le cnam Bretagne

Détecter : de la surveillance à l'évènement de sécurité

Eric DUPUIS

eric.dupuis@cnam.fr eric.dupuis@orange.com

http://www.cnam.fr

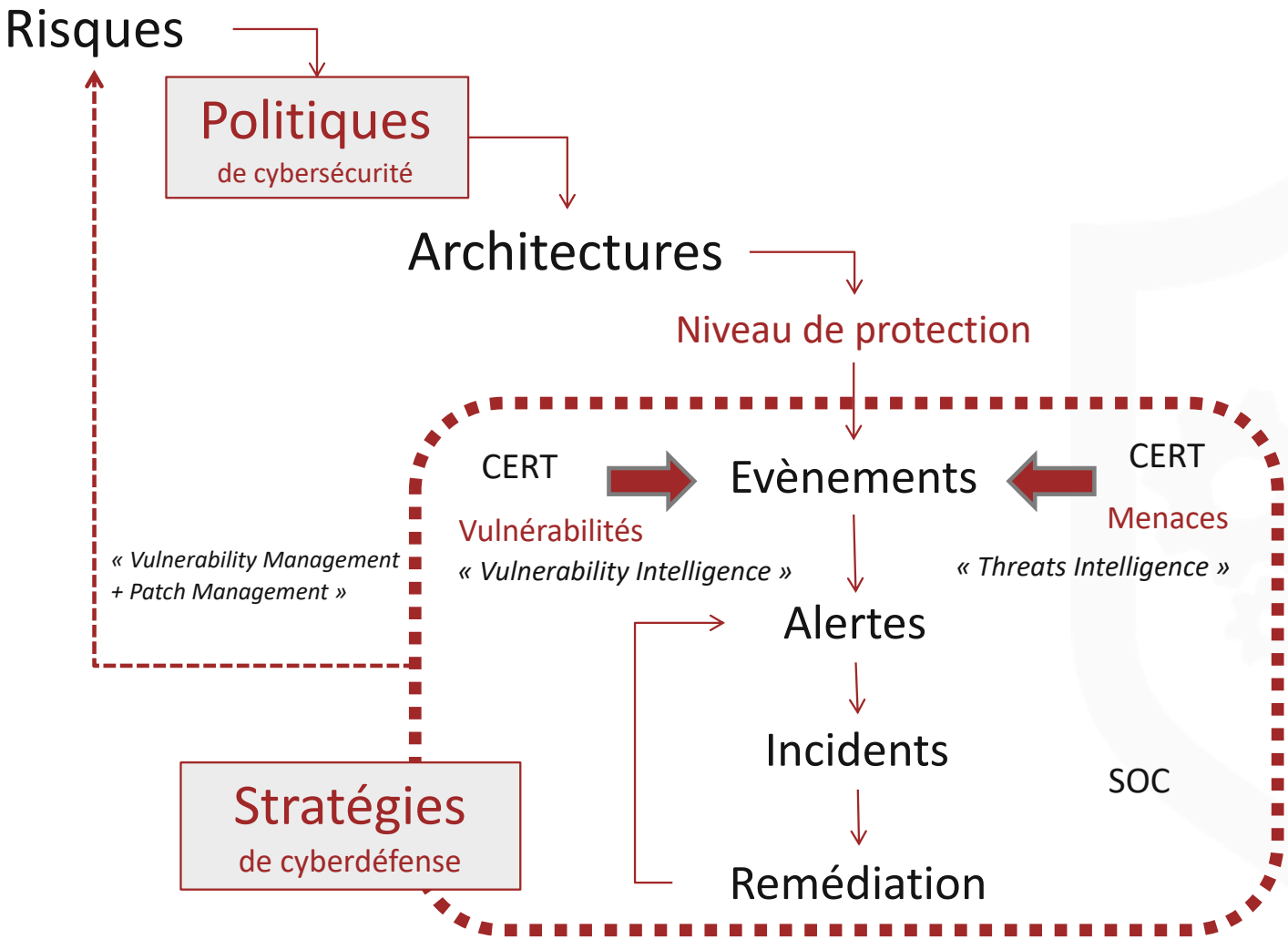
Conservatoire National des Arts et Métiers
Chaire de Cybersécurité

