  Indiquer, en justifiant vos réponses :  a) Sur quel type de système d’exploitation peut s’installer le ver Industroyer ?  b) Parmi les machines installées avec ce type de système d’exploitation, quelles sont celles qui sont particulièrement vulnérables ? |

En se basant sur votre note précédente, l’équipe informatique décide de commencer à prendre des mesures et le RSSI vous confie le soin de faire une proposition précise et argumentée.

Vous réfléchissez à l’opportunité d’installer un outil de détection d’intrusion IDS/*IPS* et synthétisez vos recherches dans une note figurant dans le dossier documentaire. Votre choix s’est porté sur le logiciel*Suricata****,*** de type *Network IDS/IPS,* plutôt que sur un logiciel de type *Host IDS/IPS*, vous prévoyez de l’installer entre le réseau administratif et le réseau de supervision SCADA.

|  |
| --- |
| **Question A2.2**  Justifier, d’une part, le choix du logiciel Suricata et, d’autre part, le choix de son positionnement. |

Votre choix est validé, il a été décidé de configurer l’outil afin de pallier une potentielle attaque du ver *Industroyer*.

|  |
| --- |
| **Question A2.3**  a) Repérer, dans le tableau d’indicateurs de compromission, les lignes identifiant la communication vers les serveurs de commande et contrôle (C&C).  b) Rédiger les quatre règles du logiciel *Suricata* permettant de bloquer ces échanges. |

**Mission A3 - Résolution d’un problème de sécurité**

Quelques jours après la mise en service de l’IDS/*IPS*, le logiciel *Suricata* a généré une première alerte.

Le texte de l’alerte ainsi qu’un extrait formaté des journaux d’événements nécessaires à la compréhension de l’incident vous ont été fournis. L’extrait provient notamment du fichier */var/log/suricata/eve.json*.

Le service informatique a réagi très rapidement en réinitialisant le périphérique responsable, ce qui a stoppé le flux correspondant et résolu provisoirement le problème.

On vous confie la recherche des causes du problème et la recherche de la résolution.

|  |
| --- |
| **Question A3.1**  Rédiger cette fiche :  a) Expliquer, pour chacune des quatre parties du relevé des journaux d’événements, à quoi correspond chaque échange : protocole utilisé, opération(s) réalisée(s).  b) En déduire le type de l’attaque qui a été lancée. |

Après une recherche rapide dans la documentation du périphérique responsable, la commande suivante vous a permis de vous y connecter avec succès :

**ncrack --user admin --pass admin telnet://172.16.128.27**

Discovered credentials for telnet on 172.16.128.27 23/tcp

172.16.128.27 23/tcp telnet: ‘admin’ ‘admin’

L’équipement à l’origine du problème est une caméra. Ce matériel ne peut pas être changé immédiatement. Vous devez faire en sorte de limiter les risques d’une nouvelle infection via ce type de matériel.

|  |
| --- |
| **Question A3.2**  a) Identifier les deux failles de sécurité révélées par le résultat de la commande.  b) Proposer deux solutions permettant d’y remédier. |

La caméra en question est positionnée dans le poste de transformation électrique numéro 1 dans lequel des interventions de techniciens ont régulièrement lieu sur le réseau électrique.

Il a été établi que les pirates ont pu accéder au flux vidéo en direct. Ainsi, ces failles de sécurité ont été susceptibles d'engendrer une atteinte à des données à caractère personnel.

|  |
| --- |
| **Question A3.3**  Rappeler les obligations juridiques du RGPD qui incombent à la société Poitourégie suite à l'incident de sécurité. |

|  |
| --- |
| **Dossier B - Audit et évolution de l’infrastructure réseau** |

**Mission B1 - Étude de la tolérance de pannes de l’infrastructure du siège**

Les centrales électriques ne peuvent souffrir d’aucune interruption de service, l’ensemble du réseau de distribution électrique (ICS) et le réseau informatique interconnecté avec ce dernier se doivent d’être disponibles.

Vous faites partie de l’équipe qui a en charge l’audit du plan de continuité d’activité (PCA). Cet audit a pour objectif, d’une part, de vérifier les éléments redondants qui permettent une tolérance aux pannes et, d’autre part, d’identifier les éléments encore critiques et les points à améliorer.

Vous avez en charge de proposer plusieurs scénarios de pannes (qui seront testés dans un second temps) puis de rédiger un compte rendu complet et argumenté à M. Jason, responsable de l’infrastructure au sein de la DSI de Poitourégie. Ce dernier vous a donné, lors d’un entretien, un certain nombre de documents avec quelques explications*.* Votre compte-rendu devra notamment expliciter, pour chaque scénario, les implémentations et les technologies sous-jacentes qui permettent théoriquement la continuité d’exploitation.

Vous vous intéressez dans un premier temps aux accès vers les agences via le réseau privé virtuel (*virtual private network – VPN*) et vers les applications métier.

Le premier scénario envisage une panne sur le routeur ADISTA 100M.

|  |
| --- |
| **Question B1.1**  a) Préciser, dans le cadre de ce premier scénario, la technologie qui permet de basculer sur le routeur de secours et expliquer son fonctionnement.  b) Lister les équipements traversés par un message émis par un poste client du bâtiment A via le réseau virtuel privé (*VPN*) vers une des agences lorsque le lien ADISTA 100M est coupé. |

Le second scénario envisagé est le suivant : le routeur ADISTA 100M est opérationnel, mais le cœur de réseau du bâtiment A est coupé à la suite d’une panne du commutateur niveau 3 Alcatel 6850.

|  |
| --- |
| **Question B1.2**  Lister, dans le cas du second scénario, en justifiant par rapport aux technologies implémentées :  a) Les équipements traversés par un message émis par un poste client du bâtiment A via le réseau virtuel privé (*VPN*) vers une des agences ;  b) Les équipements traversés par un message émis par un poste client du bâtiment A vers une des applications métier situées sur la grappe de serveurs (*cluster*) VMware. |

Vous vous intéressez maintenant aux flux étiquetés « Internet » sur le schéma réseau, et non plus aux flux spécifiques « VPN ».

Vous repérez un élément d’infrastructure critique concernant ces accès internet.

|  |
| --- |
| **Question B1.3**  Identifier cet élément d’infrastructure et proposer une solution permettant de limiter sa criticité. |

**Mission B2 – Renforcement de la sûreté et la sécurité de l’infrastructure réseau**

Pour répondre aux recommandations de l’ANSSI concernant la sécurisation des infrastructures réseau, un appel d’offres a été lancé par Poitourégie afin de remplacer les équipements de commutation de niveau 2 et 3 du réseau informatique du siège qui datent de plus de 7 ans.

