Rapport de Stage

Hugo Bisserier

13/06/2025

7/08/2025

Rapport de stage – Formation professionnelle (Bachelor Informatique)

Étudiant : Hugo Bisserier
Formation : Bachelor Informatique – Ynov Campus Aix-en-Provence
Entreprise d'accueil : S.H.F. Informatique (Marseille)
Maître de stage : Alain Dadourian
Période de stage : du 13 juin 2025 au 7 août 2025
Lieu principal : Marseille (interventions en environnements PME/TPE)
Année académique : 2024–2025

Table des matières

1. Introduction

Ce rapport présente les activités réalisées au sein de S.H.F. Informatique dans le cadre d'un stage de huit semaines en administration systèmes, réseaux et cybersécurité. Les travaux ont porté sur la professionnalisation des pratiques Windows (AD/DNS/DHCP/GPO), la mise en place d'un laboratoire Hyper-V pour sécuriser les changements, la réalisation d'une maquette réseau Fortinet et l'initiation d'une détection d'événements de sécurité via un POC IDS (Suricata/SELKS) en environnement de test. L'approche a privilégié la standardisation, la reproductibilité (procédures, checklists) et une posture de sécurité pragmatique adaptée aux contraintes des PME/TPE.

2. Présentation de S.H.F. Informatique

S.H.F. Informatique est l'enseigne commerciale de la société D. Henri et Fils (SARL), implantée dans le 12e arrondissement de Marseille. L'entreprise intervient depuis plus de trente ans auprès d'une clientèle locale, principalement des PME/TPE, avec un positionnement de proximité et de réactivité.
Les activités couvrent :

- la maintenance et l'infogérance de postes et serveurs Windows ;
- l'administration d'infrastructures (Active Directory, DNS/DHCP, sauvegardes) ;
- l'intégration réseau & télécoms (postes, imprimantes, routeurs, parfois VLAN et Wi-Fi invité) ;
- l'accompagnement sécurité opérationnelle (bonnes pratiques, durcissement) ;
- et, selon les besoins, des projets web (création/développement de sites).
  La taille maîtrisée de la structure favorise une chaîne de décision

courte, une priorisation par tickets et une culture du « simple, fiable, maintenable ».

3. Contexte, périmètre et objectifs pédagogiques

Contexte

La formation met l'accent sur les fondamentaux systèmes/réseaux, la sécurité opérationnelle et la documentation technique. Le stage transpose ces acquis en environnements réels, caractérisés par des parcs hétérogènes, des contraintes horaires et des budgets mesurés.

Périmètre

- Standardisation AD/DNS/DHCP/GPO (méthode pilote puis généralisation).
- Support N1/N2 sur incidents récurrents (imprimantes, profils, lecteurs réseau).
- Hyper-V : laboratoire bac à sable, snapshots et rollback.
- Fortinet : maquette FortiWiFi-60C (adressage, accès admin, tests IP).
- Sécurité : POC SELKS/Suricata (détection élémentaire, rejeu PCAP).
- Documentation : procédures pas-à-pas, checklists, mini-formations internes.

Objectifs pédagogiques

- Construire des baselines techniques et documentaires.
- Réduire la récurrence d'incidents via fiches réflexes.
- Sécuriser les changements grâce à la virtualisation et la réversibilité.
- Démontrer l'intérêt d'une visibilité réseau même minimale (IDS).
- Développer la pédagogie et le transfert de compétences.

4. Gouvernance, référentiels et méthodologie de travail

Méthodologie & pilotage
Organisation en Kanban léger (À faire / En cours / En revue / Terminé), revues hebdomadaires et comptes-rendus synthétiques.

Conduite du changement
Principe Pilote → Généralisation → Retour d'expérience ; validation en laboratoire avant production ; snapshots Hyper-V systématiques et plan de rollback documenté.

