PCI Resources - Modèle et Approche de l'identification de la portée de PCI DSS

Source: http://www.pciresources.com/pci-dss-scoping-model-and-approach/

L'approche et le modèle décrits ici sont des extraits du Volume 2 (Portée PCI DSS) de la série de livres PCI Resources couvrant PCI DSS. Les détails de l'analyse qui ont mené à ce modèle, ainsi que d'autres détails pertinents d'identification de la portée peuvent être retrouvés dans ce volume (surtout dans la section 2.5). Bien que l'étendue de PCI DSS couvre les individus, processus et technologies (PPT), ce modèle détaille surtout la portion technologique, les composantes des systèmes de TI. Les individus et les processus impliqués devraient aussi être couverts par les organisations.

 Cette approche modèle résulte du travail intellectuel et de l'expérience d'Yves Desharnais en lien avec PCI DSS, depuis 2012 (version 2.0). Ce modèle n'est pas endossé ou approuvé par le PCI SSC ou quiconque.

C'est mon espoir que ce modèle saura aider tous à s'entendre sur ce qui doit être considéré dans la portée, ou au moins fournir une base raisonnable pour la classification et la discussion. Je crois que ce modèle peut aussi être appliqué à d'autres données qui requièrent une protection, par exemple, les informations de santé de patients (PHI) ou de l'information personnellement identifiable (PII). La mise jour à la version 1.2 de ce modèle en décembre 2017 s'aligne avec le Supplément d'Information PCI DSS de Décembre 2016 du PCI SSC, intitulé Guidance for PCI DSS Scoping and Network Segmentation (ce supplément sera abrégé au titre de Recommandations de décembre 2016). La mise à jour n'incluait aucun changement, seulement des mises à jour.

Acronymes

Plusieurs acronymes (dans leur version originale anglaise), définis ici, sont utilisés au sein de ce modèle et de cette approche:

- CHD = Acronyme anglais de Cardholder Data, ou données du Titulaire de carte; inclut le PAN, le nom du propriétaire de la carte, la date d'expiration de la carte et parfois le code de service.
- PAN = Acronyme anglais de Primary Account Number, ou numéro de compte primaire, numéro imprimé sur le recto de la carte.
- SAD = Acronyme anglais de Sensitive Authentication Data, ou données d'identification sensibles; inclut l'information de la bande magnétique, le NIP ou le bloc-NIP, ainsi que la valeur d'autorisation pour une carte-non-présente (associée au code CVV2 mais qui peut aussi répondre d'autre formes, comme CAV2/CVC2/CID).
- SPT = Acronyme anglais de Store, Process or Transmit, ou stocke, traite ou transmet; signifie qu'un système ou processus est en contact avec du CHD et/ou SAD et se trouve obligatoirement dans la portée et sous l'égide du PCI DSS.
- CDE = Acronyme anglais de Cardholder Data Environment, ou environnement des données du titulaire de la carte; essentiellement, ce qu'il faut protéger, qui inclut les systèmes contenant (SPT) du CHD ou SAD, mais non-limité à ceux-ci.
- Isolation = Il n'existe aucun accès possible entre les systèmes.
- Accès contrôlé = Des communications limitées (restreintes) sont possibles entre les systèmes.
- RoC = Rapport sur la conformité (anglais: report on compliance); Rapport documentant les résultats détaillés de l'évaluation PCI DSS d'une entité.

- Entité = Toute organisation qui détient la responsabilité de protéger les données des cartes; en ce qui concerne la conformité au PCI DSS, une entité sera définie comme un marchand ou un prestataire de service.
- DESV = Validation supplémentaire des entités désignées du PCI DSS 3.1, un nouveau standard PCI lancé en juin 2015 qui fait maintenant partie de l'annexe A3 depuis PCI DSS 3.2.

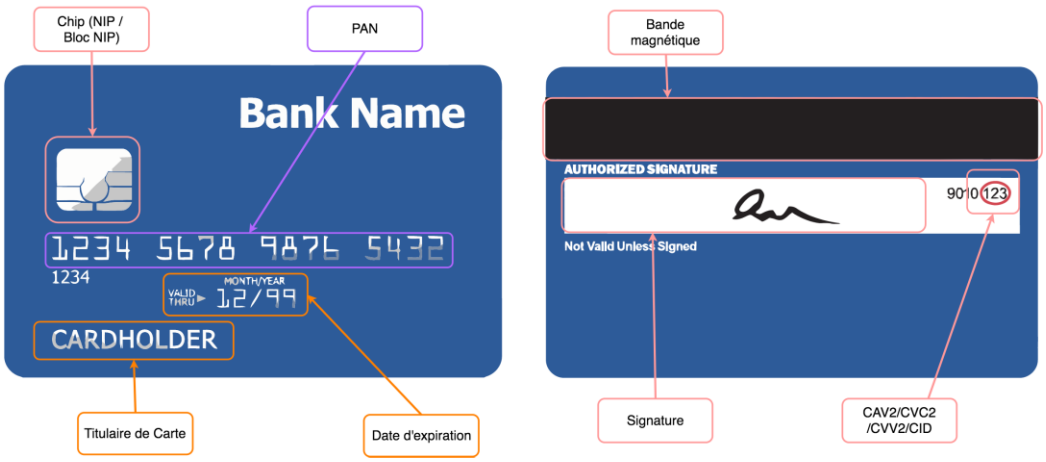

Figure 1 - Représentation d'une carte de crédit (recto et verso) montrant le CHD et le SAD

Catégories de la portée

Mon approche d'identification de la portée (à l'image de nombreuses approches) se base sur la catégorisation des systèmes. En premier lieu, j'ai défini trois (3) catégories de base qui sont inspirées du langage utilisé par le standard PCI DSS: CDE, connecté ("connected") et hors-portée ("out-of-scope"). Un problème que j'ai avec les recommandations du PCI SSC sur la portée est de définir si les dispositifs de segmentation (ou combinaisons de tels dispositifs) représentent des systèmes CDE (mon interprétation originale) ou des systèmes connectés (PSI SCC, et OPST); j'ai donc choisi les traiter comme leur propre catégorie. J'en expliquerai les détails dans le modèle révisé. Ceci n'affecte aucunement la portée mais bien la compréhension. J'entends les décrire un à la fois, en partant du coeur central qu'il faut protéger: la zone où se trouve le CHD et/ou le SAD, i.e. le CDE.

