SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam Bretagne

DETECTER : de la surveillance à l'évènement de sécurité

Eléments de sécurité opérationnelle en cyberdéfense d'entreprise

Eric DUPUIS

eric.dupuis@lecnam.net eric.dupuis@orange.com

http://www.cnam.fr

Conservatoire National des Arts et Métiers
Chaire de Cybersécurité

Publication DRAFT NOTES S2 - 2020 du
19 mai 2020, 23 h 31 CEST

Sommaire

GERER les menaces

ANTICIPER les menaces

DETECTER les attaques

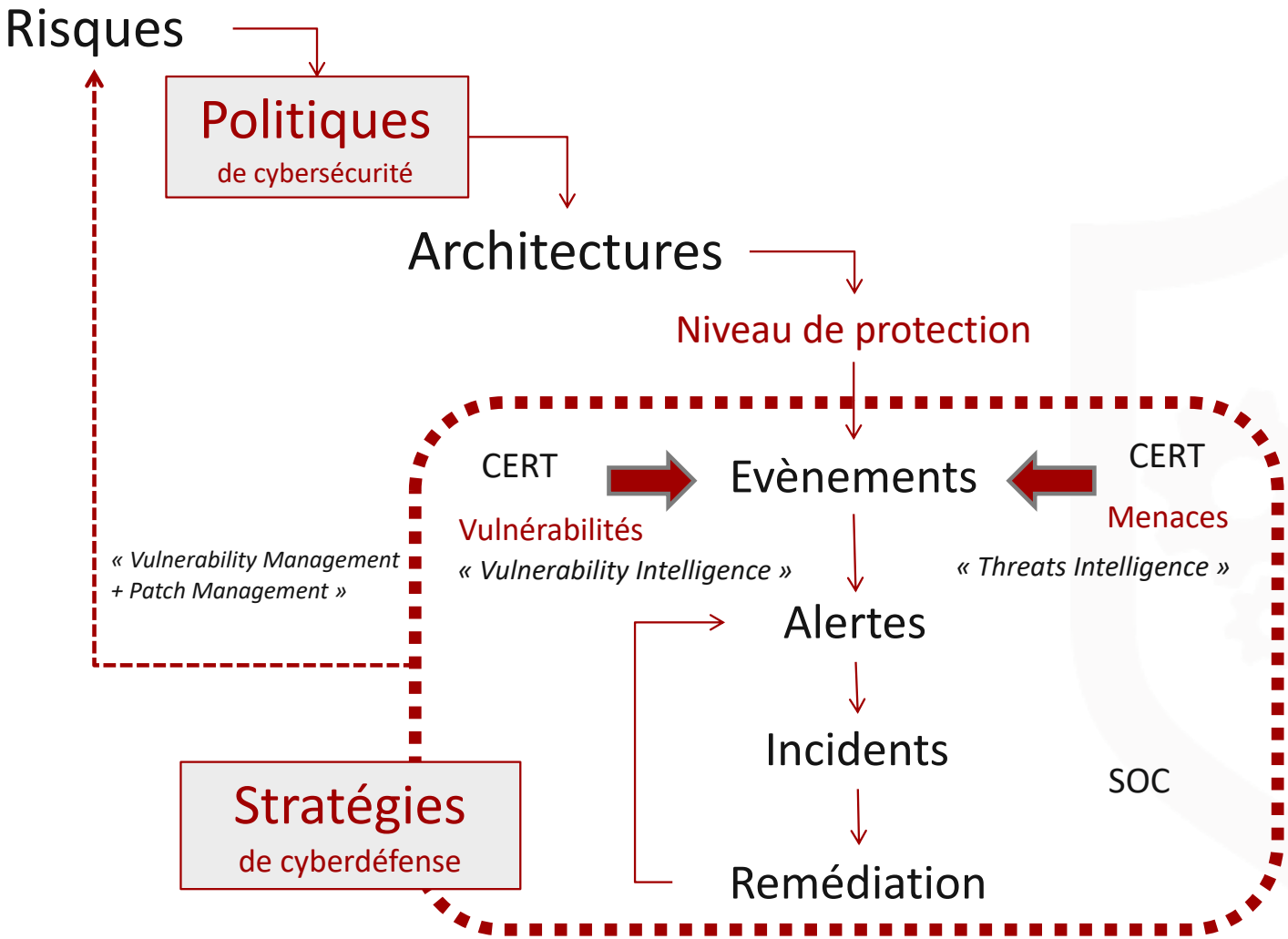
(SOC) Security Operation Center

Technologies et Organismes connexes

Botnet, des codes malveillants organisés

Contributions

Cycle de vie de gouvernance Cyberdef



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 d'évoquer l'assurance sécurité des Logs (intégrité, horodatage , valeur probante ...)
- **COMPRENDRE - PREVOIR** : Avec le *Threat Management* : Veiller, surveiller la menace dans l'environnement digital de l'entreprises, modélisation de la menace et scénarios redoutés issus d'analyse de risque ;
- **DETECTER** : Surveiller le comportement des systèmes dans le périmètre défini, faire émerger les évènements, anomalies, incidents pouvant révéler une attaque en cours, une suspicion de compromission par des menaces avancées (APT), où des attaques furtives et discrètes. Nous aborderons l'outillage avec les SIEM et l'organisation avec les SOC ;
- **ALERTER** : mettre en place les mécanismes de remontée d'alerte et d'incident permettant de gérer les alertes adaptées au niveau d'impact d'une attaque.

