| | | |
|---|---|---|
| **Parcours 1 : Mieux connaître l'écosystème de la cybersécurité** | | |
| | | |
| **Module** | **Titre** | **Date de sortie** |
| | | |
| Module 1 | Introduction & objectifs de la formation | 15/09/2020 |
| Module 2 | Panorama du cadre juridique de la cybersécurité | 17/09/2020 |
| Module 3 | Typologie des attaques selon les moyens techniques | 22/09/2020 |
| Module 4 | Étude de cas WannaCry/NotPetya (cryptovirus) | 24/09/2020 |
| Module 5 | Typologie des attaques selon les objectifs recherchés | 29/09/2020 |
| Module 6 | Étude de cas Phishing | 01/10/2020 |
| Module 7 | Systèmes vulnérables, et typologie des attaques | 06/10/2020 |
| Module 8 | Panorama des organisations juridiques | 08/10/2020 |
| | | |
| **Fin de la session** | | **31/12/2020** |
| | | |
| **Parcours 2 : Quelles prévention, attitude et répliques face à une attaque cybercriminelle ?** | | |
| | | |
| **Module** | **Titre** | **Date de sortie** |
| | | |
| Module 9 | La mise en œuvre de la protection – mesures de protection techniques et orga | 13/10/2020 |
| Module 10 | La mise en œuvre de la protection – mesures de protection techniques et orga | 15/10/2020 |
| Module 11 | La mise en œuvre de la protection : mesures juridiques | 20/10/2020 |
| Module 12 | La mise en place d'une cellule de crise, et rôle des parties prenantes. | 22/10/2020 |
| Module 13 | Les bonnes pratiques de communication à l'éco-système | 27/10/2020 |
| Module 14 | Mesures techniques & juridiques | 29/10/2020 |
| Module 15 | Obligations consécutives à la survenance d'une attaque | 3/11/2020 |
| Module 16 | Le rôle des acteurs institutionnels dans la réaction | 5/11/2020 |
| Module 17 | La restauration, ou la remédiation, du système ou des données et la résolution | 10/11/2020 |
| Module 18 | La réparation du préjudice subi par l'entreprise victime de l'attaque | 12/11/2020 |
| Module 19 | Cas pratique : La remise en état postérieur à la crise | 17/11/2020 |
| | | |
| **Fin de la session** | | **31/12/2020** |