Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ
DE L'EMPLOI

DOSSIER PROFESSIONNEL (DP)

Nom de naissance ▸ DIALLO
Nom d'usage ▸ DIALLO
Prénom ▸ FATOUMATA BINTA
Adresse ▸ 64 Montée de l'observance 69009 Lyon

Titre professionnel visé

Administratrice Infrastructures sécurisés

MODALITE D'ACCES :

☒ 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.

http://travail-emploi.gouv.fr/titres-professionnels

Sommaire

Exemples de pratique professionnelle

Intitulé de l'activité-type n° 1 Administrer et sécuriser les infrastructures	**p.**	**5**
▸ Intitulé de l'exemple n° 1 Mise en place d'un VPN Site to Site .....p.	p.	
▸ Intitulé de l'exemple n° 2 Mise en place d'un GLPI .....p.	p.	
▸ Intitulé de l'exemple n° 3 .....p	p.	
Intitulé de l'activité-type n° 2 Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution	**p.**	
▸ Intitulé de l'exemple n° 1 *Élaboration d'un Plan de Reprise d'Activité (PRA) pour une Entreprise de Commerce en Ligne*.....p.	p.	
▸ Intitulé de l'exemple n° 2 Mise en place d'un serveur de supervision Zabbix.....p.	p.	
▸ Intitulé de l'exemple n° 3 .....p	p.	
Intitulé de l'activité-type n° 3 Participer à la gestion de la cybersécurité	**p.**	
▸ Intitulé de l'exemple n° 1 Suppression et Installation d'un EDR Sentinel One sur des serveurs chez un client.....p.	p.	
▸ Intitulé de l'exemple n° 2 .....p.	p.	
▸ Intitulé de l'exemple n° 3 .....p	p.	
Intitulé de l'activité-type n° 4	**p.**	
▸ Intitulé de l'exemple n° 1 .....p.	p.	
▸ Intitulé de l'exemple n° 2 .....p.	p.	
▸ Intitulé de l'exemple n° 3 .....p	p.	
Titres, diplômes, CQP, attestations de formation *(facultatif)*	**p.**	
Déclaration sur l'honneur	**p.**	
Documents illustrant la pratique professionnelle *(facultatif)*	**p.**	
Annexes *(Si le RC le prévoit)*	**p.**	

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n°1 Mise en place d'un VPN site to site

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

Tout d'abord, j'ai installé pfSense sur deux machines virtuelles, chacun configuré comme passerelle pour un site distant. J'ai noté les adresses IP publiques des deux sites, ainsi que les plages d'adresses IP locales (LAN) à connecter.
Configuration sur le premier site (Site A)
J'ai accédé à l'interface web de pfSense sur le site A. Ensuite, je suis allé dans le menu **VPN > IPSec** pour configurer une connexion VPN.
J'ai ajouté la **Phase 1**, j'ai défini l'adresse IP publique du site distant (Site B), le type d'authentification (clé pré-partagée), et les algorithmes de chiffrement.
Ensuite, j'ai fait la configuration de la phase 2 du site A
Toujours dans la section IPSec, j'ai ajouté une **Phase 2** pour définir les sous-réseaux locaux des deux sites (Exemple : 192.168.1.0/24 pour Site A et 192.168.2.0/24 pour Site B). J'ai sélectionné les paramètres de chiffrement et validé la configuration.
Réplication sur le deuxième site (Site B)
Sur pfSense du site B, j'ai répété les mêmes étapes pour créer une configuration IPSec.
Dans la Phase 1, j'ai spécifié l'adresse IP publique du site A comme paire distante.
J'ai entré la même clé pré-partagée et les mêmes paramètres de chiffrement pour garantir la compatibilité.
Enfin, j'ai configuré la Phase 2 en miroir avec les sous-réseaux définis précédemment.
Après avoir appliqué les paramètres, j'ai vérifié que le tunnel IPSec était actif via l'onglet **Statut > IPSec** sur les deux sites. Ensuite J'ai ajusté les règles de pare-feu dans **Firewall > Rules > IPSec** pour autoriser le trafic entre les deux sous-réseaux.
J'ai testé la connectivité en faisant des pings depuis une machine du LAN de Site A vers une machine du LAN de Site B et inversement.

