Nom de naissance - *Panabieres*
Nom d'usage - *Panabieres*
Prénom - *Vincent*
Adresse - *588 chemin du clos de bouichard, 04180 villeneuve*

Titre professionnel visé

Administrateur d'infrastructures sécurisées

MODALITÉ D'ACCÈS :

☒ Parcours de formation
☐ Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel. **Ce titre est délivré par le Ministère chargé de l'emploi.**

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen**.

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.

Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.

2. du **Dossier Professionnel** (DP) dans lequel le candidat a consigné les preuves de sa pratique professionnelle.

3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation

4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- une déclaration sur l'honneur à compléter et à signer ;
- des documents illustrant la pratique professionnelle du candidat (facultatif)
- des annexes, si nécessaire.

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.

Sommaire

Exemples de pratique professionnelle

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n°1 ▸ Appliquer les bonnes pratiques dans l'administration des infrastructures

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de mon alternance au sein de l'entreprise Optimalsi, j'ai constaté, avec mon tuteur, que tous les postes de travail fonctionnaient en mode local, sans rattachement au domaine Active Directory de l'entreprise.

Cette situation posait plusieurs problèmes :

- Pas de gestion centralisée des comptes utilisateurs
- Impossible de déployer des GPO afin de gérer au mieux le parc informatique
- Aucune traçabilité ni contrôle d'accès
- Difficulté de déploiement des mises à jour et des logiciels

Objectif de l'action :

- Intégrer les postes locaux au domaine afin de permettre une gestion centralisée.
- Appliquer les bonnes pratiques d'administration en matière de sécurité, d'uniformité et de contrôle.
- Renforcer la sécurité et la cohérence de l'environnement informatique.

Tâches réalisées :

1. Recensement des postes concernés (10 postes non intégrés sur site).
2. Vérification de la connectivité réseau entre les postes et le contrôleur de domaine.
3. Sauvegarde des données utilisateurs locales avant migration (Documents, Bureau, etc.).
4. Création ou vérification des comptes utilisateurs dans l'AD.
5. Ajout des postes au domaine via l'interface système (Propriétés système > Modifier > Domaine).
6. Application des GPO standard de l'entreprise (mot de passe, antivirus, mises à jour…).

7. Tests d'accès, de session et de montée des droits.

8. Mise à jour de l'inventaire matériel et documentation de la procédure.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Les ordinateurs de l'entreprise avec une connexion internet.

Un accès au serveur active directory

3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai travaillé seul.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMALSI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécuritsées*

Période d'exercice ▸ Du : *09/10/2023* au : *01/09/2025*

5. Informations complémentaires *(facultatif)*

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n° 2 ▸ Administrer et sécuriser une infrastructure réseaux.

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Lors de mon alternance au sein de l'entreprise OPTIMALSI, les imprimantes réseau étaient connectées au même VLAN que les postes utilisateurs. Cette configuration posait plusieurs problèmes :

- Manque de segmentation du trafic
- Risques de sécurité en cas d'exploitation d'une faille sur une imprimante
- Difficultés à gérer les flux réseau et à identifier les équipements imprimantes dans les logs ou la supervision

Objectif de l’action :

- Créer un VLAN spécifique pour les imprimantes afin de mieux segmenter le réseau
- Isoler les imprimantes du reste du réseau utilisateur tout en maintenant l’accessibilité
- Améliorer la sécurité et la gestion des équipements réseau via une meilleure organisation

---

Tâches réalisées :

1. Recensement de toutes les imprimantes réseau et de leurs adresses IP actuelles.
2. Étude du plan d’adressage IP existant pour proposer une nouvelle plage dédiée
3. Création d’un VLAN imprimantes sur le pare-feu FortiGate :
    - Définition de l’interface VLAN
    - Attribution d’un ID VLAN unique
    - Configuration de la passerelle pour ce VLAN
4. Mise à jour de la configuration réseau des switchs si nécessaire (trunk/tagging).
5. Déplacement progressif des imprimantes vers le nouveau VLAN (changement d’adresse IP, configuration DHCP statique ou fixe).
6. Mise en place de règles de pare-feu FortiGate :
    - Autoriser uniquement les flux nécessaires (impressions depuis les VLAN utilisateurs)
    - Bloquer l’accès inverse (utilisateurs ne pouvant pas être attaqués depuis les imprimantes)
7. Tsts de connectivité et d’impression depuis différents postes utilisateurs.

