"Détection , supervision et traitement des évènements de sécurité".

Fondement du cours

"L'interconnexion croissante des réseaux et les besoins de dématérialisation exposent les systèmes d'information à des cyberattaques. Ainsi les points d'interconnexion avec l'extérieur et en particulier avec internet sont autant d'accès qu'un attaquant peut tenter d'exploiter pour s'introduire et se maintenir au sein d'un système d'information pour dérober, dénaturer ou détruire son patrimoine informationnel"

source: référentiel ANSSI des Prestataire de Détection des Incidents de Sécurité (PDIS)**

La réponse aux attaques externes et internes.

- Il faut donc détecter les attaques en dédiant des ressources matérielles et humaines à cette tâche: c'est le but du *"**S**ecurity **O**peration **C**enter"* ou *"centre *opérationnel de cybersécurité"*.

Security Operation Center: définitions

- L'exploitation de systèmes de détection **"d'incidents de sécurité"** concourt à la protection d'un système d'information face aux menaces de cyberattaques. Les moyens humains, techniques et organisationnels peuvent se concentrer au sein d'un ***"centre opérationnel de cybersécurité"*** dédié à la détection des incidents de sécurité.

- C'est une entité **opérationnelle**, centrale dans la cyberdéfense d'une organisation.
- Le **S.O.C.** se doit de connaître le S.I. de l'entreprise (applications, réseaux, matériels de sécurité...).

Organisation du S.O.C.

- Le S.O.C peut être interne à l'entreprise ou externalisé vers un prestataire de service.
- Son infrastructure peut être dans le Cloud ou "on premise".
- Ses équipes sont constituées d'analystes, d'ingénieurs et d'experts en sécurité.
- Il doit être un bastion de sécurité et être lui-même protégé contre les attaques.
- Il doit avoir une vue globale du S.I. de l'entreprise. (inventaire, CMDB, cartographie applicative et systèmes...)

Finalité du S.O.C.

- Il permet de **prévenir des incidents de sécurité** graves ou lorsqu'ils surviennent d'en **limiter les conséquences**, en permettant des actions de remédiation rapides pouvant être menées par un prestataire de réponse aux incidents de sécurité (PRIS) ou (CERT) qualifié.
- Son métier est de valorise la donnée brute en information exploitable par les équipes de réponse aux incidents de sécurité (CERT/CSIRT) et les opérationnels de la DSI.
- Ses domaines de responsabilités et ses domaines d'actions sont variables d'une entité à l'autre en fonction du partage des activités avec les CERT/CSIRT et les équipes de productions (un SOC ne gère

Processus de services du S.O.C.

Actions: Alerter, détecter, qualifier, analyser, traiter, communiquer, prévenir, réagir, administrer.

- Processus de détection et de qualification des évènements de sécurité.
- Processus de communication entre les équipes cyber (CSIRT) et les clients.
- Processus de prévention les incidents de sécurité (conformité).
- Processus de réaction aux incidents de sécurité.
- Processus d'administration et d'automatisation.