2. Précisez les moyens utilisés :

4 Machines virtuelles installées sur VMware dont deux Pfsense et deux Windows 10 pour accéder à la console de configuration des pfsenses et pour les tests de connectivité

3. Avec qui avez-vous travaillé ?

En Autonomie

4. Contexte

Nom de l'entreprise, organisme ou association : *Hardis Group*

Chantier, atelier, service : Atelier

Période d'exercice : Du : *02/09/2024* au : *03/09/2024*

5. Informations complémentaires *(facultatif)*

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n°2 : **Mise en place d'un GLPI**

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

GLPI est un logiciel libre de gestion de parc informatique permettant d'avoir une solution de ticketing gratuite pour le support informatique, de gérer l'inventaire des équipements, notamment les ordinateurs les imprimantes, les serveurs et mêmes les smartphones il permet aussi de gérer les contrats de licences et le suivi de configurations matérielles et logicielles.
Pour la mise en place d'un GLPI, j'ai commencé par installer un serveur et les prérequis.
GLPI a besoin d'un serveur web, de PHP et d'une base de données pour fonctionner. Etant sous linux ceci correspond à Apache2, MariaDB/MySQL, PHP j'ai installé php en tant que module apache
J'ai installé les dépendances, ensuite j'ai configuré la base de données pour GLPI.
J'ai téléchargé l'archive tgz qui contient les sources d'installation de GLPI à partir du GitHub de GLPI, j'ai récupéré le lien vers la dernière version qui est la 10.0.10, j'ai téléchargé l'image depuis le fichier tmp puis je l'ai décompressé. Ensuite, j'ai défini l'utilisateur "www-data" correspondant à Apache2, en tant que propriétaire sur les fichiers GLPI. Ensuite, j'ai créé des dossiers et j'ai sorti les données de la racine Web (/var/www/glpi) de manière à les stocker dans les nouveaux dossiers que j'ai créés. Ceci va permettre de faire une installation sécurisée de GLPI, qui suit les recommandations de l'éditeur.
Ensuite j'ai configuré Apache2, j'ai créé un nouveau fichier de configuration qui va permettre de configurer le VirtualHost dédié à GLPI. Ensuite j'active le nouveau site dans Apache2 et je vais désactiver le site par défaut. Ensuite j'ai redémarré Apache2
Après cela j'ai accédé à l'interface web de GLPI pour configurer mon serveur GLPI.
Après l'installation j'ai rajouter mes équipements et un serveur pour faire le test de fonctionnement.

2. Précisez les moyens utilisés :

Un serveur Debian pour l'installation, de mon serveur GLPI et une machine virtuelle Windows pour accéder à l'interface Web de mon GLPI

3. Avec qui avez-vous travaillé ?

En Autonomie

4. Contexte

Nom de l'entreprise, organisme ou association : *Hardis Group*

Chantier, atelier, service : Atelier

Période d'exercice : Du : *17/10/2024* au : *18/10/2024*

5. Informations complémentaires *(facultatif)*

Activité-type 2

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

Exemple n° 1 ▸ ***Élaboration d'un Plan de Reprise d'Activité (PRA) pour une Entreprise de Commerce en Ligne***

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

Elaboration d'un plan de reprise d'activité pour l'entreprise E-shop Express qui est spécialisé dans la vente de produits électroniques en ligne. L'entreprise est composée de 50 employés. Les principales ressources opérationnelles sont : Gestion des commandes, service client, gestion des stocks, paiements en ligne, expédition.
Systèmes informatiques critiques : Site web de vente en ligne, bases de données clients, serveurs de paiement en ligne.
Je vais identifier trois scénarios de risques qui pourraient perturber les opérations d'E-Shop Express.

1-Fournisseur d'accès Internet défaillant :

Description : Cela fait référence à la situation où le fournisseur de services Internet (FSI) de l'entreprise connaît des problèmes techniques ou opérationnels, ce qui entraîne une perte de connectivité à Internet pour E-Shop Express.
Impacts potentiels : Interruption des opérations commerciales, notamment la capacité à traiter les commandes en ligne. Diminution des revenus en raison de l'incapacité des clients à accéder au site web et à effectuer des achats. Perte de réputation et de confiance des clients si la déconnexion est prolongée.
Facteurs contributifs : Panne matérielle ou logicielle chez le FSI. Congestion du réseau ou surcharge du trafic. Catastrophes naturelles affectant les infrastructures du FSI.

