Loi de Programmation Militaire 2014-2019

Deuxième partie

TLS-SEC – 2019-2020

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

SOMMAIRE

AVERTISSEMENT

Le contenu et les opinions exprimés dans ce support et lors de cette présentation sont sous mon entière responsabilité et n'engage donc que moi. Même s'ils font beaucoup référence à mon employeur actuel, les retours sont basés sur toutes mes expériences.

Logistique du cours

- **Deux séances**
  - 25/11/2019 – 14h-15h45
  - 09/12/2018 – 14h-15h45
- **Support distribué a format électronique**
- **Evaluation**
  - QCM
- **Contact**
  - Julien.airaud@cnes.fr – 05 61 28 75 94

Questions sur la partie n°1 ?
Attentes pour la suite ?

cnes
CENTRE NATIONAL D'ETUDES SPATIALES

MAÎTRISER SES SYSTÈMES D'INFORMATION

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Cartographie (règle 3)

On ne peut mesurer ou sécuriser que ce l'on connaît, il est donc nécessaire d'établir la cartographie du SI.

Elle apporte une connaissance approfondie du fonctionnement d'un SIIV, elle est indispensable à la vie du système, de la conception à la gestion des incidents.

Elle comporte plusieurs niveaux pour représenter les informations demandées :

- Métier : écosystème du SIIV – acteurs, interfaces, flux entre acteurs
- Applications : applications, flux, protocoles, administration
- Infrastructures : infrastructures logiques et physiques du SIIV

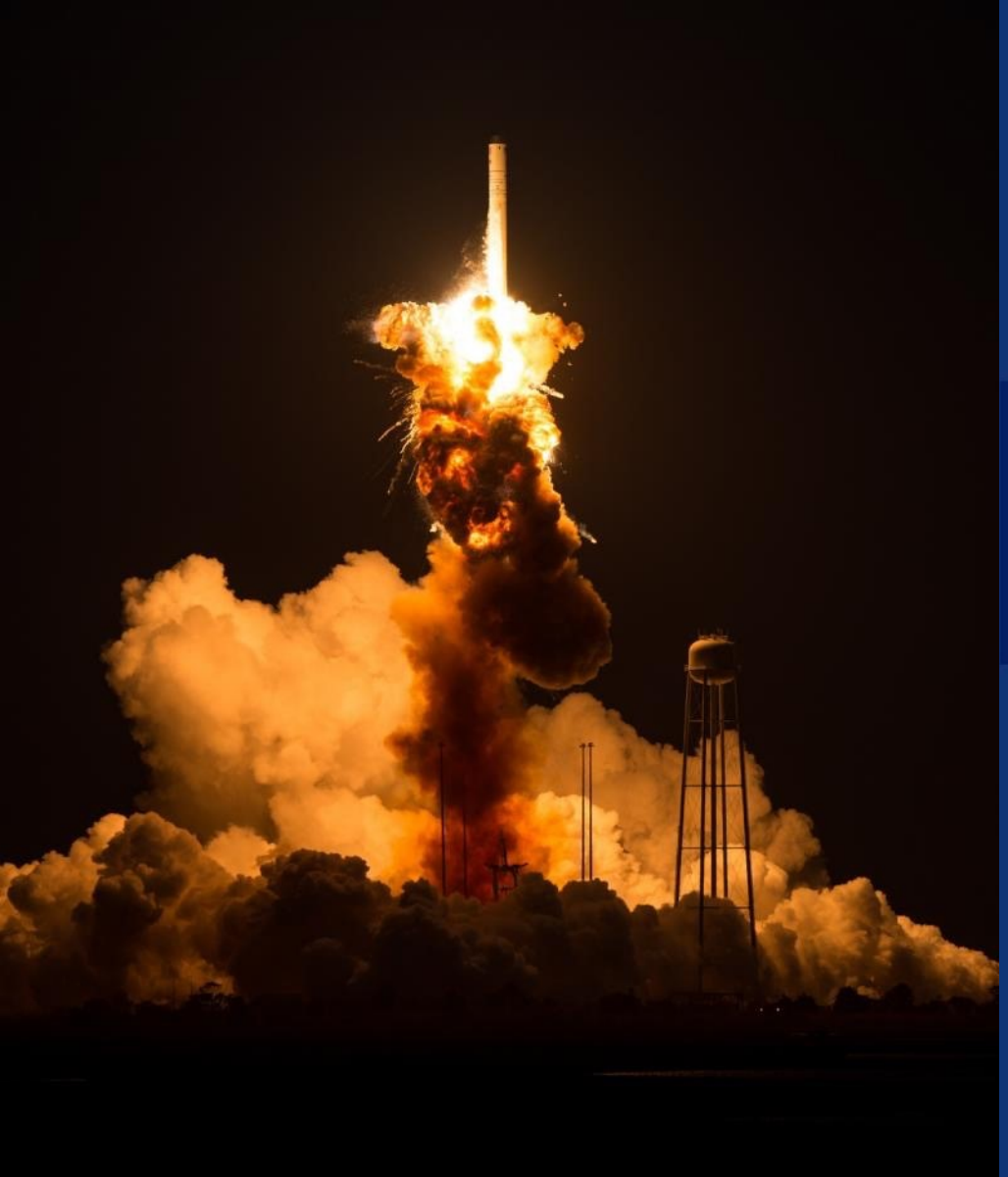
La cartographie devra être communiquée sur demande de l'ANSSI.

Maintien en Condition de Sécurité (règle 4)

Le MCS part d'une procédure (cf. PSSI), autour de deux axes :

- Veille active en sécurité (CERT-*X*, fournisseurs, éditeurs…)
- Application des mises à jour et correctifs selon un processus standard

Les « difficultés techniques » ou « opérationnelles » empêchant l'utilisation d'une version supportée ou l'application d'un correctif doivent être justifiées et faire l'objet de mesures en diminution de risques.