SOC versus CERT

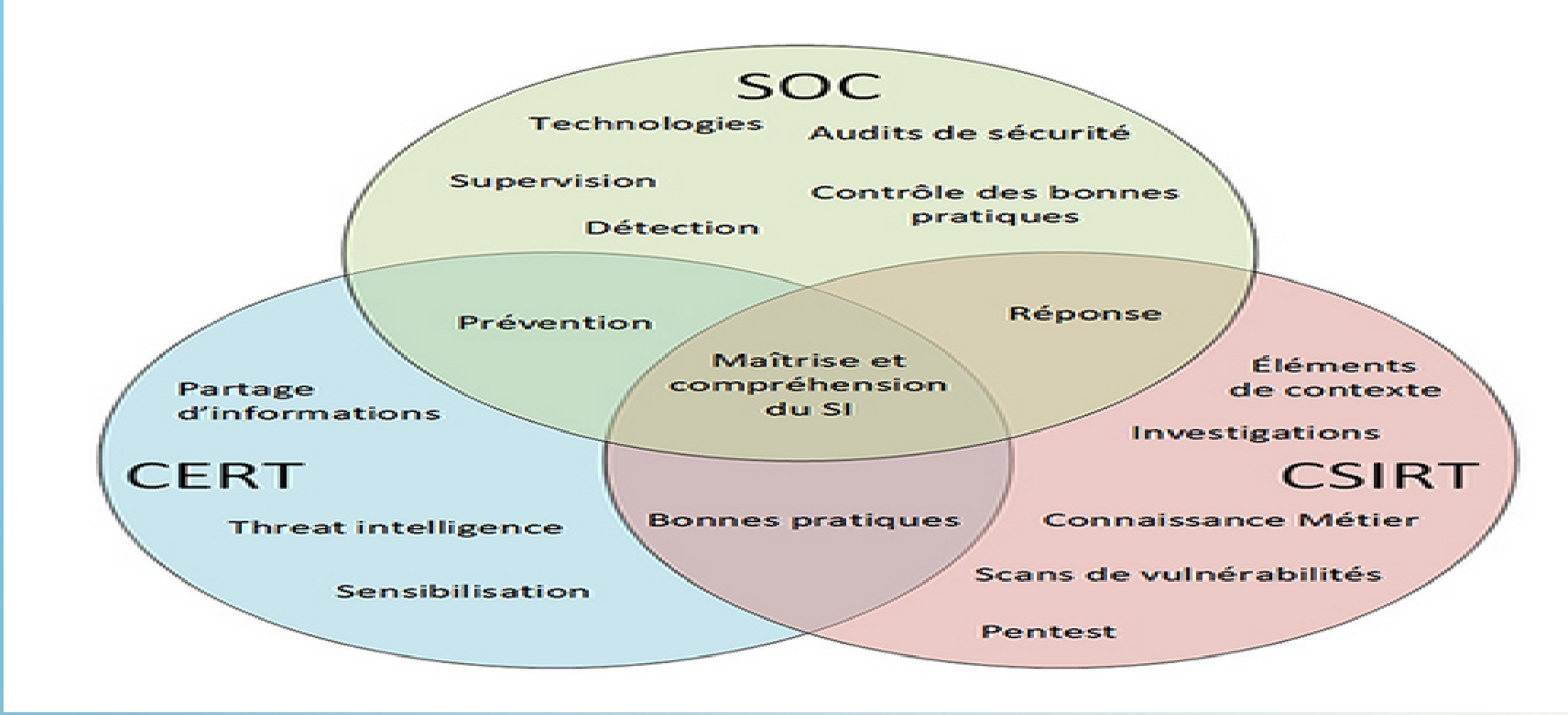
- SOC et le CSIRT/CERT travaillent en étroite collaboration et s'auto-alimentent mutuellement.
- Le SOC est plus focalisé
- Le CSIRT/CERT a un horizon de réflexion plus lointain. Il est focalisé sur la réponse aux incidents, la gestion de crise cyber et la veille autour des cybermenaces.

SOC versus CSIRT exemple du domaine bancaire

	SOC	CSIRT
Gestion des vulnérabilités sur le périmètre	Responsable	Contribue (cf. Veille)
Collecte des événements sur le périmètre	Responsable	
Gestion des règles de corrélation d'évènements	Responsable	
Pondération des événements => émission d'alertes	Responsable	
Qualification de l'incident (instruction)	Responsable/Contribute	Responsable/Contributeur
Pilotage de la remédiation	Contribue	Responsable. Veille à l'industrialisation de la remédiation.
Remédiation technique	Acteur primaire (escalade N1 > N2 > N3)	Acteur sollicité sur escalade depuis N2 ou N3
Clôture de l'incident	Responsable	
Gestion de cybercrise	Contribue	Responsable
Veille technologique / Veille menaces		Responsable
Analyse post-mortem		Responsable
Communication avec les autres CERT[2]		Responsable

Figure 3 Répartition des activités SOC/CSIRT

SOC versus CSIRT/CERT (Source MISC 120)



Analyste S.O.C.

- L'*analyste S.O.C.* a une vision **holistique** de la sécurité de l'entreprise, son but est de détecter les incidents de sécurité corréler plusieurs événements suspects provenant de systèmes différents et en découler un incident de sécurité.
- Ce positionnement au sein de l'entreprise et cette vision globale permettent également de coordonner efficacement les investigations en étroite collaboration avec les équipes de réponse sur incident CERT/CSIRT, les opérationnels et la DSI.

Bibliographie:

- PDIS ANSSI
- Hands-On Network Forensic - auteur Nipun Jaswal- Packt
- Learning Elastic Stack 7.0 - Second Edition Shukla, Pranav Kumar M N, Sharath Packt
- Introduction to Network Forensics FINAL VERSION 1.1 ENISA
- Définitions soc-siem-xdr-mdr par Orange Cyberdéfense
- SOC - Stratégie de détection par Maurugeon Cédric Menelet Alain Misc 120
- Awesome SOC