Atelier d'investigation Système, Réseau et Sécurité

Investiguer pour résoudre les problèmes sur des systèmes défaillants

Stage pratique
Opérations

Code :
AISRS

Durée :
1 jour(s) (7,00 heures)

Exposés : **20 %**
Cas pratiques : **70 %**
Echanges d'expérience : **10 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 990,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Il arrive très régulièrement de devoir comprendre pourquoi un système ne fonctionne pas. Sans pratique, le travail d'investigation est souvent long et pénible et se résume à courir après des logs et à copier/coller des messages d'erreur dans un moteur de recherche.

Cette formation propose de (re)découvrir par la pratique les erreurs classiques qui surviennent sur nos systèmes et la démarche à mettre en œuvre pour les comprendre, puis les résoudre.

Cette formation s'adresse aux développeurs, Ops ou DevSecOps qui souhaitent approfondir leurs connaissances en système. À l'issue de cette journée, vous aurez revu les techniques et outils indispensables permettant de comprendre une situation de panne..

OBJECTIFS PEDAGOGIQUES

- Analyser et mettre en pratique les architectures réseau, système, applicative et web d'environnements Linux afin d'en comprendre le fonctionnement et les interactions.
- Découvrir ou redécouvrir les problèmes liés à ce genre d'architecture
- Utiliser les principaux outils système d'investigation sous Linux pour collecter des informations, diagnostiquer des anomalies et interpréter les résultats.

PUBLIC CIBLE

- Développeur
- Administrateur
- Intégrateur
- Chef de projet technique Ops

PRE-REQUIS

Connaissances de base des architectures web / cloud. Connaissances de base des système Linux (shell, ligne de commande, etc.)

METHODE PEDAGOGIQUE

Formation basée essentiellement sur la réalisation de travaux pratiques.

Ceux-ci sont étayés par des apports théoriques, échanges sur les contextes des participants et retours d'expérience du formateur.

Déroulement de 5 à 6 exercices en fonction de la vitesse du groupe. Les thématiques des exercices portent sur :

.La compréhension des architectures web (Load-balancers, reverse-proxies, serveurs web, serveurs d'application)

.La compréhension du réseau local (routage, NAT, firewall, modèle OSI)

.Les risques de sécurité inhérents à ces architectures.

Exemple : votre application web n'est plus joignable (erreur HTTP/500). Avec des outils comme netstat, lsof ou strace, vous pourrez identifier ce qui est “cassé” pour ensuite faire le nécessaire afin de réparer.

Chaque exercice commence par une situation dans laquelle un système (assemblage de plusieurs machines) est présenté aux participants dans un état non fonctionnel ou avec un risque de sécurité. Par la pratique, les élèves sont progressivement guidés pour comprendre la situation, puis aller chercher des informations supplémentaires (sur les machines, sur Internet), et enfin proposer des commandes à lancer ou des modifications à opérer sur le système pour avancer dans l'enquête ou résoudre le problème.

À l'issue de chaque exercice, une fiche de synthèse présente les concepts abordés lors de celui-ci. Les exercices sont réalisés soit en mode hands-on (de type MOB programming par exemple) tous les participants passent à tour de rôle sur une machine qui projette l'exercice, soit en mode interactif ou les participants dictent à l'animateur les commandes à taper.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique.

Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci.

En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués.

Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

EXERCICES PRATIQUES

- Exercice 1 “Identifier la cause de la défaillance d'une applications web déployée sur une machine” (système, web, application)
- Exercice 2 “Comprendre différents cas de certificats X509 invalides” (système, sécurité)
- Exercice 3 “Découvrir et exploiter des mauvaises configuration de sécurité pour prendre le contrôle d'une machine” (système, sécurité)
- Exercice 4 “Comprendre une architecture web complexe et réparer plusieurs problèmes de configuration” (système, Web, application)
- Exercice 5 “Identifier pourquoi une adresse IP ne répond pas le contenu attendu” (système)
- Exercice 6 “Comprendre et réparer une mise à jour de paquets qui ne fonctionne pas” (système, paquets et dépendances) - exercice en option

RETOUR D'EXPÉRIENCE

CLÔTURE DE LA JOURNÉE

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com