GÉRER LES INCIDENTS DE SÉCURITÉ

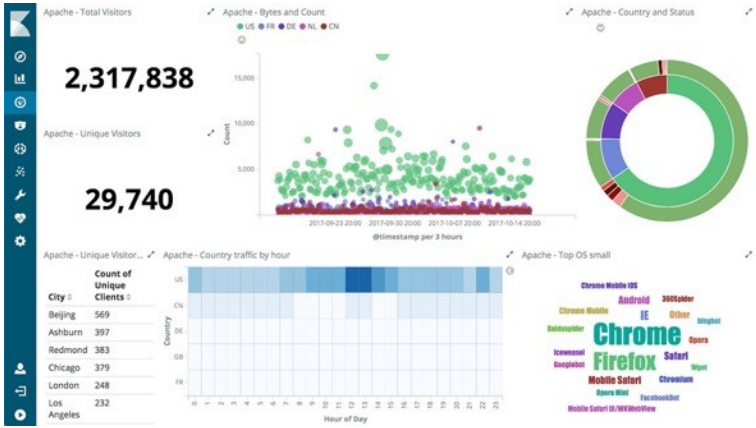
Journalisation (R5)

Le but est :

- D’enregistrer, collecter, centraliser les événements dans la perspective de détecter les incidents de sécurit (R6).
- De conserver les traces permettant de réaliser des investigations a posteriori en cas d’incident;
- De réaliser des recherches de compromission, sur la base de marqueurs communiqués par des partenaires ou par l’ANSSI.

La stratégie de collecte doit intégrer:

- Les éléments du SIIV (serveurs, sécurité, poste d’administration…). Il ne faut pas oublier de justifier les manques.
- Une procédure de prise en compte des usages et composants
- L’horodatage des éléments
- La centralisation et l’archivage des événements pendant au moins 6 mois.
- La préservation et le contrôle de l’intégrité
- Une capacité à faire des recherches automatisées dans les journaux.



Corrélation et analyse (R6)

La règle 6 vise à la mise en œuvre d'un système de corrélation et d'analyse des journaux qui exploite les éléments enregistrés par le système de journalisation (R5) pour détecter les événements / incidents de sécurité (Annexe 4 de l'arrêté sectoriel).

- Une stratégie d'analyse et d'événements redoutés est à établir.
- Il faudra gérer une base de scénarios de corrélation, des règles de détection, des marqueurs, etc. liés aux SIIV, ainsi que leur cycle de vie.

Le système de corrélation est installé et exploité au sein d'un système dédié.

- Au delà de l'architecture du système de corrélation, l'interconnexion du SIIV sera à documenter.
- La mutualisation n'est pas exclue.

L'OIV ou son prestataire doivent s'appuyer sur le référentiel PDIS – Prestataire de Détection des Incidents de Sécurité.

Détection (R7)

Elle vise à la mise en place de système de détection qualifié de type « sonde d'analyse de fichiers et protocoles ».

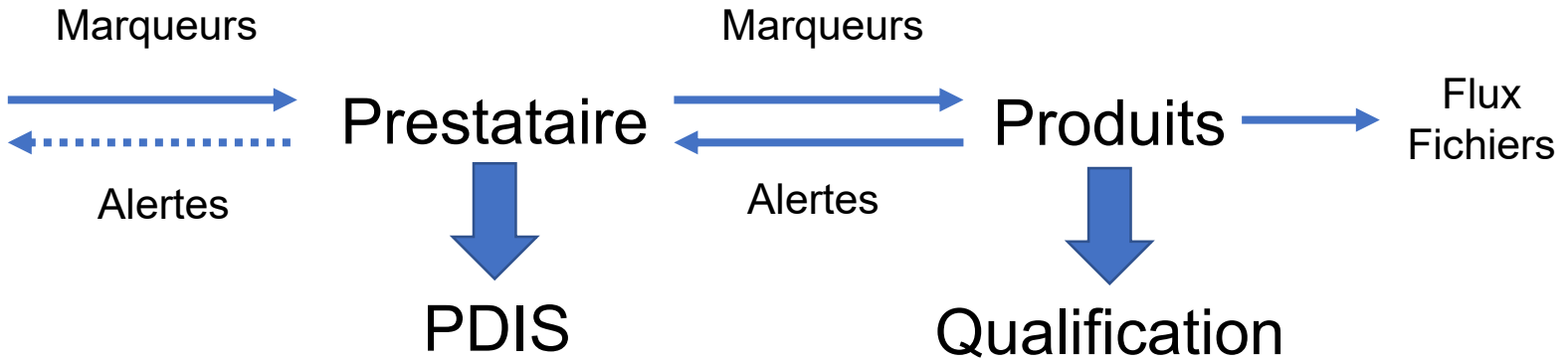
- Cible : Analyse des flux et fichiers échangés entre les SIIV et les systèmes d'information tiers à ceux de l'opérateur.
- Comment : Systèmes qualifiés exploités selon les règles PDIS, par l'Etat ou un prestataire qualifié PDIS.

Prestataire → Produits

Pourquoi viser une qualification du système ?

L'ANSSI dispose de marqueurs sensibles qu'elle ne peut partager faute d'une chaîne de confiance.