L’objectif principal est de renforcer la sécurité et la sûreté de la solution “cœur de réseau et distribution serveurs” ainsi que la solution “distribution clients”.

Sept entreprises ont répondu à l’appel d’offres. La DSI vous demande de l’aider à terminer l’analyse des deux offres qui ont retenu son attention, ceci afin de préparer les questions et les demandes de modifications lors d'un prochain entretien avec les prestataires.

|  |
| --- |
| **Question B2.1**  Préparer, en les justifiant, les éléments de réponse aux différentes questions de votre DSI pour chacune des offres A-Huawei et B-Cisco, à savoir :   1. Concernant le coeur de réseau, les solutions respectent-elles les exigences en termes de tolérance de panne ? 2. Les connexions entre équipements respectent-elles les demandes exprimées en termes de débit dans le cahier des charges ? 3. Le nombre de commutateurs distribution clients correspond-il aux demandes exprimées dans le cahier des charges ? 4. Actuellement, les grappes de serveurs (*clusters*) VMware utilisent 50 ports GigaBit T sur les commutateurs de distribution serveurs, ce nombre est-il satisfaisant ? 5. Le cahier des charges précise que les serveurs devront être connectés en 10GB-T, il est nécessaire de vérifier pour chaque offre si la proposition est correctement dimensionnée en justifiant le nombre ports 10GB-T minimum nécessaires. |

Afin de comparer les différentes offres, des critères ont été établis permettant de valoriser sous forme de notes les différents éléments contenus dans les propositions.

Trois notes sont données : la première correspond à la valeur technique de l’offre (pour 60 %), la deuxième note correspond au positionnement du prix par rapport à l’offre moins-disante (pour 30 %), les critères composant la troisième note, représentant 10 % de la note totale, sont en cours de définition.

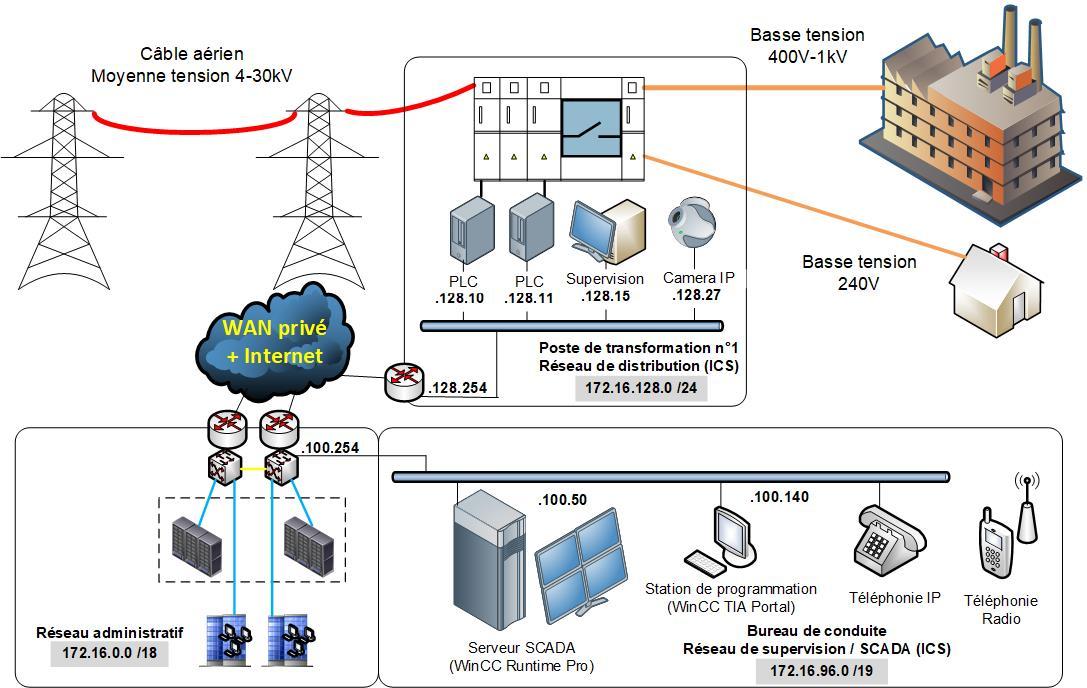
|  |
| --- |
| **Question B2.2**  Identifier deux éléments concernant l’offre et le prestataire qui pourraient constituer des critères permettant de définir la troisième note. |

Les deux offres obtiennent finalement la même note. Il faut pourtant faire un choix entre les deux prestataires.

|  |
| --- |
| **Question B2.3**  Proposer le choix qui vous semble être le plus pertinent en veillant à argumenter votre proposition. |

|  |
| --- |
| Documents associés au dossier A |

Document A1 : Schéma simplifié du réseau de distribution d’électricité



**Le réseau de distribution électrique (ICS pour *Industrial Control System*)** a en charge la distribution électrique auprès des clients en assurant la sécurité des personnes et des équipements. L’électricité de moyenne tension est convertie en basse tension par des postes de transformation : 400V à 1000V pour les clients industriels et 240V pour les autres clients (particuliers, commerçants, etc.).

Ce réseau est constitué del’ensemble des objets techniques (capteurs, actionneurs, calculateurs PLC[[4]](#footnote-4), superviseurs, caméras IP, …) et des réseaux de communication (protocoles TCP/IP, médias…) permettant l’automatisation des tâches de régulation d’un système industriel comme la gestion automatique de la distribution électrique en fonction de l’offre et de la demande. C’est par exemple à partir de ce réseau qu’une ouverture ou une coupure d’électricité chez un client peut être opérée.

**Le réseau de supervision SCADA (*Supervisory Control And Data Acquisition*)** est lapartie du réseau de distribution électrique gérant la supervision et l’acquisition des données permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance les installations techniques. L’enjeu est de gérer efficacement l’énergie électrique, de protéger, surveiller et contrôler l’ensemble du réseau électrique à tout instant.

**Le réseau administratif** fournit les ressources classiques d’un réseau informatique (serveurs de fichiers, serveur de messagerie, serveurs de bases de données, applications métier, etc.).

Document A2 : Extrait (traduit) du bulletin de sécurité SCADA Siemens SSA-697412

**SSA-697412 : Vulnérabilités multiples dans SIMATIC WinCC, SIMATIC WinCC Runtime, SIMATIC PCS 7, SIMATIC TIA Portal**

Date de publication : 14/05/2019

Dernière mise à jour : 10/08/2019

**RÉSUMÉ**

La dernière mise à jour de SIMATIC WinCC corrige plusieurs vulnérabilités. Le plus grave pourrait permettre à un attaquant d'exécuter des commandes arbitraires sur un système affecté dans certaines conditions.

