Prestataires de
de Détection des Incidents de Sécurité (PDIS)
&
de Réponse aux Incidents de Sécurité (PRIS)

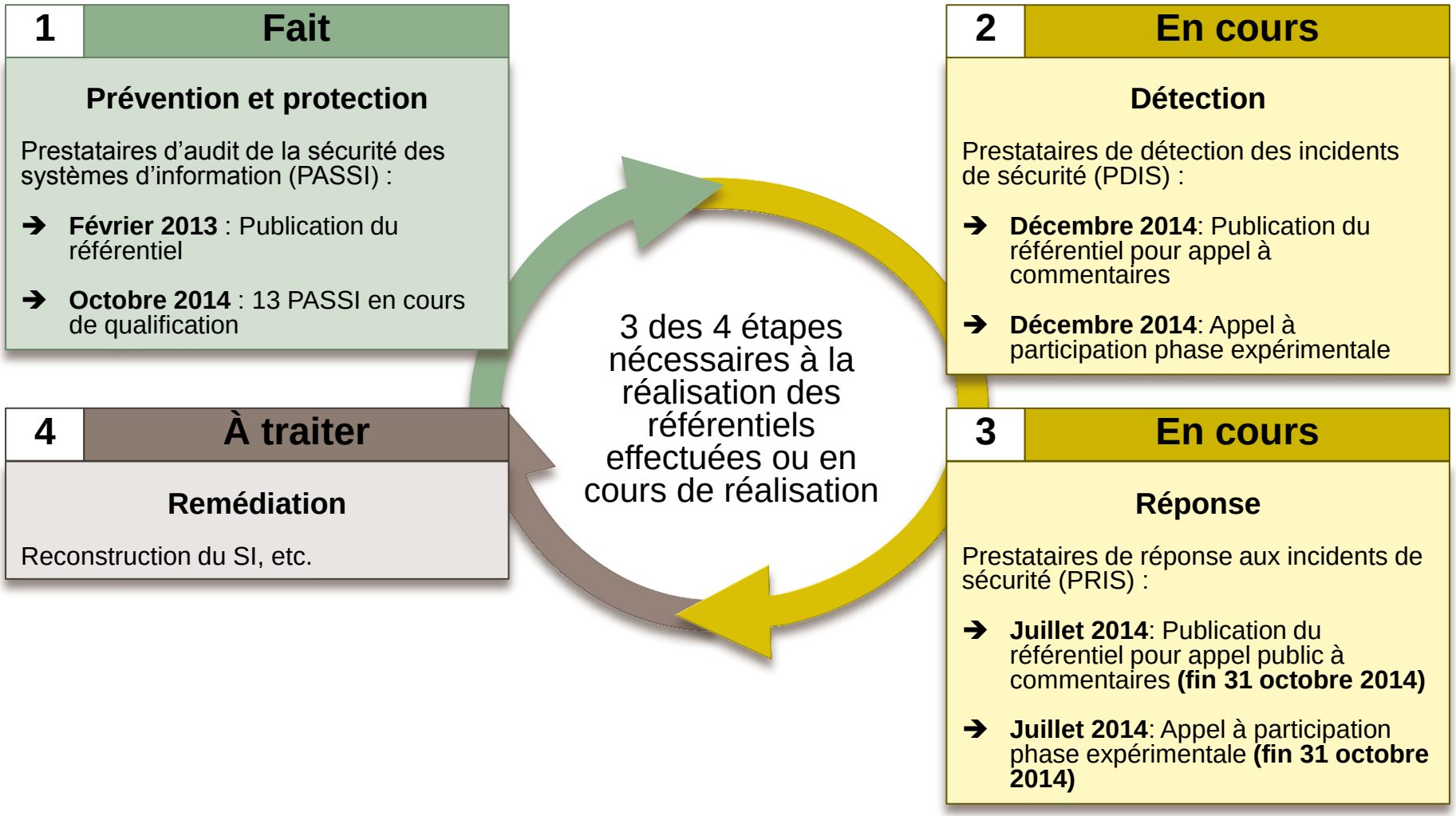
Présentation des référentiels

Mardi 14 octobre 2014

PLAN

- Feuille de route prestataires de « Cyberdéfense »
- Rappels sur la qualification
- Les prestataires d'audit de la sécurité des systèmes d'information (PASSI)
- Les prestataires de détection des incidents de sécurité (PDIS)
- Les prestataires de réponse aux incidents de sécurité (PRIS)
- Recommandations aux prestataires
- Recommandations aux commanditaires