La chaîne, qualifiée par l'ANSSI, regroupe :



Détection (R7) – Fonctions

Veille en cybersécurité
- Sources de marqueurs
- Avis

Intégration avec des tiers
- Autres sources de marqueurs
- SIEM
- Service**s IT PDIS (LDAP, PKI, DNS)**

Détection standard IDS
- Corrélation avec les marqueurs
- Analyse de protocole

Détection avancée:
- Algo Machine Learning

Enregistrement des paquets réseau et Forensics

Analyse de fichiers

Collecte
- Protection du capteur et des fonctions de détections (cloisonnement, durcissement)
- Collecte des données et des méta-données
- Stockage et recherche

Détails des fonctions de la sonde

IDS : Intrusion Detection System (Passif)

- Détection basée sur un catalogue de 40.000 règles composés de +40 catégories
- Moteur de règle se mettant à jour avec les dernières menaces

DPI :

- Détection des protocoles, enregistrement des métadata, des netflow, extraction de fichiers

STA: Static File Analysis

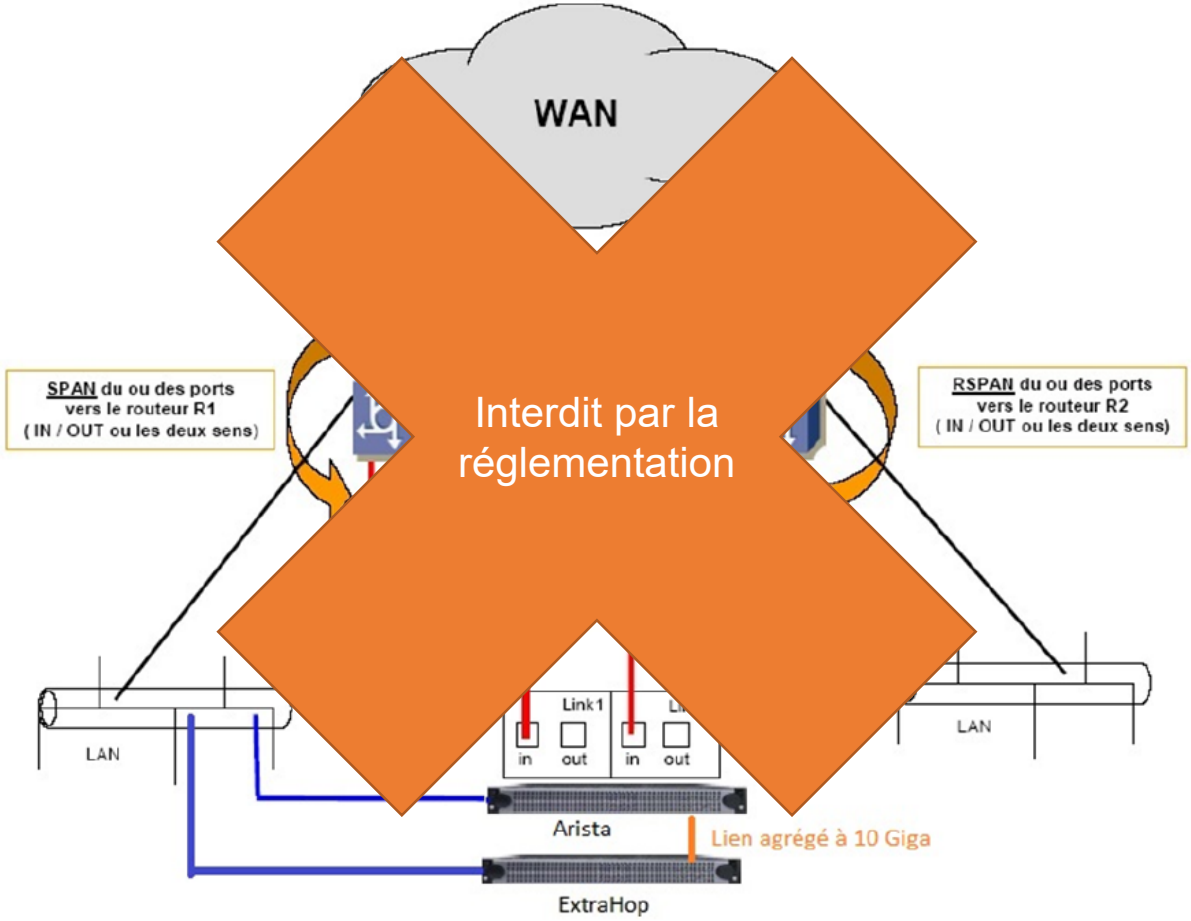
- Règle YARA et signatures.

ADS: Anomalie Detection System

- Algorithmes Machine Learning

Détection (R7) – Capture des flux

SPAN



+:

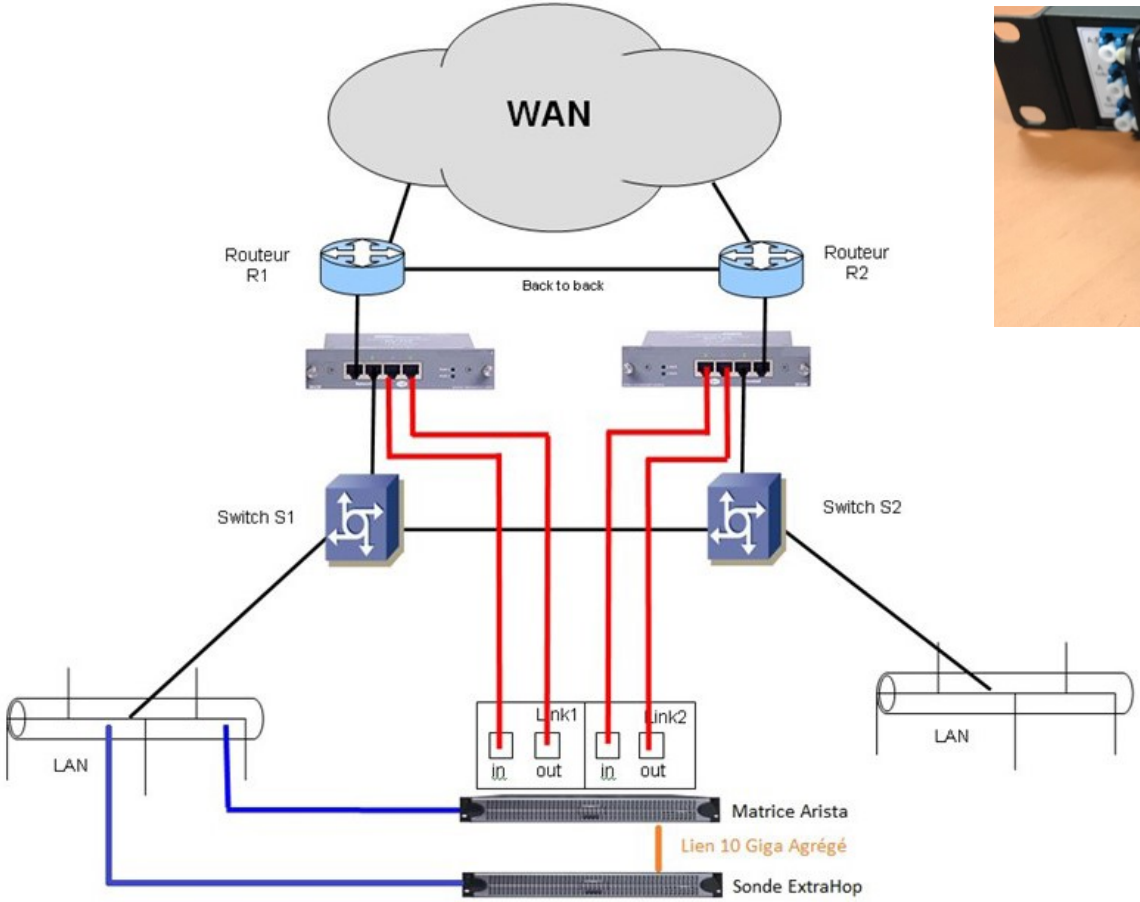
- Facile à mettre en œuvre
- Pas d'équipement en plus

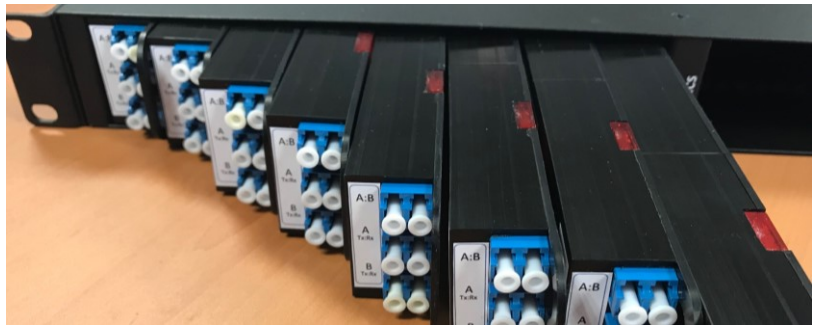
- :

- Impacts sur l'équipements
- Pertes de paquets possibles
- Pas de visibilité des paquets corrompus
- Pas d'erreur de bas niveau

Détection (R7) – Capture des flux

TAP





+:

- Pas d'erreur de config
- Pas de surcharge
- Dispositif physique non administrable

- :

- Arrêt de production pour le mettre en place
- Bilan optique nécessaire

Les SOC

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Introduction

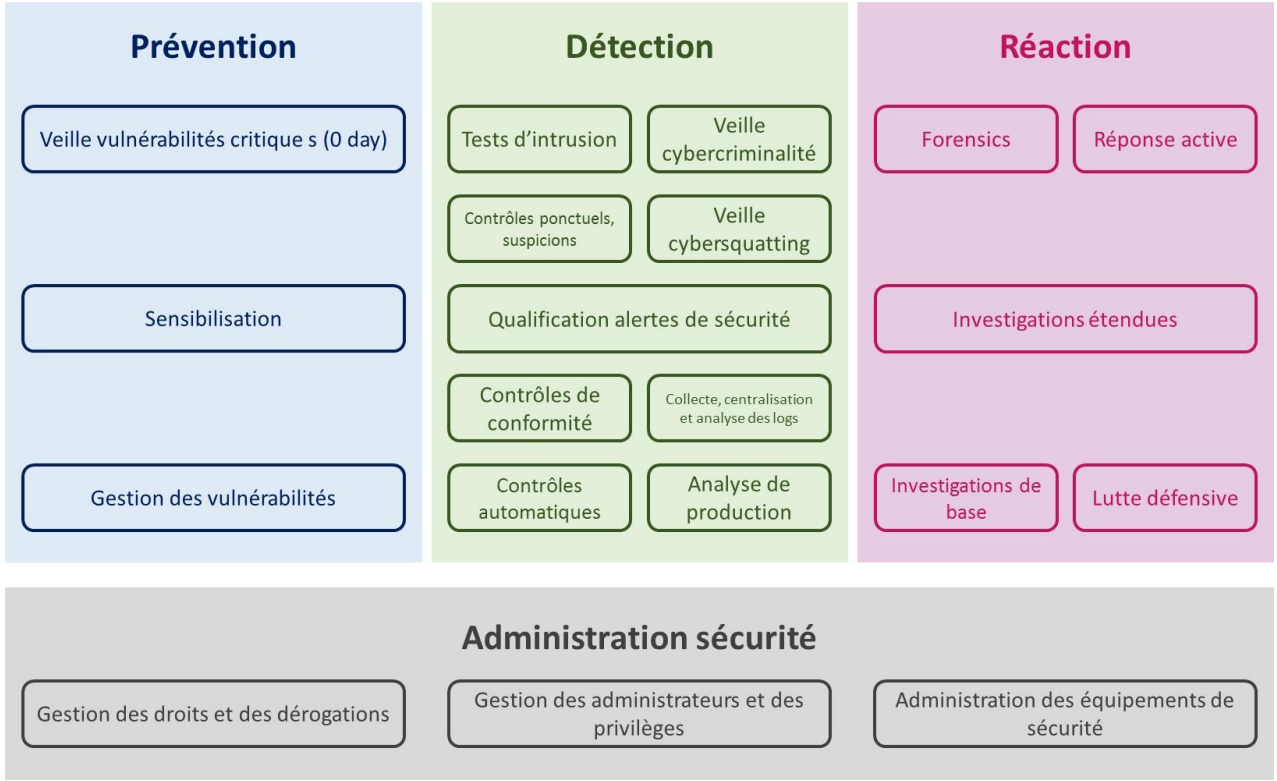
Définition

Un SOC est un ensemble de ressources humaines, organisationnelles et techniques regroupées et organisés pour détecter, analyser, répondre, informer et prévenir des incidents de sécurité.