Siemens a publié des mises à jour pour plusieurs produits concernés et recommande aux clients de mettre à jour la nouvelle version. Siemens prépare de nouvelles mises à jour et recommande des contre-mesures spécifiques jusqu'à ce que des correctifs soient disponibles.

**PRODUITS AFFECTÉS**

* SIMATIC WinCC : All versions < V7.5 Upd 3
* SIMATIC WinCC Runtime Professional : All versions < V15.1 Upd 3
* SIMATIC WinCC (TIA Portal) Professional : All versions < V14 SP1 Upd 9
* SIMATIC PCS 7 : All versions < V9.0 SP2 with WinCC V7.4 SP1Upd11

**DESCRIPTION**

SIMATIC WinCC est un système SCADA.

SIMATIC WinCC Runtime Professional est une plateforme de visualisation utilisée pour le contrôle et la supervision des machines et usines.

SIMATIC WinCC (TIA Portal) est un logiciel d'ingénierie permettant de configurer et programmer les panneaux SIMATIC, les PC industriels SIMATIC et les PC standards exécutant WinCC Runtime Advanced ou WinCC Runtime Professional.

SIMATIC PCS 7 est un système de contrôle distribué (DCS) intégrant SIMATIC WinCC et d'autres composants.

**Vulnérabilité CVE-2019-10916**

Un attaquant ayant accès au fichier de projet pourrait exécuter des commandes système arbitraires avec les privilèges du serveur de base de données local (élévation de privilège[[5]](#footnote-5)). La vulnérabilité pourrait être exploitée par un attaquant ayant accès au fichier de projet. La vulnérabilité a un impact sur la confidentialité, l'intégrité et la disponibilité du système affecté.

**Vulnérabilité CVE-2019-10917**

Un attaquant disposant d'un accès local au fichier de projet pourrait provoquer une condition de déni de service sur le produit affecté pendant le chargement du fichier de projet. Une exploitation réussie nécessite l'accès au fichier de projet. Un attaquant pourrait utiliser la vulnérabilité pour compromettre la disponibilité du système affecté.

**Vulnérabilité CVE-2019-10918**

Un attaquant authentifié disposant d'un accès réseau à l'interface DCOM pourrait exécuter des commandes arbitraires avec les privilèges SYSTEM (élévation de privilège[[6]](#footnote-6)). La vulnérabilité pourrait être exploitée par un attaquant disposant d'un accès réseau au système affecté. Une exploitation réussie nécessite une authentification avec un compte d'utilisateur à faible privilège sans aucune interaction avec l'utilisateur. Un attaquant pourrait utiliser la vulnérabilité pour compromettre la confidentialité, l'intégrité et la disponibilité du système affecté.

**SOLUTION**

De nombreuses mises à jour ont été émises.

Par ailleurs Siemens a identifié les solutions de contournement et les mesures d'atténuation spécifiques suivantes que les clients peuvent appliquer pour réduire le risque :

* activer la “communication cryptée” dans SIMATIC WinCC et SIMATIC PCS 7 ;
* ouvrir uniquement les fichiers de projet à partir d'emplacements de confiance.

Enfin, Siemens recommande fortement de protéger l'accès réseau aux produits industriels par des mécanismes appropriés.

Document A3 : Fonctionnement des réseaux d’ordinateurs zombies (botnets) et des serveurs de commande et de contrôle

Un serveur de commande et de contrôle (C&C) est un ordinateur qui donne des ordres via des commandes à des machines infectées par un logiciel malveillant et qui reçoit en retour des informations en provenance de celles-ci. Les ordinateurs contaminés peuvent être des serveurs, des machines personnelles, des routeurs, des objets connectés (comme des téléphones ou des caméras), etc.

L’ensemble de ces machines infectées constituent ce que l’on appelle un « *botnet* » (de l’anglais, contraction de « robot » et « réseau ») ; elles ont pour vocation d’agir ensemble sur Internet pour envoyer du courrier indésirable (*spam*), des virus ou déclencher des attaques DDoS (*Distributed Denial of Service*).

Le fonctionnement traditionnel simplifié peut être schématisé de la façon suivante :

|  |  |
| --- | --- |
| botnet.png | 1 - Le pirate prend le contrôle de machines distantes, par exemple avec un virus, en exploitant une faille ou en utilisant un cheval de Troie.  2 - Une fois infectées, les machines vont se signaler auprès d’un serveur de commandes, contrôlé par le pirate, qui prend donc ainsi la main sur les machines contaminées (qui deviennent des machines « zombies »).  3 - Le pirate envoie la ou les commandes aux machines infectées.  4 - Celles-ci effectuent alors les opérations souhaitées, comme lancer une attaque DoS ou envoyer des courriers indésirables (*spam)*. |

Document A4 : Industroyer - Extrait des indicateurs de compromission (IOC)

Un indicateur de compromission est un ensemble de données portant sur les menaces, qui permet de déceler de manière fiable une intrusion informatique.

Cela peut être par exemple la recherche de fichiers particuliers dans le système sur la base de différentes caractéristiques comme le nom d’un fichier installé ou supprimé (première ligne du tableau). Il est également possible de rechercher des enregistrements particuliers dans la base de registres du système (dernière ligne du tableau) ou de détecter les adresses IP sources des attaques pour les bannir du réseau.

Quelques indicateurs de compromission (*IOC*) du ver *Industroyer* sont listés et décrits dans le tableau ci-dessous :

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Sous-type** | **IOC** | **Description** |
| Hôte | Fichier | C:\Utilisateurs\<Public OR Executing User>\imapi | Exécutable nommé “imapi” déplacé dans le dossier “Public” ou dans le dossier de l’utilisateur courant. |
| Hôte | Nom du service | defragsvc | Démarrage de ce service (exploitation pour prendre la main sur la machine à distance). |
| Réseau | Adresse IP | 195.16.88.6 | Adresses IP des serveurs C&C connus vers lesquels les machines infectées envoient des informations. |
| Réseau | Adresse IP | 93.115.27.57 |
| Réseau | Adresse IP | 5.39.218.152 |
| Réseau | Chaîne de l’agent utilisateur | Mozilla/4.0 (compatible ; MSIE 7.0 ; Windows NT 5.1; InfoPath.1) | Chaîne utilisée dans l’en-tête d’une requête envoyée vers un serveur C&C (connu ou non). |
| Hôte | Clé de registre | HKLM\SYSTEM\CurrentControlSet\Services\<target\_service\_name>\ImagePath<path to malware> | Modifie le chemin de l’image d’un service dans le registre système pour pointer vers un programme malveillant permettant le démarrage du logiciel malveillant au démarrage du système. |

Document A5 : IDS, IPS et contraintes des systèmes industriels

Un système de détection d’intrusions (*intrusion detection system - IDS*) est un outil logiciel ou matériel dont le rôle est de repérer de manière passive les activités suspectes sur un réseau ou sur un hôte, permettant ainsi aux administrateurs de réagir plus rapidement en cas d’attaque.