Date de publication
8 janvier 2020

Sommaire

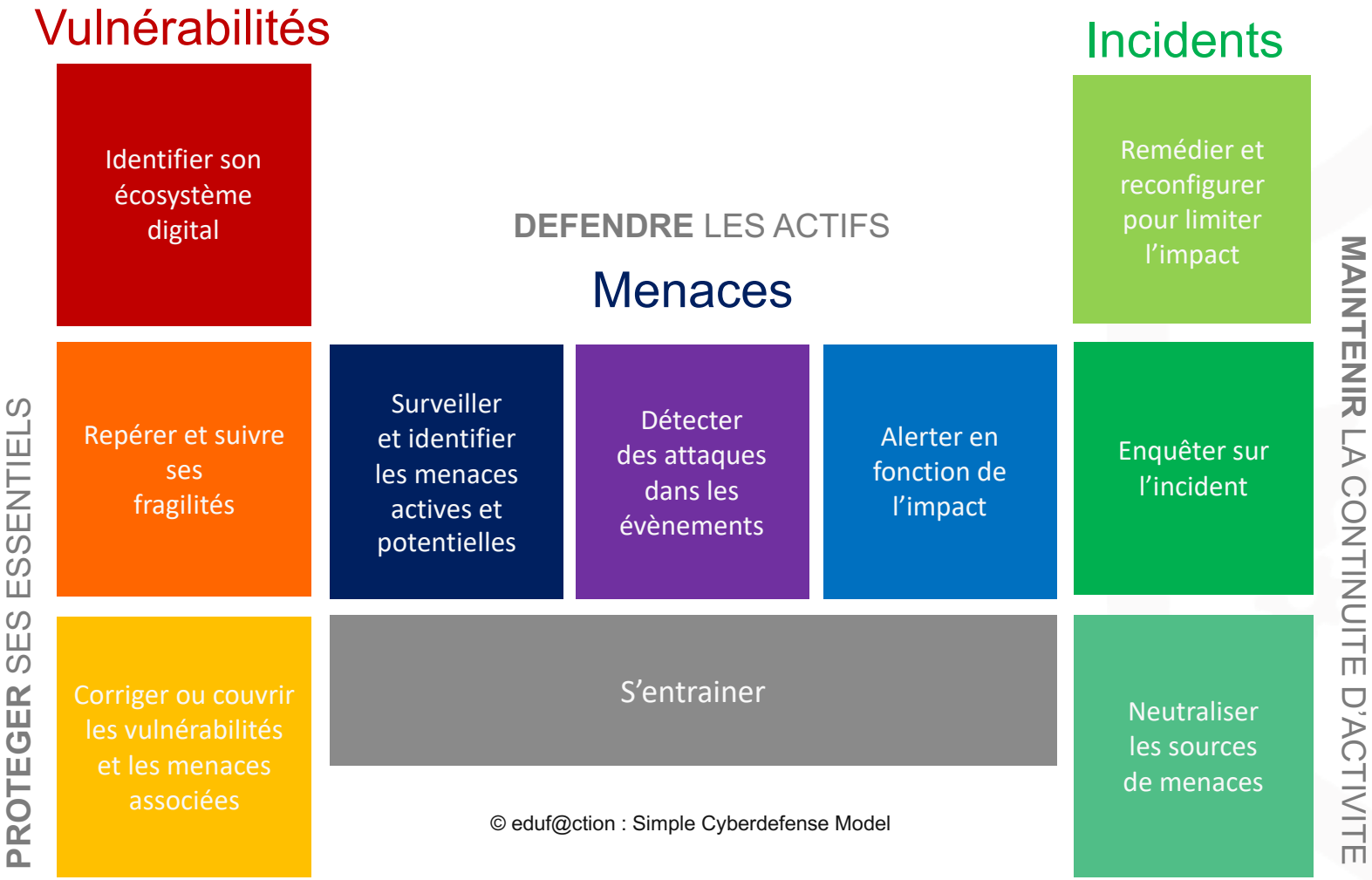
Petit rappel

Cycle de vie : SEC 101



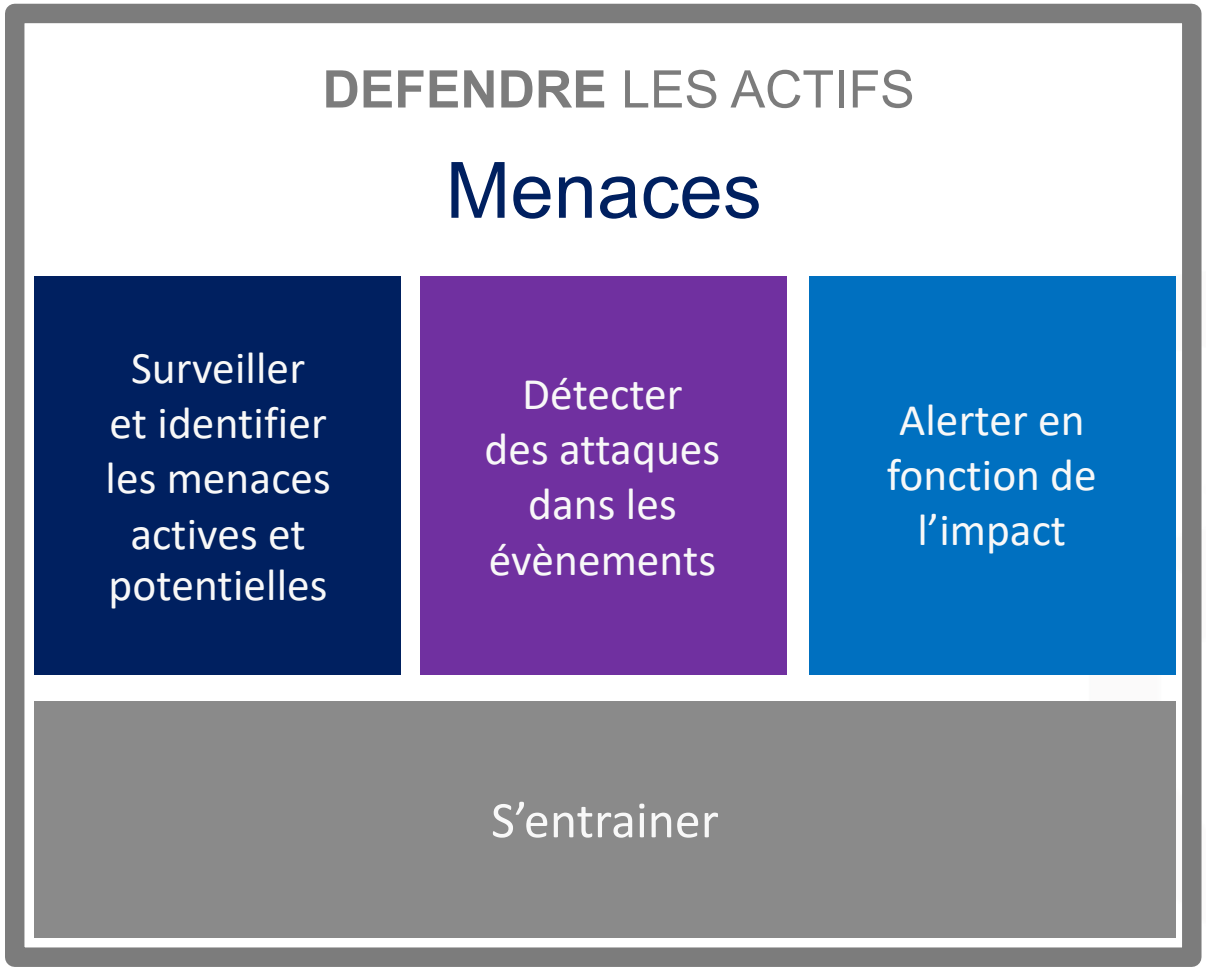
Un modèle de gestion cyberdefense

Un modèle de gestion cyberdefense



La gestion de la menace

la gestion de la menace



© eduf@ction : Simple Cyberdefense Model