2-Acte de cyber malveillance 'RANSOMWARE'

Description : Un ransomware est un type de logiciel malveillant qui chiffre les données de la victime et demande une rançon pour les déchiffrer. Dans ce scénario, une attaque de ransomware cible Spécifiquement la base de données client d'E-Shop Express.
Impacts potentiels : Perte d'accès aux informations cruciales sur les clients, ce qui affecte directement la gestion des commandes et le service client.
Risques financiers liés au paiement éventuel de la rançon. Atteinte à la réputation de l'entreprise, car les clients peuvent craindre pour la sécurité de leurs données. Sanctions légales si les informations personnelles des clients sont compromises.
Facteurs contributifs : Vulnérabilités non corrigées dans le système ou le logiciel. Absence ou inefficacité des mesures de sécurité et de prévention. Hameçonnage ou autres tactiques d'ingénierie sociale visant les employés.

3-Guerre cybernétique entre États :

Description : La guerre cybernétique entre États se réfère à des actes coordonnés de sabotage, d'espionnage ou de destruction par des acteurs étatiques utilisant le cyberespace comme champ de bataille. Même si E-Shop Express n'est pas directement ciblé, il peut être touché collatéralement.

Impacts potentiels : Perturbations des opérations dues à des attaques massives visant des infrastructures nationales, qui peuvent indirectement affecter les entreprises. Perte d'accès à des services essentiels ou à des partenaires commerciaux si ces derniers sont ciblés ou affectés. Instabilité économique et incertitude, conduisant à une baisse de la demande ou à des perturbations de la chaîne d'approvisionnement.
Facteurs contributifs : Tensions politiques ou militaires entre pays. Faiblesse des infrastructures nationales en matière de cybersécurité. Attaques ciblées de représailles entre nation

Stratégies de reprise à appliquer selon les différents scénarios

Pour FAI défaillant :

Utilisation de liaisons Internet redondantes provenant de fournisseurs d'accès différents :
Description : Avoir plusieurs connexions Internet de fournisseurs différents pour assurer la continuité des opérations en cas de panne d'un fournisseur.
Avantages : Réduit le risque d'interruptions ; offre une bascule automatique vers un FAI de secours en cas de défaillance du principal.
Mise en œuvre : Collaborer avec plusieurs FAI, configurer des routeurs et des commutateurs pour gérer la bascule.
Déploiement d'Azure ExpressRoute pour une connexion privée, rapide et fiable à Microsoft Azure :
Description : Azure ExpressRoute permet une connexion directe et privée entre l'infrastructure de l'entreprise et Microsoft Azure, en contournant Internet public.
Avantages : Offre une latence plus faible, une sécurité renforcée et des débits plus élevés.
Mise en œuvre : Travailler avec un partenaire ExpressRoute et configurer la connectivité avec Azure.

Pour RANSOMWARE :

Utilisation d'Azure Security Center pour une détection précoce :
Description : Azure Security Center offre des fonctionnalités avancées de protection contre les menaces et de détection des comportements anormaux.
Avantages : Détecte et alerte rapidement en cas d'activités suspectes ; fournit des recommandations pour améliorer la posture de sécurité.
Mise en œuvre : Activer Azure Security Center sur les ressources Azure, configurer les alertes et les politiques de sécurité.
Sauvegardes régulières via Azure Backup :
Description : Azure Backup offre des solutions de sauvegarde automatisées et sécurisées dans le cloud.
Avantages : Restauration rapide des données en cas d'incident ; conservation à long terme des données ; réduction des coûts d'infrastructure. - Mise en œuvre : Configurer les politiques de sauvegarde, sélectionner les ressources à sauvegarder, et établir un calendrier de sauvegarde.

