Rapport de stageBTS SIO option SISR 1er année

VINCI CONSTRUCTION

Samuel GOMES DOS SANTOS

16 oct. 2024

TABLE DES MATIÈRES

Introduction

Dans le cadre de ma première année de BTS SIO, option SISR (Solutions d'Infrastructure, Systèmes et Réseaux), j'ai réalisé un stage d'une durée de [durée du stage] au sein de l'entreprise [Nom de l'entreprise]. Ce stage avait pour objectif de me familiariser avec la gestion des infrastructures réseaux, la sécurité des systèmes d'information, ainsi que les processus de résolution d'incidents techniques.

J'ai été amené à travailler sur différents aspects liés aux réseaux et à la sécurité, notamment via la gestion des firewalls Fortinet, la configuration de bornes wifi et l'utilisation de divers outils professionnels comme Postman et PuTTY. Le stage a été particulièrement enrichissant grâce à la variété des missions confiées et aux problèmes concrets que j'ai eu à résoudre.

Semaine 1 : Prise en main des outils et découverte des projets

Problématique :

Lors de cette première semaine, deux des trois ordinateurs mis à ma disposition ont rencontré des dysfonctionnements, nécessitant plusieurs remplacements. Cela a retardé le démarrage de mes tâches.

Journées 1 à 4 :

Durant les quatre premiers jours, j'ai assisté à la présentation des projets en cours. En raison des restrictions imposées par la pandémie de COVID-19, l'entreprise a renforcé ses initiatives pour migrer certaines de ses ressources sur le cloud, notamment ses infrastructures de sécurité réseau.
L'objectif principal était de gérer les firewalls Fortinet déployés sur différents sites de l'entreprise via deux plateformes : FortiManager et FortiCloud. Ma première mission consistait à recenser les firewalls présents sur ces deux plateformes et identifier ceux qui n'étaient répertoriés que sur l'un des deux systèmes. Ce travail a permis de centraliser la gestion de ces équipements critiques pour la sécurité des sites distants.

En parallèle de cette mission, j'ai été impliqué dans la résolution de tickets techniques tels que :

- Problèmes d'accès à Internet sur différents sites : les causes identifiées incluaient la saturation du serveur DHCP, une route incorrecte ou un tunnel VPN défaillant.
- Problèmes de borne wifi ne fonctionnant plus, nécessitant des reconfigurations et vérifications des équipements.

Journée 5 :

Suite à l'analyse des firewalls, on m'a présenté la manière dont ces équipements sont nommés et classés au sein de l'entreprise. Mon rôle était de regrouper ces équipements par régions à travers une API, avec l'outil Postman. Cependant, cette tâche a représenté une véritable difficulté. J'ai passé la journée à me former à l'utilisation de Postman en consultant des documentations et des vidéos, mais malgré mes efforts, je n'ai pas réussi à accomplir la mission à l'aide de cet outil.

Semaine 2 : Développement des compétences et gestion des incidents

À partir de cette semaine, en plus des tâches principales qui m'étaient assignées, j'ai continué à résoudre les tickets d'incidents techniques de manière quotidienne.

Journées 1 et 2 :

Face à la complexité de Postman, j'ai finalement opté pour une gestion manuelle des firewalls sur FortiManager et FortiCloud. Cette approche était plus laborieuse, mais elle m'a permis d'acquérir une meilleure compréhension de la structure des firewalls et des politiques de sécurité en place.

Journées 3 et 4 :

J’ai consacré ces journées à la lecture de la documentation technique sur la mise en place des firewalls, notamment sur les technologies MPLS, Double Internet, et SD-WAN. Cette étape était cruciale pour comprendre la manière dont les firewalls sont déployés et gérés dans un environnement multi-sites.
De plus, j'ai participé à des réunions concernant la synchronisation des règles de sécurité à travers les firewalls.

Journée 5 :

Cette journée a été dédiée à la préparation des mises à jour de certains firewalls encore sous d’anciennes versions. Une vérification a également été effectuée pour détecter des incidents liés à l'installation du protocole BGP (Border Gateway Protocol) sur certains équipements Fortinet.

Semaine 3 : Mises à jour des firewalls et approfondissement technique

Journées 1 à 3 :

Le début de cette semaine a été similaire à la précédente, avec des vérifications approfondies des versions de firmware des firewalls et la préparation de leur mise à jour. J’ai également contribué à la résolution des tickets d’incidents, notamment liés à la connectivité et à la configuration des BGP.

Journée 4 :

J’ai effectué des configurations spécifiques de firewalls. Cette tâche m’a permis de mieux comprendre les paramètres de sécurité à définir, ainsi que les processus d’automatisation disponibles pour la gestion à distance des équipements.

Journée 5 :

Ce jour-là a été plus calme en termes de résolution d'incidents, avec uniquement des tickets habituels à traiter. Cela m’a donné l’opportunité de me concentrer davantage sur l'optimisation de la configuration des firewalls.

Semaine 4 : Gestion des incidents critiques et exploration de nouveaux outils

Journée 1 :

Cette journée a été marquée par un incident majeur : la panne du datacenter pendant la nuit précédente. Ce problème a engendré une vague de tickets d’incidents liés aux connexions réseau défaillantes. J’ai été chargé de les traiter en priorité.

Journée 2 :

Le matin, j'ai continué de travailler sur les tickets restants en lien avec la panne du datacenter. L'après-midi, j’ai appris à utiliser PuTTY, un client SSH, pour accéder aux firewalls Fortinet à distance. Cet apprentissage a été crucial pour m'aider à diagnostiquer les problèmes de configuration des équipements et effectuer des réinitialisations.

Journée 3 :

Après avoir terminé de résoudre les tickets en attente, j’ai commencé à explorer la technologie VoIP et son interaction avec les réseaux. J'ai également recensé les firewalls SD-WAN rencontrant des problèmes de connectivité pour les signaler au responsable de secteur.

Journée 4 :

La journée a été dédiée à la réinitialisation et à la reconfiguration de certains firewalls ayant rencontré des défaillances. J'ai approfondi l'utilisation de PuTTY pour effectuer ces configurations à distance.

Journée 5 :

La dernière journée de cette semaine a consisté à finaliser la configuration des firewalls et à résoudre un ticket lié à une borne wifi qui ne parvenait pas à remonter sur le contrôleur Cisco, malgré sa visibilité sur le DHCP. J'ai également communiqué avec mes collègues pour obtenir des informations supplémentaires sur certains firewalls en panne.

Semaine 5 : Finalisation et gestion des incidents

Journée 1 :

Finalisation des mises à jour de firmware sur plusieurs firewalls Fortinet. J'ai également résolu des tickets concernant des problèmes de connexion VPN pour des utilisateurs distants, en ajustant les configurations d'accès à distance.

Journée 2 :

Participation à une réunion technique sur l'optimisation des firewalls SD-WAN. J'ai ensuite utilisé PRTG pour surveiller les performances réseau et travaillé sur des scripts d'automatisation pour simplifier certaines tâches répétitives.

Journée 3 :

Réinitialisation d'un firewall défectueux sur un site distant, suivi de tests de connexion

pour rétablir l’accès réseau. J'ai aussi contribué à l’audit de sécurité en identifiant des équipements avec des configurations obsolètes.

Journée 4 :

Rédaction de la documentation des configurations et des procédures mises en place. J’ai également réalisé des tests de sécurité basiques pour m’assurer de la conformité des nouveaux réglages.

Journée 5 :

Finalisation des projets en cours, vérification des mises à jour des firewalls, et rédaction d'un rapport d'audit réseau avec des recommandations. Résolution des derniers tickets avant la fin du stage.