FEUILLE DE ROUTE QUALIFICATION DES PRESTATAIRES DE « CYBERDÉFENSE »



RAPPELS SUR LA QUALIFICATION (1/2)

Cadre réglementaire:

- Référentiel général de sécurité (RGS)
- Loi de programmation militaire (LPM)

Chaque référentiel d'exigences est…

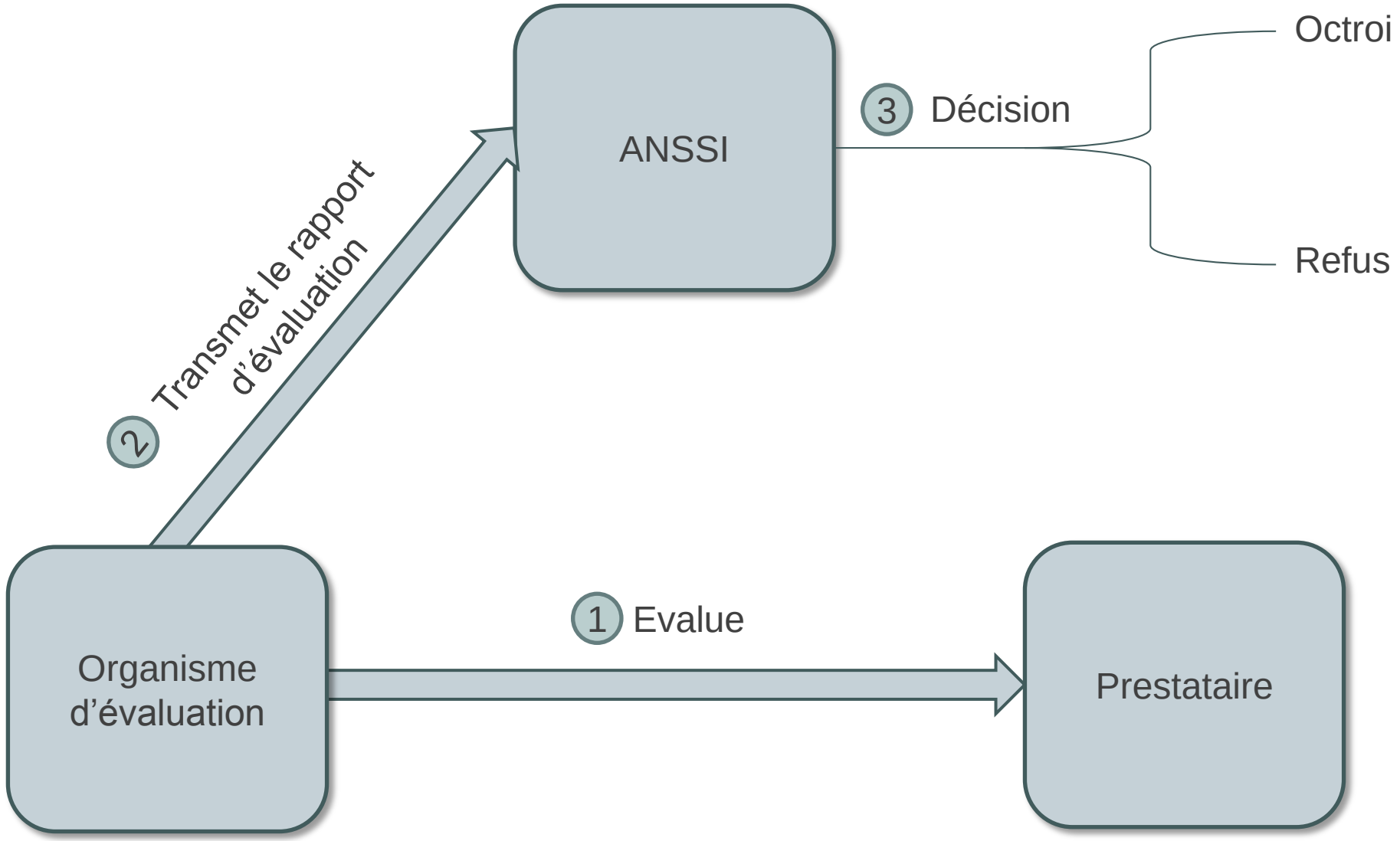
… élaboré en **groupes de travail** (prestataires, commanditaires, certificateurs / auditeurs)