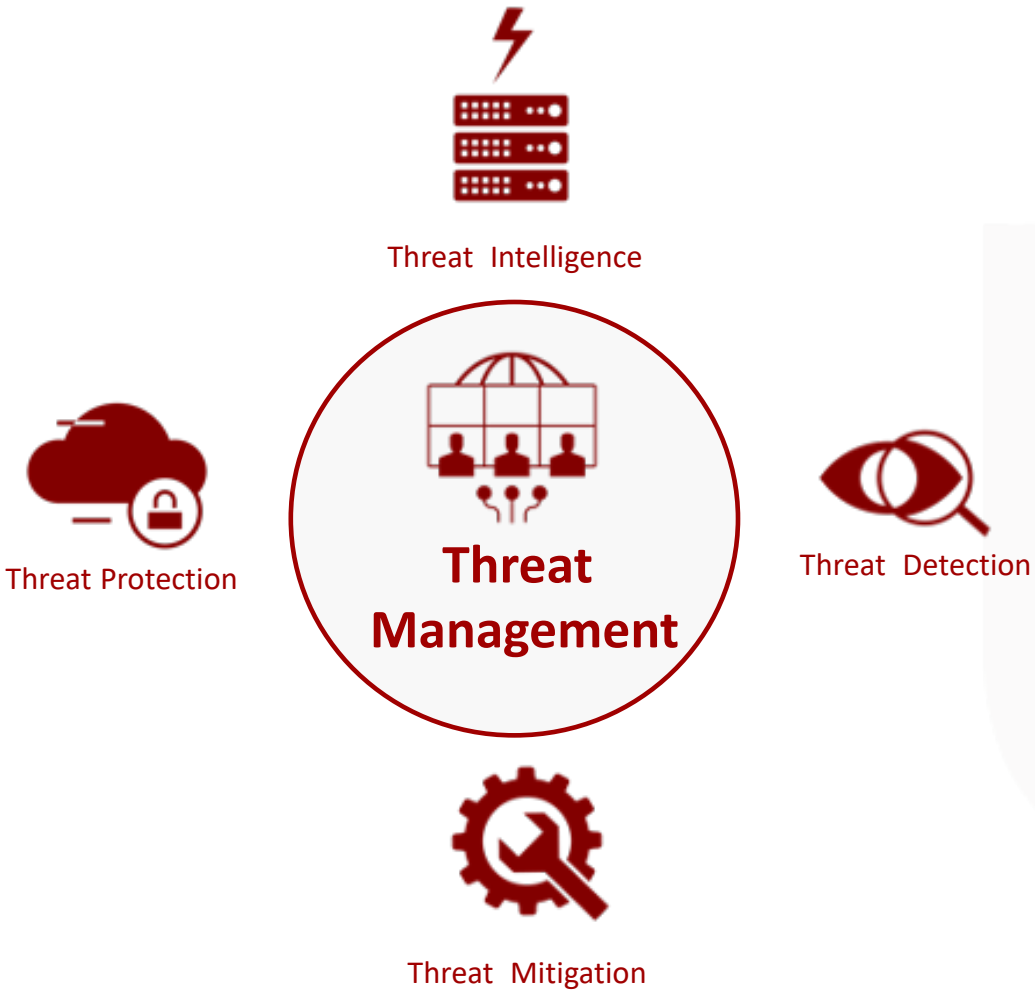
Déroulement

présentation Gestion de la menace

- **VOIR** : capacité de voir et de capter le comportement d'un système d'information via des sources et capteurs avec le *LOG management* (Systèmes et Applicatifs). En n'oubliant pas l'assurance sécurité des Logs
- **COMPRENDRE - PREVOIR** : Avec le *Threat Management* : Veiller, Surveiller la menace, Modélisation et scénarios redoutés
- **DETECTER** : Surveiller le comportement, évènements, anomalies, incidents ... menace avancée (APT), avec les SIEM et les SOC
- **ALERTER** : mettre en place les mécanismes de remontée d'alerte et d'incident.

