Portfolio de réalisations professionnelles

Épreuve E5 — Support et mise à disposition de services informatiques

BTS SIO · option SISR · session 2027

PIOCH Dorian · **Alternance 2025 → 2027**

https://dpioch.aristeecampus.org

Deux environnements

Réalisations CFA et entreprise : compétences alignées sur la matrice vérifiée. Le laboratoire personnel reste distinct.

Centre de formation

- Windows : Active Directory et GPO

Déploiement : FOG, VM, GLPI
Services : WordPress, MariaDB GSB
Réseau : pfSense (R06)
Sécurité : BIND9/RPZ, Suricata, CrowdSec
Journaux, supervision et accès : Wazuh, Zabbix, Guacamole
Automatisation : Ansible

Entreprise — alternance

- Migration de poste utilisateur

SharePoint et OneDrive
Logiciels métier après-vente et atelier
Interfaces d'impression uniFLOW (R27)
Mise à jour des certificats logiciel métier (R28)
Contexte et données anonymisés

CFA

Réalisations en centre de formation

Cas GSB : laboratoire pharmaceutique fictif, d’après le contexte officiel.
Références d’origine conservées ; année et dates de réalisation à confirmer.

AD · R01 | GPO · R02/R25 | FOG · R03 | VM · R04/R26 | LAMP · R10 | GLPI · R12/R22 | pfSense · R06

IDS/IPS Suricata | DNS BIND9 | CrowdSec | Wazuh | Zabbix | Ansible | Guacamole

MariaDB GSB · R11 : bases, comptes nominatifs et rôle d’administration.

Active Directory — service d’annuaire

Centre de formation

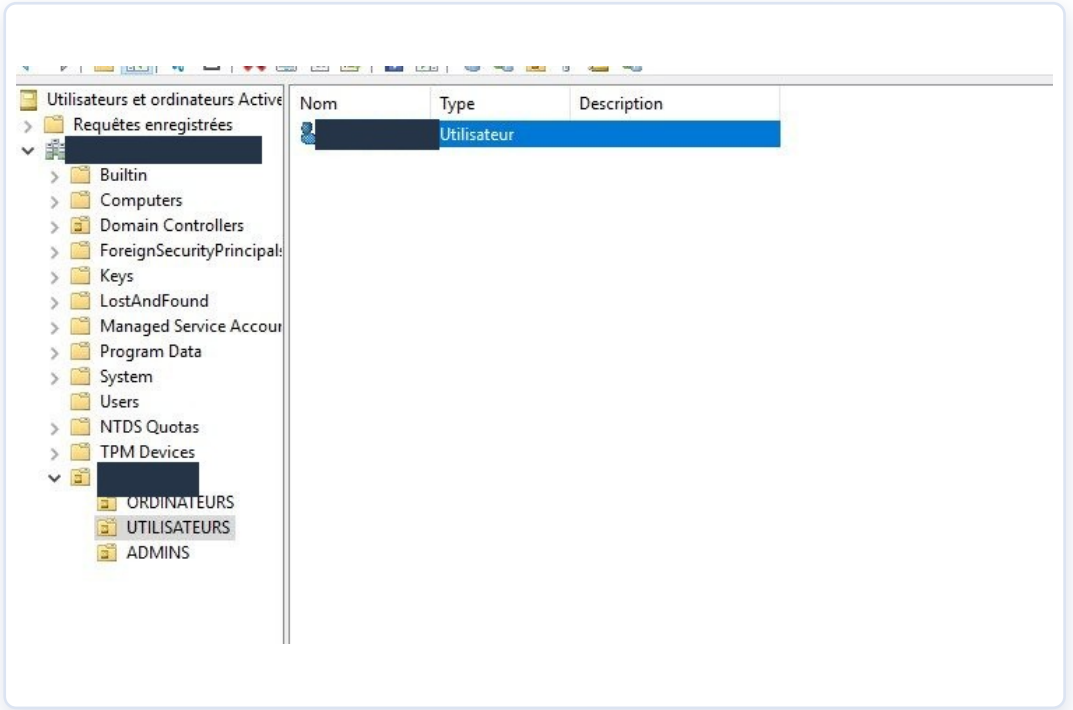
CONTEXTE & ENJEU

Mettre en place l’ossature d’un système d’information Windows : un annuaire centralisé pour authentifier les utilisateurs et administrer les postes depuis un point unique.

MISE EN ŒUVRE

- Installation du rôle AD DS et promotion en contrôleur de domaine.

Structuration des unités d’organisation pour cibler les stratégies.
Création des comptes, groupes, droits et délégations.
Jonction d’un poste Windows 10 et test de session annuaire.



Console AD — noms et compte masqués

Service rendu Authentification centralisée et gestion unifiée des identités et des postes.