8. Documentation de la configuration (schéma, liste des imprimantes, règles de firewall).

:

2. Précisez les moyens utilisés :

Un ordinateur avec une connexion internet.

Un accès au fortigate centralisé qui gère tous les VLAN

3. Avec qui avez-vous travaillé ?

j'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *09/05/2022* au : *13/05/2022*

5. Informations complémentaires *(facultatif)*

Activité-type 1 — Administrer et sécuriser les infrastructures

Exemple n° 3 ▸ Administrer et sécuriser les infrastructures systèmes

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Durant mon alternance chez OPTIMALSI, la direction souhaitait renforcer la sécurité des postes utilisateurs. Certains postes n'étaient pas protégés, et aucune console de gestion centralisée n'était en place, rendant le suivi difficile en cas de menace.

Objectif de l'action :

- Déployer l'antivirus ESET sur l'ensemble des postes de travail.
- Configurer une console d'administration centralisée pour surveiller l'état de protection.
- Mettre en place une politique de sécurité uniforme sur tous les postes.

Tâches réalisées :

1. Évaluation du parc informatique pour identifier les postes non protégés.
2. Téléchargement et installation de la console ESET Protect sur un serveur dédié.
3. Création de groupes dynamiques dans la console (par site ou service).
4. Déploiement à distance de l'agent ESET sur tous les postes via la console.
5. Définition et application de politiques de sécurité :
    - Analyse automatique des périphériques USB
    - Scan planifié chaque semaine
    - Blocage des sites web dangereux
6. Configuration d'alertes et de rapports automatiques :
    - Alertes en cas de détection de menace ou de poste non à jour
    - Rapport hebdomadaire envoyé par e-mail

7. Tests de détection avec fichiers inoffensifs de test EICAR.
8. Formation rapide des utilisateurs (bonnes pratiques, lecture des alertes).
9. Documentation complète de la procédure d'installation, de configuration et de gestion.

Résultats obtenus :

- Un envoie d'alerte en temps réel pour chaque incidents
- Suivi en temps réel de l'état de sécurité grâce à la console.
- Réduction des risques liés aux malwares, ransomwares, et clés USB non sécurisées.
- Réactivité accrue du support informatique en cas d'alerte.

2. Précisez les moyens utilisés :

Les postes locaux des utilisateurs

Un accès à la console ESET

3. Avec qui avez-vous travaillé ?

j'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *09/05/2022* au : *13/05/2022*

5. Informations complémentaires *(facultatif)*

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n° 4 - *Administrer et sécuriser les infrastructures virtualisées*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de mon alternance chez OPTIMALSI, l'infrastructure informatique reposait sur une solution de virtualisation Nutanix, utilisant l'hyperviseur AHV (Acropolis Hypervisor).

J'ai été chargé d'effectuer des tâches d'administration courantes et de renforcer la sécurité des machines virtuelles (VM), ainsi que de participer à la gestion de l'environnement Nutanix via Prism (la console de gestion).

Objectif de l'action :

- Gérer et maintenir les machines virtuelles tournant sur la plateforme Nutanix.
- Participer à la sécurisation de l'infrastructure virtualisée.
- Gérer les ressources matérielles (CPU, RAM, stockage) de façon optimisée.

Tâches réalisées :

1. Connexion à la console Nutanix Prism pour superviser l'environnement (statut des VM, alertes, performance).
2. Création et configuration de nouvelles VM (Windows Server, Linux) pour divers usages :
    - Serveur AD secondaire
    - Serveur d'impression
    - Serveur de test
3. Attribution des ressources nécessaires (CPU, RAM, espace disque) selon les besoins.
4. Gestion du réseau virtuel :
    - Association des VM aux bons VLANs (ex : VLAN imprimantes, utilisateurs)
    - Configuration des adresses IP fixes
5. Mise en place de snapshots avant chaque modification majeure ou mise à jour système.
6. Vérification de la haute disponibilité (HA) : test de bascule, tolérance aux pannes.
7. Planification et vérification des sauvegardes via le système intégré ou un outil externe (comme Veeam.)
8. Surveillance de l'état de santé de la plateforme (disques, RAM, CPU, alertes).
9. Application des mises à jour (patchs Nutanix ou OS des VM).
10. Documentation des procédures et des configurations (VM, VLAN, snapshots, accès, etc.).