… publié pour **appels publics** à commentaires

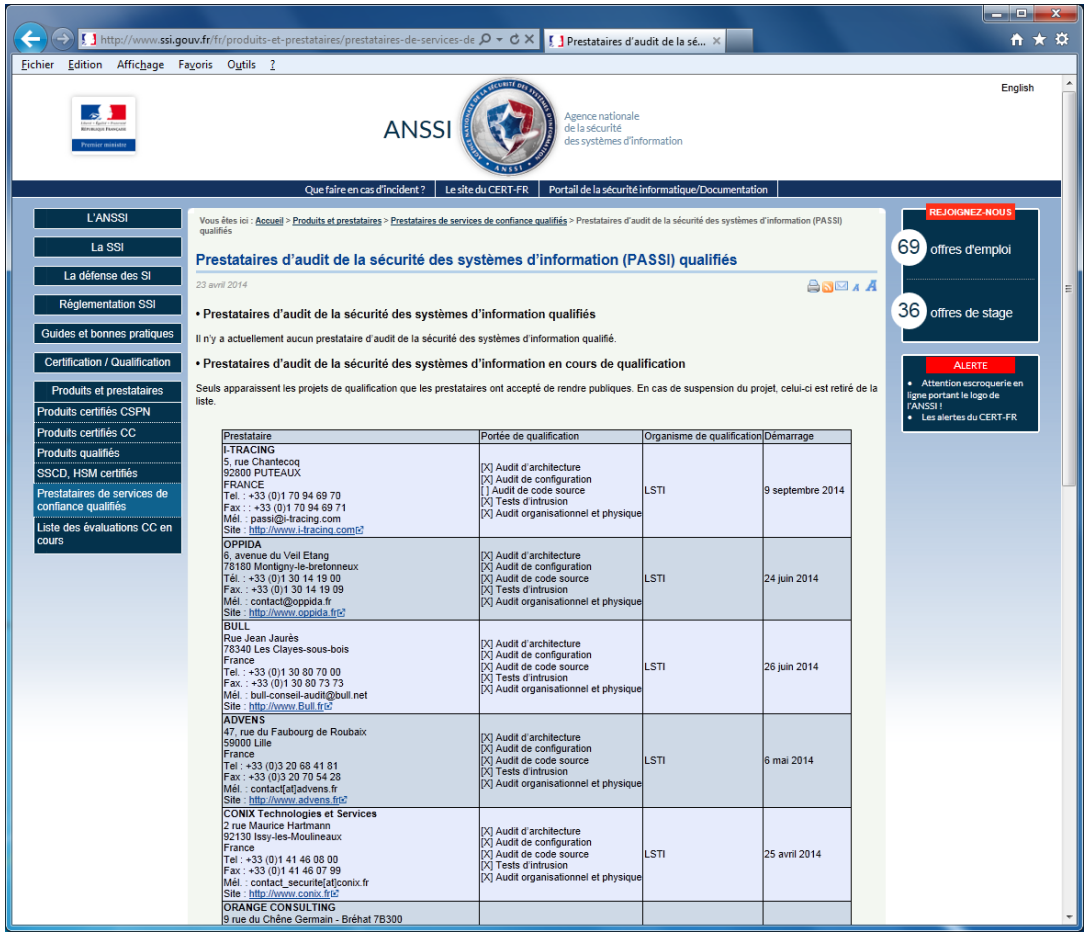
… testé en **conditions réelles** en phase expérimentale

Un prestataire qualifié
=
Un prestataire conforme aux référentiels
=
Un prestataire recommandé par l'ANNSI

RAPPELS SUR LA QUALIFICATION (2/2)



PRESTATAIRES D'AUDIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (PASSI)



Fichier Edition Affichage Favoris Outils ?