Ses missions sont regroupées dans 4 catégories

- Prévenir
- Détecter
- Réparer
- Administration de la sécurité

Catalogue de services



Source : CLUSIF « Comment déployer un SOC »

Composants

Les équipes

- Niv. 1 : Analyse les événements en continu, traite les événements et alertes procédurés.
- Niv. 2 : reçoit les escalades du Niv1, traite et investigue sur ce qui n'est pas procéduré.
- Niv. 3 : Intervient sur alertes qualifiées et crises.
- Maintien en condition opérationnelle
- Gouvernance pilotage
- Attention à bien faire la distinction entre le commanditaire et prestataire

Composants

Les outils du SOC

- Infrastructure de collecte : elle collecte les logs des systèmes supervisés, éventuellement de les normaliser, les enrichir et de les filtrer, pour ne pas saturer le SIEM. Elle peut réaliser un stockage brut des logs pour des raisons légales.
- Infrastructure SOC : elle doit être dédiée.
- SIEM : Security Incident and Event Management : permet la centralisation et la corrélation des logs. Il met en œuvre la base de règles qui permet de détecter les incidents de sécurité correspondant à la stratégie de détection
- Postes : trois types doivent exister : poste d'exploitation, poste d'administration et poste d'accès à Internet.
- Systèmes de notifications : téléphone, SMS, mail.

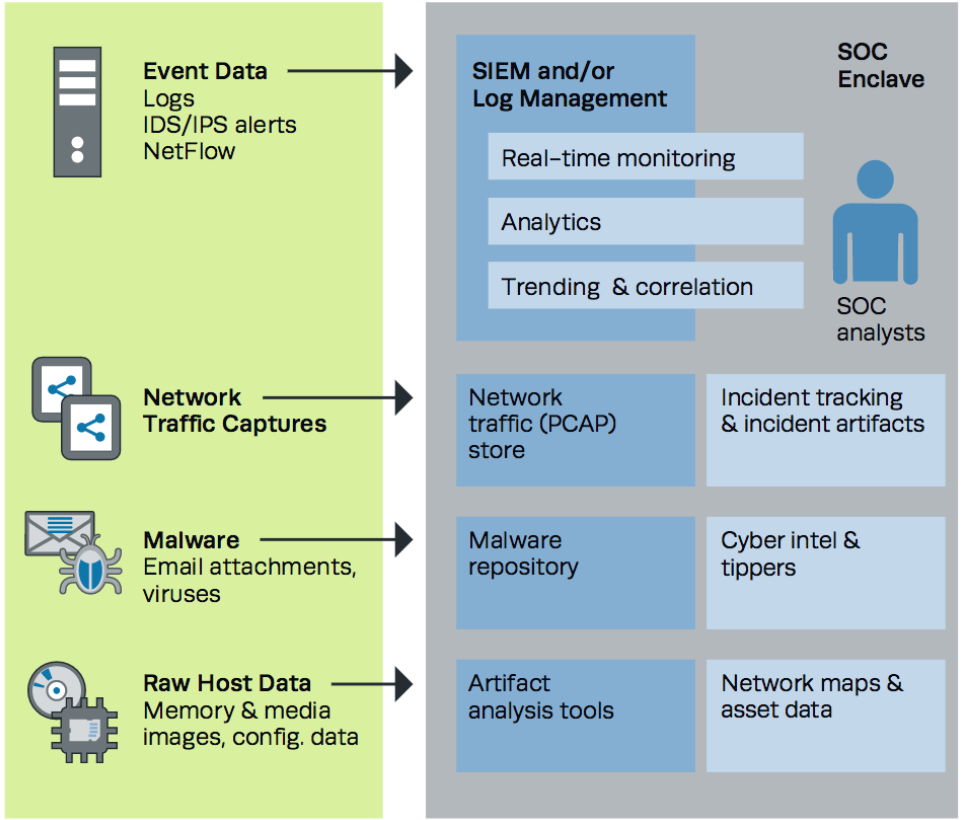
Composants

Les outils de sécurité

Optionnellement, le SOC peut mettre en place et/ou gérer ses propres outils:

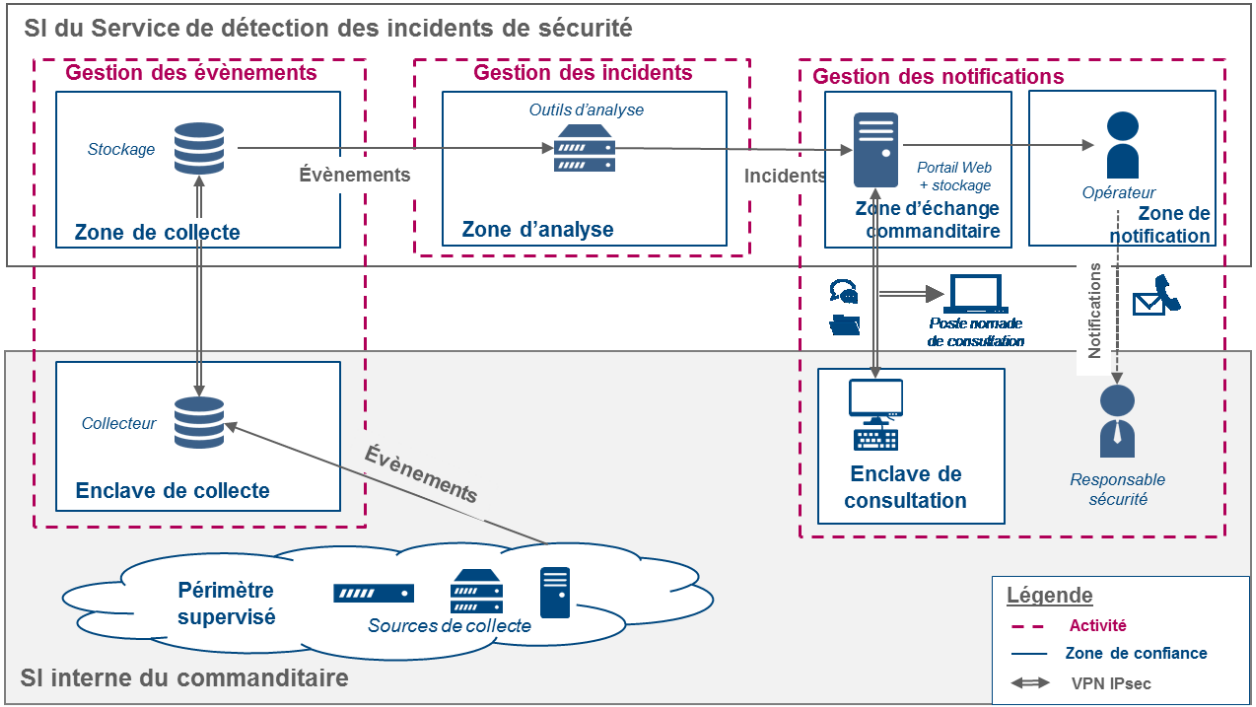
- Gestion des IOC
- Sondes de détection (qualifiées ou non)
- Anti-malware ou Endpoint protection
- Honeypot
- Systèmes de veille et de surveilance de réputation : cybersquatting, phishing, defacement, veille sur la menace.
- Plateforme forensics

Organisation

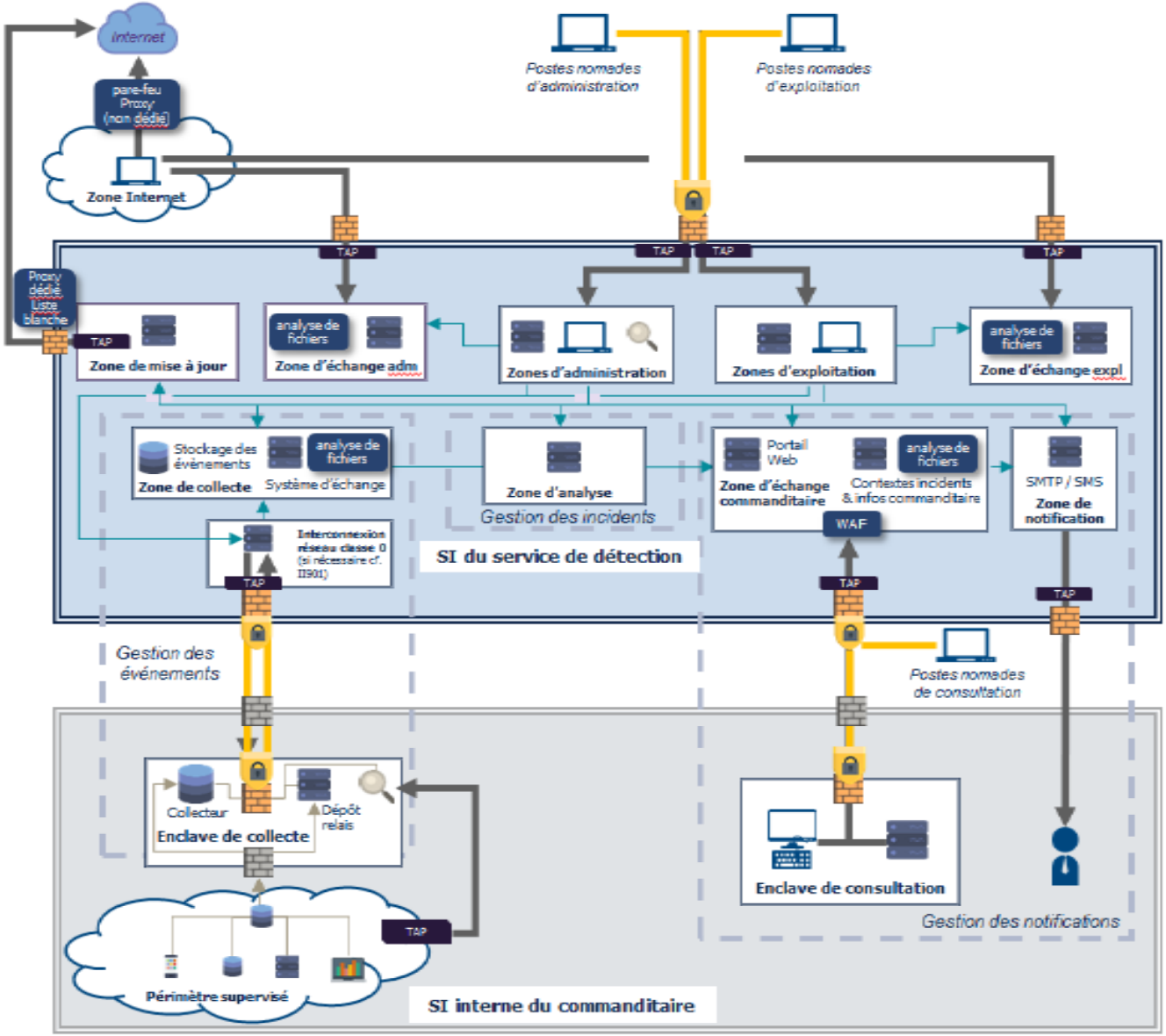


Source : MITRE

Architecture



Source : ANSSI Référentiel PDIS



Chacun des flux représentés sur ce schéma doit faire l'objet de **chiffrement et d'authentification par des solutions IPSec** agréées par l'ANSSI dès lors qu'il circule sur un réseau non dédié au service de détection