Patrimoine · Mise à disposition

R01 — année et dates à confirmer

Fiche source ↗

Stratégies de groupe (GPO) et partage réseau

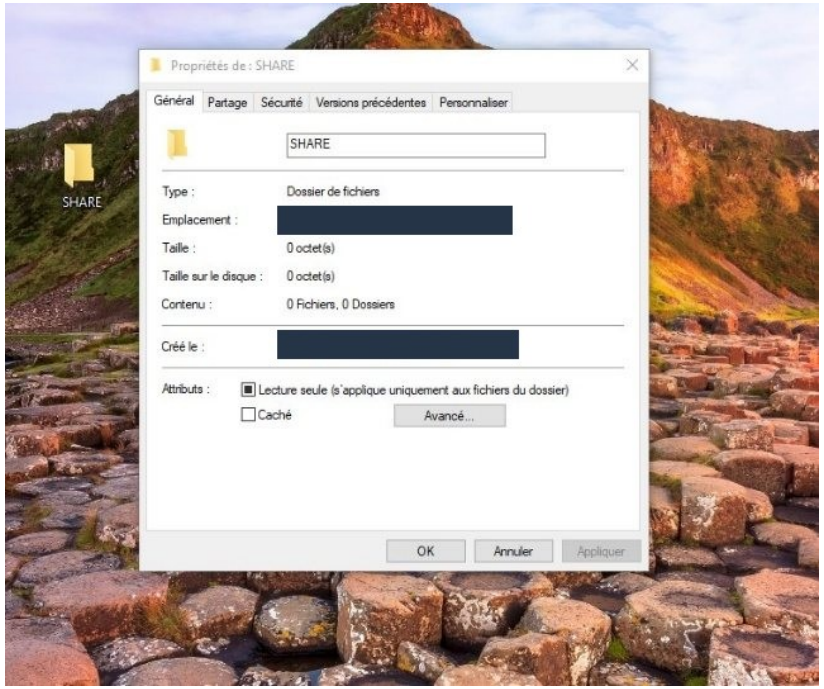
Centre de formation

CONTEXTE & ENJEU

Industrialiser la configuration des postes et sécuriser l'accès aux ressources partagées, sans intervention manuelle poste par poste.

MISE EN ŒUVRE

- Création d'un dossier partagé avec autorisations partage + NTFS (moindre privilège).
- Création d'une stratégie de groupe (GPO) liée à une unité d'organisation.
- Déploiement automatique d'un lecteur réseau et de paramètres via la GPO.
- Vérification de l'application sur les postes (gpupdate, gpresult).



Dossier partagé — vue Général, pas une preuve des permissions

Service rendu Configuration homogène et reproductible de l'ensemble du parc.

Patrimoine · Mise à disposition

R02 / R25 — année et dates à confirmer

Fiche source ↗

Déploiement d’images — serveur FOG

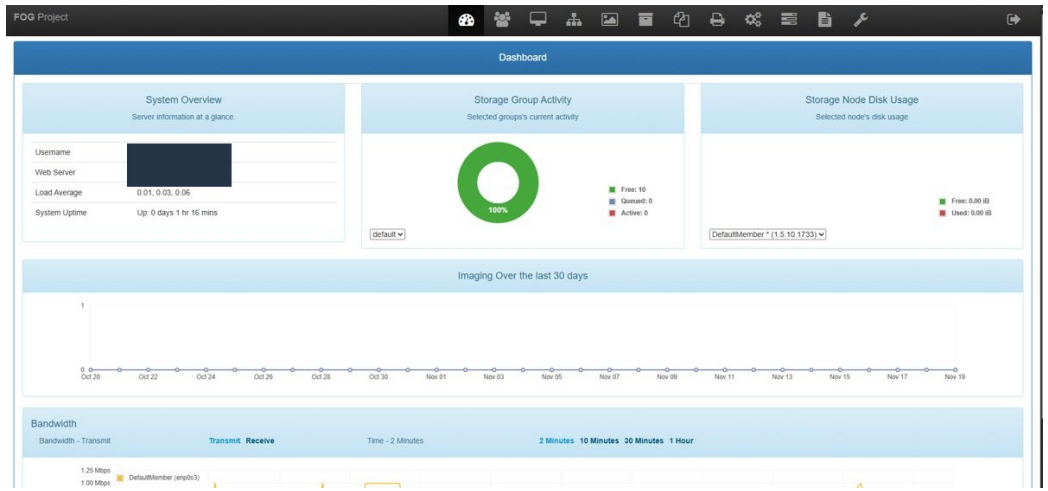
Centre de formation

CONTEXTE & ENJEU

Réduire le temps d’installation des postes en passant d’une installation manuelle à un déploiement d’images par le réseau.

MISE EN ŒUVRE

- Installation du serveur FOG sur Debian (pile LAMP : Apache, PHP, base de données).
- Capture d’une image maître à partir d’un poste de référence.
- Déploiement de l’image par amorçage réseau PXE.
- Gestion et suivi des postes depuis l’interface web FOG.



FOG — tableau de bord d’archive, pas une recette PXE

Service rendu Masterisation et redéploiement rapide et reproductible des postes.