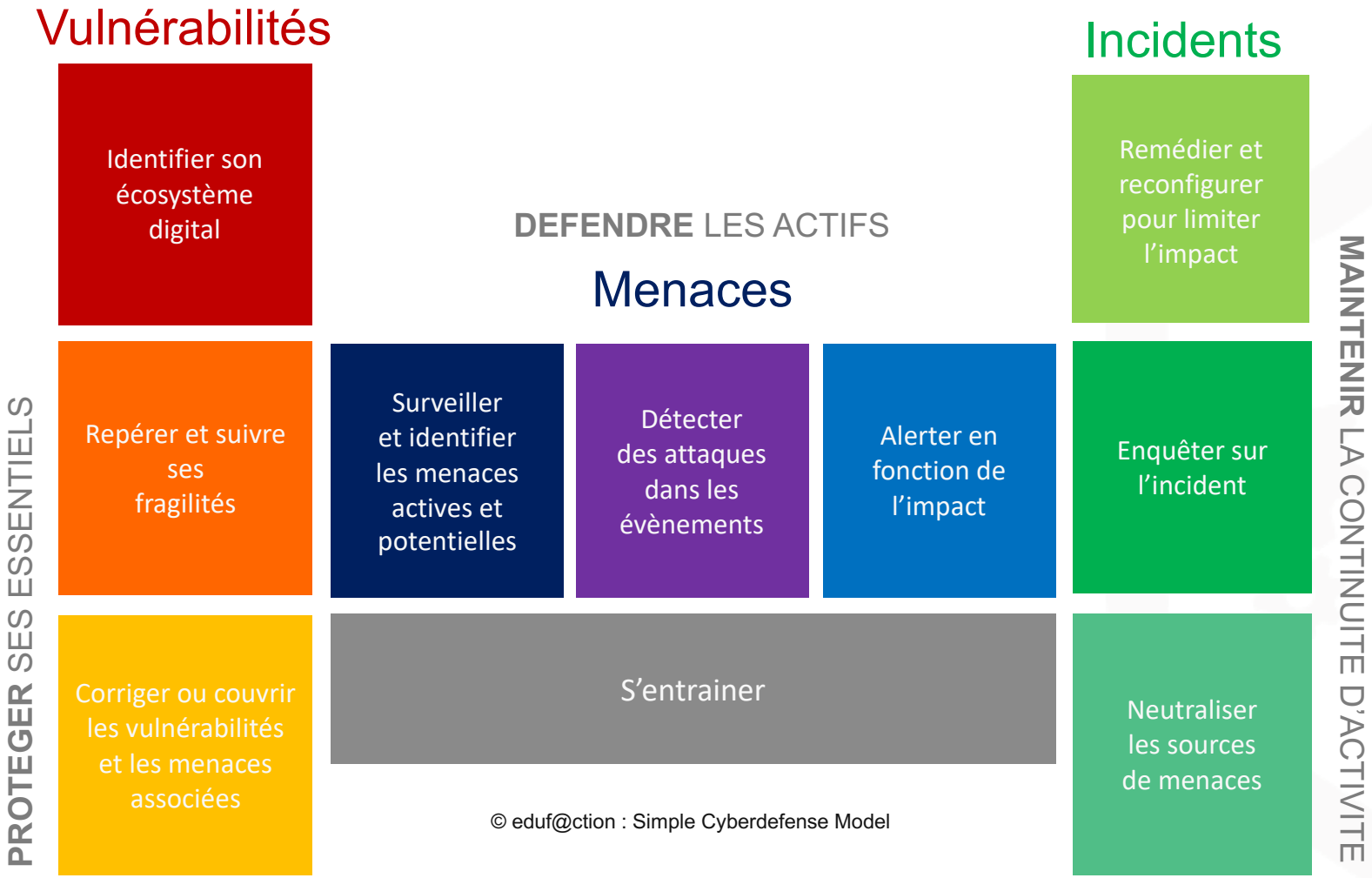
Menaces

NONE

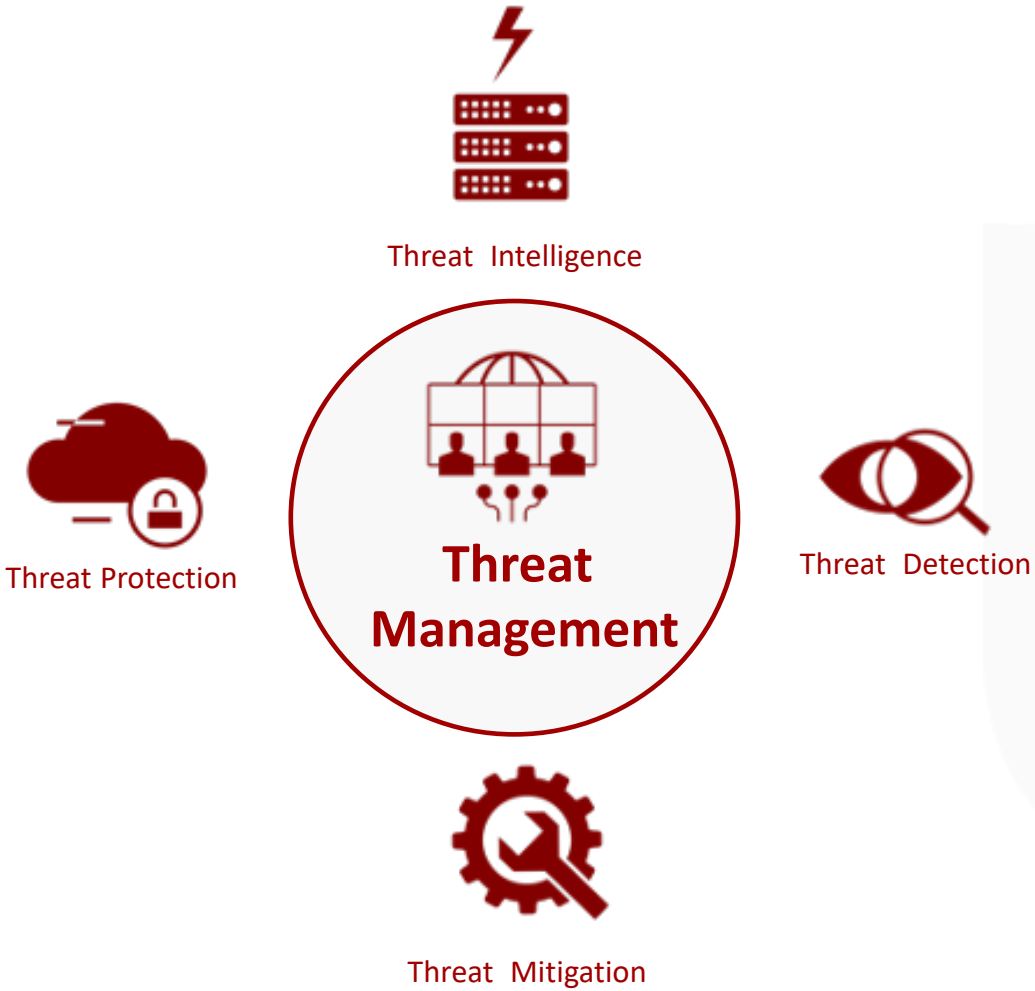
Menaces=Veille et recherche : La gestion de la menace est au coeur des stratégies de cyberdéfense de l'entreprise. Comme pour les vulnérabilités, c'est la connaissance des menaces, de leur recherche et de leur découverte qui permet de réduire les risques ;

Menaces=Évènements : La détection d'une vulnérabilité ou d'une menace est un évènement, la question est de savoir à quel moment il est important de déclencher un mécanisme d'alerte, et comment cette alerte va devenir un incident déclenchant des mécanismes de réponse (Voir Cycle de gouvernance **??** page **??**).

