Bouvier Evan 2B1

Rapport de Projet – Preuve de Concept Sécurité Cloud pour SBS Software

Introduction

Ce rapport présente la conception, la mise en œuvre et l'analyse d'un environnement cloud sécurisé sur Microsoft Azure, réalisé dans le cadre de ma formation en informatique et en préparation de mon alternance chez SBS Software. L'objectif est de démontrer, à travers un **proof of concept (PoC)**, la pertinence des technologies de sécurisation cloud (Bastion, Qualys, Windows Server 2022, Ubuntu) pour répondre aux besoins d'une entreprise du secteur bancaire/financier. Ce PoC est la suite de la démarche de veille technologique, en lien direct avec les missions qui me seront confiées chez SBS Software.

1. Présentation de SBS Software et des missions en entreprise

SBS Software est une entreprise spécialisée dans l'édition de solutions logicielles pour le secteur bancaire et financier. Elle intervient sur des problématiques de sécurité, de conformité réglementaire (ISO 27001, RGPD), de gestion des accès et de supervision des infrastructures critiques. Les missions typiques en entreprise incluent :

- Déploiement et administration d'environnements serveurs Windows/Linux
- Sécurisation des accès distants (Bastion, VPN, segmentation réseau)
- Surveillance et gestion des vulnérabilités (outils comme Qualys, SIEM)
- Documentation technique et reporting sécurité

Ce PoC vise à reproduire un environnement similaire à celui de SBS, afin de mieux comprendre les enjeux et d'être opérationnel dès le début de l'alternance.

2. Cahier des charges et architecture du PoC

2.1 Objectifs

- Déployer un réseau Azure segmenté, avec plusieurs VMs Windows et Linux
- Sécuriser les accès via Azure Bastion (aucune IP publique directe)
- Mettre en place un audit de vulnérabilités avec Qualys Community Edition
- Documenter précisément chaque étape (schémas, procédures, retours d'expérience)

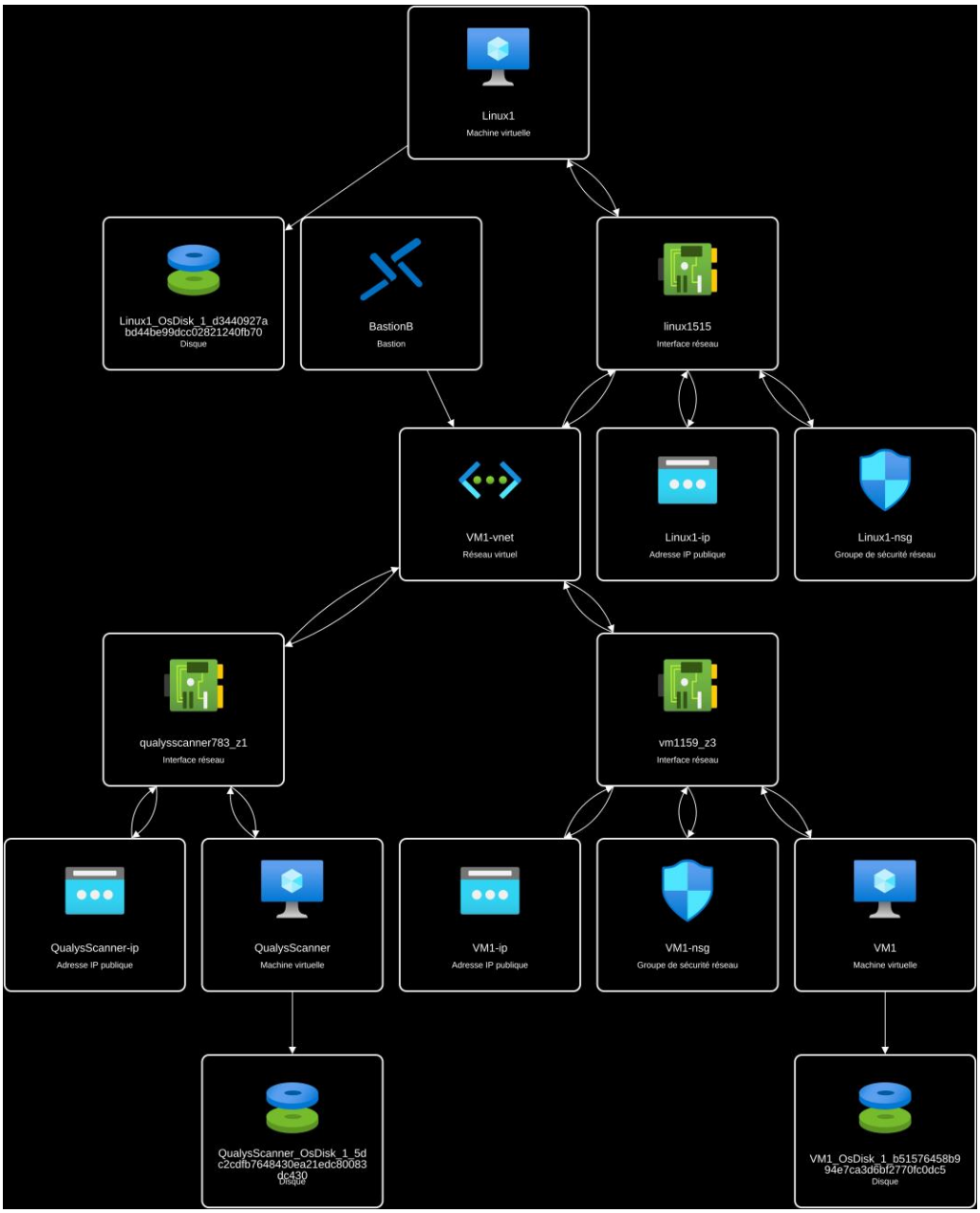
2.2 Spécifications des VMs

VM	OS	CPU	RAM	Rôle
LinuxExterne	Ubuntu 22.04	2	4Go	Machine exposée
WindowsExterne	Windows Server 22	2	4Go	Serveur exposé
LinuxVM	Ubuntu 22.04	1	1Go	Machine interne
WindowsServ	Windows Server 22	1	1Go	Serveur interne
Bastion	Azure Bastion	-	-	Saut sécurisé

