

# Simuler une attaque/défense pour les agents des services informatiques

## Contexte

---

Les professionnels des services informatiques sont au cœur de la cybersécurité d'un établissement et seront les premiers sollicités en cas d'attaque. Si beaucoup est déjà fait sur le travail de renforcement de la sécurité des systèmes, il faut également être en mesure de réagir ou d'agir efficacement lorsque les systèmes sont interrompus. À l'instar des entraînements à la sécurité incendie, la sécurité des SI doit aussi appréhender la gestion de crise lorsque le risque survient.

## Objectifs

---

Appréhender les méthodes d'attaques et prévoir les mécanismes de défenses adaptés ; Mettre en place les premières actions pour limiter les dégâts ; Informer / dialoguer efficacement avec la Direction ; Solliciter les bons acteurs extérieurs ; Faciliter le fonctionnement de l'établissement en mode dégradé ; Spécifier les procédures de gestion de crise et de communication ; Assurer et anticiper la reprise.

## Renseignements complémentaires

---

Jour 1 : Compréhension des mécanismes d'attaques :

Reconnaissance ; Découverte de vulnérabilités ; Écriture/Exploit de failles ; Exfiltration ; Couverture des traces ; Répartition travaux pratiques : 70% / 30%.

Jour 2 : Simulation réelle

Mise en pratique : avec un laboratoire comprenant un Système d'Information virtuel. Le but est de mettre en pratique en situation « réelle » une phase d'attaque et une phase défense en simultanée permettant d'activer ainsi les différents protocoles. Répartition travaux pratiques : 90% / 10%

**Échéance du marché** 19/10/2026

### Public

**Professionnels des SI, équipes SSI et administrateurs.**

**Exercice  
2026**

**Code de formation  
8-7**

**Nature  
AFR**

**Organisé par  
Ascent**

**Typologie  
Formation continue ou Développement des connaissances et des compétences**