Mise à disposition

R03 — année et dates à confirmer

Fiche source ↗

Installation, sauvegarde et clonage de VM

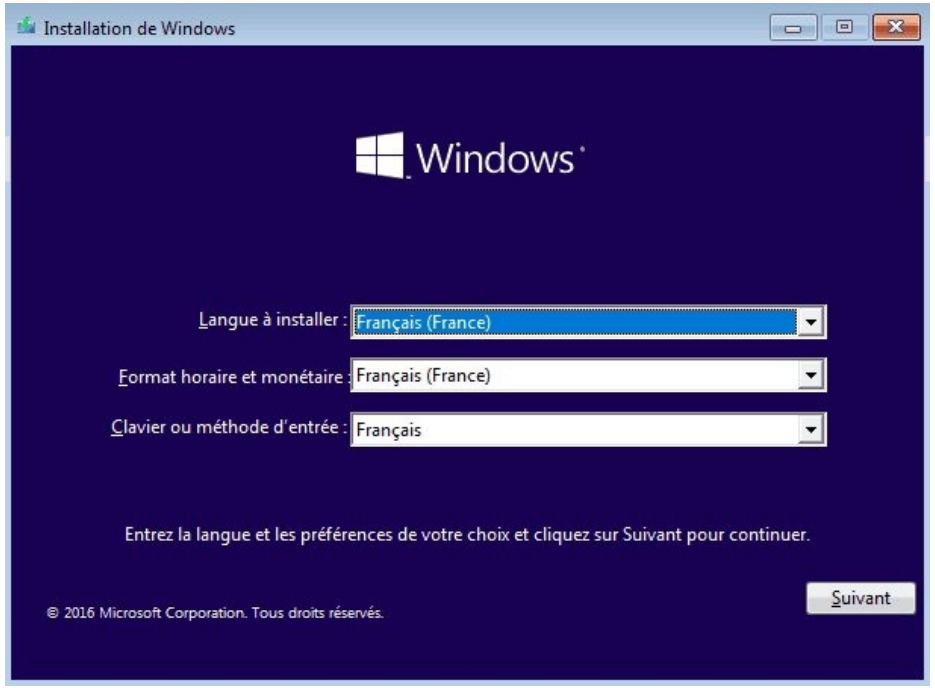
Centre de formation

CONTEXTE & ENJEU

Garantir la disponibilité et la reprise d'une machine virtuelle, et disposer d'un modèle réutilisable pour gagner du temps.

MISE EN ŒUVRE

- Création et installation d'une machine virtuelle Windows 10.
- Clonage de la VM pour produire un modèle de déploiement.
- Sauvegarde de la machine et procédure de restauration documentée.
- Gestion du stockage (dimensionnement et extension de partition).



Installation de la machine virtuelle Windows

Service rendu Capacité de restauration en cas d'incident et gabarit réutilisable.

Patrimoine

R04 / R26 — année et dates à confirmer

Fiche source ↗

Serveur web WordPress (pile LAMP)

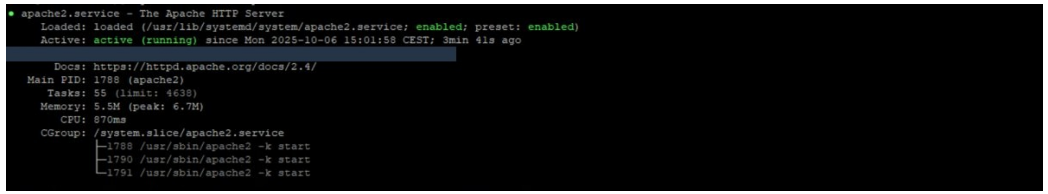
Centre de formation

CONTEXTE & ENJEU

Héberger un site web en interne sur une infrastructure entièrement maîtrisée, plutôt que sur un service tiers.

MISE EN ŒUVRE

- Installation de la pile LAMP sur Debian : Apache, PHP, base MariaDB.
- Création de la base de données et d'un compte applicatif dédié (droits limités).
- Installation et configuration de WordPress.
- Mise en service et contrôle du bon fonctionnement (service Apache actif).



Apache actif sur la capture — pas une mesure de disponibilité

Service rendu Site web hébergé en interne, administrable et maîtrisé de bout en bout.