Résultats obtenus :

- L'environnement Nutanix est stable, sécurisé et optimisé.

- Les VM critiques sont régulièrement sauvegardées et surveillées.
- Les modifications sont maîtrisées grâce aux snapshots.
- Le réseau virtuel est segmenté proprement, ce qui renforce la sécurité.

Grâce à cette mission, j'ai pu travailler dans un environnement de virtualisation professionnel avancé. J'ai appris à administrer des VM, à gérer les ressources et à sécuriser les services virtualisés via Nutanix Prism. J'ai également renforcé ma rigueur dans la documentation et le suivi des configurations.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

Un accès à PRISM CENTRAL DE NUTANIX

3. Avec qui avez-vous travaillé ?

Sur ce projet j'ai travaillé seul.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022*

5. Informations complémentaires *(facultatif)*

Activité-type 2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

Exemple n° 1 *Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

L'entreprise OPTIMALSI ne disposait pas de solution centralisée pour la protection antivirus de ses postes. Certains étaient protégés, d'autres non, et aucune politique globale de sécurité n'était appliquée.

Suite à une réunion avec le responsable informatique, un besoin a été exprimé : mettre en place une solution de sécurité globale, centralisée, homogène et facile à administrer.

Objectif de l'action :

- Étudier les différentes solutions antivirus centralisées disponibles.
- Proposer une solution adaptée aux besoins techniques et financiers de l'entreprise.

- Concevoir un plan de déploiement et d'administration.
- Accompagner la mise en œuvre de cette nouvelle solution.

Tâches réalisées :

1. Recueil des besoins : nombre de postes, type d'utilisation, contraintes réseau, budget, compatibilité.
2. Comparatif de plusieurs solutions : Windows Defender, Kaspersky, Bitdefender, ESET.
3. Choix de la solution ESET Protect, car :
    - Interface claire et en français
    - Bon rapport qualité/prix
    - Console d'administration centralisée
    - Contact auprès du fournisseur ESET France
4. Conception de la solution :
    - Architecture prévue (serveur ESET + agents déployés)
    - Méthode de déploiement (à distance via la console, GPO, ou manuel)
    - Répartition des rôles (gestion, alertes, supervision)
5. Validation de la solution avec le responsable informatique
6. Rédaction d'une documentation projet (plan de déploiement, sécurité, fiches techniques)
7. Préparation du support aux utilisateurs (communication, procédures)

Résultats obtenus :

- Une solution technique complète a été proposée et validée.
- Le déploiement a été préparé et maîtrisé, limitant l'impact sur les utilisateurs.
- La gestion de la sécurité est désormais centralisée, avec des alertes et des rapports.
- L'entreprise a gagné en sécurité et en visibilité sans investissement matériel lourd.

Cette action m'a permis de répondre à un besoin exprimé par l'entreprise avec une solution adaptée, en analysant les options techniques disponibles, en préparant un plan de déploiement concret, et en accompagnant sa mise en œuvre.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

Une réunions avec les responsables informatique de l'entreprise

Microsoft Excel

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022i*

5. Informations complémentaires *(facultatif)*

Activité-type 2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

Exemple n° 2 ▸ *Mettre en production des évolutions de l'infrastructure*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de mon alternance chez OPTIMALSI, plusieurs clients avaient besoin de nouveaux serveurs pour héberger des services comme Active Directory, le partage de fichiers ou l'accès à distance pour leurs utilisateurs.

L'entreprise utilise une infrastructure virtualisée Nutanix AHV, ce qui m'a permis de créer et configurer des VM Windows Server 2022, puis de les mettre en production dans l'environnement client.

Objectif de l'action :

- Déployer des serveurs Windows Server 2022 dans un environnement virtualisé.
- Adapter les configurations en fonction du nombre d'utilisateurs et des besoins.
- Sécuriser l'environnement et le rendre conforme aux normes légales (licences).
- Mettre les serveurs en production de façon stable et sécurisée.