Un système de prévention d’intrusions (*intrusion prevention system - IPS*) est un *IDS* qui possède la capacité supplémentaire d’agir de manière active sur les activités suspectes (blocage de trames, de ports, blocage d’une tentative de modification du contenu d’un fichier, etc…).

Il existe essentiellement trois familles d’*IDS*/*IPS* :

* Les *Network* *IDS*/*IPS* (*NIDS*/*NIPS*) qui analysent les flux sur le réseau et détectent les attaques en temps réel.
* Les *Host* *IDS*/*IPS* (*HIDS*/*HIPS*) qui analysent les activités des machines (OS) sur lesquels ils sont installés.
* Les *IDS*/*IPS* hybrides, qui centralisent l’analyse des flux réseaux et hôtes.

**Note** : les systèmes industriels nécessitent souvent des temps de réponse très courts, parfois de l’ordre de quelques dizaines de microsecondes, ce qui rend difficile l’usage de mécanismes de protection pouvant créer une latence importante, comme par exemple : la cryptographie, pour assurer l’intégrité des données ; les équipements de filtrage ou encore les *Host* *IDS*/*IPS*(*HIDS*/*HIPS*).

À contrario, un Network *IDS*/*IPS* correctement placé permettra d’améliorer les capacités de surveillance sans perturber le fonctionnement des systèmes industriels.

Document A6 : Logiciel Suricata et règles de détection

Suricata est un *Network* *IDS*/*IPS* basé sur des signatures, distribué sous licence GPL v2. Il analyse le trafic réseau en comparant les paquets à un ensemble de signatures (règles) qui correspondent à des motifs d’attaques.

Exemple de règles :

* + 1. alert tcp any any -> 192.168.1.0/24 21 (content : "USER root" ; msg : "FTP root login" ;)

Suricata déclenchera une alerte affichant le message "FTP root login" quand il détectera la chaîne de caractères "USER root" dans un segment TCP en provenance de n’importe quel réseau à destination du réseau 192.168.1.0/24 sur le port 21.

* + 1. drop ip 80.251.24.12 any -> 192.168.1.0/24 any (msg : "Blocage adr src " ;)

Suricata bloquera l’adresse source 80.251.24.12 à destination du réseau 192.168.1.0/24.

Format général simplifié :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Action** | **Protocole** | **Paramètres source** | **->** | **Paramètres destination** | **Motif** | **Message** |
| alert  drop  pass | ip  icmp  tcp  udp  http | Adresse IP port : source |  | Adresse IP port : destination | Content : "…" | Msg : "…" |
| alert | tcp | any any | -> | 192.168.1.0/24 21 | content : "USER root" | msg : "FTP root login" |
| drop | ip | 80.251.24.12 any | -> | 192.168.1.0/24 any |  | msg : "Blocage adr src " |

Document A7 : Alerte de l’attaque et extrait des journaux d’événements

***Alerte générée par Suricata sur l’IDS/IPS***

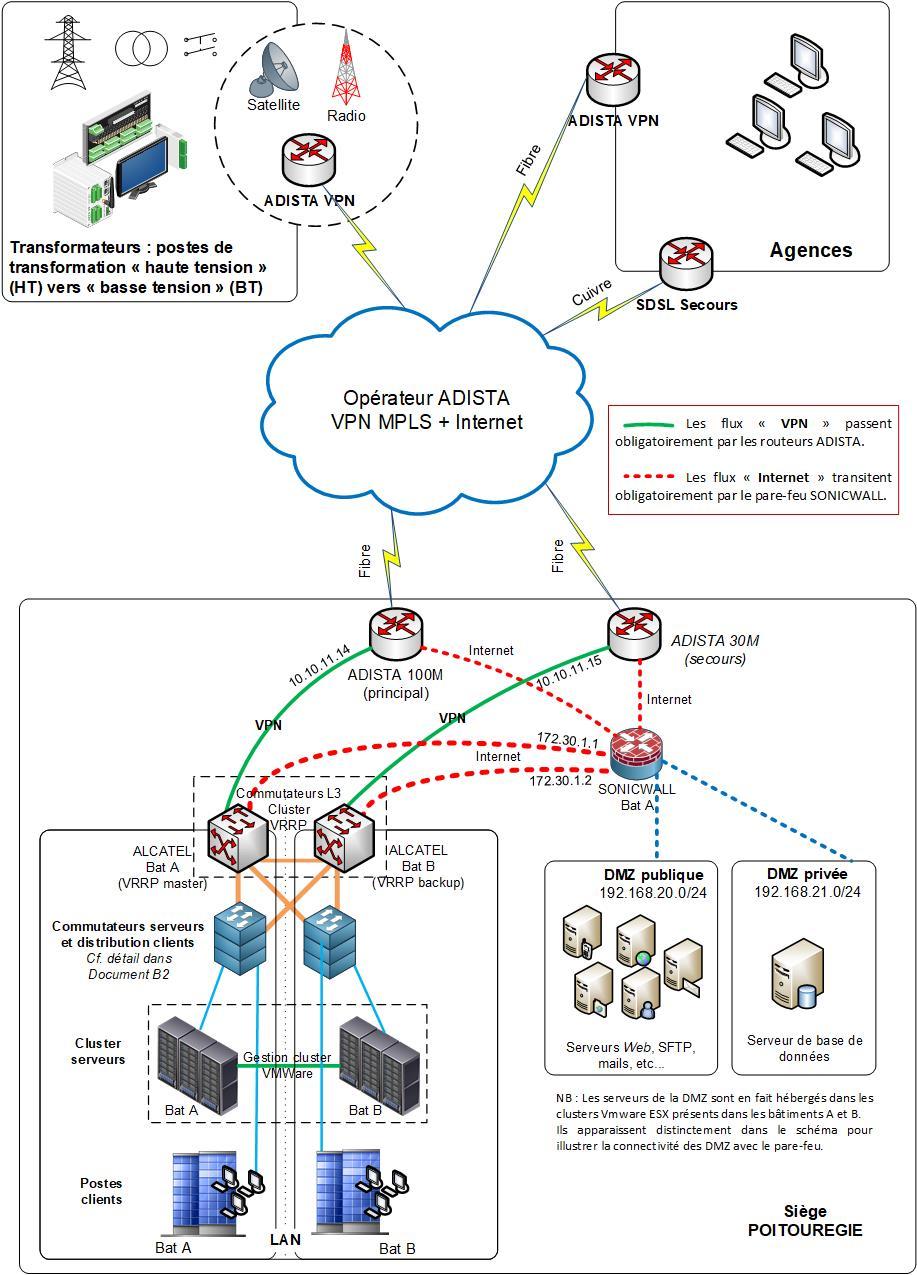
06/09/2020-17:47:48.429834 [\*\*] [1:2003068:7] DOS[[7]](#footnote-7) Potential SYN Flood Denial Of Service Attempt [\*\*] [Priority: 2] {TCP} 172.16.128.27:15831 -> 52.84.163.172:80