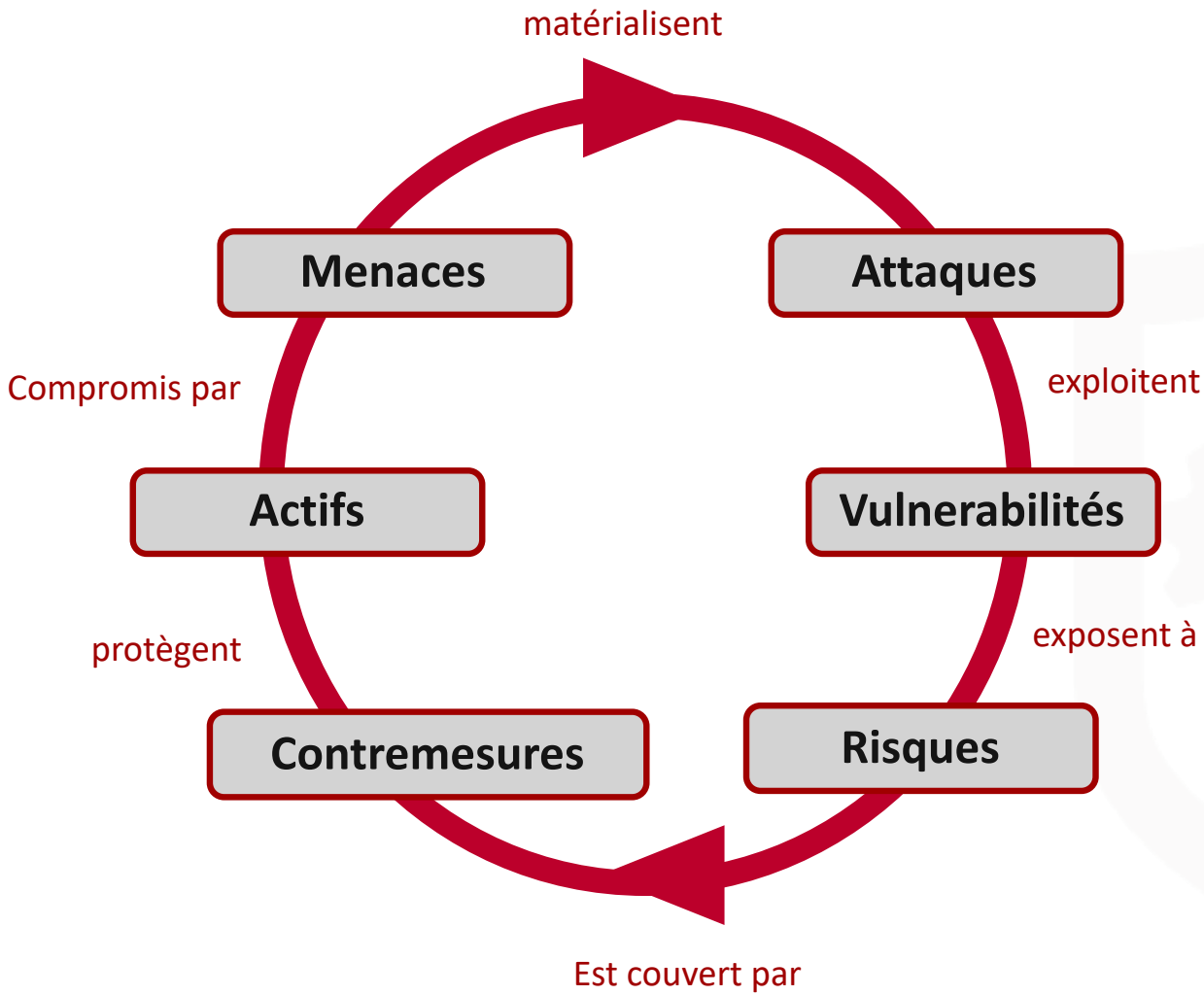
Des modèles différents

les 4 axes de la gestion de la menace



Le cycle du risque vs la menace

la gestion de la menace



les grandes menaces

quelques éléments de la menace 1/2

- Attaques par **déni de service distribuées** (DDoS). Un réseau d'ordinateurs inonde un site Web ou un logiciel avec des informations inutiles. Quand la charge sur les services est important et que le système n'est pas dimensionné ou filtré pour ce type de volume de demande, ce débordement de requêtes provoque une indisponibilité du système inopérant.
- **Codes malveillants** : Bots et virus. Un logiciel malveillant qui s'exécute à l'insu de l'utilisateur ou du propriétaire du système (bots), ou qui est installé par un employé qui pense avoir affaire à un fichier sain (cheval de Troie), afin de contrôler des systèmes informatiques ou de s'emparer de données. La mise à jour des logiciels et des certificats SSL, une forte protection antivirus et une sensibilisation des employés peuvent vous aider à éviter ces types de menace.