Tâches réalisées :

1. Analyse du besoin client :
    - Type de services attendus : AD, fichiers, application métier, accès à distance
    - Nombre d'utilisateurs et intensité d'usage estimée
2. Dimensionnement des ressources :
    - Attribution de RAM, CPU et disque en fonction des usages prévus
    - Possibilité d'évolution anticipée (scalabilité)
3. Création des VM via Nutanix Prism :
    - Déploiement de l'image ISO Windows Server 2022
    - Configuration réseau (IP fixe, VLAN, DNS…)
4. Installation et sécurisation du système :
    - Mises à jour Windows, pare-feu, stratégie de mot de passe
    - Activation de la licence Windows Server
5. Ajout de rôles nécessaires :
    - Contrôleur de domaine, serveur de fichiers, RDS (Remote Desktop Services)
6. Mise en place d'un antivirus serveur :
    - Achat et déploiement de la licence ESET Server
    - Intégration à la console ESET Protect
7. Configuration de l'accès distant sécurisé :

- Installation et activation des rôles RDS
- Achat et intégration des licences CAL RDS selon le nombre d'utilisateurs distants
- Configuration des sessions distantes, droits d'accès, tests

8. Tests de fonctionnement :
   - Connexions RDP, authentification AD, antivirus actif, partages accessibles
9. Mise en production :
   - Communication avec le client
   - Suivi du bon fonctionnement
10. Documentation complète :
    - Configurations techniques, licences utilisées, procédures d'accès et de sauvegarde

---

Résultats obtenus :

- Les serveurs ont été mis en production avec succès, avec :
  - Une configuration adaptée aux besoins
  - Un environnement sécurisé (ESET, RDP, pare-feu)
  - Des licences conformes (Windows Server, ESET, RDS CAL)
- Les utilisateurs peuvent désormais accéder à distance à leurs environnements de travail
- Le client dispose d'un serveur stable, maintenable et documenté

Cette action m'a permis de gérer une mise en production complète, en tenant compte des aspects techniques, sécuritaires et légaux (licences). J'ai mis en place un serveur Windows Server 2022, sécurisé, accessible à distance, et entièrement intégré dans l'infrastructure réseau du client.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

PRISM NUTANIX

Resources type : CAL RDS, LICENCE WINDOWS SERVER, iso ESET

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022i*

5. Informations complémentaires *(facultatif)*

Activité-type 2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

Exemple n° 3 - *Mettre en œuvre et optimiser la supervision des infrastructures*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de mon alternance chez OPTIMALSI, l'entreprise avait besoin de centraliser la surveillance de ses infrastructures clients, à la fois du point de vue technique (état des serveurs, équipements, services critiques) et de la sécurité (menaces, antivirus, accès distants…).

J'ai été amené à mettre en place et gérer plusieurs solutions de supervision :

- Zabbix pour la supervision réseau et serveur.
- Atera pour le monitoring à distance, la gestion des alertes et le suivi des interventions.
- ESET Protect pour la supervision de la sécurité antivirus.

Objectif de l'action :

- Mettre en œuvre une supervision complète des postes, serveurs, services et équipements.
- Garantir une réactivité immédiate en cas de dysfonctionnement ou d'incident de sécurité.
- Automatiser le suivi, les alertes et les rapports pour chaque infrastructure.

Tâches réalisées :

Zabbix :

1. Installation d'un serveur Zabbix (Linux).
2. Ajout des hôtes à superviser : serveurs, imprimantes, switches.
3. Création de templates personnalisés (CPU, RAM, ping, services AD, etc.).
4. Mise en place de triggers/alertes (ex : CPU > 85 %, service AD arrêté, perte de connexion).
5. Configuration de notifications par mail.

6. Visualisation via tableaux de bord dynamiques.

Atera :

1. Déploiement de l'agent Atera sur les postes et serveurs.
2. Supervision de la santé des machines (RAM, disque, CPU, services actifs).
3. Suivi en temps réel des mises à jour, alertes critiques, tickets techniques.
4. Télémaintenance à distance des clients (RDP/AnyDesk intégré).
5. Gestion centralisée des interventions : historique, prise en main, planification.

ESET Protect :

1. Supervision de la sécurité antivirus (agents actifs, menaces, mises à jour).
2. Gestion et application des politiques de sécurité.
3. Automatisation de rapports de conformité et d'alertes.

Résultats obtenus :

- Supervision technique et sécuritaire centralisée.
- Réduction significative du temps de détection d'un incident.
- Réactivité améliorée grâce aux alertes automatiques et supervision en continu.
- Outils adaptés aux besoins spécifiques : Zabbix pour l'infra, Atera pour les clients, ESET pour la sécurité.
- Traçabilité complète des interventions et anomalies.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

PRISM NUTANIX

Console ESET

PROXY ZABBIX

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022i*

5. Informations complémentaires *(facultatif)*

Exemple n° 1 - *Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure*

Activité-type 3 Participer à la gestion de la cybersécurité

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de mon alternance chez OPTIMALSI, l'équipe souhaitait avoir une vue d'ensemble du niveau de sécurité de l'infrastructure des clients. L'objectif était de vérifier que tous les postes et serveurs étaient bien protégés, à jour, et conformes aux bonnes pratiques de sécurité.