LÉGENDE

- Zone de confiance
- *Activités du service de détection*
- Solution de filtrage qualifiée par l'ANSSI
- Solution de filtrage administrée par le Commanditaire
- TAP
- Sonde qualifiée par l'ANSSI
- Solution de chiffrement agréée par l'ANSSI
- Flux chiffré par une solution agréée par l'ANSSI

Le référentiel PDIS

7 prestataires en cours de qualification

https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/

Référentiel d'exigences :

- v.1 publiée 10/2015, version anglaise disponible
- https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/
- v.2 en cours de signature

Approche

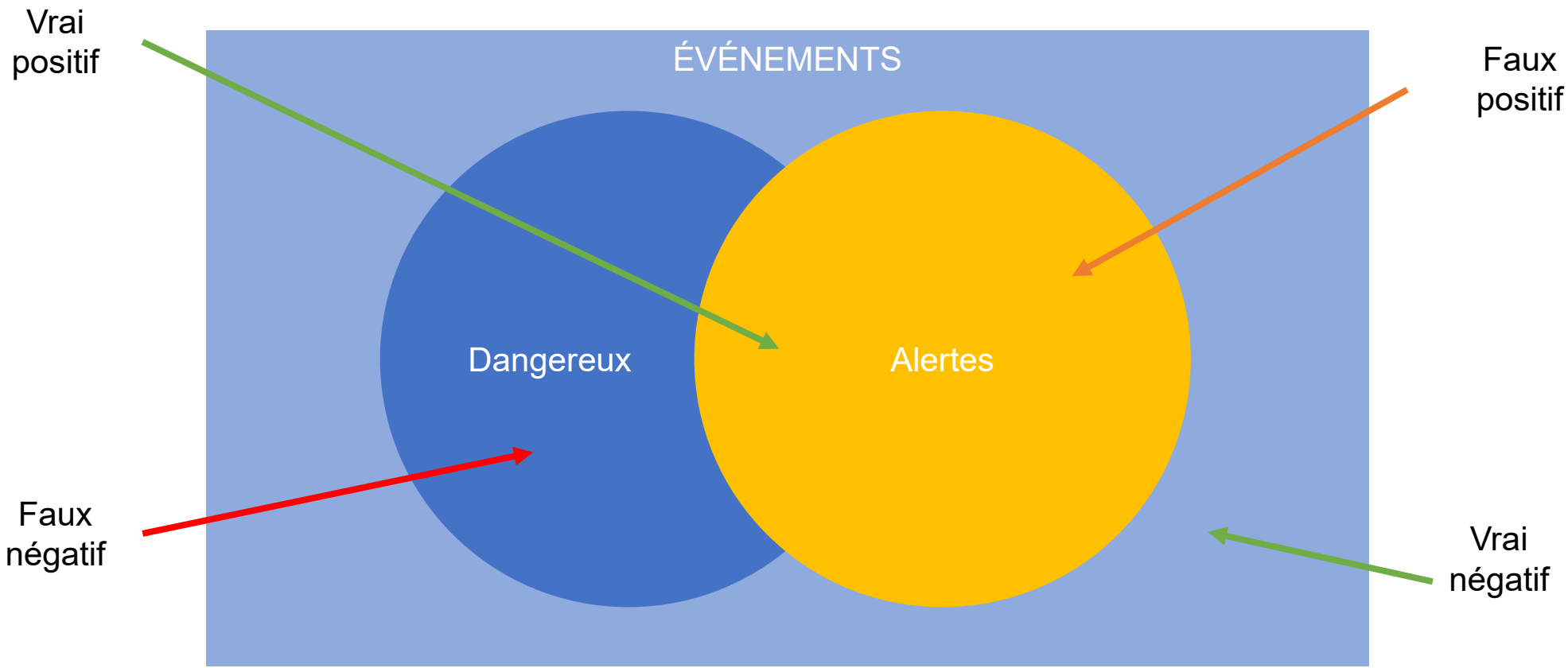
Le référentiel se concentre sur le service détection du SOC:

- Gestion des événements
- Gestion des incidents
- Gestion des notification

Il traite aussi de problématiques suivantes :

- Architecture
- Protection des informations
- Recommandations

Les enjeux du SOC



Recommandations

1. Regrouper sous une seule organisation du CND
2. Trouver l'équilibre organisationnel
3. Donner au SOC les autorités nécessaires
4. Faire peu, mais le faire bien
5. Favoriser la qualité des analystes, à la quantité
6. Maximiser la rentabilité des investissements en outils de sécurité
7. Discriminer les informations utilisées
8. Protéger le SOC
9. Être un client et producteur confirmé de *threat intel*
10. En toutes situations, garder son calme.

Traitement des incidents de sécurité (R10)

L’OIV doit mettre en place une procédure de traitement des incidents affectant le fonctionnement ou la sécurité des SIIV.

Ce traitement doit être conforme au référentiel PRIS.

Il faut mettre en place un SI spécifique cloisonné pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents.

Il doit stocker pendant 6 mois les relevés et les tenir à disposition de l’ANSSI.