Première catégorie: systèmes CDE

Tous les systèmes CDE sont souvent identifiés en tant que dispositifs de catégorie ou type 1. Il y a 2 sous-catégories au sein du CDE, mais toutes les exigences applicables le sont autant peu importe la sous-catégorie. La FAQ #1252 répond à la question "*Est-ce que les exigences PCI DSS s'appliquent à toute composante système?*", en commençant par: "*Les exigences du PCI DSS s'appliquent à toutes les composantes systèmes, à moins qu'il ne soit démontré qu'une exigence particulière n'est pas applicable pour un système particulier.*" Nous ferons référence à cette FAQ au volume 3 quand nous dresserons la liste de toutes ces exigences. En général, les systèmes CDE sont représentés en ***rouge***.

<u>CDE/CHD</u>

La portée du PCI est présentée en page 10 de la version 3.2 du standard. Le premier paragraphe va comme suit:

> *Les conditions de sécurité de la norme PCI DSS, s'appliquent à tous les composants de système inclus ou connectés à l'environnement des données de titulaires de carte. L'environnement des données de titulaires de carte (CDE) est constitué d'individus, de processus et de technologies qui stockent, traitent, ou transmettent les données de titulaires de carte ou les données d'identification*

sensibles. Les "composants de système" comprennent les dispositifs de réseau, les serveurs, les périphériques informatiques et les applications.

Divisons ce paragraphe entre ses aspects importants.

- "*s'appliquent à tous* ***les composants de systèmes***" - en ajoutant qu'ils "*comprennent les dispositifs de réseau, les serveurs, les périphériques informatiques et les applications.* " - de fait, tout système informatique (hardware, système d'exploitation, logiciel, applications) est donc soumis aux exigences.
- "*(CDE) est constitué d'individus, de processus et de technologies*" - donc, bien que le PCI DSS s'applique aux systèmes informatiques, les individus et les processus restent critiques (et je recommande, comme plusieurs le font, d'adopter une approche commençant par les processus d'affaires).
- "*qui stockent, traitent, ou transmettent les données de titulaires de carte ou les données d'identification sensibles*" - ce dont on réfère souvent sous les acronymes SPT CHD/SAD. Tous les systèmes qui entrent en contact avec du CHD ou du SAD font partie de ceux que l'on doit protéger puisqu'ils entreposent, ou ont accès, à l'information (le bien) que nous avons l'obligation de protéger.

Tous ces systèmes qui SPT CHD/SAD font parti, ou forment la base, du CDE (environnement des données du titulaire de carte - l'environnement en portée pour PCI). Nous nommerons ces systèmes CDE/CHD. Les Recommandations de décembre 2016 les identifient en tant que "systèmes qui stockent, traitent ou transmettent du CHD/SAD". L'OPST les appelle type 1a.

CDE/Contaminated

Dans la section sur la segmentation réseau, le standard établit que *"[l]a segmentation réseau, ou l'isolation (segmentation), de l'environnement des données de titulaires de carte par rapport au reste du réseau de l'entreprise n'est pas une condition de la norme PCI DSS"*. Ainsi, la segmentation réseau n'est requise que pour établir un périmètre externe au réseau. Le standard stipule aussi que "[s]ans une segmentation réseau adéquate (parfois appelée 'réseau plat'), l'ensemble du réseau est inclus dans le champ d'application de l'évaluation PCI DSS". Si vous n'utilisez aucune segmentation, tout devient sujet au PCI DSS. En somme, votre CDE en vient à inclure tous les systèmes dans le même réseau que vos systèmes CDE/CHD en portée (décrits plus haut) jusqu'à ce qu'une segmentation l'en sépare.

Ces systèmes inclus dans la même zone réseau sont identifiés sous le nom de CDE/contaminated (contaminés) puisque l'information pourrait être facilement transmise entre des systèmes qui ne seraient pas autrement restreints (par exemple, par un pare-feu ou autre dispositif). Les Recommandations de décembre 2016 leur font référence *en tant que "composante système sur le même segment de réseau (par exemple, le même subnet ou VLAN) que des systèmes qui stockent, traitent et transmettent des données du titulaire de carte"*.

Deuxième catégorie: Segmenting (ancien nom: CDE/Segmenting)

La deuxième majeure catégorie de systèmes procure (en général au niveau réseau) la segmentation et prévient la "contamination" des systèmes CDE. Typiquement, il s'agit de pare-feu, mais la catégorisation ne s'y limite pas. Ces dispositifs se nomment systèmes Segmenting. La définition de la portée inclut une instruction à cet effet (présente dans plusieurs versions du PCI DSS): "Si une segmentation réseau est mise en place et doit servir à réduire le champ d'application de l'évaluation PCI DSS, l'évaluateur doit s'assurer qu'elle convient bien à cette fin."

Notez que cette fonction peut être remplie par une combinaison de dispositifs et de systèmes, mais plus la complexité en est grande, meilleure devra être la documentation fournie à l'évaluateur.

Pour l'OPST, ces systèmes sont de type "1b" ou "2a", ce qui peut engendrer une confusion. Sans système de segmentation, on ne peut avoir de systèmes connectés; ce que les Recommandations de décembre 2016 du PCI SSC définissent comme "les composantes systèmes segmentant les systèmes CDE des systèmes et réseaux hors-portée", mais qui intègre la catégorie des systèmes connectés ("systèmes connectés ou impactant la sécurité"), j'identifie comme une catégorie séparée pour éviter toute confusion (et c'est mon seul désaccord avec le document du PSI SSC, plutôt une différence de style qu'autre chose).