J'ai participé à cette analyse de sécurité, en m'appuyant sur différents outils (ESET Protect, Atera, supervision, Active Directory, etc.).

Objectif de l'action :

- Mesurer l'état de sécurité global : antivirus, mises à jour, comptes utilisateurs, accès distants.
- Identifier les postes ou serveurs non conformes.
- Proposer des améliorations ou actions correctives.
- Participer à la remise en conformité de l'infrastructure.

Tâches réalisées :

Analyse du parc informatique :

1. Audit via la console ESET Protect :
    - Vérification de l'activation des agents antivirus
    - Détection de postes non protégés ou avec des menaces non résolues
2. Contrôle de l'état des mises à jour système :
    - Utilisation d'Atera pour repérer les postes avec des mises à jour critiques en attente
    - Suivi des patchs Windows sur les serveurs
3. Revue des comptes utilisateurs sur AD et postes locaux :

- Vérification de la présence de comptes administrateurs non justifiés
- Vérification de la complexité des mots de passe et de la politique appliquée

4. Contrôle des accès à distance :
    - Liste des postes avec RDP actif
    - Vérification des règles de pare-feu Windows
    - Identification des postes exposés sans authentification forte
5. Analyse du niveau de segmentation réseau (VLANs) :
    - Vérification que les imprimantes, serveurs et postes utilisateurs sont correctement isolés

Actions correctives et améliorations :

6. Remédiation des postes non conformes :
    - Installation d'ESET sur les machines sans protection
    - Forçage des mises à jour critiques
7. Recommandations faites à l'équipe technique :
    - Désactivation des comptes admin inutiles
    - Renforcement des règles RDP (mot de passe fort, changement de port, accès limité)
8. Rapport rédigé :
    - Liste des risques identifiés
    - Taux de conformité AV/mises à jour
    - Préconisations techniques

Résultats obtenus :

- Visibilité complète sur l'état de sécurité des postes et serveurs.
- Identification et correction des postes à risque.
- Amélioration globale du niveau de sécurité du SI client.
- Rapport exploitable transmis à l'encadrement et utilisé pour planifier les prochaines actions.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

PRISM NUTANIX

Console ESET

PROXY ZABBIX

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMALSI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022i*

5. Informations complémentaires *(facultatif)*

Activité-type 3 Participer à la gestion de la cybersécurité

Exemple n° 2 *Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Chez plusieurs clients, j'ai constaté que les emails malveillants représentaient une menace sérieuse : spam, phishing, virus en pièce jointe, etc.

Pour améliorer leur protection, l'entreprise m'a chargé de participer à la mise en œuvre d'une solution anti-spam et de sécurité mail : Mailinblack.

J'ai aussi intégré cette démarche dans les formations de sensibilisation à la cybersécurité destinées aux utilisateurs.

Objectif de l'action :

- Renforcer la sécurité du courrier électronique chez les clients.
- Mettre en œuvre et paramétrer Mailinblack.
- Former les utilisateurs à reconnaître et gérer les mails suspects.
- Contribuer à une politique de sécurité cohérente autour des emails.

Tâches réalisées :

Mise en place de Mailinblack :

1. Paramétrage du filtrage antispam via les enregistrements DNS (MX, SPF, DKIM, DMARC) dans leurs gestionnaire Mail (OVH, Gandi)
2. Création des comptes utilisateurs sur la plateforme Mailinblack.
3. Définition des règles de filtrage (niveaux de sensibilité, liste blanche, quarantaine).
4. Activation du challenge de validation pour les expéditeurs inconnus.
5. Tests d'envoi et de réception de mails pour valider le bon fonctionnement.

Sensibilisation et accompagnement :

6. Présentation de l'outil aux utilisateurs (fonctionnement de la validation, accès à la quarantaine).
7. Formation sur les bons réflexes face aux emails suspects :
    - Ne pas cliquer sur des liens non vérifiés.
    - Vérifier les adresses d'expéditeurs.
    - Signaler les tentatives de phishing.
8. Intégration de Mailinblack dans le guide de politique de sécurité diffusé aux clients.

