Shibboleth

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Outils

Rubrique : Fortinet - Shibboleth

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Savoir mettre en place une application fédérée avec droits d'accès, interprétation des logs, compréhension des fichiers de configuration et d'Installation SP et IDP.

Public visé

Informaticiens

Pré-requis

Aucun

PROGRAMME

JOUR 1

1.Introduction
1.1 Fédération des identités

- Historique WAM / SSO
- SAML
- Evolutions

1.2 Pour quelle utilisation ?

- Délégation d'identité
- Informations d'identité
- Habilitations (Attribute Based Acces Control)

1.3 Ecosystème de fédération

- Protocoles complémentaires : XACML, SCIM, UMA, WS-Trust, Oauth 2, CloudAuthZ

2. Shibboleth

- Historique
- Périmètres
- Réputation
- Qui l'utilise ?
- Version 3
- Version 4
- Forces, faiblesses par rapport aux concurrents

3. Architecture

- IdP, SP, authentication, annuaire, attributs
- Point à point, opérateurs de fédération
- IdP discovery

Code de formation : NE531

€ Tarifs

Prix public : 3100 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 28 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

- Authentification depuis internet
- Cas de l'annuaire local dans le périmètre de protection
- Disponibilité / performances

JOUR 2
4. SAML
4.1 Norme SAML

- Bindings et profils SAML - HTTP POST - Artifact…
- Browser SSO
- Métadonnées / certificats SP / IdP initiated
- Analyse AuthnRequest
- Analyse AuthnR réponse
- Éventail des possibilités

4.2 Cas d'utilisation

- Applications Saas
- SSO
- CIAM

4.3 Limitations

5. OpenID Connect (OIDC)

- 5.1 Cas d'utilisation
- 5.2 Limitations

6. OAuth

- 6.1 Cas d'utilisation
- 6.2 Limitations

JOUR 3
7. MFA
7.1 Les enjeux
Dans quel but ?

7.2 Déploiement
Mise en place

8. Sécurité
Création d'une fausse assertion
Interception, modification d'une assertion
Interception et rejet d'une assertion valide
Déni de service
Divulgation de données confidentielles

9. Identity Provider
9.1 Configuration de base

- Échange de métadonnées
- Authentification formulaire LDAP
- Transmission de l'email
- Logout

9.2 Interface avec les applications
Problèmes souvent rencontrés

9.3 Transmission d'attribut

- DataConnector
- Offre de base
- Ajout d'un nouveau DataConnector
- Traitements sur les attributs

9.4 Configuration avancée

- Chainage
- Passage en revue des fichiers de configuration

- 9.5 Personnalisation
- Modification composant existant

- Exemple login.jsp
- Plugins

9.6Interface web

10. Service Provider

- 10.1 Shibboleth
- Principe de fonctionnement
- Configuration

10.2 Autres SP

- Kits de développement dédiés (Java, C#, PHP)
- Bibliothèques de sécurité
- Filtres (Java)
- Agent serveur d'applications
- Frontal
- Même fonctionnement que Shibboleth, possibilité cookie au lieu en-tête
- SP de rebond

JOUR 4

11. Retour d'expérience

- Problèmes rencontrés
- Limitations Evolutivité

12. Travaux Pratiques

- Installation IdP / authentification LDAP
- Installation SP
- Tests

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.