L'existence de cette deuxième catégorie est requise par l'inclusion d'une nouvelle exigence depuis PCI DSS 3.0 concernant le test de la segmentation durant les tests annuels obligatoires de pénétration interne (#11.3.4). La section 3.3 (segmentation réseau) du gabarit du RoC de PCI DSS 3.2 ajoute une documentation en rapport à la validation d'un évaluation adéquate de segmentation. À noter: les règles de pare-feu qui n'ont aucun lien avec l'environnement CDE sont considérées hors-portée. Ceci peut se produire si le pare-feu gère le point de connexion entre le CDE et plusieurs autres segments de réseau. Dans ce cas, seules les règles qui se rapportent à l'accès au CDE sont en portée (pour une révision), bien qu'il soit recommandé de les traiter toutes de la même manière.

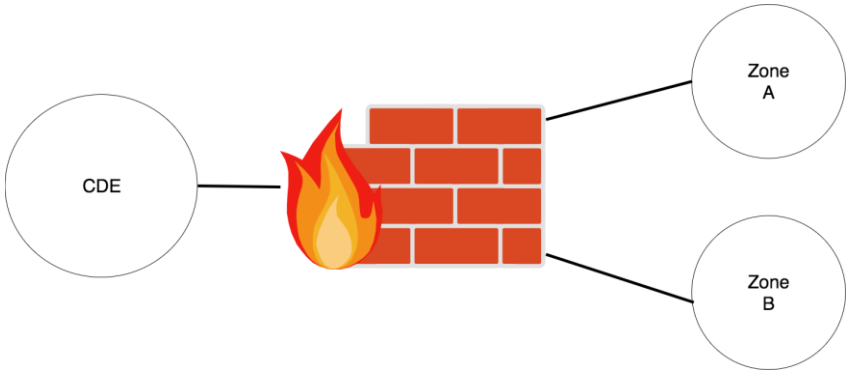

Figure 2 - Image d'un pare-feu et de 3 zones réseau (incluant le CDE)

Par exemple, dans le diagramme précédent, les règles qui limitent les connections entre les zones A et B seraient hors-portée.

En bout de ligne, à moins d'utiliser un pare-feu physique comme machine de segmentation directe, les entités devraient fournir une évaluation qui couvre l'exigence 11.3.4 en rapport aux tests de pénétration de la segmentation.

Les systèmes Segmenting sont généralement représentés en orange.

Segmentation en virtualisation et en infonuagique

Le supplément "Recommandations PCI DSS pour l'infonuagique" parle de segmentation aux sections 4.4 jusqu'à 4.4.3. Il énonce clairement: "La segmentation sur une infrastructure nuagique doit fournir un niveau d'isolation équivalent à ce qui est faisable via une séparation physique de réseau." Bien qu'on y mentionne l'infonuagique, il s'agit aussi du test critique pour tout environnement virtuel. Une entité doit "s'assurer que leur environnement est adéquatement isolé des autres environnements clients". Pour ce qui est du nuage ou des fournisseurs d'hébergement, cette assurance est entre les mains du fournisseur, alors que la validation pour un environnement interne provient de l'entité elle-même. En bout de ligne, la responsabilité de cette validation (peu importe par qui elle est faite) reste entre les mains de l'entité.

Dans la section 4.4.1, la recommandation est faite d'utiliser un "hyperviseur dédié au CDE" afin de simplifier le problème de segmentation (rendu plus complexe à cause des environnements nuagiques

contrairement aux serveurs privés). Dédier l'hyperviseur aux systèmes CDE (aucun mode mixte) est également ce que plusieurs QSA à qui j'ai parlé utilisent comme exigences minimales.

Pour plus de détails, consultez la section 2.7 du volume 2.

Troisième catégorie: systèmes connected (connectés)

Il impose de se demander quand un système CDE peut en contaminer un autre. Certains cas sont plus faciles à comprendre que d'autres. Par exemple, si deux systèmes sur le même segment de réseau peuvent communiquer plus ou moins librement (en lien aux services ouverts), il est évident que la contamination peut arriver (la possibilité étant suffisante pour forcer l'inclusion). Mais comment empêcher un système "connected" (connecté) de devenir contaminé? Analysons le processus étape par étape.

Selon l'exigence #1.2.1, nous savons que la communication entre les systèmes doit être restreinte seulement aux services que requièrent des opérations d'affaires (cette limite est appelée "accès contrôlé"). Il est impossible de garder tous les systèmes nécessaires au sein d'une seule zone, car cela irait à l'encontre de l'idée de réduction de portée vers laquelle on doit s'orienter. Quoi faire, dans ce cas?

Le standard affirme que tout dispositif qui est "connectés [sic] à l'environnement des données de titulaires de carte" (CDE) est dans la portée, n'étant pas complètement isolé. Le standard place en portée "[l]es systèmes" ... "qui pourraient avoir un impact sur le CDE (par exemple, des serveurs de résolution de nom ou de redirection Web)". Il s'agit probablement d'une des plus importantes lignes concernant la portée dans le standard. La présentation à la conférence RSA 2013 ainsi que la présentation aux PCI Community Meetings de 2013 en reparlent à de multiples occasions:

> *Si ça peut impacter la sécurité du CDE, c'est dans la portée*
> *Il faut se rappeler que les systèmes non-CHD peuvent aussi être dans la portée*

et

> *Si un système "hors-portée" peut compromettre le CDE, il n'aurait pas dû être considéré hors-portée.*

Ainsi, si la certitude sur l'inclusion dans la portée d'un système est en doute (comme système "connecté"), nous devons regarder si le fait de compromettre ce système pourrait autoriser une attaque vers un système CDE sans à prime abord requérir qu'un autre système soit compromis. Si tel est le cas, ce système tombe en portée. Le second sous-type de système connecté en fera état également.