Un modèle de gestion cyberdéfense



les 4 axes de la gestion de la menace

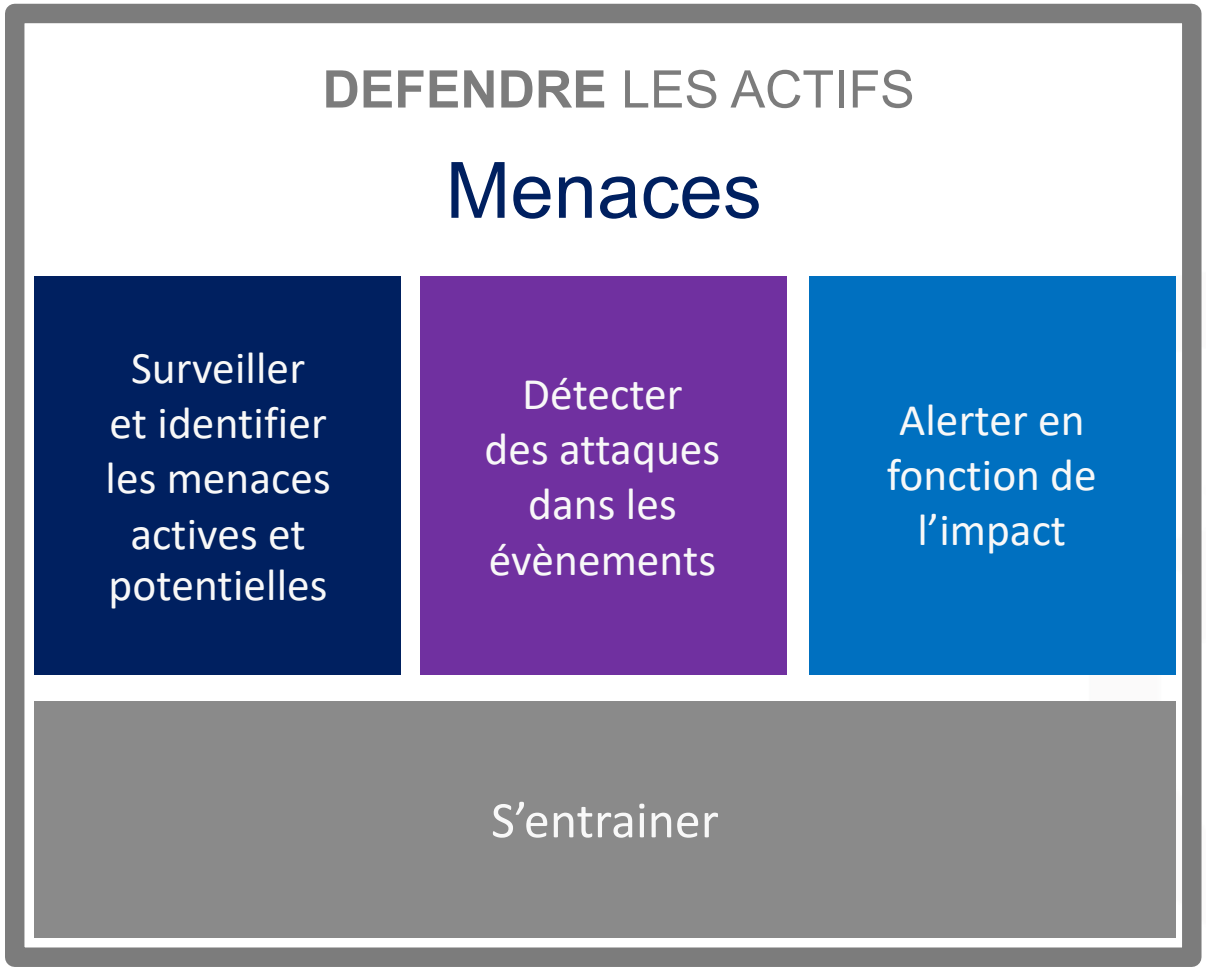


les grandes menaces

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. L'exemple, le plus classique est celui d'un serveur WEB. Quand la charge sur les services est trop importante 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 gestion de la menace



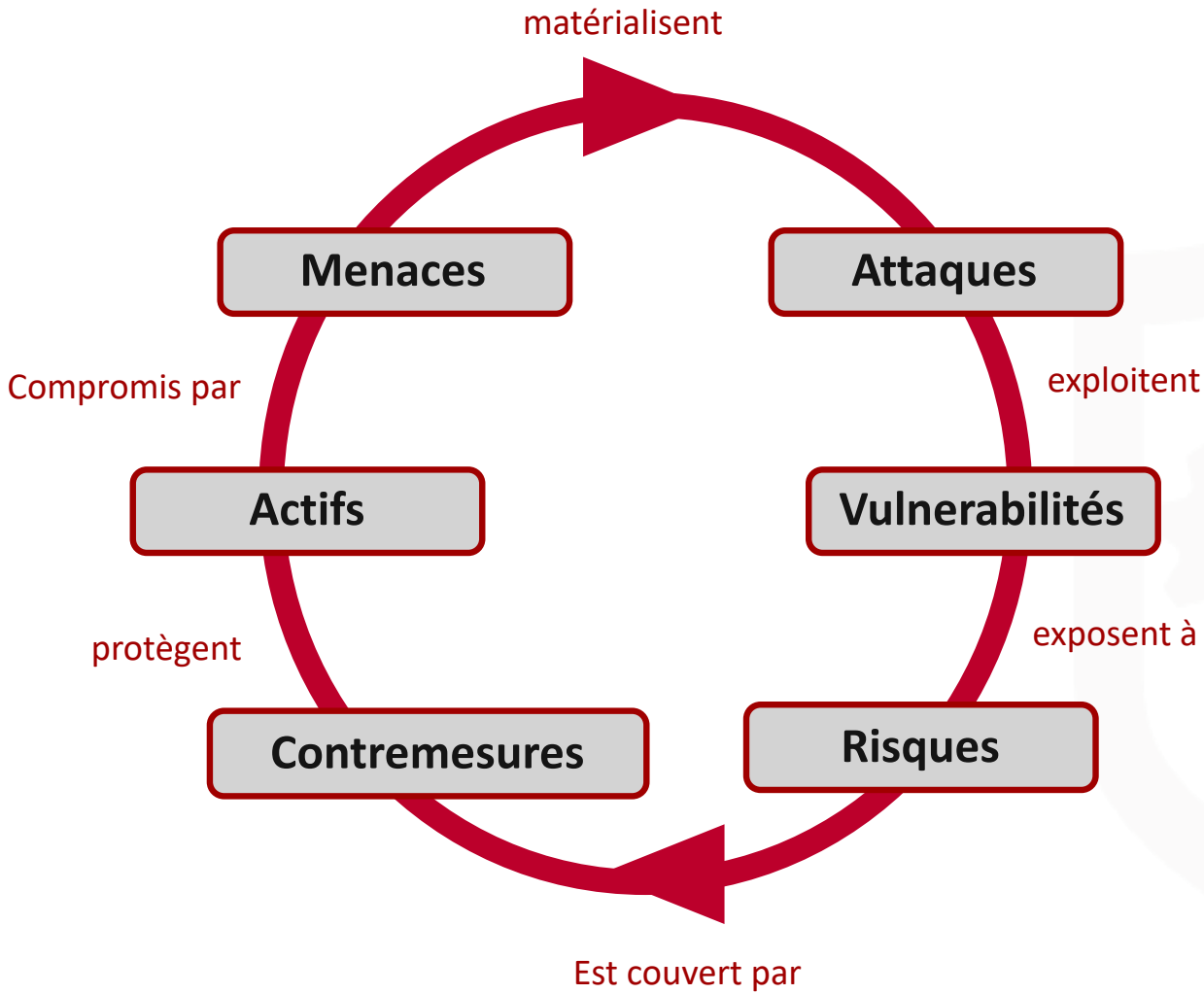
© eduf@ction : Simple Cyberdefense Model