***Extraits formatés des journaux d’événements, concernant cette attaque, organisés en 4 parties pour en faciliter l’exploitation.*** *Les parties sont séparées par 2 lignes vides.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Time** | **Source** | **Destination** | **Protocol** | **Info** |
| 05:40:52.655 | 172.16.128.27 | 8.8.8.8 | DNS | Standard query 0x0e55 A xf1.pw |
| 05:40:52.697 | 8.8.8.8 | 172.16.128.27 | DNS | Standard query response 0x0e55 A xf1.pw A 141.8.226.53 |
| … |  |  |  |  |
| 05:41:56.623 | 172.16.128.27 | 141.8.226.53 | TCP | 54650 > 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK\_PERM=1 WS=128 |
| 05:41:57.525 | 141.8.226.53 | 172.16.128.27 | TCP | 23 > 54650 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK\_PERM=1 WS=64 |
| 05:41:58.438 | 172.16.128.27 | 141.8.226.53 | TCP | 54650 > 23 [ACK] Seq=1 Ack=1 Win=29312 Len=0 |
| 05:42:06.624 | 172.16.128.27 | 141.8.226.53 | TELNET | Telnet Data ... |
| 05:42:08.129 | 141.8.226.53 | 172.16.128.27 | TCP | 23 > 54650 [ACK] Seq=1 Ack=5 Win=28992 Len=0 |
| 05:42:09.332 | 172.16.128.27 | 141.8.226.53 | TELNET | Telnet Data ... |
| 05:42:17.525 | 141.8.226.53 | 172.16.128.27 | TCP | 23 > 54650 [ACK] Seq=1 Ack=6 Win=28992 Len=0 |
| 05:42:18.729 | 172.16.128.27 | 141.8.226.53 | TELNET | Telnet Data ... |
| 05:42:19.332 | 141.8.226.53 | 172.16.128.27 | TCP | 23 > 54650 [ACK] Seq=1 Ack=8 Win=28992 Len=0 |
| 05:42:24.632 | 141.8.226.53 | 172.16.128.27 | TELNET | Telnet Data ... |
| 05:42:28.655 | 172.16.128.27 | 141.8.226.53 | TCP | 54650 > 23 [ACK] Seq=8 Ack=3 Win=29312 Len=0 |
| 05:42:29.623 | 172.16.128.27 | 141.8.226.53 | TELNET | Telnet Data ... |
| … |  |  |  |  |
| 16:51:05.004 | 172.16.128.27 | 8.8.8.8 | DNS | Standard query 0xf13b A www.minecraft.net |
| 16:51:05.073 | 8.8.8.8 | 172.16.128.27 | DNS | Standard query response 0xf13b A www.minecraft.net A 52.84.163.172 A 52.84.163.118 A 52.84.163.58 |
| … |  |  |  |  |
| 16:51:56.623 | 172.16.128.27 | 52.84.163.172 | TCP | 29482 > 80 [SYN] Seq=0 Win=8192 Len=0 |
| 16:51:56.624 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 29482 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 |
| 16:51:56.922 | 172.16.128.27 | 52.84.163.172 | TCP | 63132 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:56.923 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 63132 [SYN, ACK] Seq=0 Ack=1 Win=23490 Len=0 |
| 16:51:57.223 | 172.16.128.27 | 52.84.163.172 | TCP | 14218 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:57.223 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 14218 [SYN, ACK] Seq=0 Ack=1 Win=18700 Len=0 |
| 16:51:57.525 | 172.16.128.27 | 52.84.163.172 | TCP | 10296 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:57.525 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 10296 [SYN, ACK] Seq=0 Ack=1 Win=14900 Len=0 |
| 16:51:57.827 | 172.16.128.27 | 52.84.163.172 | TCP | 57279 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:57.829 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 57279 [SYN, ACK] Seq=0 Ack=1 Win=14700 Len=0 |
| 16:51:58.128 | 172.16.128.27 | 52.84.163.172 | TCP | 12640 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:58.129 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 12640 [SYN, ACK] Seq=0 Ack=1 Win=11370 Len=0 |
| 16:51:58.438 | 172.16.128.27 | 52.84.163.172 | TCP | 32111 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:58.438 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 32111 [SYN, ACK] Seq=0 Ack=1 Win=840 Len=0 |
| 16:51:58.728 | 172.16.128.27 | 52.84.163.172 | TCP | 10605 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:58.729 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 10605 [SYN, ACK] Seq=0 Ack=1 Win=660 Len=0 |
| 16:51:59.030 | 172.16.128.27 | 52.84.163.172 | TCP | 12697 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:59.031 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 12697 [SYN, ACK] Seq=0 Ack=1 Win=422 Len=0 |
| 16:51:59.332 | 172.16.128.27 | 52.84.163.172 | TCP | 42057 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:59.332 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 42057 [SYN, ACK] Seq=0 Ack=1 Win=370 Len=0 |
| 16:51:59.632 | 172.16.128.27 | 52.84.163.172 | TCP | 50379 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:59.632 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 50379 [SYN, ACK] Seq=0 Ack=1 Win=290 Len=0 |
| 16:51:59.939 | 172.16.128.27 | 52.84.163.172 | TCP | 1681 > 80 [SYN] Seq=0 Win=1000 Len=0 |
| 16:51:59.940 | 52.84.163.172 | 172.16.128.27 | TCP | 80 > 1681 [SYN, ACK] Seq=0 Ack=1 Win=280 Len=0 |
| … |  |  |  |  |