Dans cette méthodologie, le terme isolé indique que deux systèmes ne peuvent aucunement communiquer entre eux. Si la communication est limitée (note: l'utilisation des règles "ANY" et "génériques" sont interdites dans PCI DSS), nous parlons d'accès contrôlé. Les présentations de la conférence RSA le confirment:

- *Être hors-portée = isolation = aucun accès*
- *Accès contrôlé ≠ isolation*
- *L'accès contrôlé*
    - *Demeure un accès*
    - *Est une exigence de PCI DSS*
    - *N'isole par un système/réseau d'un autre*
    - *Crée des points d'entrée dans le CDE*
    - *Reste en portée pour PCI DSS*

- *Vérifier que les contrôles d'accès sont fonctionnels*
- *Vérifier que la connexion / point d'entrée est sécurisé*

Les systèmes connectés sont souvent appelés des dispositifs de catégorie 2 ou type 2. Comme dans le cas du CDE, il y a plusieurs types de dispositifs "connectés" présentant des niveaux de risque différents. Les systèmes connectés sont généralement représentés en **jaune**. Examinons ces sous-types.

Connected/Security

Certains systèmes comme les répertoires d'utilisateurs (Active Directory, LDAP), systèmes de gestion des correctifs, systèmes de gestion des vulnérabilités, ainsi que plusieurs autres (cette liste ne se veut pas inclusive) fournissent des 'services de sécurité'. Dans notre comparaison avec la sécurité physique, on pourrait parler des gardes de sécurité qui distribuent les clefs pour les différentes pièces, ou l'équipe de nettoyage qui dessert cette pièce en particulier. On peut appeler ceux-ci des systèmes connected/security.

Les Recommandations de décembre 2016 pour la portée de PCI DSS et la segmentation réseau, dans une section intitulée "Systèmes connectés ou impactant la sécurité", a identifié 3 catégories de systèmes que je considère comme connected/security.

- Le composant de système impacte la configuration ou la sécurité du CDE
- Le composant de système fournit des services de sécurité au CDE
- Le composant de système supporte les exigences du PCI DSS

Je considère que tous ces types de système sont inclus dans mon modèle initial, mais la clarification supplémentaire du conseil PCI est appréciée.

L'OPST les nomme de type "2a".

Systèmes Connected/Communicating

Tout système 'connecté au' CDE (à des systèmes CDE) est considéré comme un système 'connecté'. Les systèmes qui qui se situent "en-dehors" des systèmes Segmenting sont l'exception, par exemple, quand une segmentation affecte aussi le trafic qui n'est pas en lien avec le CDE, comme ce qui décrit dans la section Segmenting et présenté en figure 2.

Certains systèmes connectés (qui ont une connexion avec des systèmes CDE) peuvent être éventuellement considérés hors-portée, mais une évaluation doit être formellement documentée par l'entité afin de déterminer si PCI DSS doit s'appliquer. Il pourrait s'agir d'un système qui reçoit de l'information en-dehors du CDE avec aucune possibilité de réentrance. Par exemple, prenons un système connecté qui reçoit périodiquement des transferts d'information initiés d'un système CDE et sécurisé en fonction d'assurer de ne jamais transmettre du CHD/SAD. Le protocole utilisé pour le transfert de données est le sftp (une composante de la suite d'applications SSH). Le transfert est initié à partir du CDE; un fichier est téléchargé vers le système connecté, puis la connexion est fermée. Autre qu'un message de retour sur le statut qui fait partie du protocole, il n'y a aucune information qui revient vers le système CDE. J'argumenterais que le système connecté tel que décrit ici pourrait être adjugé hors-portée parce qu'il ne peut avoir d'impact sur la sécurité du CDE (bien qu'un outil DLP soit probablement justifié). La documentation du processus d'évaluation doit être rédigée, tenue et conservée, afin d'être présentée à l'évaluateur. Les Recommandations de décembre 2016 identifient ces systèmes en tant que "composant de système connecté directement au CDE". L'OPST les identifie comme "2b" ou "2c". Je ne fais aucune distinction basée sur la direction du transfert, mais bien sur les détails de communication.

Connected/Indirectly

Il y a aussi des systèmes qui n'ont aucun accès direct aux systèmes CDE (ils sont isolés du CDE) qui demeurent en portée. En fait, ils auraient généralement accès aux autres systèmes connected ou segmenting et, par leur intermédiaire, pourraient affecter la sécurité du CDE. Un exemple classique serait celui d'un terminal d'administrateur qui peut gérer un outil de sécurité (répertoire d'utilisateur, etc.) ou des systèmes de transfert d'information en amont vers des systèmes connectés (i.e. système de correctif, ou une connexion http telle que décrite précédemment). Dans le cas d'un répertoire d'utilisateur, un administrateur pourrait théoriquement se donner accès (ou le donner à d'autres) aux systèmes du CDE, et ainsi en pénétrer la sécurité.

En fait, le standard fait état que tout système qui "pourrait avoir un impact sur le CDE" est en portée. On peut parler de ces systèmes comme connected/indirectly. Les Recommandations de décembre 2016 appellent ceux-ci "composant système indirectement connecté au CDE". L'OPST les nomme type "2x".

Quatrième catégorie: systèmes out-of-scope (hors-portée)

Finalement, tout système qui n'est ni CDE ni connected est considéré hors-portée pour la conformité à PCI. Ce système doit être complètement isolé (aucune connexion quelconque) vers un système CDE, bien qu'il puisse interagir avec un système connected (et peut même se retrouver dans la même zone réseau qu'un système connected). Il faut se rappeler, cependant, que s'il peut indirectement affecter la sécurité d'un CDE via un autre système connected, il s'agit donc d'un système connected/indirectly qui se trouve donc en portée.

Des systèmes hors-portée sont généralement présentés en **vert**. Les Recommandations de décembre 2016 pour la portée et la segmentation réseau du PCI DSS présentent 4 tests qu'un système hors-portée doit passer (l'équivalent de s'assurer que le système ne se trouve dans l'une des autres catégories précédemment définies).