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, en utilisant ou pas un code malveillant. Par exemple, un changement régulier des mots de passe et la mise à niveau des systèmes de sécurité est fondamentale pour limiter les impacts.
- **Hameçonnage** ou dévoiement. Tentative d'obtenir des informations sensibles en se faisant passer frauduleusement pour une entité digne de confiance. Le hameçonnage se fait généralement par e-mail, mais il ne faut pas oublier les SMS et les services utilisant du message (Webmail, mail intégré comme Linkedin, ...),

la gestion de la menace



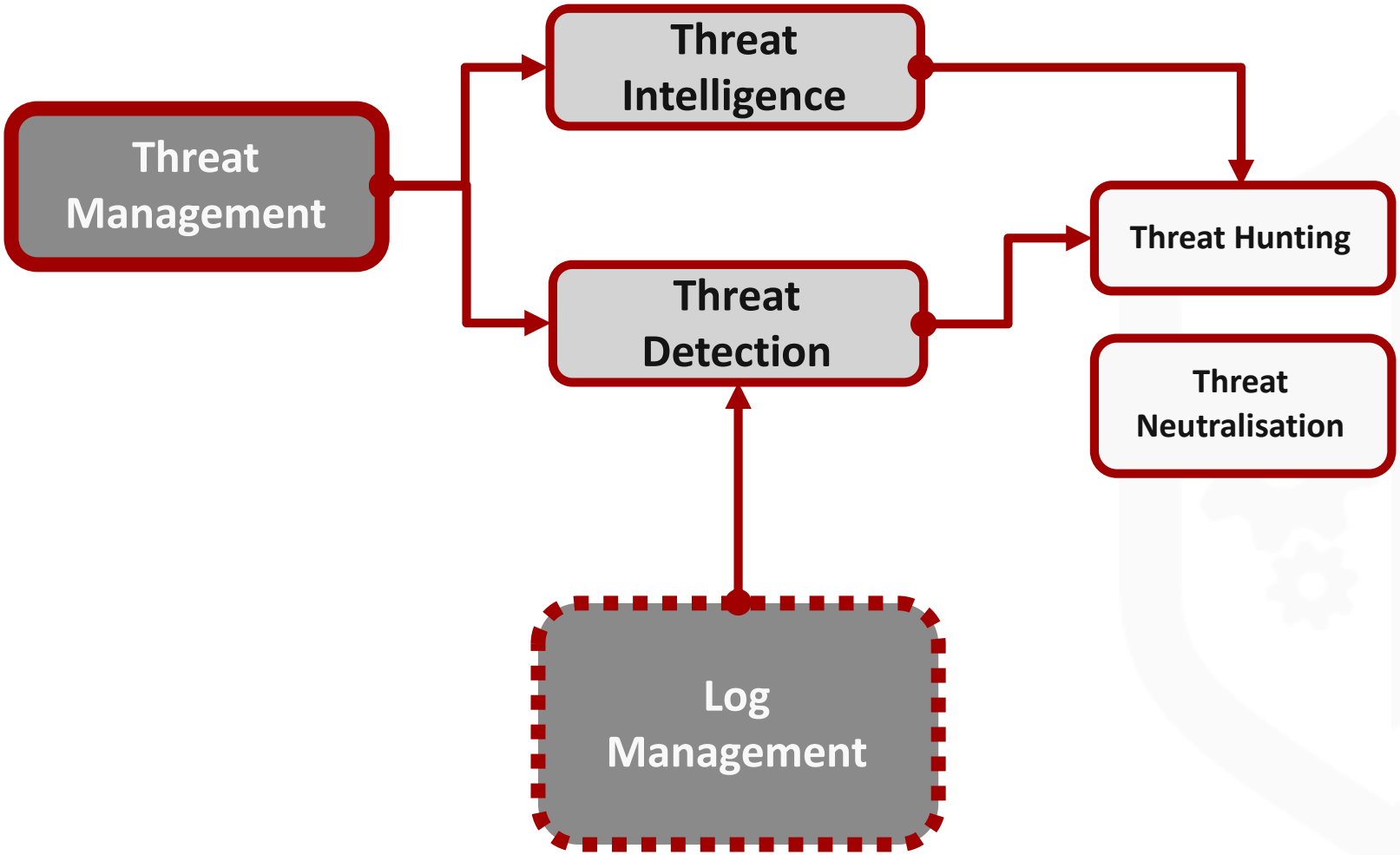
Gérer la menace

Threat Intelligence et Detection

Gérer la menace comporte deux donc domaines d'activités :

- La veille, au sens renseignement sur la menace (Threat Intelligence) ;
- La détection d'attaque, ou de menaces potentielles au sein de l'environnement (Threat Detection).

la gestion de la menace



Threat Intelligence

Sources identifiées menaçantes

Nous parlerons ici de sources de menaces comme les indicateurs permettant d'identifier l'origine technique d'une menace. Cela peut être une adresse mail, un serveur/service de mail , une adresse IP de provenance d'un code malveillant, d'une attaque, ou d'un comportement anormal. On peut citer par exemple :