Pour Guerre cybernétique :

Sécurisation renforcée des systèmes et réseaux :
Description : Adopter des mesures de sécurité robustes pour protéger l'infrastructure contre des cyberattaques d'envergure.
Avantages : Réduction de la surface d'attaque et de la vulnérabilité aux attaques ; protection des actifs essentiels.
Mise en œuvre : Mise à jour régulière des systèmes, déploiement de pare-feux avancés, utilisation

d'IDS/IPS, formation des employés.
Surveillance accrue via Azure Sentinel :
Description : Azure Sentinel est un système d'information et d'événement de sécurité (SIEM) et une solution de gestion des événements et des informations de sécurité (SOAR) basée sur le cloud.
Avantages : Collecte, stockage et analyse en temps réel des données de sécurité pour une détection rapide des menaces ; automatisation des réponses.
Mise en œuvre : Configurer Azure Sentinel, intégrer les sources de données, établir des règles et des alertes, automatiser les réponses aux incidents.

Les ressources nécessaires à la continuité des activités :

1. Infrastructure IT :
- Systèmes redondants : Serveurs de secours, systèmes de stockage, etc.
- Sauvegardes régulières : Solutions de sauvegarde locales et hors site pour assurer la disponibilité des données.
- Connexions Internet redondantes : De multiples FAI pour prévenir les temps d'arrêt en cas de défaillance d'un fournisseur.

2. Logiciels et Licences :
- Licences pour tous les logiciels critiques utilisés dans l'entreprise.
- Solutions de virtualisation pour déployer rapidement des serveurs et des postes de travail en cas de besoin.

3. Emplacement physique de secours :
- Espaces de travail alternatifs pour le personnel en cas d'indisponibilité des locaux principaux.
- Sites de récupération d'urgence équipés de matériel informatique, de télécommunications et d'autres installations nécessaires.

4. Ressources humaines :
- Équipe dédiée à la continuité des activités : Responsables de la mise en œuvre, de la gestion et de la révision du PCA/PRA.
- Formations régulières : Assurer que le personnel est formé et au courant des procédures à suivre en cas d'interruption.

5. Fournisseurs et Partenaires :
- Contrats avec des fournisseurs alternatifs pour garantir l'approvisionnement en ressources essentielles.
- Accords de niveau de service (SLA) pour s'assurer de la rapidité de la réponse et du soutien en cas d'urgence.

6. Systèmes de communication :
- Solutions de communication d'urgence (ex. : radios satellitaires, téléphones par satellite) pour le cas où les méthodes de communication traditionnelles échouent.
- Outils de collaboration en ligne et plateformes de conférence pour le travail à distance.

7. Documentations et Procédures :
- Documentations claires et accessibles détaillant les processus et procédures à suivre.
- Listes de contacts d'urgence, plans d'évacuation et autres documents essentiels.

8. Finances :
- Fonds d'urgence pour couvrir les coûts imprévus associés à la récupération et à la continuité des

Opérations.
- Accords avec les institutions financières pour assurer l'accès aux fonds en cas de crise.

9. Soutien externe :
- Contrats avec des consultants ou des entreprises spécialisées pour fournir une expertise et un soutien en matière de continuité des activités.

10. Mesures de sécurité :
- Solutions de surveillance et de sécurité pour protéger les ressources physiques et informatiques.
- Planification pour la protection et la sécurisation des données sensibles.

2. Précisez les moyens utilisés :

Recherches forums sur google et sur les sites internet fiables
Utilisation de Word la documentation et excel pour les tableaux

3. Avec qui avez-vous travaillé ?

En groupe c'est un TP qui a été réalisé à l'école

4. Contexte

Nom de l'entreprise, organisme ou association *Simplon*

Chantier, atelier, service ▸ Atelier

Période d'exercice ▸ Du : *10/04/2024* au : *12/04/2024*

5. Informations complémentaires *(facultatif)*

Images en annexe

Activité-type 2

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

Exemple n° 1

Mise en place d'un serveur de supervision zabbix

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

Zabbix est un outil de surveillance open source qui permet de suivre en temps réel la performance et la disponibilité des systèmes informatiques, tels que les serveurs, les réseaux, et les applications. Il recueille des données sur ces éléments, génère des alertes en cas de problème et fournit des rapports pour aider à maintenir une infrastructure informatique stable.

Pour la mise en place de mon serveur zabbix, j'ai commencé par installé un serveur Debian et faire les mises à jour système, ensuite j'ai installé Zabbix Server en suivant les instructions de la documentation officielle. J'ai aussi installé un serveur de base de données MySQL.