- Le composant de système NE peut PAS stocker, traiter ou transmettre du CHD/SAD => autrement il s'agit d'un système CDE/CHD.
- Le composant de système NE se trouve PAS sur le même segment de réseau ou sur le même subnet ou VLAN qu'un système qui stocke, traite ou transmet du CHD => autrement, il s'agit d'un système CDE/contaminated.
- Le composant de système NE peut PAS se connecter ou accéder à aucun système du CDE => autrement, il s'agit d'un système connected/communicating (je continue de stipuler que certaines connections pourraient être considérées hors-portée si on peut démontrer qu'elles ne posent aucun risque, par exemple, les pings).
- Le composant de système NE peut PAS accéder au CDE ou impacter un contrôle de sécurité du CDE via un système en-portée => autrement, il s'agit d'un système connected/security ou connected/indirectly.

L'OPST identifie cette catégorie comme type "3".

Sommaire des catégories

Bref, en ce qui concerne le PCI DSS, il existe quatre types de systèmes de base. Le premier groupe est l'environnement des données des titulaires de cartes (CDE). Le second groupe comprend les systèmes de segmentations, requis pour séparer les autres groupes. Le troisième groupe inclut les systèmes connected, ces systèmes qui ont une connexion directe ou indirecte avec le CDE (qui selon les Recommandations de décembre 2016 sont appelés "Systèmes Connecté-à ou Systèmes impactant la Sécurité"). Le quatrième contient les systèmes hors-portée, complètement isolés des systèmes CDE. En ce qui les concerne, il faut toujours se rappeler que les systèmes "qui pourraient avoir un impact sur le CDE (par exemple, des serveurs de résolution de nom ou de redirection Web)" sont toujours en portée ou, en d'autres mots: "Si ça peut impacter la sécurité du CDE, c'est dans la portée".

La classification est la clef qui nous permet de ne pas avoir à appliquer les exigences du PCI DSS à tous les systèmes.

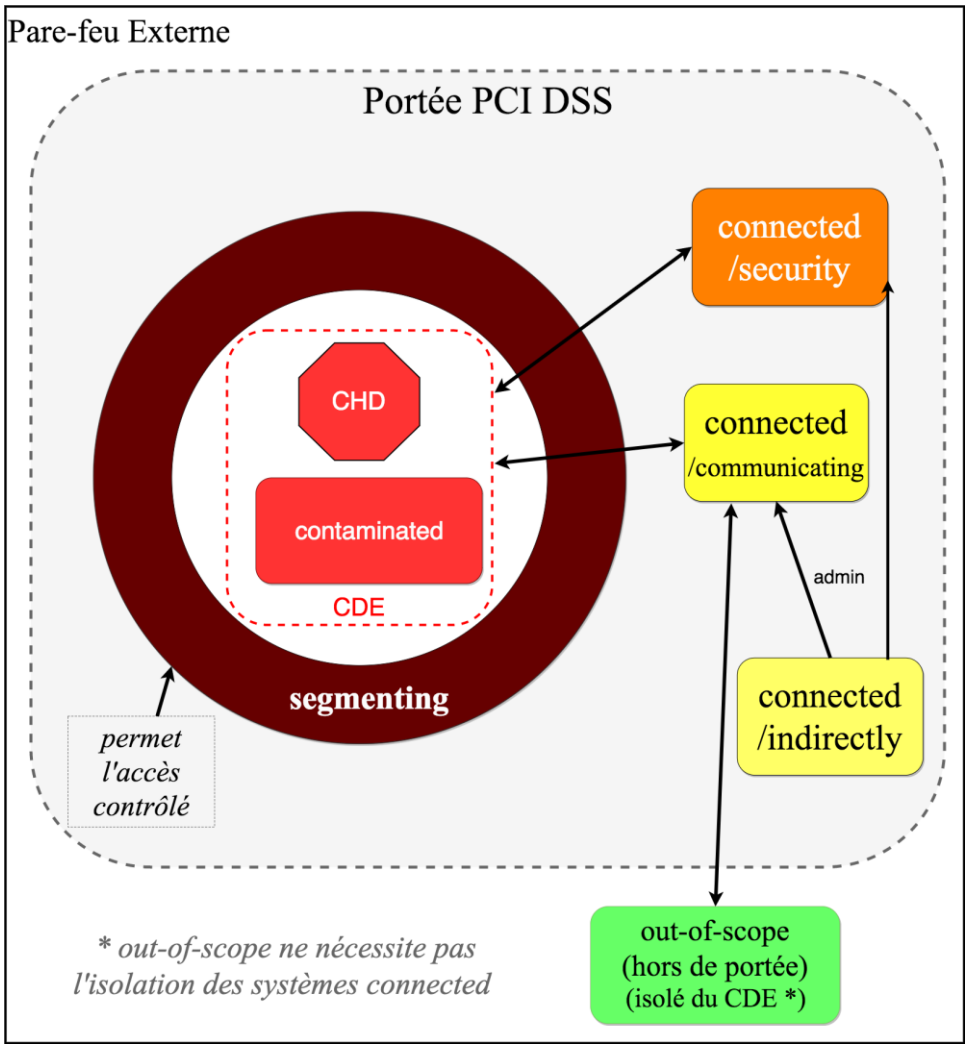

Figure 3 - Diagramme de type de systèmes dans la portée PCI DSS

Type	Sous-type	Segmentation	CHD/SAD	Dans la portée
CDE	CHD	Aucune	Oui	Oui
CDE	Contaminated	Aucune	Non	Oui
Segmenting		Fournit la segmentation	Non	Oui
Connected	Communicating	Accès contrôlé	Non	Oui
Connected	Security	Accès contrôlé	Non	Oui
Connected	Indirectly	Accès indirect	Non	Oui
Out-of-scope		Isolation	Non	Non