Résultats obtenus :

- Réduction drastique des spams et mails frauduleux dans les boîtes de réception des clients.
- Adoption facilitée grâce à un accompagnement utilisateur personnalisé.
- Politique de sécurité renforcée sur l'un des points les plus critiques : la messagerie électronique.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

MAILINBLACK CENTRALISE

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022i*

5. Informations complémentaires *(facultatif)*

Activité-type 3 — Participer à la gestion de la cybersécurité

Exemple n° 3 ▸ *Participer à la détection et au traitement des incidents de sécurité*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Durant mon alternance chez OPIMALSI, j'ai été régulièrement confronté à des incidents de sécurité affectant les postes clients : tentatives de phishing par email, détection de logiciels malveillants par ESET, ou encore alertes réseau signalées via Zabbix ou Atera.

J'ai participé activement à leur identification, analyse et traitement, en collaboration avec l'équipe technique.

Objectif de l'action :

- Détecter rapidement les incidents de sécurité en s'appuyant sur les outils en place (ESET Protect, Mailinblack, Zabbix, Atera).
- Qualifier et comprendre la nature des menaces.
- Réagir efficacement pour sécuriser les postes ou bloquer les accès.
- Sensibiliser les utilisateurs suite à l'incident.

Tâches réalisées :

Détection des incidents :

1. Surveillance des alertes de sécurité ESET (virus détectés, agents désactivés…).
2. Analyse de la console Mailinblack pour repérer des mails suspects (phishing, fausses factures, fausses livraisons).
3. Suivi des logs Zabbix et Atera pour détecter des comportements anormaux (CPU élevé, ports ouverts, services arrêtés).
4. Réception d'alertes directes de la part des utilisateurs (clics sur liens douteux, pièces jointes suspectes).

Analyse et qualification :

5. Vérification des informations de l'alerte (chemin du fichier, comportement, expéditeur…).
6. Blocage immédiat du fichier/machine si besoin (quarantaine via ESET, coupure réseau).
7. Recherche d'autres machines potentiellement touchées par la même menace.
8. Vérification si le phishing a été cliqué ou si les identifiants ont été saisis.

Traitement :

9. Suppression manuelle ou automatique du fichier malveillant.
10. Restauration ou nettoyage du poste.
11. Changement des mots de passe si des données sensibles ont été exposées.
12. Mise à jour du système ou de l'antivirus si nécessaire.

Communication & documentation :

13. Avertissement à l'utilisateur concerné (avec explications simples).
14. Rédaction d'un rapport d'incident pour l'équipe ou le client.
15. Recommandations à l'utilisateur : ne pas cliquer, vérifier les expéditeurs, signaler toute suspicion.

Résultats obtenus :

- Plusieurs menaces ont été détectées et neutralisées avant qu'elles ne causent des dommages.
- Les postes touchés ont été nettoyés rapidement, sans impact majeur pour les utilisateurs.

- Les utilisateurs concernés ont été sensibilisés à la sécurité pour éviter que l'incident ne se reproduise.

- Amélioration de la réactivité globale de l'entreprise face aux menaces.

2. Précisez les moyens utilisés :

Les moyens utilisés pour ce projet :

Un ordinateur avec une connexion internet.

MAILINBLACK CENTRALISÉ

CONSOLE ESET

CONSOLE ATERA et ZABBIX

3. Avec qui avez-vous travaillé ?

J'ai travaillé seul sur ce projet.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *OPTIMAL SI*

Chantier, atelier, service ▸ *Dans le cadre de la formation Administrateur d'infrastructure sécurisées*

Période d'exercice ▸ Du : *10/12/2021* au : *25/01/2022i*

5. Informations complémentaires *(facultatif)*

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Bac Série S spécialité Mathématiques chimie.	**Lycée Félix Esclangon MANOSQUE**	06/2018.

Déclaration sur l’honneur

Je soussigné(e) PANABIERES Vincent ,

déclare sur l’honneur que les renseignements fournis dans ce dossier sont exacts et que je suis l’auteur(e) des réalisations jointes.

Fait à Marseille le 21/07/2025

pour faire valoir ce que de droit.

Signature : *VINCENT PANABIERES*

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé
Cliquez ici pour taper du texte.

ANNEXES

(Si le RC le prévoit)