J'ai créé une base de données et un utilisateur pour Zabbix. Puis, j'ai configuré les paramètres de connexion dans le fichier zabbix_server.conf.

J'ai ensuite installé le frontend Zabbix sur un serveur web Apache en suivant les étapes fournies.

J'ai modifié le fichier zabbix_server.conf pour définir les paramètres nécessaires, comme la connexion à la base de données. J'ai redémarré le serveur Zabbix pour appliquer la configuration et vérifier que tout fonctionne correctement.

J'ai installé l'agent Zabbix sur les serveurs et équipements à surveiller. J'ai modifié leur fichier de configuration pour lier chaque agent au serveur zabbix.

J'ai accédé à l'interface web de Zabbix pour terminer l'installation, en configurant les paramètres du serveur Zabbix et de la base de données.

Dans l'interface web, j'ai ajouté les hôtes à surveiller et configuré les éléments comme la CPU, la mémoire, et l'espace disque.

J'ai configuré les actions de notification pour recevoir des alertes par courriel ou autre moyen en cas de problème sur les hôtes surveillés.

J'ai testé la configuration en vérifiant que les données étaient bien collectées et que les alertes étaient générées en cas de dépassement de seuils.

2. Précisez les moyens utilisés :

Une machine Virtuelle Debian, Tuto sur le site officiel de Zabbix

3. Avec qui avez-vous travaillé ?

En Autonomie

4. Contexte

Nom de l'entreprise, organisme ou association *Hardis Group*

Chantier, atelier, service Atelier

Période d'exercice Du : *07/11/2024* au : *08/11/2024*

5. Informations complémentaires *(facultatif)*

Capture en Annexe

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

Exemple n° 1 ▸ ***Suppression et Installation d'un EDR Sentinel One sur des serveurs chez un client***

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

À la suite de la fin des licences de notre client IT-SOLUTIONS depuis fin février, nous avons été sollicités pour une situation urgente qui s'est présentée, nécessitant la mise en place de nouvelles licences sur leurs serveurs. Après l'expiration des licences précédente, la console de la première migration a été supprimé, laissant ainsi les serveurs sans protection pendant un laps de temps. Pour remédier à cette situation, nous avons élaboré une procédure détaillée pour supprimer les agents existants afin de pouvoir mettre en place les nouvelles licences. Les machines étant hébergés chez un autre client, une intervention de leurs parts étaient nécessaire pour nous donner l'accès au Vms depuis le VCenter.
SentinelOne est une solution de cybersécurité qui protège les appareils et les systèmes informatiques contre les menaces telles que les malwares, ransomwares et attaques de type zero-day. Utilisant l'intelligence artificielle, elle détecte, bloque et répond automatiquement aux menaces en temps réel, sans nécessiter d'intervention manuelle. SentinelOne offre également des fonctionnalités avancées de gestion des incidents, d'analyse forensique et de visibilité complète sur l'ensemble du réseau pour garantir une sécurité optimale des environnements informatiques.
MIGTATION
Préparation en amont des scripts pour la migration, préparation des lots des serveurs à migrer et mise en place d'un planning ensuite validation avec le client
Pour cette migration, l'hébergeur des machines réalisait une snapshot par serveur de prod et une sauvegarde instantanée qui permet revenir en arrière en cas de problème pendant l'intervention.
Ensuite, on met en pause les sondes des serveurs concernés pour éviter de déclencher une alerte pendant l'intervention sur sheinken.
Shinken est un logiciel de supervision.
Ensuite, on fait le dépôt des outils sur le serveur à migrer, elle contient les scripts de désinstallation avec la bonne version de l'agent et le script d'installation avec le bon Token.
Lancement des scripts de désinstallation de l'ancien agent. Ensuite on redémarre le serveur en mode sans échec pour forcer la désinstallation de l'agent sentinel one.
Ensuite redémarrage en mode nominal puis lacement des scripts d'installation du nouvel agent
Vérification que l'agent remonte dans la console et que l'interface de l'agent annonce la configuration recherchée

2. Précisez les moyens utilisés :

Les serveurs à migrer, la console d'administration de sentinel one , les agents de sentinel one avec la

bonne version et le bon Token

3. Avec qui avez-vous travaillé ?

En équipe

4. Contexte

Nom de l'entreprise, organisme ou association : *Hardis Group*

Chantier, atelier, service : Service

Période d'exercice : Du : *14/02/2024* au : *04/03/2025*

5. Informations complémentaires *(facultatif)*

Captures en Annexe

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Technicien d'assistance informatique	Online FormaPro	10/02/2023
BAC Littéraire	ESMI	10/09/2020

Déclaration sur l'honneur

Je soussigné(e) [prénom et nom] Fatoumata Binta Diallo ,

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 Lyon le 05/01/2025

Pour faire valoir ce que de droit.