|  |
| --- |
| Documents associés au dossier B |

Document B1 : Schéma général actuel du réseau de Poitourégie



Document B2 : Architecture actuelle de l’infrastructure du siège

**Schéma de principe actuel des commutateurs du siège**

|  |  |
| --- | --- |
|  | L’ensemble du réseau de Poitourégie est basé sur un principe de redondance. Le cœur du réseau est constitué d’un commutateur niveau 3 Alcatel 6850 U 24 dans chacun des bâtiments A et B, formant un cluster VRRP.  Les liaisons vers les sites techniques, les agences et internet sont assurées par l’opérateur ADISTA via un réseau MPLS.  Dans chaque bâtiment, le commutateur cœur de réseau est connecté aux 2 commutateurs de distribution des serveurs ainsi qu’à l’ensemble des 7 autres commutateurs de distribution clients.  Dans les salles serveurs de chacun des bâtiments se trouvent en redondance 3 clusters VMware ESX reliés directement par une fibre Gigabit.  Le site bâtiment de secours est relié via une fibre optique multimode au coeur de réseau de chacun des bâtiments. |
| Les deux salles serveurs sont distantes d’environ 100 mètres. Leurs interconnexions sont réalisées à l’aide de rocades fibre optique multimode. La « distribution clients » est composée exclusivement de commutateurs Alcatel 6248 en double attachement sur les bâtiments A et B.  Au sein des salles serveurs, l’interconnexion du commutateur « distribution serveurs » s’appuie sur une liaison Gigabit Ethernet cuivre pour la connexion avec le commutateur Alcatel 6850-U24 (universel fibre + GBIC[[8]](#footnote-8)) et une liaison fibre optique pour l’Alcatel 6850-U24 de l’autre salle serveur qui est utilisée pour la redondance du commutateur.  Les commutateurs d’extrémités (clients) sont placés physiquement dans la même salle serveur que le cœur de réseau. La distance qui les sépare est de quelques mètres. | |

**Mise en œuvre du protocole VRRP** (*Virtual Router Redundancy Protocol*)

**En ce qui concerne le cœur de réseau**, le protocole de redondance de routeur virtuel **VRRP** est implémenté. Il s’agit d’un protocole standard décrit par l’IETF dans la RFC 579 qui a pour but de fournir un service de haute disponibilité de la passerelle par défaut des hôtes d’un même réseau, ceci de façon transparente.

Un ensemble de routeurs (ou de commutateurs de niveau 3) forme un routeur virtuel identifié par un VRID (*Virtual Router IDentifier*) auquel est associé une adresse IP virtuelle ainsi qu’une adresse MAC virtuelle. Des rôles *routeur master* et *routeur backup* sont attribués aux différents routeurs du groupe grâce à la définition d’une priorité allant de 1 à 255.

En cas de panne du routeur maître *(master)*, le routeur de secours *(backup)* prend automatiquement le relais.

En cas de problème ; par exemple en cas de détection d’un lien externe désactivé) le routeur maîtrese "dégradera" volontairement en routeur de secoursen baissant sa priorité, et permettra ainsi au routeur de secoursde passer maître.

Dans un groupe VRRP, il n’y a pas de notion de partage de la charge, c’est le routeur maître qui assure exclusivement la transmission des paquets pour le routeur virtuel.

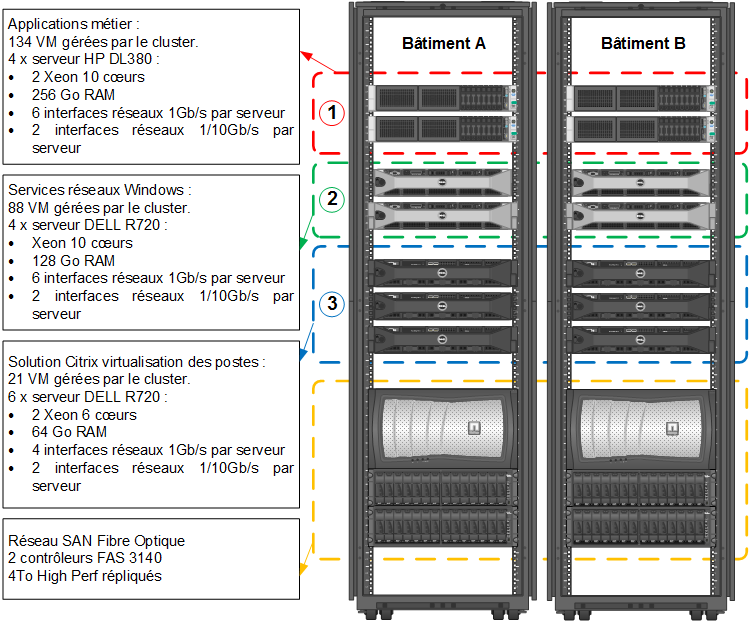
Document B3 : Extrait d’un rapport de M. Jason, responsable infrastructure réseau

Un message émis par un poste client du bâtiment A à destination d’une des agences transitera vers son commutateur de distribution client puis sera commuté vers le cœur de réseau du bâtiment A pour enfin être routé vers le lien ADISTA 100M (débit : 100 Mbits/s).

Un message émis par un client du bâtiment B à destination d’une des agences transitera vers son commutateur de distribution client correspondant puis sera commuté vers le cœur de réseau du bâtiment B qui commutera vers le cœur de réseau bâtiment A pour enfin être routé vers le lien ADISTA 100M.

En cas de panne au niveau du routage du bâtiment A ou de rupture du lien ADISTA 100M, c’est le commutateur de niveau 3 du bâtiment B qui prend le relais en routant vers le lien ADISTA 30M (débit 30 Mbits/s).

Document B4 : Organisation des 3 clusters VMware ESX



Document B5 : Extrait du plan d’adressage des réseaux de Poitourégie

|  |  |
| --- | --- |
| 1. **Désignation** | 1. **Réseaux** |
| Postes clients (bâtiments A et B) | 172.16.0.0 /18 |
| Serveurs | 172.16.64.0/19 |
| SCADA / ICS | 172.16.96.0/19 |
| Réseaux postes de transformation | 172.16.128.0/24 à 172.16.159.0/24 |
| Réseaux agences (16 agences actuellement) | 172.16.192.0/24 à 172.16.207.0/24 (utilisées)  172.16.192.208/24 à 172.16.223.0/24 (disponibles) |
| DMZ privée | 192.168.20.0/24 |
| DMZ publique | 192.168.21.0/24 |

Document B6 : Extrait du cahier des charges "Solution réseau - Poitourégie"

1. **Objet de l’appel d’offres**

La consultation a pour objet d’acquérir et de remplacer des équipements du réseau informatique au siège de Poitourégie.

*Objectifs de la prestation et résultats attendus :*

* Remplacer les commutateurs couche 2 et 3 Alcatel vieillissant de 7 ans qui ne bénéficieront plus de mise à jour de sécurité d’ici peu de temps et dont la maintenance est devenue plus difficile ;
* Fiabiliser le réseau informatique en renforçant la redondance ;
* Améliorer la performance des équipements sur l’ensemble des accès réseaux (la connectique entre les équipements et vers les serveurs devra passer en 10 Gbits) ;
* Permettre une montée en charge.

