Offres Sécurité Azure

Azure, en tant que plateforme Cloud leader, est au cœur de nombreuses opérations stratégiques pour les entreprises, stockant des données sensibles et propulsant des applications cruciales. La sécurité dans Azure revêt une importance critique, non seulement pour protéger les données contre les menaces persistantes, mais aussi pour assurer la conformité réglementaire dans un paysage en constante évolution. La confiance des utilisateurs, la protection de la propriété intellectuelle et la continuité des opérations dépendent directement de la robustesse des mesures de sécurité mises en place sur la plateforme Azure.

Sur ce besoin, Blue Soft Empower propose plusieurs approches allant de l'audit jusqu'à la remédiation afin de garantir une infrastructure initialement sûre. Nous proposons également la mise en œuvre des outils afin de maintenir un niveau élevé de sécurité tout au long de l'utilisation d'Azure, de renforcer la posture de sécurité et de garantir une réaction rapide face aux incidents.

Scénario 1 : Présentation de la sécurité et Audit du Tenant

Temps estimé ± 5j

Comprendre les enjeux de la sécurité dans Azure
Assurer une présentation détaillée de la sécurité
Evaluer la configuration initiale du tenant Azure
Identifier les éventuels points de faiblesse et les zones nécessitant une attention immédiate.
Définir une road map dans le contexte IT

- 1 atelier de présentation des principes de la sécurité et des best practices par segment (identité, accès …)
- 2 ateliers de présentation technologique (ID Protection, Accès conditionnel, PIM, Azure Defender for cloud)
- 2 ateliers de définition d'une road map dans le contexte client
- 1 document PPT de synthèse (restitution)

Scénario 2 : Audit Azure et remédiation des quick Win

Temps estimé ± 24j

Réaliser un audit pour détecter les vulnérabilités et les lacunes potentielles dans la sécurité de l'environnement Azure.
Mettre l'accent sur l'identification des Quick Wins, des solutions rapides et efficaces pour améliorer la sécurité sans perturber les opérations.
Développer des plans de remédiation rapides et spécifiques garantissant ainsi une amélioration continue de la posture de sécurité.

- 1 atelier de présentation de l'existant
- 2 ou 3 ateliers de revue des
- 1 ou 2 ateliers de définition des attendus (spécifications)
- Mise en œuvre de la Sécurité sur l'environnement Azure
- 1 document de spécification
- 1 document d'exploitation
- 1 transfert de connaissances formalisé

Scénario 3 : Mise en œuvre Log Analytics et Sentinel

Temps estimé ± 10j

Mettre en place Log Analytics pour centraliser les journaux d'activité et les événements de l'environnement Azure, offrant une vue unifiée pour une surveillance efficace.
Exploiter les fonctionnalités avancées de Sentinel pour une détection proactive des menaces,
Configurer des flux automatisés pour une réponse rapide et efficace aux incidents de sécurité, réduisant ainsi le temps de réaction face aux menaces potentielles.

- 1 atelier de présentation de Sentinel et d'état des lieux des fonctionnalités à surveiller (connecteurs)
- 1 atelier de mise en œuvre de l'outil dans Azure (déploiement + gestion des contenus)
- 1 atelier de présentation détaillée des fonctionnalités (configuration + Run, alertes, hunting, investigation...etc)
- 1 document de compte-rendu de l'implémentation et 1 document d'exploitation (utilisation de l'outil)

Comprendre les enjeux de la sécurité cloud afin d'appréhender les menaces

Bien commencer dans Azure en suivant les bonnes pratiques (CAF : Cloud adoption Framework)

Pouvoir suivre et améliorer sa sécurité dans le temps (WAF : Well-Architected Framework)

Maitriser et comprendre la gestion des coûts de la sécurité dans Azure (FinOps et Cost management)