Référentiels sécurité
Bonnes pratiques ANSSI (hygiène, durcissement), principes de NIS2 (gouvernance, gestion des risques, notification d'incident), lignes ISO/IEC 27001/27002 (contrôles) et cadre NIST CSF (Identify/Protect/Detect/Respond/Recover).

Documentation
Procédures pas-à-pas versionnées (horodatées), checklists avant/pendant/après, gabarits (modèles d'e-mails utilisateurs, modèle de compte-rendu d'intervention).

5. Environnement technique (systèmes, réseau, sécurité)

- Systèmes : Windows 10/11 ; Windows Server 2019/2022.
- Rôles : Active Directory DS, DNS, DHCP, GPO.
- Virtualisation : Hyper-V (laboratoire cloisonné), snapshots à chaque jalon.
- Réseau : topologies PME (LAN plat ou VLAN limités), routage de base, imprimantes réseau, Wi-Fi invité selon sites.
- Sécurité : durcissement Windows (pare-feu activé, UAC, désactivation SMBv1, politiques MDP/lock), POC IDS (SELKS/Suricata, rejeu PCAP), journaux Windows (Event Viewer).

- Outillage : RSAT, gpresult, Event Viewer, PowerShell, Wireshark/Tcpdump (lab), éditeurs YAML/JSON (Suricata), gestionnaires de mots de passe.

6. Missions réalisées

6.1 Support & maintenance N1/N2

- Triage standard : connectivité (ipconfig, ping, tracert), résolution DNS (A/PTR), lecture des événements (Application/Système), vérification GPO effective (gpresult /r).
- Incidents récurrents :
    - Imprimantes réseau « offline » : tests ICMP, port TCP/IP, pilotes adaptés, redémarrage du spouleur, ré-ajout propre.
    - Profils temporaires : sauvegarde des données, nettoyage des clés SID orphelines, recréation du profil.
    - Lecteurs réseau non mappés : contrôle des scripts GPO (chemins UNC), droits NTFS/partage, disponibilité du partage.
- Livrables : trois fiches réflexes (1 page chacune) et modèles d'e-mails aux utilisateurs (prévention, bonnes pratiques).

6.2 Annuaire, DNS, DHCP et GPO (standardisation)

Active Directory (AD DS)

- Cartographie des OU (séparation Utilisateurs/Ordinateurs), création d'une OU Pilote.
- Hygiène des comptes (inactifs, renommage normalisé, désactivation progressive avant suppression).
- Autorisations selon AG-UDLP à petite échelle (groupes globaux → domaines → permissions).

DNS/DHCP

- Cohérence baux ↔ enregistrements DNS, TTL raisonnables, nettoyage d'entrées obsolètes.
- Réservations pour équipements critiques (imprimantes, bornes, NAS) avec descriptions renseignées.
- Options DHCP alignées (DNS, passerelle, NTP).

GPO (baseline & durcissement)

- Politiques : mots de passe complexes et verrouillage automatique ; pare-feu activé (profils domaine/privé/public) ; UAC actif ; SMBv1 désactivé.
- Scripts de connexion (mappages lecteurs/imprimantes) par groupes.
- Déploiement par OU Pilote, observation sur X jours, extension graduelle ; documentation de l'ordre des liens et procédure de rollback.

6.3 Virtualisation & sauvegardes (Hyper-V)

- Laboratoire composé de VMs Windows Server et clients, isolement complet, instantanés avant/après changements.
- Vérification des plans de sauvegarde existants et tests de restauration fichier sur VM de test (cohérence, ACL).
- Bénéfice : accélération du cycle idée → test → validation et réduction du risque de régression.

6.4 Maquette réseau Fortinet (FortiWiFi-60C)

- Objectif : évaluer un boîtier Fortinet en environnement de test ; valider l'accès d'administration, le routage, le DNS et la supervision des baux.
- Plan d'adressage : LAN 192.168.1.0/24 ; Fortinet .99 (admin), passerelle .1, postes .110 et .111 (IP fixes) ; tests ICMP croisés et contrôle du DHCP Monitor.
- Livrable : fiche d'implantation (interfaces, plan IP, étapes d'accès admin, commandes de test).