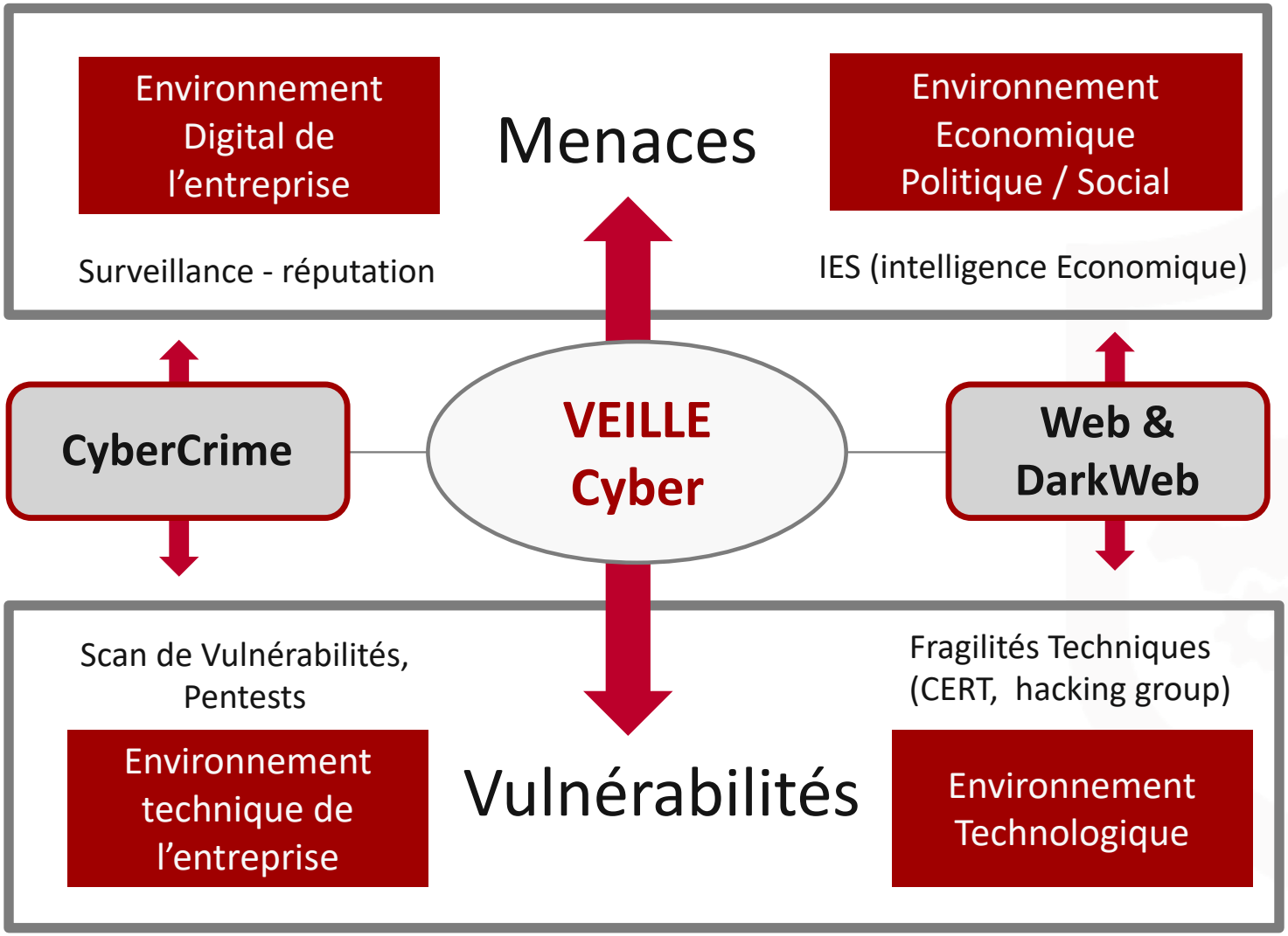
- Une adresse mail connue pour envoyer des codes malveillants ;
- des adresses IP ou des adresses de serveur Mail pour Spam.

Threat Intelligence

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.

Veille cyber, une veille sur les risques



Veiller et surveiller

2 axes

Veiller et surveiller les menaces, détecter les attaques nécessite d'analyser deux axes :

- Les menaces génériques, ou ciblant un domaine particulier (Santé, Industrie, Banque ...) que l'on trouve généralement en utilisant des technologies de « threat Intelligence » ;
- Les menaces ciblées, dont les indices d'émergence peuvent être détecter en analysant la menace ou en recherchant des indices de compromissions quand ces menaces sont actives dans le périmètre de l'entreprise. « threat Detection, Hunting ... »

Veiller et surveiller

2 manières

et ceci de deux manières :

- Surveillance de l'écosystème de la menace (IOC, DarkWeb, Threat Intelligence...)
- Recherche de compromission, ou d'infection (Threat Hunting, ...)

Les sources

Menaces

Environnement Digital de l'entreprise

Surveillance - réputation

- Les SI de l'entreprise (SIG et SI Métiers)
- L'environnement digital externe (Réseaux sociaux, Services cloud)
- L'environnement partenaire et « clients »

Environnement Economique Politique / Social

IES (intelligence Economique)

- L'environnement numérique mondial (Internet, DarkWeb ...)

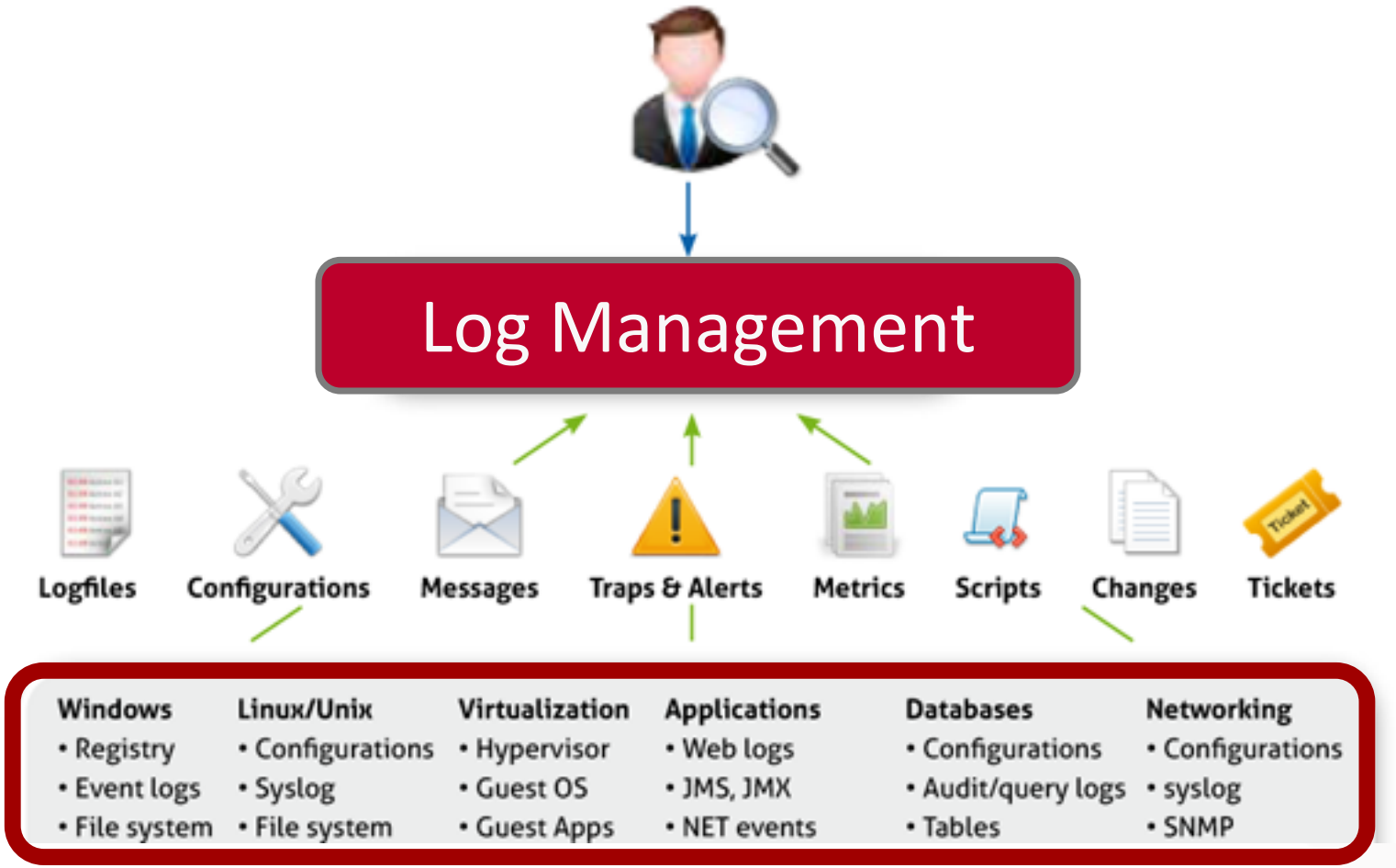
Surveillance du ciblage

l'outillage du « targetting »