English

ANSSI — Agence nationale de la sécurité des systèmes d'information

Que faire en cas d'incident ? | Le site du CERT-FR | Portail de la sécurité informatique/Documentation

L'ANSSI
La SSI
La défense des SI
Réglementation SSI
Guides et bonnes pratiques
Certification / Qualification
Produits et prestataires
Produits certifiés CSPN
Produits certifiés CC
Produits qualifiés
SSCD, HSM certifiés
Prestataires de services de confiance qualifiés
Liste des évaluations CC en cours

Vous êtes ici : Accueil > Produits et prestataires > Prestataires de services de confiance qualifiés > Prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés

Prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés

23 avril 2014

• **Prestataires d'audit de la sécurité des systèmes d'information qualifiés**

Il n'y a actuellement aucun prestataire d'audit de la sécurité des systèmes d'information qualifié.

• **Prestataires d'audit de la sécurité des systèmes d'information en cours de qualification**

Seuls apparaissent les projets de qualification que les prestataires ont accepté de rendre publiques. En cas de suspension du projet, celui-ci est retiré de la liste.

Prestataire	Portée de qualification	Organisme de qualification	Démarrage
I-TRACING 5, rue Chantecoq 92800 PUTEAUX FRANCE Tel. : +33 (0)1 70 94 69 70 Fax : : +33 (0)1 70 94 69 71 Mél. : passi@i-tracing.com Site : http://www.i-tracing.com	[X] Audit d'architecture [X] Audit de configuration [ ] Audit de code source [X] Tests d'intrusion [X] Audit organisationnel et physique	LSTI	9 septembre 2014
OPPIDA 6, avenue du Veil Etang 78180 Montigny-le-bretonneux Tél. : +33 (0)1 30 14 19 00 Fax. : +33 (0)1 30 14 19 09 Mél. : contact@oppida.fr Site : http://www.oppida.fr	[X] Audit d'architecture [X] Audit de configuration [X] Audit de code source [X] Tests d'intrusion [X] Audit organisationnel et physique	LSTI	24 juin 2014
BULL Rue Jean Jaurès 78340 Les Clayes-sous-bois France Tel. : +33 (0)1 30 80 70 00 Fax. : +33 (0)1 30 80 73 73 Mél. : bull-conseil-audit@bull.net Site : http://www.Bull.fr	[X] Audit d'architecture [X] Audit de configuration [X] Audit de code source [X] Tests d'intrusion [X] Audit organisationnel et physique	LSTI	26 juin 2014
ADVENS 47, rue du Faubourg de Roubaix 59000 Lille France Tel : +33 (0)3 20 68 41 81 Fax : +33 (0)3 20 70 54 28 Mél. : contact[at]advens.fr Site : http://www.advens.fr	[X] Audit d'architecture [X] Audit de configuration [X] Audit de code source [X] Tests d'intrusion [X] Audit organisationnel et physique	LSTI	6 mai 2014
CONIX Technologies et Services 2 rue Maurice Hartmann 92130 Issy-les-Moulineaux France Tel : +33 (0)1 41 46 08 00 Fax : +33 (0)1 41 46 07 99 Mél. : contact_securite[at]conix.fr Site : http://www.conix.fr	[X] Audit d'architecture [X] Audit de configuration [X] Audit de code source [X] Tests d'intrusion [X] Audit organisationnel et physique	LSTI	25 avril 2014
ORANGE CONSULTING 9 rue du Chêne Germain - Bréhat 7B300			

REJOIGNEZ-NOUS
69 offres d'emploi
36 offres de stage

ALERTE
- Attention escroquerie en ligne portant le logo de l'ANSSI !
- Les alertes du CERT-FR

- Catalogue des PASSI publié sur le site de l'ANSSI[1]
- 13 PASSI en cours de qualification (par ordre alphabétique):
  - Advens
  - Amossys
  - Bull
  - Conix
  - Hsc
  - Intrinsec
  - I-Tracing
  - Lexsi
  - Oppida
  - Orange Consulting
  - Sogeti Esec
  - Solucom
  - Thales C&S

1 http://www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies/prestataires-d-audit-de-la-securite-des-systemes-d-information-passi-qualifies.html

PRESTATAIRES DE DÉTECTION DES INCIDENTS DE SÉCURITÉ (PDIS) : PRÉSENTATION DES ACTIVITÉS

Gestion des événements
Recueil et stockage des éléments techniques permettant de détecter les incidents de sécurité

➔ *Sources à collecter, fréquence de collecte, architecture du système de collecte, etc.*