6.5 POC IDS en lab (SELKS/Suricata)

- But : démontrer l'intérêt d'une visibilité réseau minimale en PME.
- Mise en œuvre : SELKS en Docker, configuration Suricata (sources de règles), rejeu de PCAP, alertes collectées au format EVE JSON.
- Signatures testées : TLS handshake, utilisation de curl, tentatives de brute force SSH.
- Résultats : tableau d'observations (détections vs bruit) et pistes d'affinage (seuils, sous-réseaux de test, suppression de règles trop bavardes).
- Recommandations : déploiement progressif, port miroir, tuning par itérations, rétention des logs et sauvegardes des configurations.

6.6 Documentation, transferts et sensibilisation

- Procédures : création d'un utilisateur AD, jointure d'un poste au domaine, baseline GPO, réservations DHCP et contrôle DNS.
- Checklists : Avant (snapshot/sauvegarde), Pendant (journaliser), Après (tests de validation, compte-rendu).
- Mini-formations (15–30 min) : lecture Event Viewer, usage de gpresult, symptômes DNS, hygiène de poste.

7. Études de cas techniques (avant → après)

Cas 1 — Normalisation GPO (périmètre pilote)

- Avant : lecteurs non mappés, politiques hétérogènes, héritages peu lisibles.
- Action : OU Pilote, baseline minimaliste, observation X jours, généralisation graduelle.
- Après : baisse sensible des incidents « imprimantes/lecteurs », meilleure lisibilité (ordre des liens, filtrage), rollback documenté.

Cas 2 — Imprimantes réseau "offline"

- Avant : incidents récurrents (pilotes/ports), perte de productivité.
- Action : standardisation des pilotes, ports TCP/IP, script de réinitialisation du spouleur, fiche utilisateur.
- Après : récurrence d'incidents diminuée ; résolution accélérée via fiches réflexes.

Cas 3 — Maquette Fortinet 60C

- Avant : matériel ancien à qualifier, incertitudes sur l'accès admin et le plan IP.
- Action : adressage propre, accès d'administration, tests ICMP croisés, vérification DHCP.
- Après : procédure réutilisable et base pour intégrer des règles de filtrage simples.

Cas 4 — POC IDS (Suricata/SELKS)

- Avant : visibilité réseau limitée dans de petites structures.
- Action : SELKS, signatures ciblées, rejeu PCAP, collecte et tri des alertes.
- Après : détection élémentaire avérée ; plan d'amélioration (tuning, port miroir, rétention).

8. Résultats, indicateurs et apports

- Standardisation : baseline GPO et référentiel de procédures réutilisable.
- Maintenabilité : fiches réflexes et scripts → MTTR réduit sur les incidents récurrents.
- Sécurité : premier jalon IDS (en lab) et sensibilisation à la qualité/centralisation des journaux.
- Transfert : documentation versionnée, checklists et mini-formations favorisant l'autonomie de l'équipe.

9. Difficultés rencontrées et solutions mises en œuvre

1. Parc hétérogène (pilotes, versions) → tableaux de compatibilité, remplacements planifiés, recettes standard.
2. Conflits GPO (héritages multiples) → usage systématique de gpresult /r, clarification de l'ordre des liens, OU Pilote obligatoire.
3. Faux positifs IDS → affinage progressif des signatures et filtres réseaux, seuils d'alerte.
4. Fenêtres d'intervention courtes → snapshots + rollback + communication claire (compte-rendus post-intervention).