Tableau 1 - Sommaire des catégories de classification

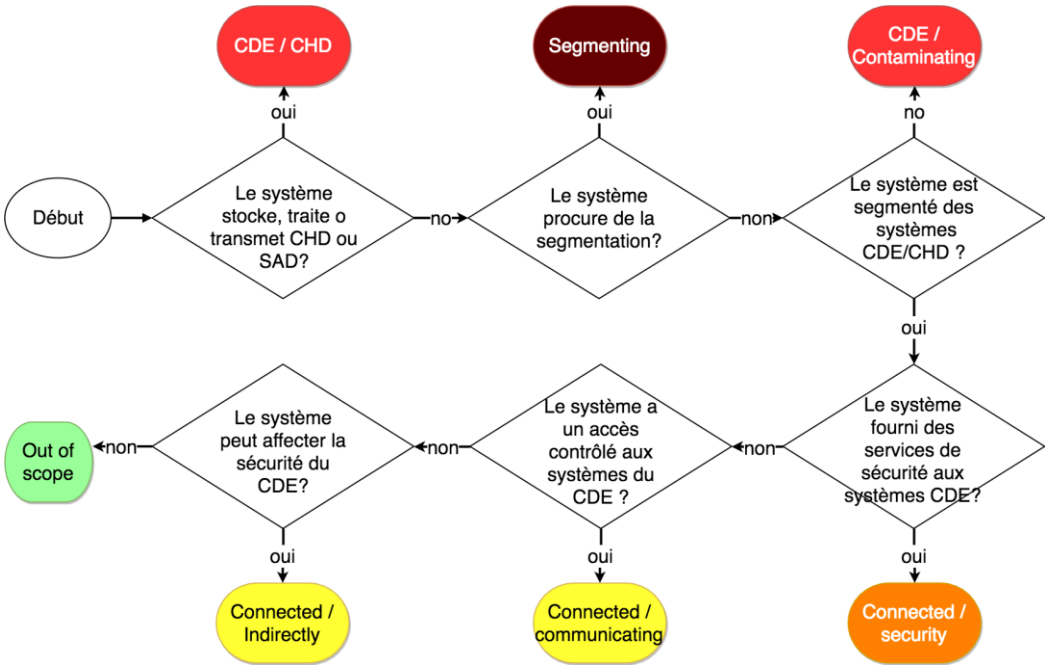

Figure 4 - Arbre décisionnel de type de systèmes dans la portée PCI DSS

Approche d'identification de la portée et documentation de la portée

Maintenant que nous avons décrit le modèle de classification de la portée, nous devons voir comment adéquatement documenter la portée. L'approche suit étroitement le modèle, y ajoutant quelques éléments de validation. Encore une fois, les pages 10 et 11 du standard nous fournissent l'approche générale, tandis que l'annexe A3 (DESV) ajoute des recommandations à cette définition, en particulier dans les exigences #A.3.2.* (DE.2.* dans le DESV). Comme nous avons deux types de systèmes en portée (CDE et connected), nous diviserons le processus en deux parties (une par type).

Partie 1 - Identifier le CDE (un processus en quatre étapes)

Étape 1.1. - Identifier les systèmes qui stockent, traitent ou transmettent du CHD/SAD (systèmes CDE/CHD). On y inclut les serveurs, bureaux de travail, appareils et équipement réseau. Les flux de CHD doivent être documentés en diagrammes (#1.1.3) et détaillés en descriptions textuelles produites à cette fin (RoC #4.2). Les flux et les descriptions doivent couvrir la capture, l'autorisation, le règlement et les remboursements.

Étape 1.2 - Identifier où la segmentation se produit (systèmes Segmenting). Ceux-ci préviennent la contamination et limitent la portée du CDE. Les segments identifiés séparant les zones CDE sont généralement représentés en rouge dans les diagrammes de réseau.

Note: à chaque implémentation d'un nouveau type de segmentation, vous devriez effectuer un test de pénétration tel que stipulé dans l'exigence #11.3.4 et confirmer l'efficacité (et réparer les problèmes identifiés) avant de déployer la nouvelle technologie sur la production (également requis par #A3.2.4).

Étape 1.3 - Identifier tous les autres systèmes qui sont contaminés (CDE/contamined). Il faut pour cela se servir de l'inventaire maintenu à jour (selon #2.4) mais aussi inclure une découverte du système à l'aide d'outils de scan (le ping sweep est d'usage ici). Toute différence avec l'inventaire devrait être vue comme une défaillance du processus d'inventaire et servir à réviser et corriger le processus. Les systèmes couverts incluent les serveurs, bureaux de travail, appareils, équipement réseau dans la même zone segmentée du réseau ou qui fonctionne sous le même hyperviseur segmentant (plus de détails sur les hyperviseurs seront fournis dans la section 2.7.1 sur la virtualisation).

Note: puisque les systèmes CDE/contamined nous offrent des opportunités de réduction de la portée, cette étape peut servir à réviser si un système devrait être retiré du CDE. Plus de détails à ce sujet se trouvent dans le volume 3 en rapport au coût total de propriété (TCO).

Étape 1.4 - Finalement, valider qu'il n'existe de PAN dans aucun autre système (#A3.2.5) ou emplacement. Cette "recherche de données" est généralement effectuée via des outils spécialisées (prévention de pertes de données, ou en acronyme anglais DLP) mais un simple 'grep' sur Unix/Linux fonctionne également. Ces recherches utilisent généralement des 'expressions régulières', mais une inspection manuelle peut être applicable quand on doit réviser un petit nombre de systèmes, ou pour des systèmes où de tels outils n'existent pas (par exemple, un ordinateur central, ou mainframe). Pour ceux dont les ressources sont limitées, des options abordables et gratuites existent également.

