Formation « Sécurité des Architectures »

Réf : SECUARCH

Vous vous demandez pourquoi ne pas laisser votre infrastructure reposer sur un réseau à plat ? Vous désirez migrer votre architecture dans le cloud ? Vous cherchez comment déployer une infrastructure de supervision de manière propre ? Répondez à ces questions et bien d'autres en (ré)apprenant les composants de base d'une architecture réseau complexe, les risques associés aux mises en œuvre courantes et le déploiement de certaines architectures spécifiques. Découvrez les moyens de réduire ces risques ainsi que les points d'attention à prendre en compte lors de chaque décision d'évolution de votre architecture.

Objectifs

- Connaître les problématiques liées à l'architecture des réseaux complexes
- Connaître les solutions associées
- Savoir auditer une architecture
- Développer un plan d'évolution sécurisée d'une architecture

Durée & horaires

- 5 jours soit 35 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Architectes réseaux
- Administrateurs systèmes et réseaux
- Consultants en sécurité
- Auditeurs en sécurité
- RSSI

Pré-requis

- Bonnes connaissances en informatique et connaissances de base en sécurité, par exemple une certification SECUCYBER d'HS2 ou GSEC de GIAC ou CISSP d'(ISC)2 ou équivalent.
- Très bonnes connaissances en réseaux (VLAN, pare-feux, etc), par exemple une certification CCNA+CCNP de Cisco ou NSE4 de Forninet ou CCSA de Checkpoint ou CSNA de Stormshield ou équivalent.

Méthode pédagogique

- Cours magistral
- Démonstrations
- Exercices de mise en œuvre

Supports

- Support de cours en français au format papier en présentiel et au format numérique en distanciel
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**
- **Evaluation de pré-formation envoyée avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUARCH par HS2.**

Programme

Introduction générale

- Logistique
- Tour de table
- Objectifs de la formation
- Non-objectifs de la formation
- Signalétique

Introduction de la formation

- Principes d'architecture
  - Exposition
  - Connectivité
  - Attractivité
- Vocabulaire
  - Segmentation / risque / persona
- Lien avec d'autres domaines
  - Administration
  - Urbanisation
  - Gestion des risques
- Dessine-moi un schéma d'architecture

Notions de réseaux

- Modèles théoriques
- Quiz introductif
- Couche 2 - Liaison
  - Domaine de collision / domaine de diffusion
  - Composants de base et adressage
  - Segmentation - LAN / VLAN / PVLAN
  - Sécuriser le lien local
- Couche 3 - Réseau
  - Composants de base et adressage
  - Segmentation
- Échanges d'informations
- Composants spécifiques
  - Diode / WDM / sonde

Flux

- Filtrage
- Modes de connexion
- Chiffrement
- Authentification

Architecture de base : risques, points d'attention, contraintes et solutions

- Notion de bulle et niveaux : tiers-{0,2}
- Séparation des environnements
  - Production vs. hors-production
- Authentification et autorisation
- Administration
  - Zones d'administration
  - Spécificités de Windows et Active
  - Postes d'administration
- Composants d'infrastructure et de sécurité
  - Services d'infrastructure
  - Cas pratiques : DNS / supervision / sauvegarde / accès Internet / VPN
- Applications, 2-tiers / 3-tiers
- Continuité
  - Redondance et haute disponibilité
  - Dépendance circulaire

Architectures spécifiques

- Virtualisation de l'infrastructure
- Cloud
- Sous-traitants

- Architectures industrielles & SCADA
- Gestion technique des bâtiments
- Divers
  - ToIP / Wi-Fi / Grid / virtualisation et infrastructures "agiles" / IoT