OBJECTIFS

Objectifs pédagogiques

Surveillez les menaces potentielles à la sécurité de vos applications et de vos systèmes
Comprendre les avis de sécurité et les descriptions de failles ; utiliser des bases de données de vulnérabilité
Configurer votre accès ssh selon les bonnes pratiques
Configurer et diagnostiquer le pare-feu du système
Configurez un pare-feu réseau ; utiliser des systèmes de protection avancés
Configurer l'authentification des applications selon les bonnes pratiques
Connaître les principaux algorithmes cryptographiques et leur utilisation.

Compétences développées :

Configurer le pare-feu du système
Effectuer une veille technologique
Connaissances des pare-feu du système et des pare-feu du réseau
Connaissance des principes de la supervision
S’assurer que les transactions sont sécurisées
Connaissance des règles de sécurisation des accès ssh
Diagnostiquer un dysfonctionnement et le corriger
Identifier les problèmes et déterminer les équipes concernées

Démarche pédagogique (projet, ressources ...)

Ce module utilisera différents ensembles d'outils pour les sous-projets. Nous allons réutiliser l'application "conduit", utiliser un système fraîchement installé, installer une appliance, modifier le code d'une application pour ajouter l’autorisation. Nous couvrirons en fin de module le protocole OAuth 2 largement utilisé pour les autorisations en manipulant ses différents flux à utiliser dans différentes situations.

Compétences

Itération 1

- Effectuer une veille technologique
- Identifier les problèmes et déterminer les équipes concernées
- Comprendre les normes communes de dénomination des problèmes de sécurité (CVE, GHSE etc)

Itération 2

- Diagnostiquer un dysfonctionnement et le corriger
- Mettre à jour le projet avec ses dépendances

Itération 3

- Connaissance des principes de la supervision

Itération 4

- Connaissance de l'authentification multifactorielle
- Connaissance des règles de sécurisation des accès ssh

Itération 5

- Configurer le pare-feu du système
- Connaissances des pare-feu du système et des pare-feu du réseau

Itération 6

- S'assurer que les transactions sont sécurisées

MODALITÉS

Durée

10 jours soit 70 heures au total.
Lancement le 18/03/2024 et clotûre le 29/03/2023.

Formateur(s)

Marta RYBCZYNSKA, référent module
Louis RANNOU

TRAME

		Planning	Jour	Sujet/Activités
18/03	Cyber	Louis RANNOU	1	Itération 1 - Failles de sécurité
19/03	Cyber	Louis RANNOU	2	Itération 2 - Dépendances
20/03	Cyber	Autonomie	3	Itération 2 - Dépendances Itération 3 - Monitoring de sécurité
21/03	Cyber	Louis RANNOU	4	Itération 3 - Monitoring de sécurité
22/03	Cyber	Marta Rybczynska	5	Itération 4 - 2FA et SSH
25/03	Cyber	Marta Rybczynska	6	Itération 5 - Pare feu système
26/03	Cyber	Autonomie	7	Itération 5 - Pare feu système
27/03	Cyber	Marta Rybczynska	8	Itération 5 - Pare feu réseau
28/03	Cyber	Louis RANNOU	9	Iteration 6 - OAuth
29/03	Cyber	Louis RANNOU	10	Iteration 6 - OAuth