



# SEC 101

Analyse de risques  
Politiques et architectures de sécurité  
Sécurité opérationnelle

# le cnam Bretagne

## Réagir : De l'évènement de sécurité à la crise

Éléments de sécurité opérationnelle en cybersécurité d'entreprise

Eric DUPUIS

[eric.dupuis@cnam.fr](mailto:eric.dupuis@cnam.fr)   [eric.dupuis@orange.com](mailto:eric.dupuis@orange.com)

<http://www.cnam.fr>

Conservatoire National des Arts et Métiers  
Chaire de Cybersécurité

Date de publication  
4 mai 2020



# Sommaire

Gestion des incidents

ANTICIPER

REAGIR

ENQUETER

Techniques connexes

CERT et CSIRT

Gestion de crises

Contributions





# La réponse à incident

quelques éléments de définition

La réponse à incident est le processus qui permet de déployer les moyens nécessaires pour traiter un événement de sécurité classé comme incident de sécurité. Un incident de sécurité peut être enregistré en provenance de systèmes de sécurité, de veille ou d'audit. Le besoin d'intervention peut être immédiat comme différé. La réponse peut nécessiter des équipes de compétences larges comme expertes sur un domaine donné. L'intervention peut nécessiter des moyens techniques important ou pas, et mettre en isolation tout ou partie d'un système d'information.



# Les axes de la gestion des cyber-Incidents



## ANTICIPER

**Gouverner, Organiser,  
mesurer, architecturer**

Mise en œuvre d'une cellule de gestion des incidents de sécurité disposant des capacités et de la légitimité pour répondre techniquement et piloter éventuellement une gestion de crise



## REAGIR

**Remédier, Isoler,  
Contenir, neutraliser**

Intervention sur incidents pour réduire l'impact de l'attaque



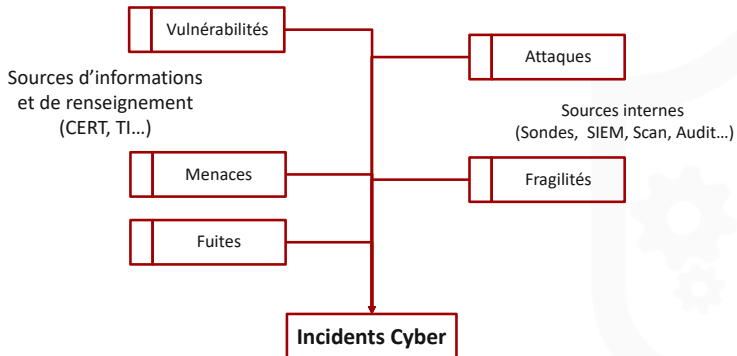
## ENQUETER

**Identifier, Imputer,  
Evaluer Impact, Comprendre,  
modéliser**

investigation numérique pour déterminer les caractéristiques de l'attaque (intentions et objectifs, sources, cibles, mécanismes)

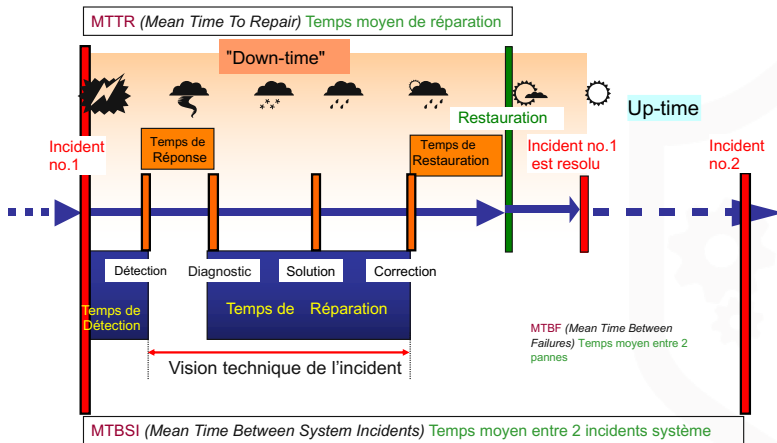


# Les axes de la gestion des cyber-Incidents





# Incidents





# Incidents

## MAINTENIR LA CONTINUITE D'ACTIVITE

### Incidents

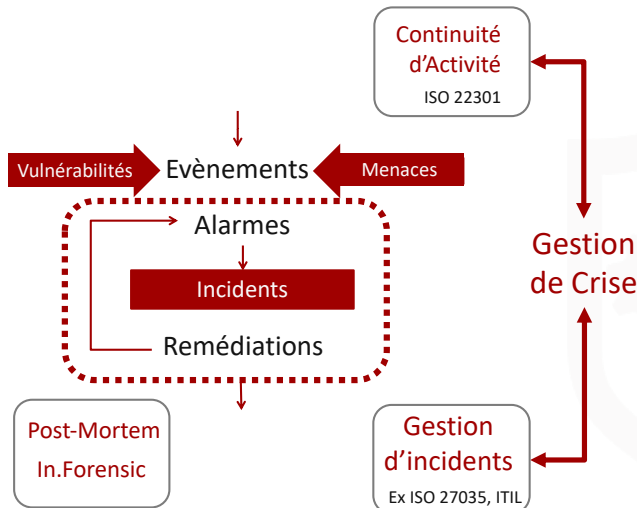
Remédier et  
reconfigurer  
pour limiter  
l'impact

Enquêter sur  
l'incident

Neutraliser  
les sources  
de menaces



# Incidents







# des questions ?

contacter [eric.dupuis@cnam.fr](mailto: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  $\text{\LaTeX}$ .

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) <sup>a</sup>. 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>