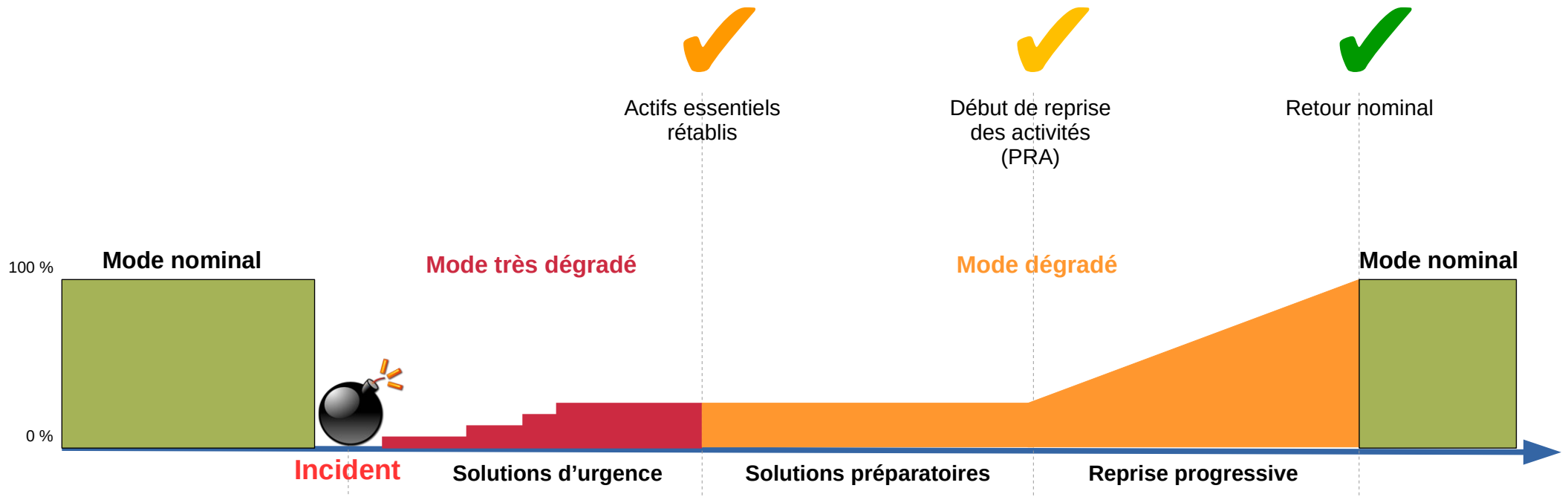
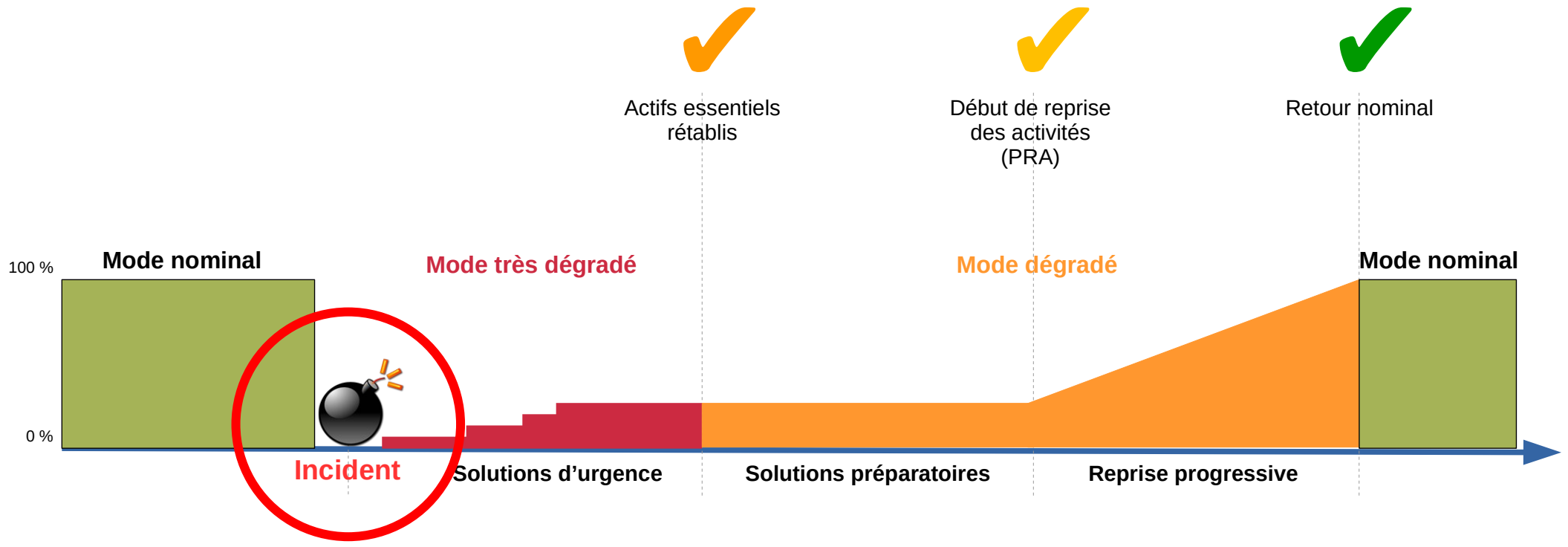
amU Aix Marseille Université