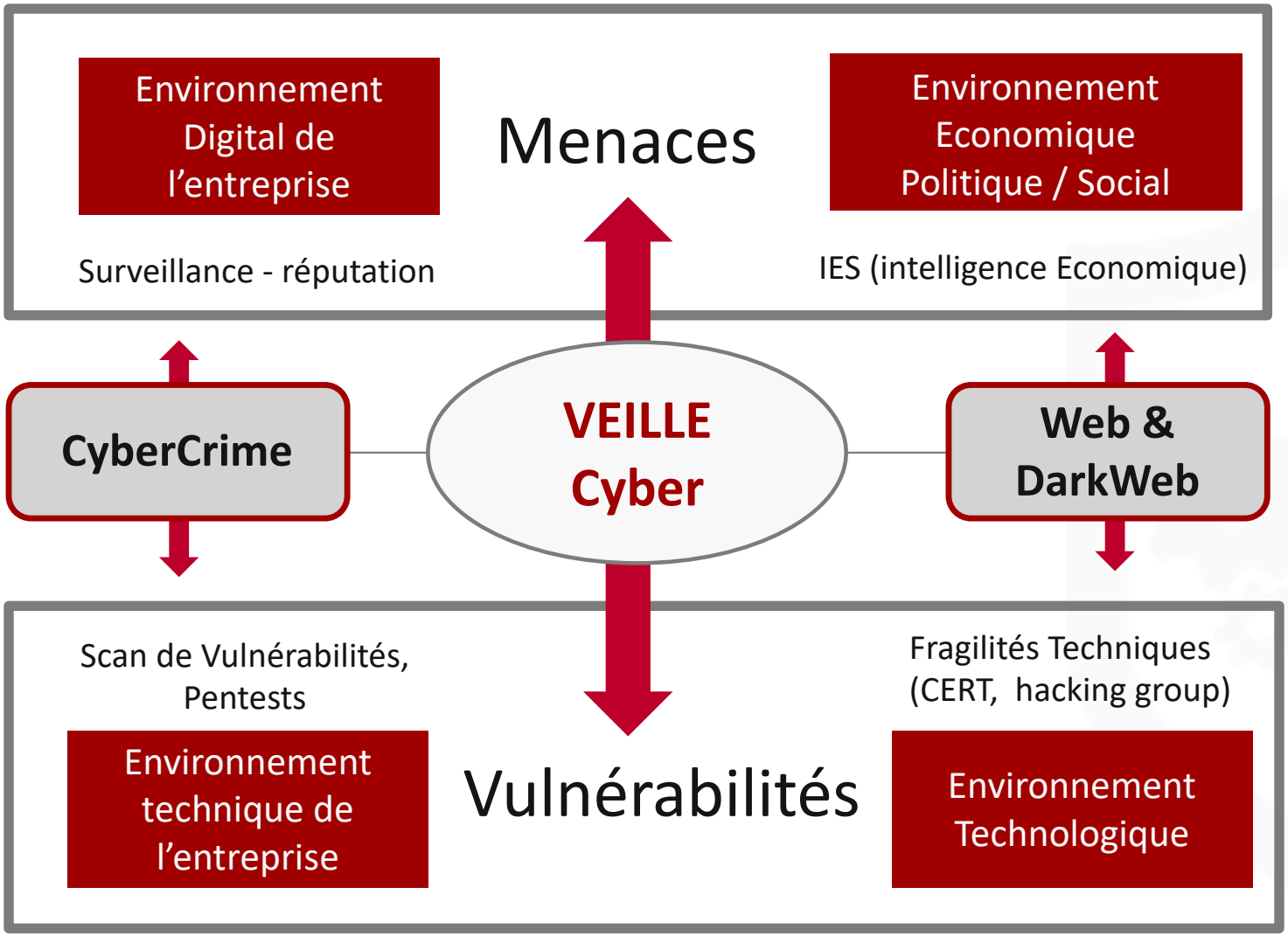
les grandes menaces

quelques éléments de la menace 2/2

- **Piratage**. Lorsque des acteurs externes exploitent des failles de sécurité afin de contrôler vos systèmes informatiques et voler des informations. Une mise à jour régulière des mots de passe et des systèmes de sécurité est fondamentale pour déjouer ce type de complot.
- **Hameçonnage** ou dévoiement. Tentative d'obtenir des informations sensibles en se faisant passer frauduleusement pour une entité digne de confiance. Le hameçonnage se fait par e-mail, tandis que le dévoiement utilise des sites ou serveurs fictifs. Une sensibilisation des employés est indispensable afin de ne pas tomber dans ce piège.