Mise à disposition

R10 — année et dates à confirmer

Fiche source ↗

Inventaire de parc GLPI

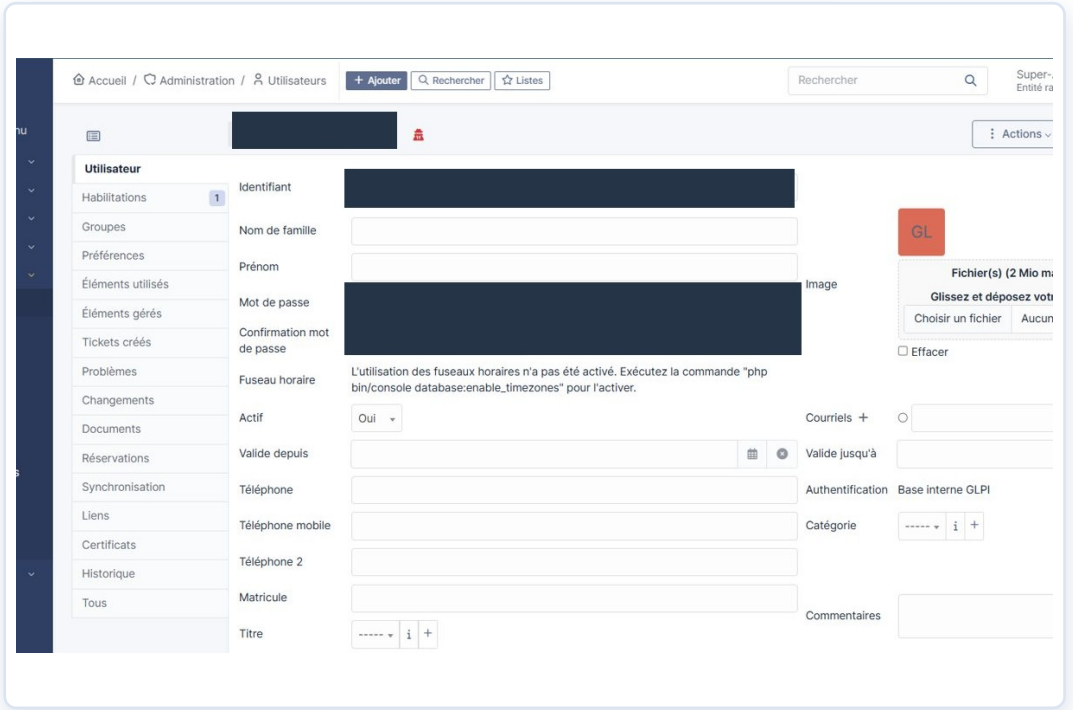
Centre de formation

CONTEXTE & ENJEU

Disposer d’un inventaire fiable du parc et d’un outil de gestion des demandes, base de toute administration sérieuse.

MISE EN ŒUVRE

- Installation du serveur GLPI (interface web sur pile LAMP).
- Déploiement de l’agent GLPI sur les postes (paquet MSI) pour l’inventaire automatique.
- Remontée automatique de l’inventaire matériel et logiciel.
- Gestion des utilisateurs, des droits et des tickets d’assistance.



GLPI — gestion utilisateur, compte et champs masqués

Service rendu Inventaire à jour et support utilisateur outillé.

Patrimoine · Incidents & demandes · Mise à disposition

R12 / R22 — année et dates à confirmer

Fiche source ↗

Commutateur Cisco SF302-08PP

Homelab · hors matrice E5

CONTEXTE & ENJEU

Intégrer et administrer un commutateur managé réel, préparer la segmentation réseau et sécuriser son administration.

MISE EN ŒUVRE

- Prise en main du Cisco SF302-08PP par console série.

Administration SSH : paramètres hérités à encadrer.
Sauvegarde de configuration documentée.
Réseau actuel documenté : WAN → Juniper SRX300 → Cisco.
État des ports et disponibilité non testés dans cette mise à jour.

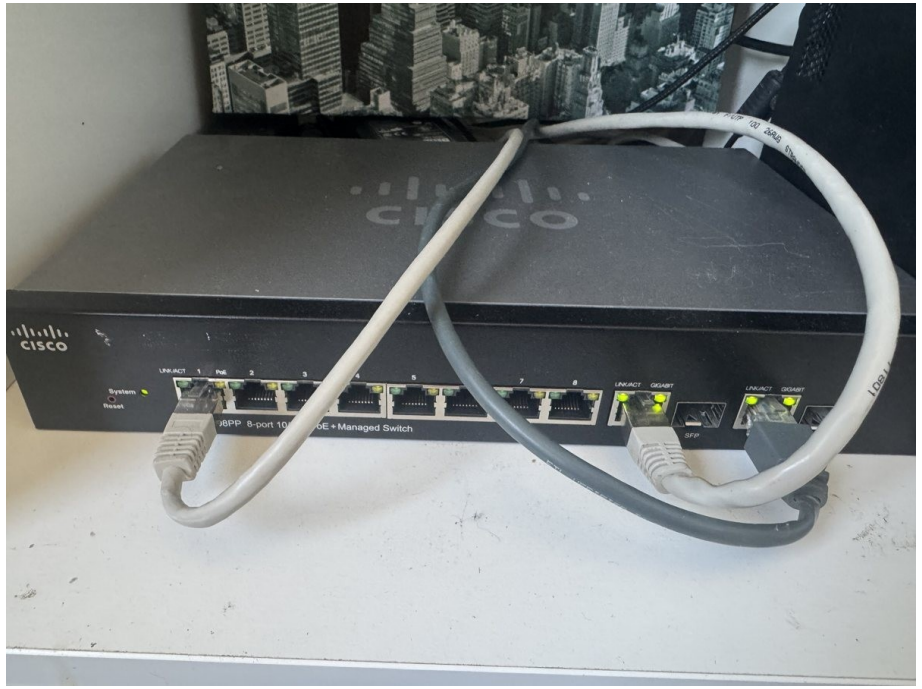


Photo du matériel — ne prouve pas la configuration actuelle

Laboratoire personnel Cisco conservé comme référence réseau, sans validation E5.

PBS : installé sur l'hôte PVE3, sans VM/LXC ; restauration à valider.

Hors matrice E5

Personnel

Détection et prévention d’intrusion — Suricata

Centre de formation

CONTEXTE & ENJEU

Inspecter le trafic réseau en temps réel et bloquer activement les intrusions, et non seulement les signaler.

MISE EN ŒUVRE

- Déploiement de Suricata en mode IPS inline (NFQUEUE) : chaque paquet passe par le moteur avant le réseau.
- Intégration des jeux de règles Emerging Threats (signatures à jour).
- Blocage (drop) des scans et flux malveillants détectés.
- Journalisation structurée (EVE JSON) exploitable pour l’analyse.

CONTRÔLES À DOCUMENTER

Mode inline / NFQUEUE
Chargement des règles
Test de blocage et journal EVE

Aucune sortie exécutée reproduite.
Homelab : prévu, non déployé.

Service rendu Filtrage actif des intrusions au niveau du réseau.

