BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2022**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR) - Coefficient 4

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

N° réalisation : 1

Nom, prénom : RUGGERI Jamy

N° candidat :

Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒ **Date :** 10 / 05 /2023

Contexte de la réalisation professionnelle

Une entreprise de taille moyenne spécialisé dans la production de cosmétique gère actuellement une grande quantité machines, de serveurs et d'autres équipements informatiques pour gérer son activité constante. Elle fait appel à nos services pour intégrer un outil de gestion d'incidents de sécurité et d'un outil d'analyse de vulnérabilités à son environnement informatique existant. L'objectif est d'améliorer la visibilité de l'infrastructure informatique, d'optimiser les opérations informatiques et de minimiser au maximum les vulnérabilités présentes.

Intitulé de la réalisation professionnelle

Conception et mise en place d'un système de surveillance et de protection de la sécurité informatique à l'aide d'un logiciel de gestion d'incidents de sécurité et d'un outil d'analyse de vulnérabilités

Période de réalisation : 02/09/2022 - XX/XX/XXXX **Lieu :** Lycée Saint-Exupéry, Saint-Raphaël

Modalité : ☒ Seul(e) ☐ En équipe

Compétences travaillées

- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation (ressources fournies, résultats attendus)

Ressources fournies :

- Schématisation et architecture de l'infrastructure réseau comprenant et la liste des équipements et logiciels requis.
- Documents informatifs, techniques et analyse de situation
- Fichiers de configuration
- Plan d'adressage réseau
- Cahier des charges indiquant les objectifs à atteindre et réaliser

Résultats attendus :

- Mise en œuvre concrète et fonctionnelle des solutions incorporées au réseau concernant la gestion d'incidents de sécurité et l'analyse de vulnérabilités.
- Tests de mise en service et de fonctionnement de l'outil de supervision et d'automatisation.
- Cahier des charges complété et respecté, rapport et protocole de tests, analyse et simulation de mise en situation une fois déployée.

Description des ressources documentaires, matérielles et logicielles utilisées

Matériels et logiciels spécifiques à la réalisation de ce projet :

- Une ou des machines virtuelles avec une capacité de stockage suffisante pour les données collectées et les logs générés.
- Une connexion réseau stable et fiable pour accéder au serveur et pour permettre la communication entre les différents outils.
- Un système d'exploitation Linux, comme Ubuntu, Debian ou CentOS, qui sera installé sur le serveur ou la machine virtuelle.
- TheHive : le logiciel de gestion d'incidents de sécurité et Greenbone Vulnerability Manager : l'outil d'analyse de vulnérabilités
- Documentation complète et informative sur les spécificités techniques des outils utilisés, avec comparatif des solutions proposées.
- Schématisation de l'infrastructure informatique concernée par les modifications
- Guides d'utilisations des outils fournis aux personnes manipulant les logiciels.

Modalités d'accès aux productions et à leur documentation

https://jamy-ruggeri.fr/realisation-professionnelle/

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2022**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR) - Coefficient 4

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

1./ Demande de l'entreprise

Au sein de l'entreprise, nous avons été chargé de concevoir et de mettre en place un système sécuriser associant la gestion d'incidents de sécurité et l'analyse de vulnérabilités pour améliorer la sécurité de l'infrastructure informatique. Cette réalisation avait pour objectif dans un but final de réduire les failles de sécurité et ainsi de réduire les temps d'arrêt et de faciliter la gestion de la cybersécurité.

Dans le cadre de cette mission, nous avons collaboré avec l'équipe technique pour identifier les besoins spécifiques de l'entreprise en matière de sécurisation. Elle rencontre des difficultés dans la gestion de son infrastructure informatique et aimerait améliorer son efficacité opérationnelle. Nous avons ensuite choisi les outils appropriés pour répondre à ces besoins, en nous assurant que les outils étaient compatibles avec l'environnement de l'entreprise et pouvaient être intégrés à l'infrastructure existante.

La schématisation de l'infrastructure est répertorié à l'adresse suivante : https://jamy-ruggeri.fr/realisation-professionnelle/

2./ Outils et solutions envisageables

Pour répondre aux besoins d'affaires de l'entreprise, trois solutions sont disponibles pour chacun des outils et ont été envisagées.

Gestion d'incidents de sécurité :

TheHive / Splunk / QRadar

Vulnérabilité:

GreenBone / Nessus / Metasploit

Un tableaux comparatif ainsi qu'un graphe analytique des outils sont disponible à l'adresse suivante :
https://jamy-ruggeri.fr/realisation-professionnelle/

3./ Outil retenu

Afin de répondre au mieux aux exigences de l'entreprise et de la meilleure façon possible pour la gestion future de ce dernier, les solutions suivantes ont été réservées : **TheHive** / **GreenBone**

Efficace, permettant de regrouper plusieurs avantages face à ses concurrents :

- Automatisation : Ouverture de tickets, l'envoi d'e-mails, l'exécution de scripts, etc.
- Fonctionnalités avancées : Détection automatique de doublons, l'analyse de similarité, la corrélation de données, la visualisation de données, la création de tableaux de bord, la génération de rapports, etc.
- Complet : Scanner OpenVAS, le gestionnaire de vulnérabilités Greenbone Security Assistant (GSA), le gestionnaire de tâches Greenbone Vulnerability Manager (GVM)**.**
- Automatisation : Planification de scans, la configuration de politiques de sécurité, la gestion de tâches, etc.
- Rapports détaillés : Rapports détaillés sur les vulnérabilités détectées, des recommandations de correction, des références CVE, et des informations sur la criticité de la vulnérabilité.

4./ Mise en place de l'outil

Le déploiement comprend l'installation du logiciel de gestion d'incidents de sécurité puis par la suite d'analyse de vulnérabilités.

Les étapes ci-dessous sont requises pour finaliser l'intégration de l'outil :

- *1ère étape :* Sélection de la ou les plateformes où seront installés TheHive et GreenBone
- *2ème étape :* Installer les prérequis matériels et logiciels
- *3ème étape :* Télécharger, installer et configurer GreenBone
- *4ème étape :* Installation et configuration du logiciel TheHive
- *5ème étape* : Effectuer des tests pour assurer que l'intégration fonctionne correctement.
- *6ème étape :* S'assurer de surveiller régulièrement l'intégration pour que les alertes et les actions fonctionnent correctement.

5./ Conclusion

Nous avons assuré la formation de l'équipe technique sur l'utilisation du système de gestion d'incidents de sécurité et d'analyse de vulnérabilités, en fournissant des guides et des procédures pour garantir une utilisation efficace et efficiente.

Grâce à cette réalisation, l'entreprise a bénéficié d'une infrastructure informatique plus fiable, plus performante et plus facile à gérer, avec une réduction significative des temps d'arrêt et des failles. En fin de compte, ces outils réseau puissant et personnalisable peuvent aider l'entreprise à maintenir la disponibilité et/ou prévenir en cas d'attaques de leur infrastructure réseau, tout en améliorant les compétences de leurs équipes informatiques.