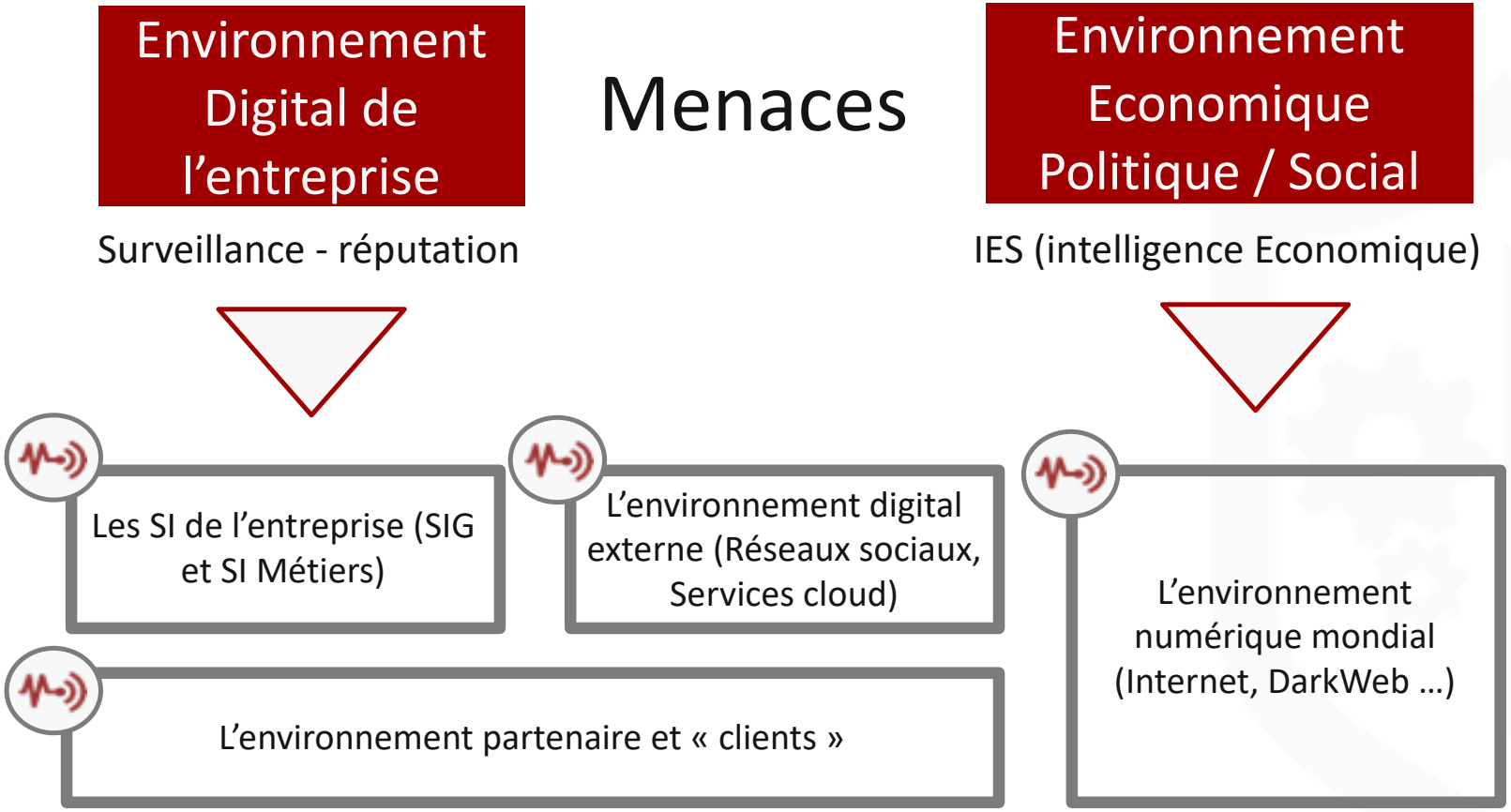
Veille

Veille cyber, une veille sur les risques



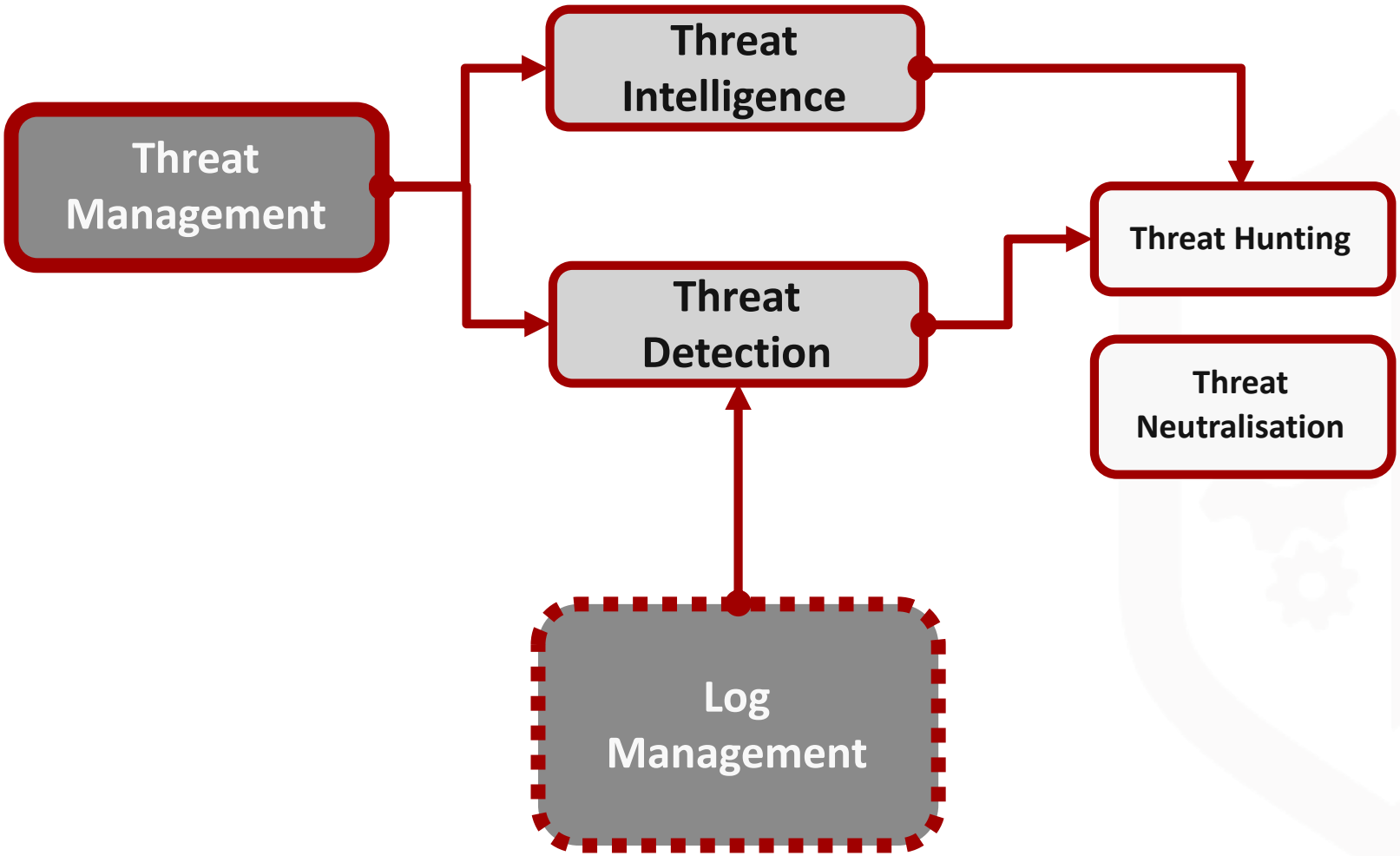
Les sources

Les sources



La gestion de la menace

la gestion de la menace



Threat Detection

La surveillance et le renseignement de la menace au sens général du terme (Threat Intelligence) devrait contenir les 2 niveaux :

- Le renseignement à vocation cyber qui comprend toutes les analyses et information permettant d'anticiper et de caractériser une menace qui pourrait s'exprimer dans le monde numérique,
- Le renseignement d'origine Cyber, dont les données techniques liées à des attaques, menaces qui permettent de configurer des systèmes de détection et de réponse.

des questions ?

contacter eric.dupuis@cnam.fr

CYBERDEF

101

Tous les documents publiés dans le cadre de ce cours sont perfectibles, ne pas hésiter à m'envoyer vos remarques !

Contributions

Les notes et les présentations sont réalisées sous LaTeX.
Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) [a] . Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.
Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

a. https://github.com/edufaction/CYBERDEF