Mise à disposition

R13 — année et dates à confirmer

Fiche source ↗

Serveur DNS et filtrage de domaines — BIND9 + RPZ

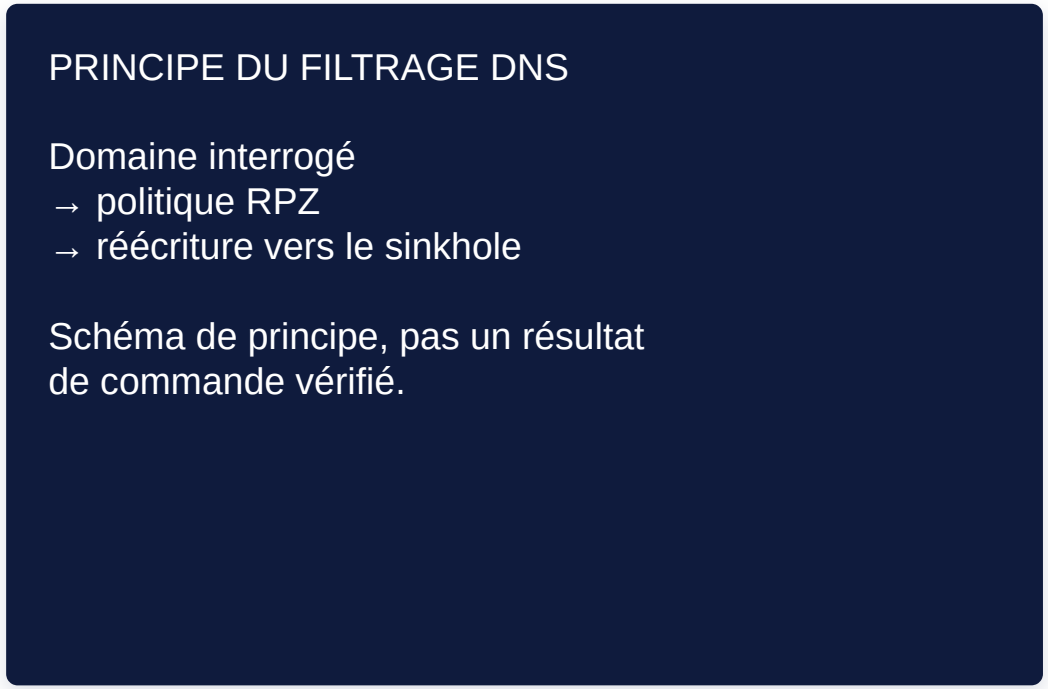
Centre de formation

CONTEXTE & ENJEU

Maîtriser la résolution DNS interne et bloquer les domaines malveillants directement à la résolution.

MISE EN ŒUVRE

- Mise en place d'un serveur DNS d'entreprise BIND9 (zones internes).
- Configuration de zones RPZ (Response Policy Zones) pour le filtrage.
- Alimentation par des flux de threat intelligence (URLhaus, ThreatFox).
- Redirection (sinkhole) des domaines dangereux vers une adresse de contrôle.



Service rendu Blocage préventif des domaines malveillants, dès la résolution.

Mise à disposition

R09 — année et dates à confirmer

Fiche source ↗

Détection comportementale et blocage d’IP — CrowdSec

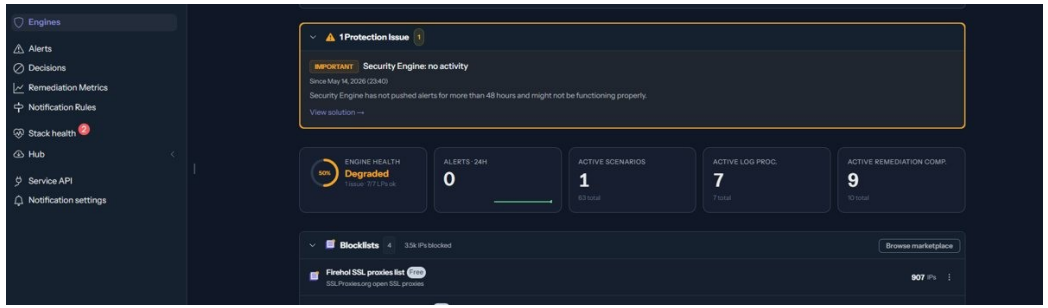
Centre de formation

CONTEXTE & ENJEU

Détecter les comportements hostiles (force brute, scans) et bannir automatiquement les adresses responsables.

MISE EN ŒUVRE

- Installation de CrowdSec et de ses scénarios de détection comportementale.
- Mise en place d’un bouncer nftables qui applique les décisions de blocage.
- Bénéfice de la blocklist communautaire (renseignement partagé).
- Suivi des alertes, décisions et état des moteurs depuis la console.



Archive CrowdSec : état dégradé, aucune activité depuis plus de 48 h

Service rendu Réponse automatisée et continue aux attaques répétées.

Mise à disposition

R14 — année et dates à confirmer

Fiche source ↗

Centralisation des journaux (HIDS) — Wazuh

Centre de formation

CONTEXTE & ENJEU

Centraliser les journaux de tous les hôtes, détecter les anomalies et déclencher une réaction automatique.

MISE EN ŒUVRE

- Déploiement du gestionnaire, de l’indexeur et du tableau de bord.

Installation d’agents sur les hôtes surveillés.
Règles de détection et contrôle d’intégrité (FIM).
Réponse active décrite dans la fiche ; efficacité non retestée ici.