1. **Durée du contrat de maintenance et clause d’actualisation**

Le contrat qui résultera de cette consultation sera conclu pour une durée de 3 ans, non-renouvelable. Il est constitué d’un lot unique.

**3 - Description technique des besoins**

La solution de commutation matérielle doit permettre de remplacer les commutateurs Alcatel 6850 U24 et Alcatel 6850-P48X. L’objectif principal est de de renforcer la sécurité et la sûreté de la solution “cœur de réseau et “distribution serveurs ainsi que de la solution “distribution clients”.

***Solution cœur de réseau et distribution serveurs***

L’impact de ces fonctionnalités devra apporter une réelle plus-value sur la performance globale du système tant au niveau sécurité que sureté. La solution devra embarquer un système de haute disponibilité ainsi qu’une bascule (la plus transparente possible) avec reprise des données de configuration. Nous souhaitons palier toute perte de connectivité en cas de panne d’un commutateur ou d’une salle serveur complète. Une dégradation des performances est tolérée (coupure des serveurs de tests) pour favoriser la continuité de la production.

Les fonctionnalités attendues sont les suivantes :

* Une connectique 10Gb/s pour l’interconnexion des serveurs de production (les rocades entre les commutateurs et serveurs sont déjà mises en œuvre avec cette technologie) est souhaitée. Les serveurs sont déjà équipés d’une carte 10GbE 2-ports cuivre que l’on utilisera avec les nouveaux commutateurs. On gardera deux connectiques Gigabit Ethernet pour des équipements d’administration sur chaque serveur. Afin de prévoir des évolutions futures, la solution devra permettre des connexions Gigabit supplémentaires pour des serveurs physiques indépendants.

***Solution distribution clients***

Le périmètre de remplacement comprend tous les commutateurs Alcatel 6248-P48X. La technologie utilisée sera du 1 GbE, compatible PoE+. Il est impératif que les commutateurs de distribution "client" soient séparés physiquement du cœur de réseau. Les équipements seront installés dans une baie différente, séparée d’une dizaine de mètres de la baie "cœur de réseau". Les types d’appareils connectés à ces commutateurs sont des PC fixes et portables, des terminaux légers (Wyses, Itium), des téléphones IP (PoE Class : IEEE 802.3af) et des bornes Wi-Fi (PoE Class : IEEE 802.3af/at).

***Solution Bâtiment de secours***

Le site "Bâtiment de secours" (visible sur le schéma de principe) a pour objectif de devenir un site de PCA pour notre bureau de conduite du réseau électrique (BIC). Il devra intégrer un nouveau commutateur de niveau 3 pour permettre à nos collaborateurs de continuer leur activité de gestionnaire de réseau électrique. Actuellement, le routeur opérateur permet le pilotage du réseau mais il y a toujours une adhérence avec les cœurs de réseau des bâtiments A et B pour le routage. Si un incident se produit sur ces derniers, nous souhaitons être autonome sur les configurations de routage dans le Bâtiment de secours.

1. **Prestations attendues par le prestataire**

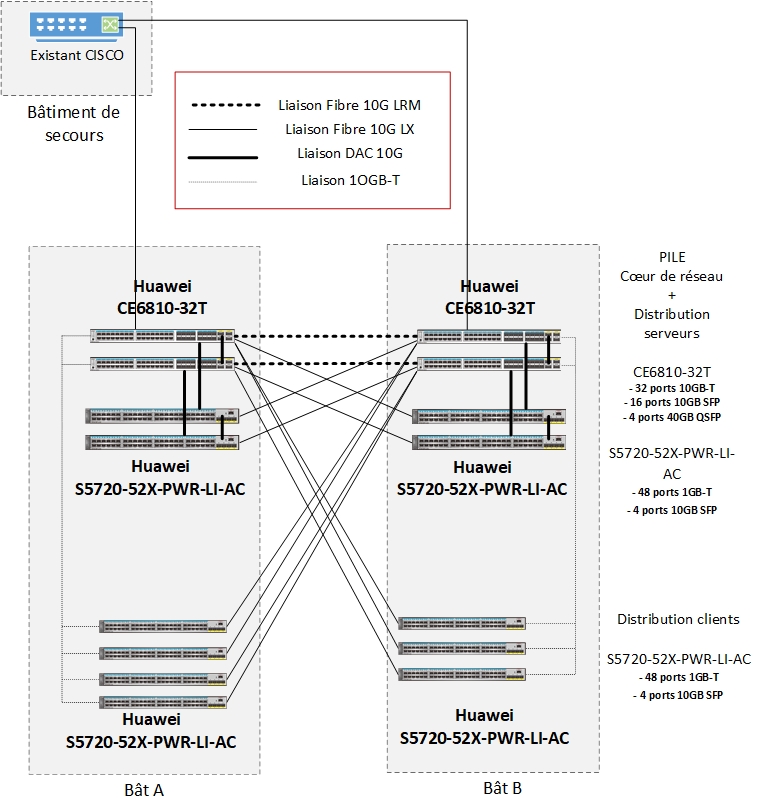
* Fourniture des équipements nécessaires ;
* Configuration des équipements ;
* Mise en production ;
* Recette de la configuration ;
* Formation des équipes techniques Poitourégie ;
* Suivi de la mise en production.