Josy Sécurisation AD
- Remédiation -

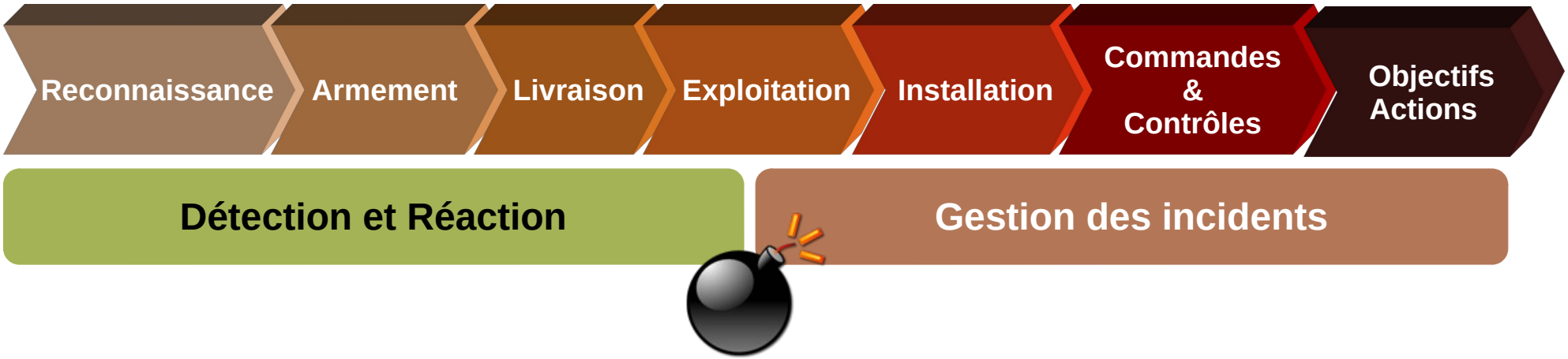
L’incident


Actifs essentiels rétablis
Début de reprise des activités (PRA)
Retour nominal
100 %
0 %
Mode nominal
Mode très dégradé
Mode dégradé
Mode nominal
Incident
Solutions d’urgence
Solutions préparatoires
Reprise progressive