POINTS DE CONTRÔLE

Manager, indexeur, tableau de bord
Enrôlement des agents
Remontée des événements
Contrôle d’intégrité

Pas de liste d’agents attestée ici.

Service rendu Surveillance et réponse de sécurité centralisées.

Mise à disposition

R15 — année et dates à confirmer

Fiche source ↗

Supervision de l’infrastructure — Zabbix

Centre de formation

CONTEXTE & ENJEU

Superviser en continu la disponibilité et la performance de l’infrastructure pour anticiper les pannes.

MISE EN ŒUVRE

- Installation du serveur Zabbix et déploiement des agents (Agent 2) sur les hôtes.
- Application de modèles de supervision (CPU, mémoire, disque, services).
- Définition de seuils, de déclencheurs et d’alertes.
- Tableaux de bord de disponibilité et historisation des métriques.

POINTS DE CONTRÔLE

Disponibilité des hôtes
CPU, mémoire et disques
Seuils et déclencheurs
Réception des alertes

Aucune métrique actuelle reproduite.

Service rendu Supervision proactive : détection des dérives avant l’incident.

Patrimoine · Mise à disposition

R16 — année et dates à confirmer

Fiche source ↗

Automatisation du déploiement — Ansible

Centre de formation

CONTEXTE & ENJEU

Automatiser le déploiement des agents et des configurations pour gagner en rapidité et en fiabilité.

MISE EN ŒUVRE

- Mise en place d'un nœud de contrôle Ansible (inventaire et playbooks).
- Déploiement automatisé et idempotent des agents (supervision, sécurité).
- Configurations reproductibles, versionnées et documentées.
- Journalisation des exécutions pour la traçabilité.

DÉMARCHE DOCUMENTÉE

Inventaire → rôles → playbooks
Test sur environnement de développement
Contrôle d'idempotence
Versionnement

Pas de compte rendu exécuté ici.
Homelab : Ansible prévu.

Service visé Déploiements reproductibles ; les erreurs restent à contrôler.

Mise à disposition

R17 — année et dates à confirmer

Fiche source ↗

Bastion d’accès sécurisé — Apache Guacamole

Centre de formation

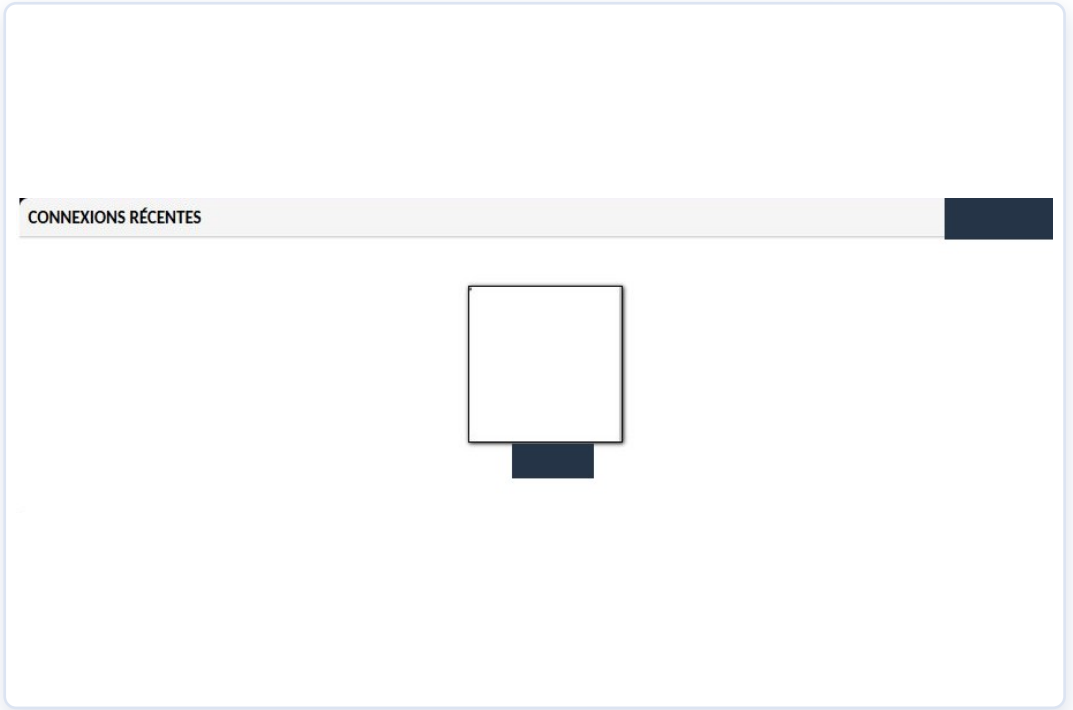
CONTEXTE & ENJEU

Centraliser et sécuriser les accès d’administration via un point d’entrée unique, tracé et sans client à installer.

MISE EN ŒUVRE

- Guacamole derrière un reverse proxy HTTPS.

Connexions SSH/RDP et gestion des utilisateurs/groupes.
Restriction SSH au bastion par filtrage nftables.
Journalisation des sessions décrite dans la fiche.



Archive du portail, informations internes masquées ; pas de session testée

Service rendu Point d’accès unique, sécurisé et auditable pour l’administration.