Document B7 : Tableau comparatif des offres des prestataires A et B

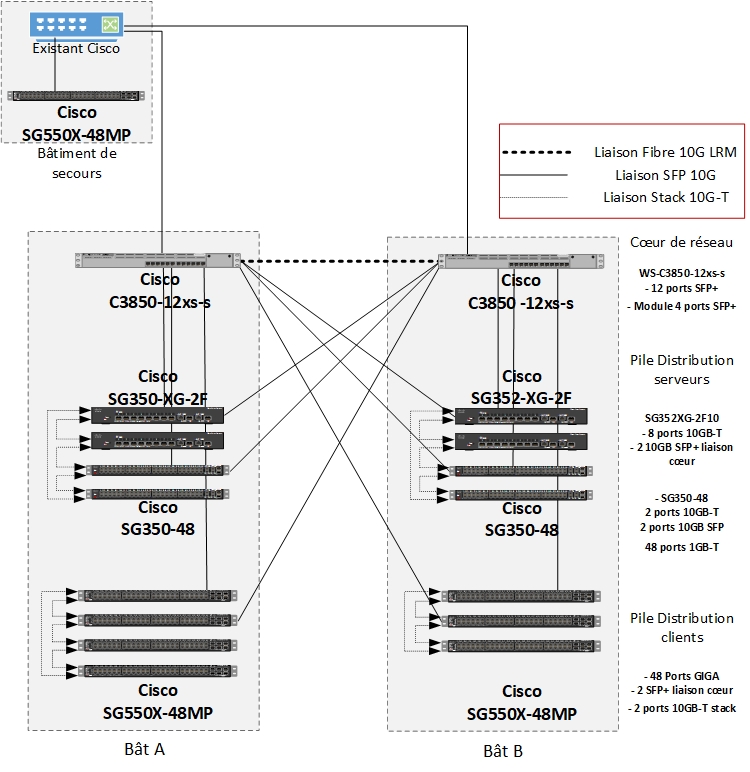
|  |  |  |
| --- | --- | --- |
| **Prestataire** | **A** | **B** |
| **Constructeur** | **Huawei** | **Cisco** |
| **Société** |  |  |
| Chiffre d’affaires | 1.6M€ | 16M€ |
| Références clients | Société PoitouForm | MACIF, Aéroport de Paris, etc. |
| Certifications générale et technique | Certification ISO 9001[[9]](#footnote-9) et 14001[[10]](#footnote-10) Certification Huawei | ISO 9001 et 27001[[11]](#footnote-11) Certification Cisco |
| **Matériel** |  |  |
| Commutateurs niveau 3  Cœur de réseau | 4 x Huawei CE6810-32T16S4Q-LI :   * 32x 10Gbps base-T * 16x 10Gbps SFP+ * Double alimentation * HI-CARE support 3ans   4 x Huawei S5720-52X-PWR-LI-AC   * 48 ports 1GB-T * 4 ports 10GB SFP * mono alim * Garantie à vie J+1   L’ensemble empilé est utilisé selon les ports à l’interconnexion vers les autres bâtiments, les opérateurs, le pare-feu et vers les serveurs | 2 x Cisco WS-C3850-12XS-S   * 12x10GBASE-QSFP+ * Double alimentation |
| Commutateurs  Distribution serveurs | 4 x Cisco SG352XG-2F10   * 8x10G base-T * 2x10 GB SFP+   4 x Cisco SG350X   * 48x1GB-T * 2x10GB-T * 2x10GB SFP |
| Commutateurs  Distribution clients | 7 x Huawei S5720-52P-PWR-LI-AC   * 48x1GB-T * 4x10 GB SFP * Garantie à vie J+1 | 8 x Cisco SG550X-48MP   * 48x1GB-T * 2x10GB SFP+ * 2x20GB-T * PoE+ |
| **Coût** |  |  |
| Coût 1 : Acquisition Matériel | 38 798,00 € | 50 597,65 € |
| Coût 2 : Maintenance pour 3 ans | 3 812,00 € | 5 956,58 € |
| Coût 3 | 7 950,00 € | 12 367,60 € |
| **PRIX TOTAL DE L’OFFRE** | **50 560,00 €** | **68 921,83 €** |
| **Notes** |  |  |
| Note1 :  valorisation technique sur 60 | 45 | 55 |
| Note2 :  valorisation du prix sur 30[[12]](#footnote-12) | 30 | 14 |
| Note3 : | 3 | 9 |
| **NOTE TOTALE** | **78** | **78** |

Le coût 3 est essentiellement composé des prestations inhérentes à la mise en œuvre du projet nécessitant des heures de main d'œuvre facturées : réunion de lancement, déploiement (mise en production), installation et configuration des outils d'administration, test et recette, réunion de suivi, formation des équipes techniques Poitourégie, suivi de la mise en production.

Document B8 : Offres des prestataires A et B – Représentation schématique

****

**Offre Prestataire A basée sur des équipements HUAWEI**

****

**Offre Prestataire B basée sur des équipements CISCO**

1. MPLS (MultiProtocol Label Switching) est un service unifié de transport de données utilisant une technique de commutation de paquets. Il peut être utilisé pour transporter tout type de trafic, par exemple la voix ou des paquets IPv4, IPv6 et même des trames Ethernet ou ATM tout en les isolant. [↑](#footnote-ref-1)
2. **CVE** pour **Common Vulnerabilities and Exposures** est une liste des vulnérabilités publiquement connues, relatives à la cyber sécurité. Chaque vulnérabilité est référencée par un identifiant standardisé de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro d'identifiant) constituant une référence mondiale. [↑](#footnote-ref-2)
3. **Le réseau de distribution (ICS** **pour Industrial Control System**) a en charge la distribution électrique auprès des clients. [↑](#footnote-ref-3)
4. **Le calculateur PLC (Programmable Logic Controller**) est un calculateur temps réel programmable capable d'agir sur son environnement en fonction notamment des données acquises par ses capteurs. Il peut fonctionner de manière autonome ou être commandé à distance via un serveur de contrôle. Il utilise les services réseaux (serveur *Web*, FTP, SNMP, etc.). [↑](#footnote-ref-4)
5. **Une élévation de privilèges** est un mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux dont il dispose normalement afin d'effectuer des tâches qu’il ne peut effectuer habituellement. Cette technique peut être utilisée de manière frauduleuse par un attaquant pour prendre le contrôle d'un système. [↑](#footnote-ref-5)
6. **Une élévation de privilèges** est un mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement afin d'effectuer des tâches qu’il ne peut effectuer normalement. Cette technique peut être utilisée de manière frauduleuse par un attaquant pour prendre le contrôle total d'un système. [↑](#footnote-ref-6)
7. **DoS (Deny of Service**) : attaque visant à rendre un serveur ou un service indisponible (services *Web*, *streaming*, DNS, routeurs, etc...) par l'envoi d'une grande quantité de requêtes simultanées. Une organisation peut être à l’origine de ce type d’attaque (via des logiciels malveillants par exemple) ou en être directement la cible. [↑](#footnote-ref-7)
8. GBIC (Gigabit Interface Converter) : module pouvant servir à convertir un signal électrique en un signal optique. [↑](#footnote-ref-8)
9. **L’ISO 9001** définit des exigences pour la mise en place d'un système de management de la qualité. [↑](#footnote-ref-9)
10. **L’ISO 14001** définit les éléments caractéristiques d’un système de gestion efficace et écologique de l’entreprise. [↑](#footnote-ref-10)
11. **L’ISO 27001** définit les exigences relatives aux systèmes de management de la sécurité des informations (SMSI). [↑](#footnote-ref-11)
12. **La note sur le prix** s’obtient en attribuant la note maximale à l’offre la moins chère. Les autres offres obtiennent un score en fonction de l’écart qui les sépare du montant le plus faible. [↑](#footnote-ref-12)