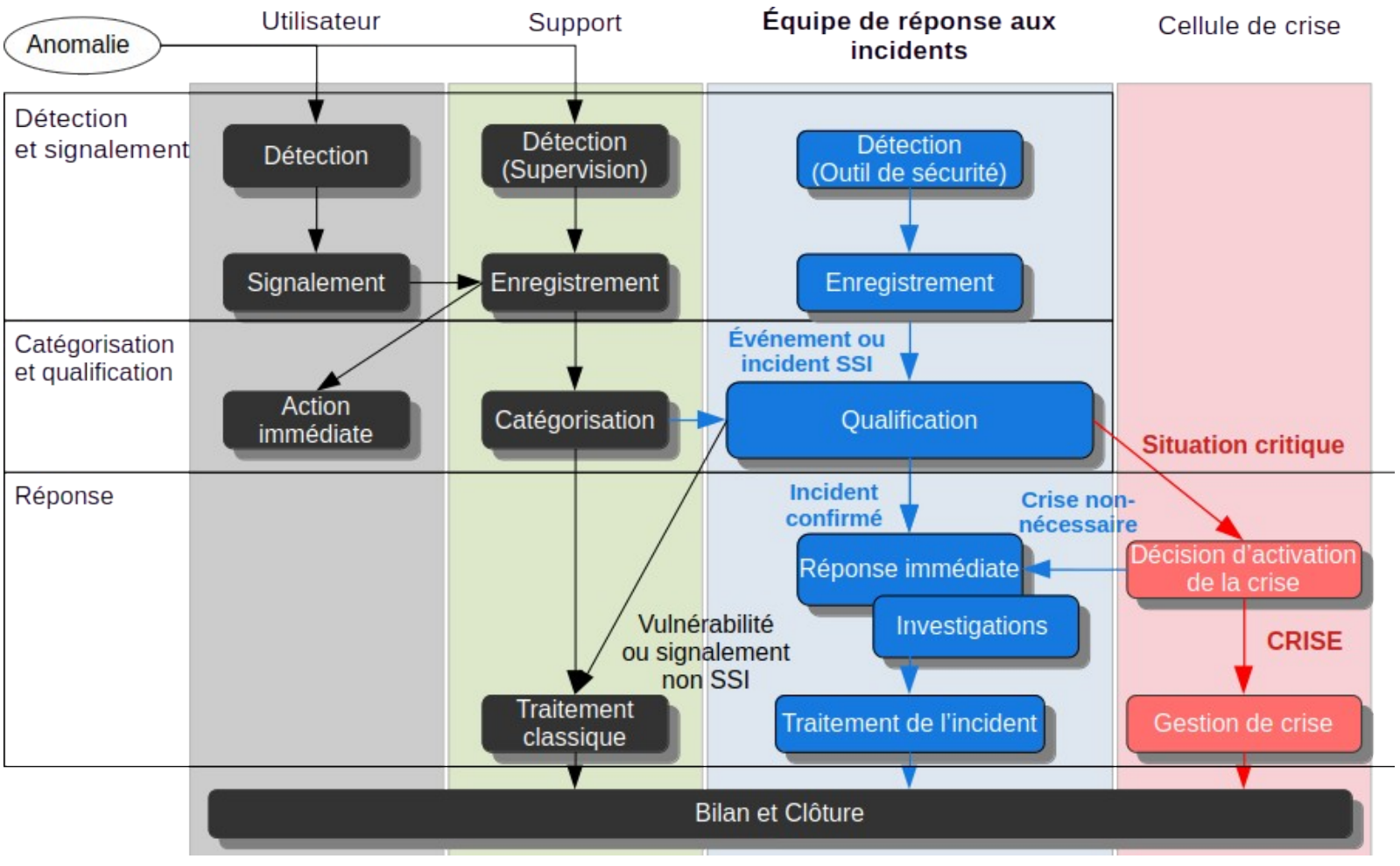
L’incident


Actifs essentiels rétablis
Début de reprise des activités (PRA)
Retour nominal
100 %
0 %
Mode nominal
Mode très dégradé
Mode dégradé
Mode nominal
Incident
Solutions d’urgence
Solutions préparatoires
Reprise progressive

L'incident

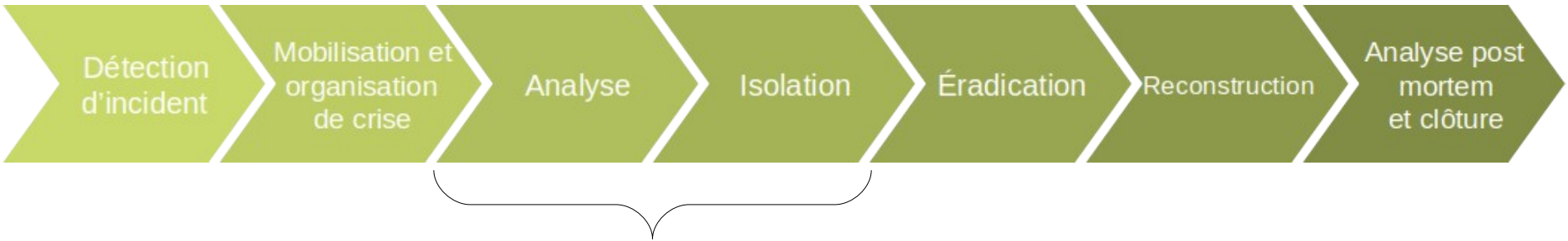

Reconnaissance
Armement
Livraison
Exploitation
Installation
Commandes & Contrôles
Objectifs Actions
Détection et Réaction
Gestion des incidents