2.3 Schéma d'architecture

- **Schéma 1** : Vue globale du réseau Azure (VNet, sous-réseaux, Bastion, VMs)

Bouvier Evan 2B1



3. Documentation technique

3.1 Déploiement des VMs et du Bastion

- Procédure pas à pas pour la création des VMs (choix des tailles, images, disques)
- Création du Bastion dans le sous-réseau dédié (`AzureBastionSubnet`)
- Association des VMs au Bastion pour accès sécurisé (RDP/SSH via portail Azure)

- Configuration des NSG : seuls les flux nécessaires sont autorisés (RDP/SSH depuis Bastion, blocage total des autres ports)

3.2 Configuration réseau (NSG, routage)

- Détail des règles NSG appliquées à chaque sous-réseau/VM
- Justification des choix (principe du moindre privilège, Zero Trust)
- Vérification de l'isolation réseau (tests de connectivité, ping, nmap)

3.3 Sécurité native des OS

- **Windows Server 2022** (rôle : serveurs applicatifs ou AD) : Secure Boot, Credential Guard, mises à jour automatiques, gestion des rôles et stratégies de groupe
- **Ubuntu 22.04** (rôle : serveurs web ou applicatifs) : durcissement SSH, gestion des utilisateurs, mises à jour régulières, logs centralisés

4. Mise en œuvre de l'audit de vulnérabilités avec Qualys

4.1 Déploiement et paramétrage

- Création d'un compte Qualys Community Edition
- Ajout des IP publiques des VMs exposées dans Qualys
- Lancement de scans externes (impossible d'installer les agents sur les VMs, limitation majeure)

4.2 Limites rencontrées

- **Impossibilité d'installer les agents Qualys** sur les VMs (droits, version Community, absence d'UI graphique sur Linux, restrictions sur Windows)
- **Conséquence** : seuls les services exposés sur Internet sont audités, aucune visibilité sur les vulnérabilités internes, les patchs manquants ou les mauvaises configurations système
- **Interprétation** : le rapport de scan est incomplet, mais reflète la réalité d'un attaquant externe ou d'un audit de conformité de surface

5. Analyse et interprétation des résultats du scan

5.1 Résumé des résultats

- **1 seul host détecté comme vivant** (LinuxExterne)
- **3 hosts non scannés** (protection efficace par Bastion/NSG, ou absence d'IP publique)

5.2 Vulnérabilités détectées sur LinuxExterne

- **SHA1 deprecated setting for SSH** : algorithme cryptographique obsolète, à désactiver
- **OpenSSH Expected Behavior Violation (CVE-2025-32728)** : version vulnérable, nécessite une mise à jour
- **Remote Access Service Detected** : SSH accessible publiquement, à restreindre

5.3 Interprétation

- **Points positifs** : la segmentation réseau et le Bastion protègent efficacement les VMs internes (aucune surface d'attaque détectée)
- **Points à améliorer** : la VM exposée présente des failles classiques (SSH, version, configuration), typiques d'un déploiement non durci
- **Limite** : sans agent, impossible de vérifier la sécurité interne (patchs, comptes, services non exposés)

5.4 Exemples précis

- **Exemple 1** : SSH sur LinuxExterne détecté avec support SHA1 → action : modifier `/etc/ssh/sshd_config` pour n'autoriser que SHA2
- **Exemple 2** : OpenSSH version 9.6p1 vulnérable → action : mise à jour via `apt update && apt upgrade`
- **Exemple 3** : SSH accessible publiquement → action : restreindre l'accès SSH à l'IP du Bastion ou à un sous-réseau d'admin

6. Gestion de la vulnérabilité et plan d'action

- **Fréquence des scans** : recommander un scan externe hebdomadaire, scan interne mensuel (si agents ou appliance disponibles)
- **Rapport** : chaque scan doit générer un rapport PDF/CSV, analysé et archivé
- **Plan d'action** : corriger les failles critiques (mise à jour SSH, restriction accès), documenter les actions, vérifier la correction lors du scan suivant

- **Lien avec le secteur bancaire** : cette démarche est conforme aux exigences de l'ISO 27001 et des audits internes/externe du secteur financier

7. Conclusion et pertinence du PoC

Ce PoC démontre la faisabilité et la pertinence d'une architecture cloud sécurisée, inspirée des pratiques de SBS Software : segmentation réseau, Bastion pour l'accès sécurisé, audit de vulnérabilités avec Qualys. Malgré les limitations (pas d'agent, scan incomplet), il met en lumière l'importance de la configuration réseau et du durcissement des services exposés. Ce travail me permet d'acquérir des compétences directement transférables pour mon alternance chez SBS, et de mieux comprendre les enjeux de sécurité dans le secteur bancaire.