10. Conformité & cybersécurité (ANSSI, NIS2, ISO/IEC, NIST CSF)

- Hygiène ANSSI : mots de passe robustes/MFA, patching régulier, moindre privilège, journalisation renforcée, sauvegardes déconnectées, cloisonnement réseau (VLAN), VPN pour accès distants.
- NIS2 : gouvernance et gestion du risque (inventaire, criticité), mesures techniques et organisationnelles, notification d'incident en temps utile, amélioration continue.
- ISO/IEC 27001/27002 : contrôle des accès, cryptographie, sécurité physique/environnementale, exploitation, journaux, continuité d'activité.
- NIST CSF : structuration des pratiques autour d'Identify/Protect/Detect/Respond/Recover.

Mémo cryptographie (opérationnel)

- Symétrique : AES-256, ChaCha20 pour données au repos/en transit.
- Asymétrique : RSA-2048/3072, ECC pour échange de clés et signature.

- Transport : TLS ≥ 1.2 ; gestion/rotation des clés ; exclusion des algorithmes obsolètes.
- Bonnes pratiques : IV non réutilisé, sel correct, coffre à clés (HSM/logiciel chiffré), politique de rotation.

11. Journal de bord synthétique (S1 → S8)

- S1 (13–16 juin) : onboarding, tickets N1/N2, première fiche réflexe (imprimantes).
- S2 (17–23 juin) : cartographie AD/OU, hygiène comptes, revue DNS/DHCP, préparation de la baseline GPO.
- S3 (24–30 juin) : déploiement OU Pilote, scripts de mappage, observation utilisateur.
- S4 (1–7 juillet) : maquette Fortinet 60C (plan IP, accès admin, tests ICMP), fiche d'implantation.
- S5 (8–14 juillet) : Hyper-V (VMs, snapshots), test de restauration fichier, procédure de rollback.
- S6 (15–21 juillet) : SELKS/Suricata en Docker, signatures ciblées, rejeu PCAP, tableau d'observations.
- S7 (22–28 juillet) : consolidation documentaire, mini-formations, tuning GPO et fiches.
- S8 (29 juil. – 7 août) : bilan, recommandations, finalisation des livrables et passation.

12. Conclusion & perspectives

Le stage a permis de passer d'une approche expérimentale à une pratique d'exploitation : procédures fiables, changements testés en laboratoire, réduction de la dette opérationnelle (incidents récurrents) et premiers jalons de sécurité crédibles pour des PME.

À court terme, l'objectif est de poursuivre en alternance sur un périmètre mêlant administration systèmes & réseaux et SecOps (durcissement Windows, journalisation, sauvegardes testées, segmentation, détection). À moyen terme, la trajectoire visée se concentre sur des missions SecOps/Administration Systèmes & Réseaux avec un accent défense : IDS/EDR/SIEM, qualité des journaux, réponse à incident et amélioration continue.

13. Annexes

Annexe A — Procédure : créer un utilisateur AD & joindre un poste au domaine

1. Création utilisateur (ADUC) : nommage prenom.nom, OU *Utilisateurs*, appartenance aux groupes, adresse e-mail si utilisée.
2. Stratégies : vérification de l'héritage GPO (OU cible), scripts de connexion si requis.
3. Jointure poste : DNS pointant vers le DC ; Système > Nom de l'ordinateur > Domaine ; identifiants administrateur de domaine ; redémarrage.
4. Validation : whoami, gpresult /r, accès lecteurs/imprimantes, création du profil.
5. Checklist : entrée DNS correcte, temps d'ouverture de session, appartenance aux groupes, tests de partage.

Annexe B — Baseline GPO (extraits)

- Sécurité : mot de passe (longueur/complexité), verrouillage automatique 10–15 min, pare-feu activé (3 profils), UAC élevé, SMBv1 désactivé.
- Poste : scripts de connexion (mappings), restrictions nécessaires, services obsolètes désactivés si présents.

- Journalisation : élévation de verbosité pour logon/logoff, échecs d'authentification, modifications de comptes.
- Déploiement : OU Pilote → observation → extension ; documentation de l'ordre des liens ; rollback prêt.