Processus de gestion d'incident



Processus de gestion d'incident grave

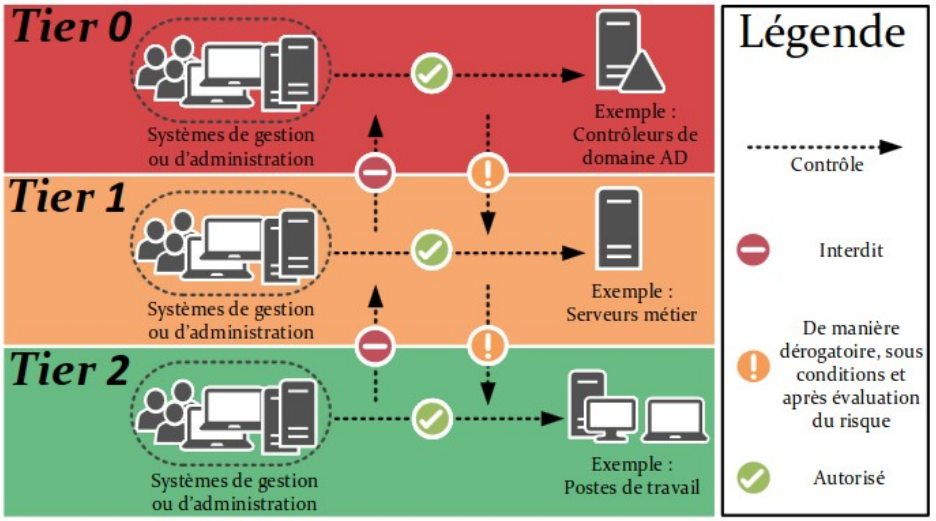
Processus de gestion d'incident grave



- État de la compromission **latérale**
- État de la compromission **verticale** → AD
- État de l'intégrité des systèmes

Prévention

- Isolation : réseau, tiers, etc.
- Gestion des logs / supervision
- Durcissement système
- Audit
- PCRA
- Etc.



https://cyber.gouv.fr/publications/recommandations-pour-ladministration-securisee-des-si-reposant-sur-ad

Réaction

- Isolation / cloisonnement
- Inforensique : logs & métadonnées de réplication
- Gestion d’incident / de crise
- PCRA
- Etc.

https://github.com/ANSSI-FR

Windows-Forensics-checklist-cheatsheet

Remédiation

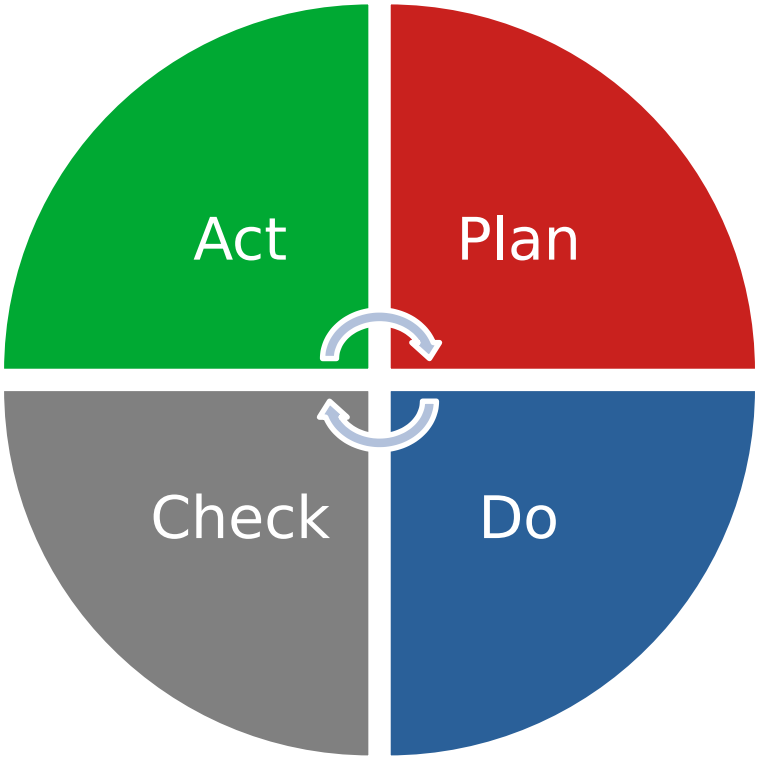
Récupération	Réinstallation
- des objets - des permissions - peu d'impacts	- confiance
- malware / backdoors	- recréation des objets - réapplication des délégations - reconstruction du parc

Remédiation

Récupération	Réinstallation
- des objets - des permissions - peu d'impacts	confiance
- malware / backdoors	recréation des objets réapplication des délégations reconstruction du parc

Préférable, à condition d'être sûr de son PCRA

Conclusion



Roue de Deming

Merci pour votre attention