Patrimoine · Mise à disposition

R18 — année et dates à confirmer

Fiche source ↗

Entreprise

Réalisations en entreprise — alternance

Support dans la distribution automobile ; données anonymisées.
R27 : contrôle des interfaces d’impression uniFLOW.
R28 : mise à jour des certificats logiciel métier.
Année et dates de chaque intervention à confirmer.

Migration de poste

SharePoint / OneDrive

Logiciels métier

Migration de poste utilisateur

Entreprise — alternance

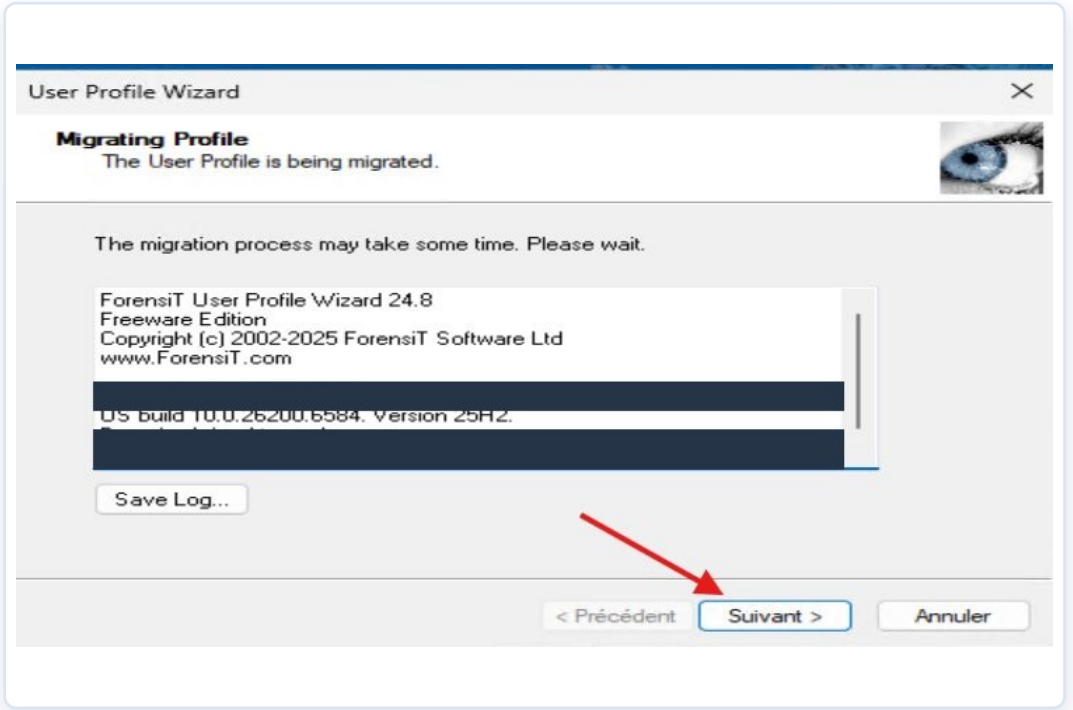
CONTEXTE & ENJEU

Remplacer le poste d'un utilisateur sans interrompre son activité ni perdre ses données et son environnement de travail.

MISE EN ŒUVRE

- Inventaire préalable des logiciels, périphériques et lecteurs réseau.

Sauvegarde des données, du profil et des favoris.
Préparation du poste, jonction au domaine et migration du profil.
Réinstallation des applications puis recette avec l'utilisateur.



Migration en cours — noms internes masqués ; pas une preuve de recette

Service rendu Continuité de travail préservée et transition transparente.