Gestion des incidents
Identification et qualification des incidents de sécurité sur la base des évènements collectés

➔ *Compétences des équipes d'analyse, fonctionnalités des outils utilisés, qualification des incidents, etc.*

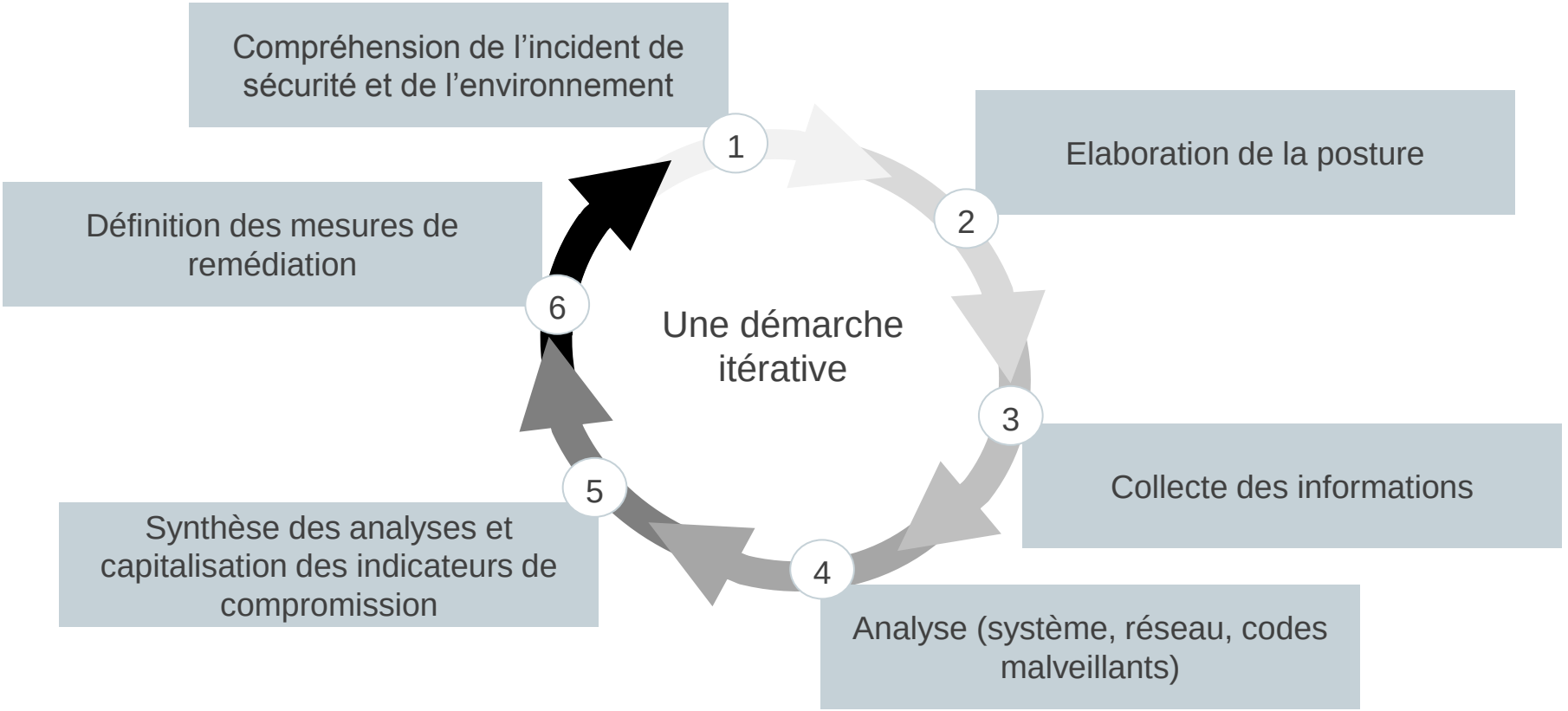
Gestion des notifications
Signalement au commanditaire des incidents de sécurité portant atteinte à son système d'information

➔ *Délai d'alerte, format utilisé, mise à disposition de tableaux de bords, etc.*