Le référentiel PRIS

Concerne les prestataires dans les activités suivantes :

- Analyse des systèmes
- Analyses des réseaux
- Analyse des applications

Traitement des alertes (R9)

L'OIV met en place un service de permanence pour prendre connaissance « à tout moment et sans délai » des informations transmises par l'ANSSI.

Un point de contact bidirectionnel doit être établi.

Gestion des crises (R10)

« Entraînement difficile, guerre facile »

Une procédure doit être établie, notamment pour la mise en application de mesures décidées par l'ANSSI en cas de crise:

- Appliquer une configuration système
  - Proscrire l'utilisation de supports
  - Installer des mesures correctrices
  - Imposer un protocole de routage
- Mettre en place des règles de filtrage
  - Restreindre les accès à un système
  - Bloquer les échanges de fichiers
- Isoler un réseau d'Internet

LA DÉFENSE EN PROFONDEUR

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Identification (R11)

La loi préconise l'utilisation de comptes individuels pour les utilisateurs et des comptes dédiés pour les processus.

L'utilisation de comptes partagés est possible pour des raisons techniques ou opérationnelles mais cet usage doit être accompagné de mesures en diminution de risques.

Authentification (R12)

L’accès aux systèmes doit être protégé par un élément secret.

Les secrets doivent pouvoir:

- Ne pas correspondre à ceux définis par l’installateur ou le fabricant.
- Être changés par les personnes autorisées.
- Lorsqu’ils sont des mots de passe, ils ne doivent pas être réutilisés entre comptes et doivent être durcis.

Droits d'accès (R13)

Doivent respecter le « juste besoin »

Ce qui est strictement nécessaire à l'exercice des missions de l'utilisateur ou au fonctionnement du processus automatique.

L'opérateur doit:

- **Définir une politique d'attribution des droits**
- **Réviser régulièrement les droits attribués**
- **Etablir et tenir à jour la liste des comptes privilégiés**

Administration (R14 et R15)

Comptes (R14)

- L'utilisation de comptes dédiés à l'administration est obligatoire. Ils doivent être gérés selon R12 et R13.

SI d'administration (R15)

Les ressources matérielles et logicielles doivent être dédiées aux opérations d'administration, gérées par l'opérateur ou le prestataire.

Les ressources ne doivent pas être détournées :

- pas d'utilisation bureautique du poste d'administration,
- pas d'accès à Internet ou messagerie depuis les postes.

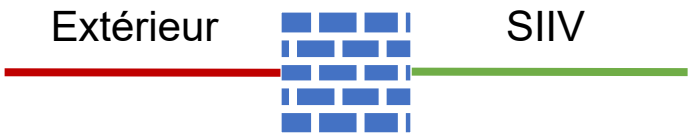
Les flux doivent être protégés : cloisonnement physique ou chiffrement.

Des aménagements sont possibles pour les « petits » SIIV.

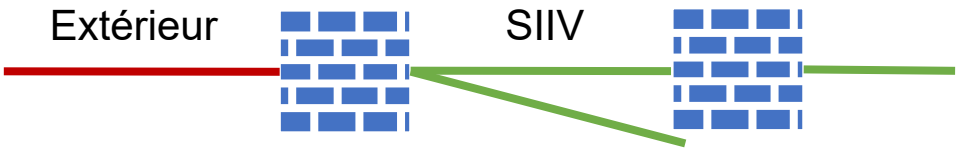
Cloisonnement (R16)

Le cloisonnement a pour but :

- De cloisonner le SIIV des autres systèmes



- De cloisonner les sous-systèmes du SIIV entre eux.



- La granularité est laissée à l'appréciation de l'opérateur.

- Le cloisonnement peut être physique ou logique, en fonction de la sensibilité.
- En logique, VLAN et VRF sont déconseillés au profit de mécanismes cryptographiques.
- Seules les interconnexions strictement nécessaires sont mises en place.

Filtrage (R17)

Les flux de données doivent être filtrés, pour les connexion inter et intra systèmes.

Accès à distance (R18)

L'accès à distance au SIIV peut être :

- Direct : l'accès se fait directement au SIIV.
- Indirect : l'accès se fait par rebond via un autre SI (celui de l'entreprise par exemple).
- Selon trois types

1. Les accès publics : si le SIIV est accessible au grand public, dont les postes sont non maîtrisés et l'accès est direct ou non.
2. Les accès nomades : l'accès au SIIV se fait depuis un poste maîtrisé, directement ou non.
3. Accès internes : depuis un poste et un site de l'opérateur.

Accès à distance

Dans le cas 1:

- Il est recommandé de scinder le SIIV en deux : une partie publique, une non.

Dans tous les cas, il est requis:

- D'utiliser un VPN IPSec (préférable) ou TLS, conformes aux guides de configuration ANSSI.
- De mettre en place une authentification à double facteur.
- De fournir le matériel (pas de BYOD)
  - Dont les mémoires sont chiffrées par un mécanisme conforme au Référentiel Général de Sécurité (RGS), protégé par un secret.

Installation de services et d'équipements (R19)

Le SIIV doit être installé dans une configuration particulière

- Uniquement avec les services et fonctionnalités indispensables au fonctionnement sont présents. Il faut de préférence désinstaller et non désactiver.
- Les matériels doivent être répertoriés
- + Les périphériques amovibles doivent être dédiés (liste blanche)
- Les supports amovibles sont analysés avant chaque utilisation et les appareils auxquels ils sont connectés sont protégés contre l'exécution de code malveillant.

ESA-CNES-ARIANESPACE/Optique Vidéo du CSG - OV

CONCLUSION

Conclusion

La LPM présente un ensemble de bonnes pratiques.

Des points difficiles ou opportunités variables en fonction des organismes :

- Qualification des prestations et produits
- Détection
- Administration