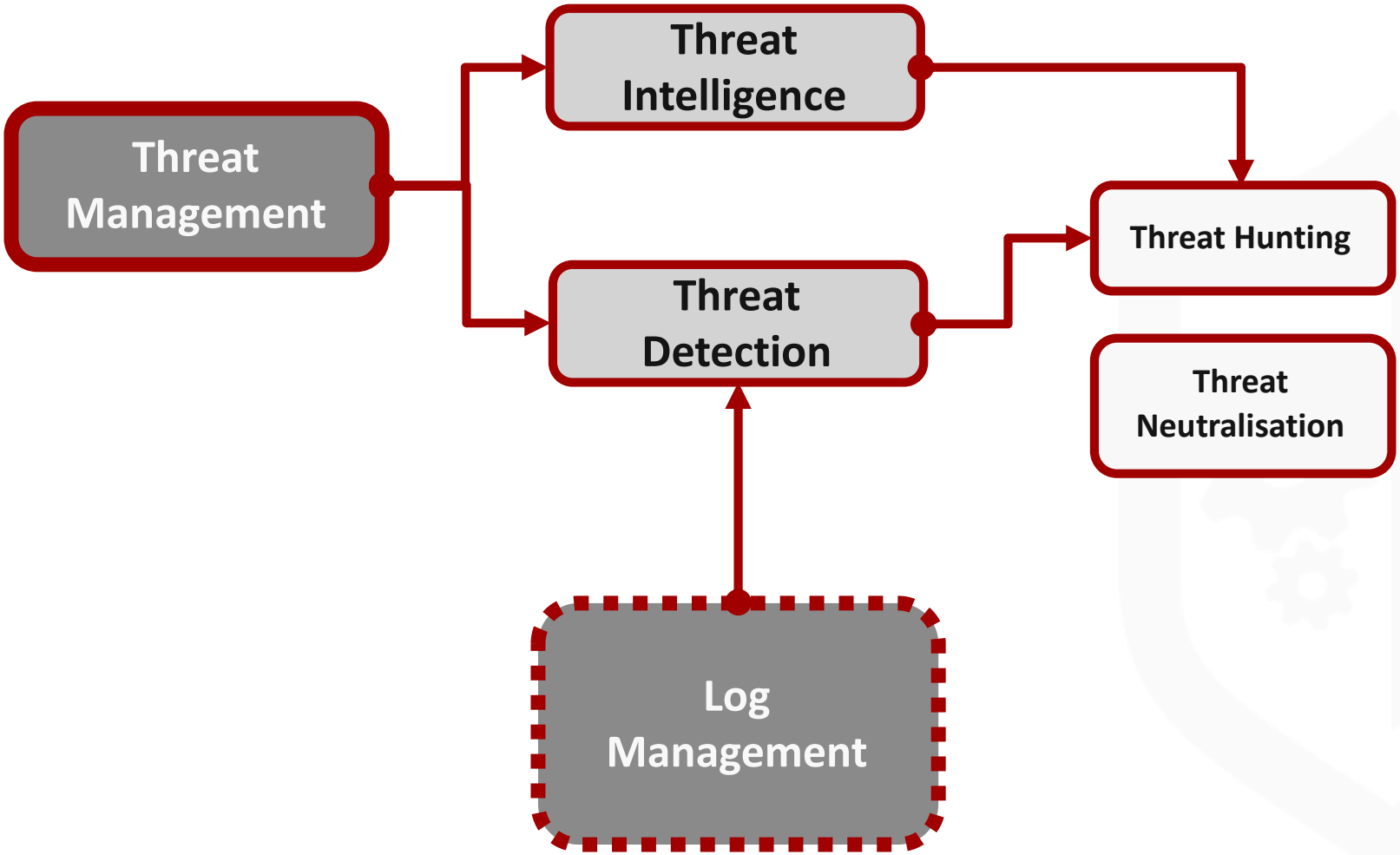
Il y a deux types d'outils pour ce se faire :

- La surveillance classique du web de type « cyberveille », qui permet de découvrir des éléments compromis appartenant à l'entreprise (soient les données, soient des informations permettant de déduire que l'entreprise a été compromise).
- L'analyse en temps réel des codes malveillants qui peut permettre en regardant de manière détaillée l'évolution du code pour comprendre et connaitre les modalités des attaques et les nouvelles cibles.