La "recherche de données" devrait être effectuée sur tout système avec un potentiel de stocker du PAN; au minimum, ceci doit couvrir tous les systèmes dans le CDE et tous les systèmes connected (mais en fait, devrait aussi inclure les serveurs, ordinateurs de bureau et portables). Si quelconque système contient du PAN, les options suivantes se présentent:

- Considérer le système comme CDE/CHD et refaire les étapes précédentes d'identification
- Migrer le système vers le CDE et recommencer les étapes précédentes

- De façon sécuritaire, effacer le CHD et déterminer comment et pourquoi le PAN a été transféré au système ou à l'emplacement, ceci afin d'éviter d'augmenter la portée

Dans tous les cas, on doit traiter le tout comme un incident de sécurité, selon les exigences #12.10.*.

Note 1: la version 3.2 du PCI DSS clarifie la portée de ce qui doit être vérifié en ajoutant la ligne suivante: "*Tous les types de systèmes et d'emplacements doivent être pris en compte dans le processus de la détermination du champ d'application, y compris les sites de sauvegarde/rétablissement et les systèmes de reprise des services.* "

Note 2: il s'agit également d'un bon moment pour réviser l'exigence #3.1 et la procédure de test #3.1.b afin de s'assurer que le CHD est détruit après la période de rétention approuvée.

Partie 2 - Identifier les systèmes connected (un processus en cinq étapes)

Une fois que le CDE a été correctement validé, il faut identifier les autres systèmes aussi dans la portée.

Étape 2.1 - Réviser toutes les règles de pare-feu en portée (ou équipement équivalent qui implémente les ACL) des systèmes de segmentation pour dresser une liste de tous les systèmes qui peuvent se connecter au CDE. Si des règles existent pour une étendue réseau plutôt que pour des systèmes individuels, alors l'utilisation d'un outil de découverte du système pour l'étendue totale est requise (voir étape 1.3 de l'identification CDE). Notez que si une règle affecte un système qui n'existe plus, cette règle doit être retirée, tel que stipulé par #1.1.7. Le fait que la mise hors service n'ait pas retiré le système du pare-feu devrait être traité comme un incident et demander une révision du processus de contrôle des changements. Avec une liste complète, on peut procéder à la classification de ces systèmes selon le modèle.

Étape 2.2 - Identifier les systèmes qui fournissent des services de sécurité, ou des services qui peuvent affecter la sécurité du CDE, et qui seront classifiés comme systèmes connected/security. On y trouve, au minimum:

- Services d'identité et de répertoire (Active Directory, LDAP)
- Systèmes de noms de données (DNS), systèmes de temps de réseau (NTP)
- Systèmes de gestion des correctifs
- Systèmes de gestion des vulnérabilités
- Systèmes de gestion des anti-virus
- Gestion de l'intégrité des fichiers (FIM) ou systèmes de détection de changements
- Systèmes de surveillance des performances
- Systèmes de gestion des clefs de chiffrement
- Systèmes d'accès à distance (VPN)
- Systèmes d'authentification multi-facteurs
- Systèmes de gestion de registre et solutions de surveillance (SIEM, syslog, etc.)
- Systèmes de détection des intrusions/systèmes de prévention des intrusions (IDS/IPS)

Étape 2.3 - Identifier les systèmes tierces-parties qui peuvent être connectés au CDE via internet ou un lien privé. Les systèmes qui sont hors de votre contrôle sont également hors-portée, mais les fournisseurs tierces-parties doivent être gérés selon les exigences #12.8.*. Notez bien que si les connections traversent via un équipement du réseau interne, comme un routeur, alors cet équipement se retrouve dans la portée.

Étape 2.4 - Identifier les systèmes connectés qui ne font que recevoir de l'information et qui peuvent (après analyse) être considérés hors-portée s'ils ne présentent 'aucun risque' pour le CDE. Ces

systèmes, en général, ne peuvent pas établir de connexion avec le CDE par eux-mêmes et n'offrent pas de retour vers le système initiateur (le ping, ou protocole ICMP, peut être une exception). Il pourrait s'agir d'une connexion sftp, telle que décrite préalablement. Notez bien que certains protocoles (DNS, NTP) qui pourraient avoir été mis hors-portée ont été utilisés lors de brèches précédentes pour extraire de l'information. Dans ces situations, cependant, IDS/IPS, DLP ou un autre contrôle sur les points de connexion du CDE ou sur le système initiateur peuvent être plus appropriés pour surveiller la sécurité. L'analyse devrait être hautement documentée et cette documentation doit être maintenue à jour pour une révision par votre évaluateur (QSA, ISA, etc.).

Les systèmes restants dans la liste produite durant la première étape sont simplement considérés comme des systèmes connected/communicating.

Étape 2.5 - Finalement, identifier les systèmes qui sont isolés du CDE mais pourraient toujours affecter sa sécurité, indirectement via d'autres systèmes connectés. On les identifie naturellement comme connected/indirectly. Souvent, on parle de consoles administratives ou d'ordinateurs de bureau ou portables d'un administrateur.

Recommandation supplémentaire

Le gabarit du rapport RoC offre plus de détail sur ce qui doit être documenté. Notre documentation devrait inclure l'information dans les sous-sections suivantes des sections 2, 3 et 4 du gabarit de rapport RoC. Les endroits identifiés comme "évaluateur" ne sont d'usage que pour l'évaluateur, pas l'entité, même si l'évaluateur travaille à l'interne, soit un ISA ou quelqu'un responsable de responsable le questionnaire d'auto-évaluation (acronyme anglais SAQ, Self-Assessment Questionnaire).

