OCÉAN INDIEN
Axe 4 : TRANSITION ECOLOGIQUE ET EVOLUTION SOCIETALE

Module n°5 : SERVICES TECHNIQUES - mise en situation d'une cyberattaque [CRISALYDE]

Contexte

Si la cybersécurité constitue l'un des enjeux majeurs du numérique, les risques et les bons comportements à adopter face aux cyberattaques sont encore peu connus. Cette formation, dont l'objectif est de confronter les participants à une cyber crise, vous apportera des connaissances théoriques sur la notion même de la cyber crise, mais vous permettra également de savoir mesurer les impacts de celle-ci sur les appareils connectés, en vous y confrontant, grâce à un exercice de mise en situation réaliste.

Objectifs

- Identifier ce qu'est une crise cyber
- Connaître le risque de piratage des appareils connectés techniques
- Comprendre les interactions entre les appareils connectés techniques et le service de sécurité informatique
- Se confronter à une gestion de crise informatique et savoir identifier les risques d'une cyberattaque sur les appareils connectés

Programme

Qu'est-ce qu'une crise cyber ?

- La définition de la crise cyber
- Les typologies des crises cyber

Le risque de piratage des appareils connectés techniques

- Identification des appareils utilisés quotidiennement
- Connaître les conséquences d'un dysfonctionnement majeur de ces appareils
- Identifier les risques de piratage liés à une cyberattaque

Les interactions entre les appareils connectés et le service de sécurité informatique

- La reconnaissance d'une situation de crise
- Identifier les actions les plus efficaces à mettre en place pour répondre à une situation de crise cyber
- L'identification des besoins et de ses interlocuteurs en situation de crise cyber
- Comprendre et identifier les risques générés par une cyberattaque sur les appareils connectés

Identification des bonnes pratiques et axes d’amélioration

Public

Personnel des services techniques

Exercice
2026

Code de formation
4-01

Nature
AFR

Organisé par
ASCENT FORMATION / CRISALYDE / DEMETER SANTE

Durée
7 heures