Patrimoine · Incidents & demandes · Mise à disposition

R19 — année et dates à confirmer

Fiche source ↗

Espaces collaboratifs SharePoint / OneDrive

Entreprise — alternance

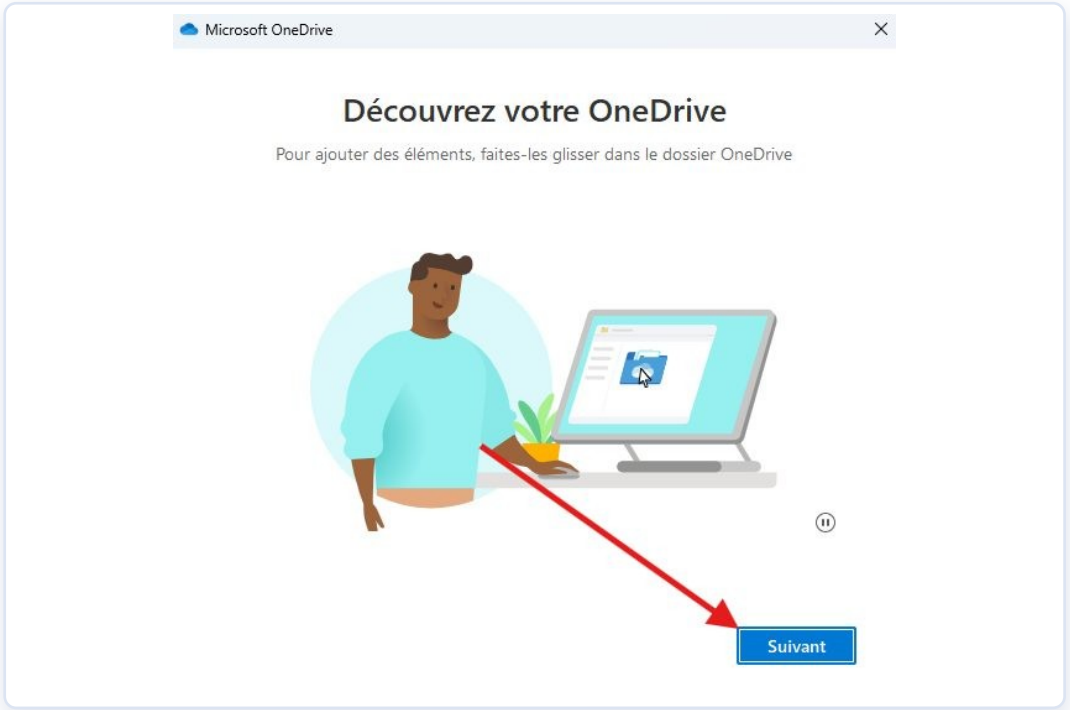
CONTEXTE & ENJEU

Faciliter le travail collaboratif et garantir un accès fiable aux fichiers d'équipe depuis n'importe quel poste.

MISE EN ŒUVRE

- Vérification de la connexion OneDrive sur le poste.

Ajout de raccourcis vers les bibliothèques SharePoint d'équipe.
Contrôle de la synchronisation des fichiers.
Résolution des incidents et accompagnement des utilisateurs.



Écran d'accueil OneDrive — ne démontre pas la synchronisation

Service rendu Accès simple, synchronisé et fiable aux fichiers partagés.

Incidents & demandes · Mise à disposition

R20 — année et dates à confirmer

Fiche source ↗

Déploiement de logiciels métier

Entreprise — alternance

CONTEXTE & ENJEU

Mettre à disposition des équipes après-vente / atelier les applications métier nécessaires à leur activité quotidienne.

MISE EN ŒUVRE

- Installation des applications après-vente et atelier.

Configuration des accès et des synchronisations.
Paramétrage DMS, comptes et droits par profil métier.
Recette avec un référent métier avant mise en production.

Déroulé de l'intervention

Installation des applications métier

Configuration des accès / synchronisation

DMS, comptes et droits par profil

Recette avec un référent métier

Service rendu Outils métier opérationnels et fiables pour les équipes.

Patrimoine · Incidents & demandes · Mise à disposition

R21 — année et dates à confirmer

Fiche source ↗

Tableau de synthèse des compétences

Synthèse de travail alignée sur l'Excel vérifié ; format et justificatifs à valider avant dépôt.

Référence / réalisation	Patr.	Incidents	En ligne	Projet	Service	Dév. pro.
R01 · Active Directory — domaine et annuaire	X	—	—	—	X	—
R02 · Stratégies de groupe et partage réseau	X	—	—	—	X	—
R03 · Masterisation et déploiement de postes avec FOG	—	—	—	—	X	—
R04 · VM Windows 10 : installation, sauvegarde et restauration	X	—	—	—	—	—
R06 · Pare-feu pfSense : filtrage et routage	—	—	—	—	X	—
R09 · Filtrage DNS des domaines malveillants — BIND9 et RPZ	—	—	—	—	X	—
R10 · Serveur web WordPress sur pile LAMP	—	—	—	—	X	—
R11 · Bases MariaDB pour le projet GSB	X	—	—	—	X	—
R12 · Inventaire et centre de services avec GLPI	X	X	—	—	X	—
R13 · Détection et prévention d'intrusion avec Suricata	—	—	—	—	X	—
R14 · Blocage comportemental des IP avec CrowdSec	—	—	—	—	X	—
R15 · Centralisation des journaux et SIEM Wazuh	—	—	—	—	X	—
R16 · Supervision de l'infrastructure avec Zabbix	X	—	—	—	X	—
R17 · Automatisation des déploiements avec Ansible	—	—	—	—	X	—
R18 · Bastion d'administration avec Apache Guacamole	X	—	—	—	X	—
R22 · Gestion de parc avec GLPI et son agent	X	—	—	—	X	—
R25 · Création et déploiement d'une stratégie de groupe	—	—	—	—	X	—
R26 · Restauration de données et d'environnement	X	—	—	—	—	—
R19 · Migration d'un poste utilisateur	X	X	—	—	X	—
R20 · Espaces collaboratifs SharePoint et OneDrive	—	X	—	—	X	—
R21 · Déploiement des logiciels métier après-vente et atelier	X	X	—	—	X	—
R27 · Contrôle des interfaces d'impression uniFLOW	X	X	—	—	—	—
R28 · Mise à jour des certificats logiciel métier	X	X	—	—	—	—

Centre : R01–R18, R22, R25, R26 selon les fiches retenues. Entreprise : R19–R21, R27, R28.
Dates et année à confirmer. Homelab exclu ; colonnes sans preuve laissées sans coche.

Une démarche, pas une collection

Des réalisations CFA et entreprise documentées, un laboratoire personnel séparé, et des limites explicites sur les preuves et les dates.

Rigueur

Distinguer une configuration, un test et un fonctionnement démontré.

Documentation

Sources et références conservées ; dates à confirmer avant dépôt.

Laboratoire

PBS sur PVE3 ; Suricata et Ansible prévus. Pas de disponibilité déduite.

Veille

Veille SOC et Threat Intel séparées ; publication automatique suspendue.

Merci de votre attention • https://dpioch.aristeecampus.org