Section		**Détail**
2	Aperçu Sommaire	Titre
2.1	Description de l'activité d'affaires de carte de paiement de l'entité	
2.2	Diagramme(s) de réseau de haut-niveau	PCI DSS 1.1.2
3	Description de la portée du travail et approche adoptée	Titre
3.1	Validation de l'évaluateur de la définition de l'environnement des données du titulaire de carte (CDE) et de la précision de la portée	Évaluateur
3.2	Survol de l'environnement des données du titulaire de carte (CDE)	Individus, processus et technologies
3.3	Segmentation réseau	Comment la segmentation est implémentée
3.4	Détails des segments du réseau	Toutes les zones du CDE contenant les systèmes qui contiennent SPT CHD/SAD
3.5	Entités connectées pour le traitement	PCI DSS 12.8.*
3.6	Autres entités d'affaires dont la conformité avec le PCI DSS est exigée	
3.7	Sommaire du sans-fil	
3.8	Détails du sans-fil	
4	Détails du l'environnement révisé	Titre
4.1	Diagramme(s) détaillé(s) du réseau	PCI DSS 1.1.2
4.2	Description des flux de transferts de données des titulaires de carte	PCI DSS 1.1.3
4.3	Stockage des données des titulaires de carte	Une sous-catégorie des systèmes CDE/CHD
4.4	Matériel critique en usage dans l'environnement des données du titulaire de carte	Systèmes CDE et connected/security
4.5	Logiciels critiques en usage dans l'environnement des données du titulaire de carte	Systèmes CDE et connected/security
4.6	Échantillonnage	Évaluateur
4.7	Groupe d'échantillons pour le rapport	Évaluateur
4.8	Fournisseurs de services et autres tierces-parties avec qui l'entité partage les données des titulaires de carte	PCI DSS 12.8.*
4.9	Applications et solutions de paiement tierce-partie	PA-DSS
4.1	Documentation révisée	Évaluateur
4.11	Individus interviewés	Évaluateur
4.12	Fournisseurs de services gérés	Inclus dans la portée ou en PCI DSS 12.8.*
4.13	Sommaire divulgué pour les réponses "mises en place avec contrôles de compensation" (Oui avec CCW)	Évaluateur
4.14	Sommaire divulgué pour les réponses "non-testées"	Évaluateur

Tableau 2 - Sections de rapport requises pour la documentation en portée dans le Gabarit de Rapport sur la conformité

Les sous-sections identifiées sous "évaluateurs" seraient remplies par cet évaluateur durant l'évaluation de conformité (RoC ou SAQ). L'appellation "Titre" ne représente qu'un entête.

Références:

Ce modèle s'inspire des pages 10 et 11 du standard ainsi que de quelques autres documents:

- Une présentation par le PCI SSC à la conférence RSA en 2013 [1] (publique) et une série de diapositives similaires provenant des PCI Community Meetings de 2013 (disponible aux évaluateurs PCI: QSAs, ISAs, PCIPs).
- Les réponses à la Foire Aux Questions (FAQ) du PCI SSC [2]
- PCI DSS Validation complémentaire des entités désignées pour PCI DSS 3.1 (DESV, lancée en juin 2015) - Une nouvelle série d'exigences assurant qu'une entité maintient sa conformité continue auprès du PCI DSS et qui permet la détection de non-conformité dans un processus de vérification continue; ces exigences s'appliquent aux entités désignées par les marques de cartes ou les acquéreurs qui présentent un haut degré de risque pour l'industrie. Le DESV est maintenant intégré sous la forme de l'annexe A3 dans le PCI DSS 3.2. [3]
- Gabarit de Rapport sur la conformité [4]
- Suppléments d'information
    - Meilleures Pratiques pour le Maintien de la conformité PCI DSS (lancé en août 2014 mais mise à jour en mars 2016) [5] (qui de plus d'une manière est remplacé par le DESV)
    - La Protection des données de carte de paiement par téléphone (mars 2011) [6]
    - Assurance Sécurité des Tierces-Parties [7] (août 2014)
    - Recommandations PCI DSS 3.0 pour la l'infonuagique [8] (avril 2018)
    - Recommandations de virtualisation version 2.0 [9] (juin 2011)
    - Supplément d'information PCI DSS: Recommandations pour la portée PCI DSS et la segmentation réseau [10] (décembre 2016)

[1] (RSA PCI DSS Scope, 2013). less is more pci dss scoping demystified - RSA Conference. Récupéré le 2 juillet 2015, de https://www.rsaconference.com/writable/presentations/file_upload/dsp-w21.pdf.
[2] (PCI SSC FAQs). FAQs - PCI Security Standards Council. Récupéré le 2 juillet 2015, de https://www.pcisecuritystandards.org/faq/.
[3] PCI DSS 3.2.1. Récupéré le 1 juillet 2018, de https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.
[4] Gabarit de Rapport sur la conformité. Récupéré le 1 juillet 2018, de https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-ROC-Reporting-Template.pdf.
[5] (2014). Best Practices for Maintaining PCI DSS Compliance. Récupéré le 2 juillet 2015, de https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf.
[6] (2011). Protecting Telephone-based Payment Card Data - PCI ... Récupéré le 2 juillet 2015, de https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf.
[7] (2016). Third-Party Security Assurance v1.1 - PCI Security Standards. Récupéré le 31 mai 2016, de https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf.
[8] (2013). PCI DSS Cloud Computing Guidelines - PCI Security ... Récupéré le 1 juillet 2018, de https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.
[9] (2011). Virtualization Guidelines - PCI Security Standards Council. Récupéré le 13 juillet 2015, de https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.
[10] (2017). December 2016 PCI council scoping guidance vs PCI Resources model - PCI Resources. Récupéré le 16 janvier 2017, de https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

Historique des versions

Version	Auteur	Description	Date
1.0	Yves Desharnais	Version initiale	Juillet 2015
1.1	Yves Desharnais	Clarifications, Formatage et Actualisations à PCI DSS 3.2 et autres documents actualisés du PCI SSC	Juillet 2016
1.2	Yves Desharnais	Clarifications et changements reliés au document December 2016 PCI council scoping guidance	Décembre 2017
1.2.1	Yves Desharnais	Changements mineurs pour PCI DSS 3.2.1, et versions initiales en espagnol et français	Juillet 2018

Auteur:

Yves Desharnais, 8850895 CANADA INC.
Email: info@pciresources.com
Site web: www.pciresources.com