Annexe C — DNS/DHCP : bonnes pratiques PME

- DNS : cohérence A/PTR, TTL raisonnables, nettoyage des entrées obsolètes ; clients pointant vers les DNS internes.
- DHCP : plan d'adressage, réservations pour équipements critiques, options (DNS, passerelle, NTP), documentation des baux.

Annexe D — Hyper-V : routine snapshots & rollback

- Avant : snapshot "Pre-Change-YYYYMMDD-HHMM".
- Pendant : journal des actions.
- Après : snapshot "Post-Change-YYYYMMDD-HHMM", tests (authentification, partages, GPO).
- En cas d'anomalie : revert vers Pre-Change + compte-rendu d'incident.

Annexe E — POC SELKS/Suricata (lab)

- Installation : SELKS via Docker ; interface d'écoute dédiée (lab).
- Règles test : TLS handshake, curl, tentatives SSH.
- Contrôles : lecture des événements EVE JSON, tri par sévérité, suppression des règles trop bavardes.
- Limites : déploiement en production conditionné au tuning ; prévoir la rétention et la sauvegarde des configurations.

Annexe F — Maquette Fortinet 60C : fiche d'implantation

- LAN 192.168.1.0/24 ; GW .1 ; Fortinet .99 (admin) ; postes .110/.111 ; DNS local.
- Accès admin : port d'administration, IP d'admin, profils ; tests ICMP/HTTP/SSH.

- Contrôles : DHCP Monitor, tests croisés PC1↔PC2↔Fortinet, résolution DNS.
- Évolution : règles de filtrage simples ; VLAN invité si matériel compatible.

Annexe G — Checklists « Avant / Pendant / Après » intervention

- Avant : périmètre validé, sauvegarde/snapshot, fenêtre de maintenance, point de contact.
- Pendant : journaliser les actions, tests intermédiaires, communication en cas de décalage.
- Après : tests finaux, compte-rendu (changements/risques résiduels), archivage du rollback.

Annexe H — Compte-rendu d'intervention (exemple rempli)

Objet : Normalisation GPO — Site Marseille — 18/07/2025 (09:00–11:30)
Contexte : récurrence d'incidents « lecteurs réseau non mappés » sur plusieurs postes ; héritage GPO peu lisible sur l'OU Ordinateurs ; absence de baseline commune.
Actions réalisées :

1. Sauvegarde des GPO existantes (export).
2. Création d'une OU Pilote et déplacement de deux postes de test.
3. Liaison d'une baseline GPO (verrouillage session, pare-feu activé, scripts de mappage lecteurs, UAC).
4. Forçage et vérification de l'application (gpupdate /force, puis gpresult /r).
5. Ajustement du script de mappage (partage \srv-files\commun en lecteur X: ; \srv-files\metier en Y: par groupe).
6. Tests utilisateurs encadrés (déconnexion/reconnexion, ouverture de session chronométrée).
   Tests & résultats :

- gpresult conforme ; lecteurs X:/Y: présents ; impression réseau valide ; temps d'ouverture de session amélioré (~40 s → ~28 s).
- Événements Windows sans erreurs liées à la stratégie ; absence de réapparition du symptôme sur 48 h.
  Risques résiduels / limites : conflits possibles avec anciens pilotes d'imprimantes sur quelques postes ; besoin d'un déploiement progressif pour éviter une rupture de service.
  Recommandations : généraliser la baseline sur l'OU Ordinateurs par lots de 10 postes ; mettre à jour les pilotes d'impression standard ; réaliser une revue après une semaine ; documenter l'ordre des liens GPO.
  Suivi : revue planifiée au 25/07/2025 ; ouverture du ticket interne SHF-OPS-2025-0718-01 pour le suivi des actions et métriques.