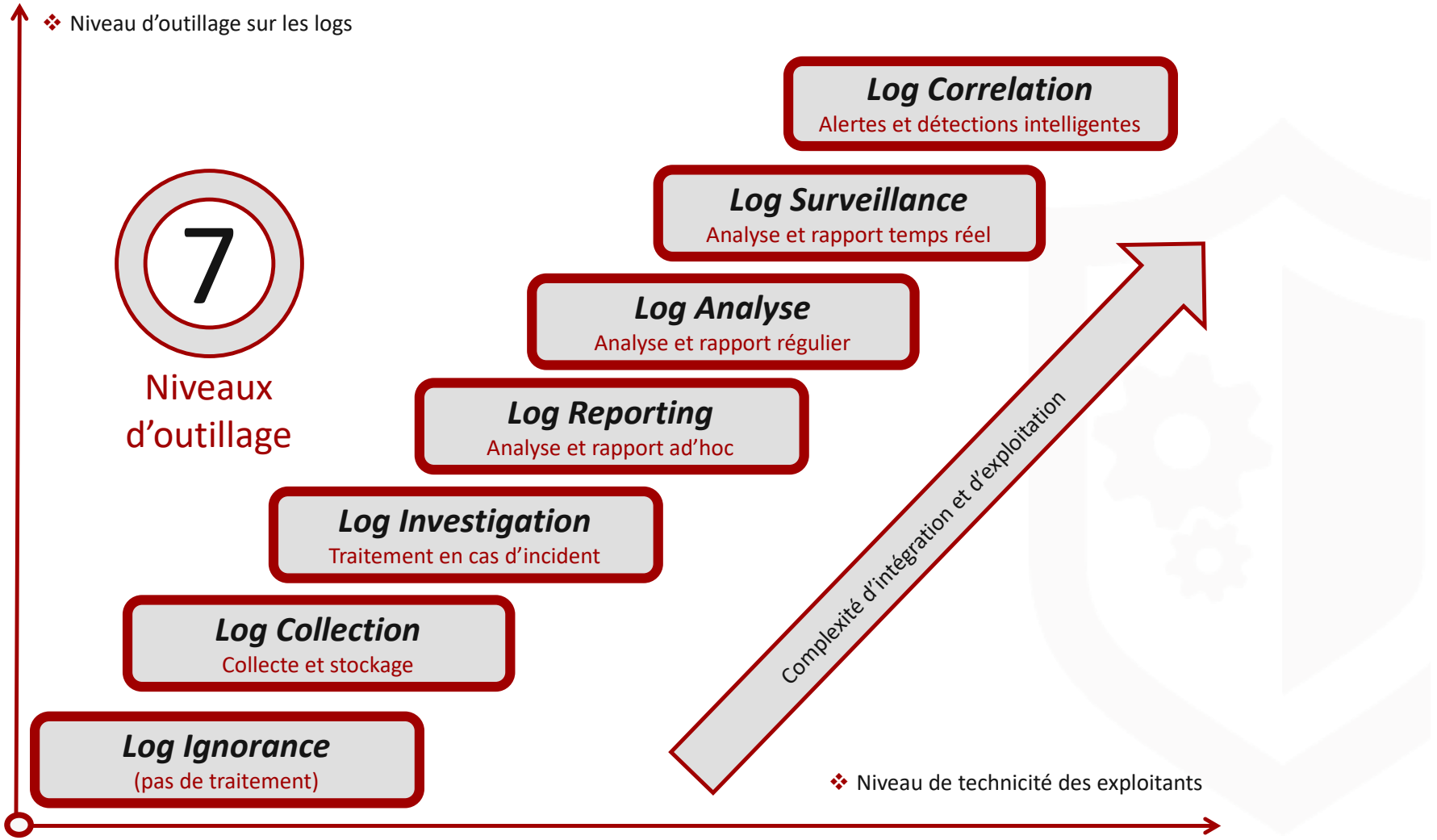
Sources de log



Les logs au coeur de la détection



Les niveaux d'outillage



SIEM et Log

Threat and leak

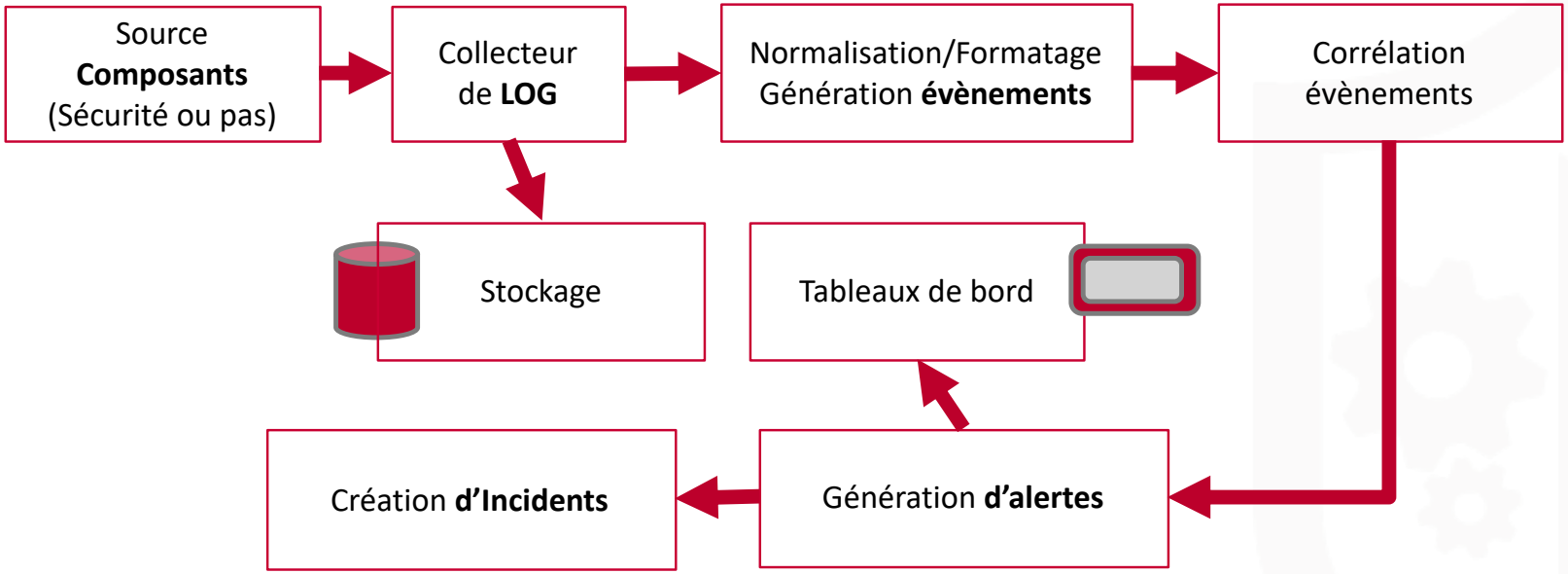
Puisque nous disposons maintenant d'une capacité de capter de l'information pertinente pour détecter des attaques, que nous avons une architecture de collecte, ainsi qu'une architecture de stockage et de filtrage, nous pouvons injecter des informations dans des outils de recherche et de corrélation d'attaque. Ceci pour peu que l'architecture et les outillages puissent suivre la charge d'analyse en temps réel.
Il ne faudra pas aussi oublier que les traces informatiques et réseaux ne sont pas les seules sources d'information nécessaires à la détection d'attaques (en temps réel ou différé), il faut aussi connecter des sources de menaces :

- **Threat Intelligence Database** : IOC et identifiants des sources malveillantes (IP, noms de domaine, serveur mail ...)
- **Leak** : Fuite de données détectés par la surveillance du Web et du Darknet.

Fonction SIEM

- la première fonction d'un SIEM est déjà de corréler les événements provenant des composants de sécurité ;
- la deuxième fonction de corréler des événement de comportement du SI ;
- la troisième fonction de corréler avec des événements externes au SI sur la base de capteurs externes (threats intelligence de type renseignement).

architecture d'un SIEM



Cadre méthodologique

Services et actifs du SI

- sondes de sécurité
- points d'accès et de contrôle de politique SSI
- systèmes et applications
- réseau
- équipements de chiffrement

Données externes

- Sources de malware
- Rapport de scan vulnérabilité
- Base de Threat Intelligence interne client

Expertise et savoir faire

- Catalogue des scénarios de menace
- Listes dynamiques
- Flux de veille
- Expérience antérieure sur incident

Modélisation des risques "métier"