PRIS: PRÉSENTATION DES ACTIVITÉS

- Activités visées par le Référentiel (chapitre III)
  - Pilotage technique
  - Analyse système
  - Analyse réseau
  - Analyse de codes malveillants
- Exigences relatives au prestataire (chapitre IV)
- Exigences relatives aux analystes (chapitre V)
- Exigences relatives au déroulement d'une prestation (chapitre VI)
- Missions et compétences requises pour les analystes (annexe 1)
- Recommandations à l'intention des commanditaires (annexe 2)
- Prérequis à fournir par les commanditaires (annexe 3)

PRIS: PRÉSENTATION DES ACTIVITÉS



PRIS : COMPRÉHENSION DE L'INCIDENT DE SÉCURITÉ

Le prestataire doit confirmer / identifier

- Le **caractère malveillant** de l'incident de sécurité
- La **présence active** de l'attaquant dans le système d'information
- La **date** de compromission initiale
- Le **vecteur** de compromission initial
- La **chronologie** des activités de l'attaquant
- Les **phases** de l'attaque
- Le **niveau de complexité** de l'attaque
- Le **périmètre** de la compromission
- Les **ressources compromises**
- La **nature** des compromissions
- Les **scénarii** de compromission
- Les **indicateurs** de compromission

- Les **vulnérabilités exploitées** et les **outils utilisés** par l'attaquant
- Les **moyens de persistance**
- Les **moyens** utilisés par l'attaquant pour **exécuter des commandes à distance** sur les ressources compromises
- Les **moyens** utilisés par l'attaquant pour **se déplacer latéralement** dans le système d'information
- Le **niveau de privilège** obtenu par l'attaquant
- Les **moyens** utilisés par l'attaquant pour **élever ses privilèges**
- La **nature des données ciblées** par l'attaquant

PRIS: EXIGENCES RELATIVES AU PRESTATAIRE (2/2)

- Convention en deux étapes possible (→ meilleure réactivité)
- Niveau de discrétion vis-à-vis de l'attaquant
- Politique de recherche en sources ouvertes
- Protection de l'information
  - SI de niveau *Diffusion Restreinte*
  - Application du guide d'hygiène
  - SI dédié pour l'analyse de codes malveillants
- Mesures de remédiation (durcissement, assainissement, bascule)

PRIS: CAS DES ENQUÊTES JUDICIAIRES

- Chapitre III.1, Modalités de la qualification:

  « La qualification ne se substitue pas à l'inscription sur une liste d'experts en investigation numérique auprès d'une cour d'appel et n'accorde pas de droits afférents à la qualité d'expert. »

- Chapitre VI.10, Cas des enquêtes judiciaires

  Une enquête judiciaire peut être déclenchée avant, pendant ou après la prestation.

Les exigences et recommandations du référentiel doivent donc être compatibles avec une enquête judiciaire.

INTÉRÊTS DE LA QUALIFICATION POUR LES COMMANDITAIRES

- Critère de comparaison entre prestataires
- Garantit la compétence des prestataires (évaluation individuelle de la compétence des personnes)
- Garantit la protection des informations
- Possibilité de déposer des réclamations contre des prestataires qualifiés

NOS RECOMMANDATIONS AUX COMMANDITAIRES

- Demandez à vos prestataires de s'engager dans le processus de qualification
- Consultez le catalogue des prestataires qualifiés sur le site de l'ANSSI[1]
- Exigez dans vos contrats, appels d'offres, etc. que vos prestataires soient qualifiés (« Guide d'achat de produits et prestations qualifiés »)
- Sollicitez l'ANSSI pour participer à la rédaction de vos cahiers des charges
- Transmettez à l'ANSSI vos commentaires sur les référentiels

[1] http://www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies

GUIDE D'ACHAT DE PRODUITS DE SÉCURITÉ ET DE SERVICES DE CONFIANCE QUALIFIÉS

- Publié sur le site de l'ANSSI[1]
- Elaboré par:
  - l'ANSSI
  - le Service des achats de l'Etat (SAE)
  - la Direction des affaires juridiques (DAJ) des Ministères économiques et financiers
- Publics visés:
  - Pouvoir adjudicateur / services des achats
  - MOE / MOA
  - RSSI
- Conformité au Code des marchés publics (CMP)
- Méthodes / infos pratiques pour exiger des produits de sécurité et des services de confiance qualifiés dans les appels d'offres

[1] http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/choix-des-produitsde-securite/achat-de-produits-de-securite-et-de-services-de-confiance-qualifies.html