Annexe I — Tableau de risques (exemple PME)

- Perte de journaux (rétention insuffisante) → détection affaiblie → mesures : centraliser, augmenter quotas, sauvegarder.
- Conflits GPO → dérives de configuration → mesures : gpresult, OU pilote, documentation des liens.
- Sauvegardes non testées → restauration incertaine → mesures : tests mensuels, suivi RTO/RPO.
- Postes non patchés → vulnérabilités → mesures : routine WSUS/Windows Update, fenêtres planifiées, suivi de conformité.

Annexe J — Modèles d'e-mails (utilisateurs)

- **Information maintenance** : « Une intervention aura lieu le [date] de [heure] à [heure]. Impact : brève indisponibilité des partages. Contact support : [coordonnées]. »
- **Résolution d'incident** : « Votre incident [référence] est résolu. Actions menées : [liste]. Recommandations : [bonnes pratiques]. »
- **Prévention** : « Rappel sur les mots de passe et la détection d'e-mails suspects : ne cliquez pas sur les pièces jointes inattendues, signalez les messages douteux au support. »

14. Glossaire (termes clés)

ACL : liste de contrôle d'accès (droits appliqués à des objets/fichiers/partages).
AD DS : service d'annuaire Windows (comptes, groupes, machines).
ADUC : console « Active Directory Users and Computers » (gestion des objets AD).
AG-UDLP (AGDLP) : modèle d'autorisations (comptes → groupes globaux → groupes de domaine → permissions).
DHCP : attribution automatique d'adresses IP et d'options réseau aux clients.
DHCP Reservation : association IP/MAC fixe délivrée par le serveur DHCP.
DNS : service de résolution de noms (enregistrements A/PTR/CNAME).
DNS Scavenging : mécanisme de nettoyage des enregistrements obsolètes.
EDR : outil de détection et réponse sur les terminaux (Endpoint Detection & Response).
EVE JSON : format d'export des événements Suricata (journalisation).
FortiWiFi-60C : équipement Fortinet combinant fonctions routeur/pare-feu/Wi-Fi (selon modèle).
GPO : politiques appliquées aux utilisateurs/ordinateurs via Active Directory.
GPO Link Order : ordre d'application des GPO liées à une OU.
GPResult : outil de diagnostic des stratégies effectivement appliquées à une machine/utilisateur.
Hyper-V : hyperviseur Microsoft (machines virtuelles).
IDS/IPS : détection/prévention d'intrusions réseau.
IPAM : gestion des plans d'adressage IP et allocations.
Kerberos / NTLM : protocoles d'authentification en environnement Windows (Kerberos recommandé).
MFA : authentification multifacteur.
NAT : translation d'adresses réseau entre réseaux internes et externes.
NIS2 : directive européenne renforçant les exigences cybersécurité.

NIST CSF : cadre de cybersécurité (Identify/Protect/Detect/Respond/Recover).
NTP : synchronisation de l'heure sur le réseau.
OU (Organisation Unit) : conteneur logique AD pour structurer et déléguer.
PCAP : capture de paquets réseau pour analyse.
RDP : protocole d'accès distant à un bureau Windows.
RPO/RTO : objectifs de perte de données et de reprise (continuity/disaster recovery).
RSAT : outils d'administration à distance pour les rôles Windows Server.
SELKS : distribution intégrant Suricata et une suite d'analyse (ELK).
SIEM : plateforme de collecte/corrélation des événements de sécurité.
Snapshot/Checkpoint : cliché instantané d'une VM (retour arrière possible).
Spooler : service de gestion des files d'impression Windows.
Suricata : moteur de détection d'intrusions réseau (signatures/flux).
Syslog : protocole standard d'export de journaux.
TLS 1.2/1.3 : protocoles de sécurisation des communications.
UAC : contrôle de compte utilisateur (élévation des privilèges).
VLAN : segmentation logique du réseau.
WMI Filtering : ciblage conditionnel des GPO selon caractéristiques des machines.
WSUS : service de mise à jour Windows en entreprise.
ZTNA : approche « Zero Trust Network Access » (accès fondé sur l'identité et le contexte).