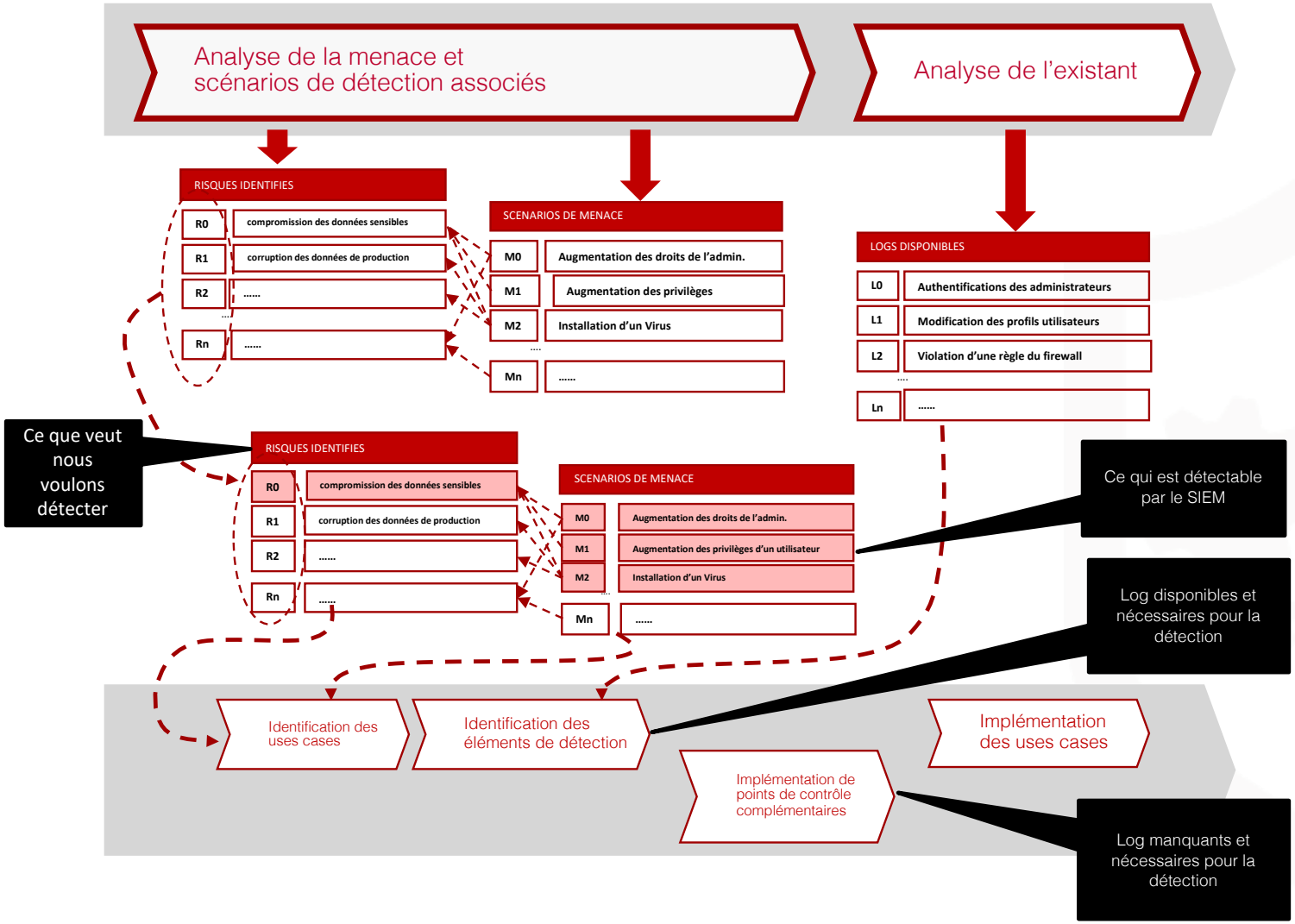
- Activité normale
- Activité a priori anormale
- Besoins business

Rapports & tableaux de bord

Alertes

- Type de notification
- Criticité et priorité
- Instructions de supervision
- Instructions spécifiques de remediation

Construction des UseCase



Quelques SIEM

en provenance du Gartner

Le Gartner positionne régulièrement des produits et services dans son magic Quadrant. en 2019, Splunk, IBM QRadar et LogRythm NextGen SIEM sont toujours bien positionnés. Dell Technologies (RSA NetWitness), Exabeam (Security Management Platform), McAfee (Enterprise Security Manager) et Securonix complètent le carré des Leaders. Toutefois des entreprises comme Microsoft challenge ces acteurs.

Threat Hunting

La chasse aux menaces est une tactique permettant de connaître avec plus d'acuité l'environnement de la menace et donc le degré de risque de cyber-attaques auquel est soumise une entreprise.
La terminologie threat hunting regroupe plusieurs types d'action et la définition de n'est pas totalement stabilisée. Globalement on y trouve deux grandes classes de « *threat hunting* » :

- Celles travaillant autour de l'environnent, de la surface d'attaque et qui orientent ses actions sur des méthodes de « recherche » permettant de débusquer des menaces latentes ou des menaces dormantes, de les réveiller, de les suivre , de les comprendre pour établir le contact avec l'attaquant.
- Et une autre plus active ou proactive dont l'objectif est de rester, conserver le contact avec l'attaquant lors d'une réaction à une alerte.

SOC

Security Operation Center

Il intègre l'ensemble des fonctions liées à la menace :

- Veille sur la menace
- Détection d'évènements à risques et gestion de ceux ci
- Détection d'attaques ou de comportement critiques
- Réaction aux incidents et remédiation

Cotations connexes

gérer le niveau de gravité de l'alerte

- **l'origine** de l'attaque qui mesure la puissance potentielle de la source de menace : du hacker de base à la menace étatique ;
- Le type de **cible** qui mesure la précision de la diffusion de la menace : de la cible au hasard à la menace ciblée ;
- Le **vecteur** d'attaque qui mesure le niveau de sophistication de la menace : du malware « sur étagère » à l'APT élaborée ;
- Le **préjudice** qui mesure l'impact subit par la cible : d'une perte faible à une mise en péril de la résilience même de l'organisme ;
- La **visibilité** de la menace qui mesure de nombreux éléments comme la motivation ou durée de l'attaque : d'un DDOS immédiatement constaté à une attaque invisible ;
- La **persistence** qui mesure la fréquence de l'attaque sur sa cible : d'une fréquence forte de type robotisée (Bots) à une fréquence unitaire visant un but précis, ou la furtivité.

Automatisation, SOAR

Orchestration

On y trouve par exemple dans ces outils de « *Security Orchestration, Automation, and Response* » (SOAR) :

- l'introduction de sources de menaces de manière automatique au base SIEM (abonnement de threat-intelligence) ;
- la production de règles sur la base de déviances relevées ;
- le pilotage automatique des composants de sécurité (modification de règles, passage en mode dégradé ...) ;
- l'exécution de tâche de conservation de traces légales (notarisation) ;
- la gestion automatisée de « patchs » critiques (intégration au DEVSECOPS)

...

Efficacité du CSOC

métrologie

Pour mesurer l'efficacité d'un CSOC, il existe plusieurs moyens de mesures :

- La **couverture fonctionnelle et technique** du CSOC pour estimer l'efficacité de l'articulation entre les stratégies de cyberdéfense, de cyber-protection et les stratégies de surveillance détection,
- La **performance de la détection** pour évaluer l'efficacité des règles de corrélation en place, basée sur les indicateurs de services (Nombre de détections, nombre d'évènement ...) ;
- La **maturité du service CSOC**, mesurée sur le niveau d'organisation des services (ITIL par exemple), les coûts, les compétences, les services connexes ...

des questions ?

contacter eric.dupuis@lecnam.net

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`

Mises à jour régulières

Eduf@ction eric.dupuis@lecnam.net

Vérifiez la disponibilité d'une version plus récente de

SEC101-C3-ThreatMan.prz.pdf sur GITHUB CYBERDEF [1]