Signature : Fatoumata Binta Diallo

Documents illustrant la pratique professionnelle

(facultatif)

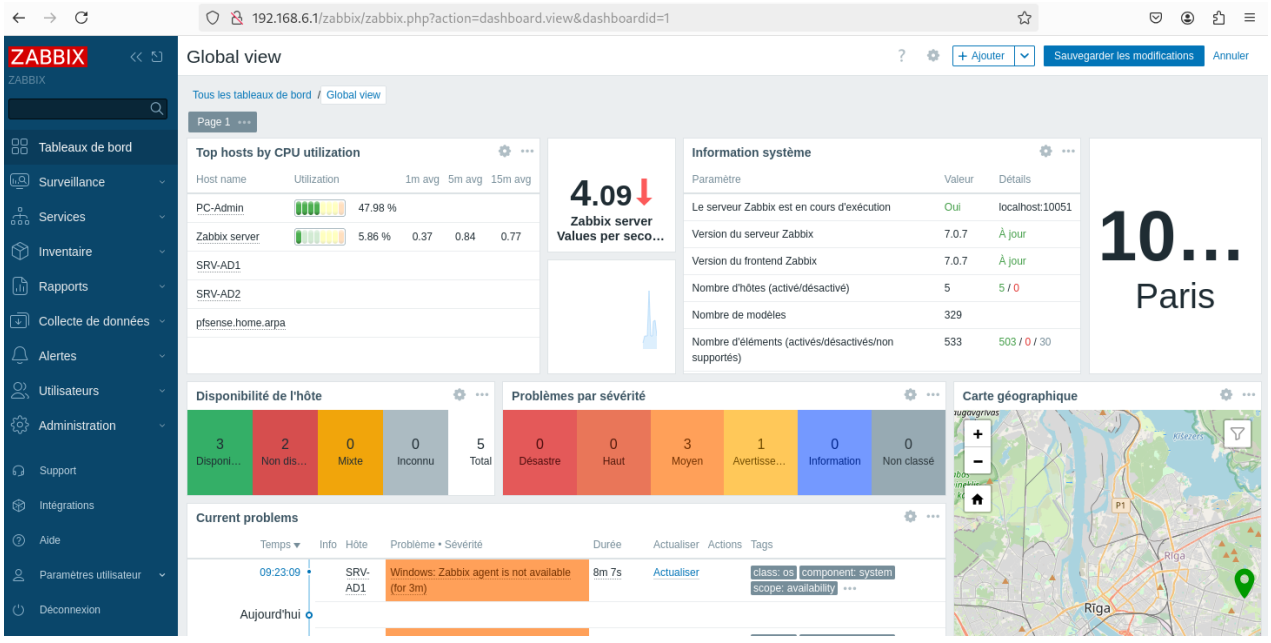
Intitulé
Cliquez ici pour taper du texte.
ANNEXE 1 et 2 : PRA plan de reprise d'activité
ANNEXE3 : Serveur de supervision ZABBIX
ANNEXE4 : Installation EDR VisionOne

Objectifs de Temps de Reprise (RTO) et Point d'Objectif de Récupération (RPO)

Scénario	RTO	RPO
Fournisseur d'accès Internet défaillant	4 heures	6 heures
Acte de cybermalveillance: RANSOMWARE	2 heures	4 heures
Guerre cybernétique entre États	6 heures	12 heures

Classification des Risques

Scénario	Probabilité	Impact
FAI défaillant	Moyenne	Élevé
RANSOMWARE	Moyenne	Très élevé
Guerre cybernétique	Faible	Très élevé



PowerShell

```
Start-Process [redacted]-S1Migration\Outils\SentinelOneInstaller_windows_64bit_v23_3_3_264.exe" -
ArgumentList "--clean_only"
```