Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ
DE L'EMPLOI

DOSSIER PROFESSIONNEL (DP)

Nom de naissance ▸ Dif
Nom d'usage ▸ Dif
Prénom ▸ Meihdi
Adresse ▸ 129 Rue de la Granière
13011 Marseille

Titre professionnel visé

Cliquez ici pour entrer l'intitulé du titre professionnel visé.

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

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 — Administrer et sécuriser les infrastructures

Exemple n°1 ▸ Mise en place d'un serveur PXE avec intégration Active Directory

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

Dans le cadre d'un projet encadré par l'école, j'ai déployé une solution complète permettant le démarrage réseau (PXE) de postes clients, leur installation automatique de Windows 10 via une image personnalisée, puis leur intégration dans un domaine Active Directory.

J'ai effectué toutes les manipulations sur une machine virtuelle Windows Server.

Les principales tâches réalisées :

- Installation et configuration des rôles : DHCP, DNS, ADDS, WDS (PXE)
- Promotion du contrôleur de domaine et création d'un utilisateur test
- Configuration d'une image d'installation Windows 10 (conversion install.esd → install.wim)
- Intégration des fichiers boot.wim et install.wim dans WDS
- Tests de démarrage réseau d'un poste client sans OS
- Vérification de l'intégrité de l'image .wim via CertUtil (SHA256)

Création de deux scripts :

- Script PowerShell de configuration automatique du DNS client
- Script .bat utilisant netdom pour intégrer automatiquement le poste au domaine

2. Précisez les moyens utilisés :

Machine virtuelle Windows Server 2019

Windows ADK (Assessment and Deployment Kit)

Rôles Windows : WDS, DHCP, DNS, ADDS

ISO Windows 10 pour les fichiers WIM

PowerShell et Batch pour les scripts d'automatisation

Hyper-V pour le poste client à déployer

CertUtil pour le hachage SHA-256

Interfaces graphiques + netsh, netdom, dism

3. Avec qui avez-vous travaillé ?

Projet individuel réalisé sous la supervision de l'équipe pédagogique.
J'ai également échangé avec mes camarades pour comparer les méthodes d'intégration automatique au domaine.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Déploiement automatisé**

Période d'exercice ▸ **Du 11/03/2024 au 15/03/2024**

5. Informations complémentaires *(facultatif)*

J’ai documenté le projet dans un fichier Markdown et fourni une démonstration à l’oral.

Ce projet m’a permis d’approfondir l’automatisation Windows via PowerShell et d’anticiper des déploiements en entreprise.

Activité-type 1 — Administrer et sécuriser les infrastructures

Exemple n°2 ▸ Sécurisation d'un serveur Linux avec Fail2Ban et iptables

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

Suite à un incident fictif dans une entreprise simulée, où un administrateur aurait effacé la configuration du pare-feu, j'ai été chargé de restaurer la sécurité réseau d'un serveur Linux.

Le projet s'est déroulé dans une VM Debian en environnement de test, avant déploiement sur l'infrastructure réelle.

Les opérations réalisées :

- Reprise complète de la configuration iptables :
  - Suppression des anciennes règles (flush)
  - Réécriture des règles : SSH restreint à une IP, FTP autorisé localement, services non essentiels bloqués
- Création d'un script de configuration automatique pour appliquer les règles à chaque redémarrage
- Intégration de Fail2Ban comme IPS pour protéger l'accès SSH contre les attaques par force brute
- Mise en place de la surveillance des logs avec Logwatch
  - Génération automatique d'un rapport quotidien via crontab
  - Surveillance ciblée des services sensibles (SSH, FTP)
- Tests fonctionnels : blocage/autorisation IPs, bannissement automatique, visualisation du statut Fail2Ban

2. Précisez les moyens utilisés :

- Système : Debian sans interface graphique
- Outils :
  - iptables, iptables-save
  - fail2ban, logwatch
  - crontab, bash
- Scripts :
  - /etc/iptables/iptables-save.sh
  - generation_rapport.sh pour automatisation Logwatch
  - jail.local personnalisé pour SSH
- Journalisation dans /var/log + extraction et vérification avec fail2ban-client

3. Avec qui avez-vous travaillé ?

Projet individuel réalisé sous la supervision de l'équipe pédagogique.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Reconfiguration pare-feu + automatisation de sécurité**

Période d'exercice ▸ **Du 08/04/2024 au 12/04/2024**

5. Informations complémentaires *(facultatif)*

Le projet a été réalisé en condition simulée mais réaliste (post-incident).

L'approche a été sécuritaire, automatisée et documentée.

J'ai mis en place une logique complète IPS + surveillance + redondance.

Activité-type 1 — Administrer et sécuriser les infrastructures

Exemple n°3 ▸ ***Mise en place d'un annuaire LDAP centralisé avec gestion des utilisateurs et services réseau***

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

Dans le cadre de ma formation, j'ai mis en place une infrastructure d'authentification centralisée basée sur LDAP.
Ce projet visait à faciliter la gestion des comptes utilisateurs au sein d'une infrastructure réseau, tout en assurant la sécurité et la cohérence des accès.

Les opérations réalisées :

- Installation et configuration d'un serveur LDAP sur Debian
- Création d'une arborescence hiérarchique LDIF personnalisée pour l'entreprise
- Ajout de plusieurs comptes utilisateurs et groupes (service compta, RH, etc.)
- Configuration du service DNS interne pour résolution des clients LDAP
- Intégration de la base LDAP avec PAM pour l'authentification locale des utilisateurs Linux
- Test de connexion de comptes LDAP sur plusieurs machines
- Déploiement d'une interface graphique LAM (LDAP Account Manager) pour faciliter la gestion
- Configuration du service DHCP pour attribution d'adresses IP cohérentes avec les noms LDAP

2. Précisez les moyens utilisés :

Système Debian

Outils :

- slapd, ldap-utils
- LAM (interface Web)
- bind9, isc-dhcp-server
- libnss-ldap, libpam-ldap

Scripts et fichiers LDIF personnalisés

Commandes ldapadd, ldapsearch, getent passwd

3. Avec qui avez-vous travaillé ?

Projet réalisé individuellement, avec relecture des configurations par un encadrant technique.

Les tests d'accès LDAP ont été réalisés en local sur différentes VM Linux.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Annuaire LDAP et infrastructure centralisée**

Période d'exercice ▸ **Du 12/02/2024 au 16/02/2024**

5. Informations complémentaires *(facultatif)*

Le projet m'a permis de comprendre le lien entre DNS, DHCP et LDAP dans une architecture réseau.

L'authentification centralisée via PAM renforce la sécurité et simplifie la gestion des accès.

L'arborescence LDIF a été conçue pour être évolutive et facilement exploitable par des scripts.

Activité-type 2 — Concevoir et mettre en œuvre une solution technique

Exemple n°1 ▸ Conception et déploiement d'une infrastructure sécurisée pour TechSecure

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

Dans le cadre d'un projet pédagogique avancé, j'ai réalisé une mission d'audit et de remédiation complète pour la PME fictive TechSecure, spécialisée en cybersécurité.
L'objectif était de concevoir une nouvelle infrastructure sécurisée, capable de répondre aux exigences de confidentialité, de résilience et de conformité réglementaire.

Les principales tâches menées :

Analyse de l'existant

- Étude de l'architecture actuelle : 6 VLANs, DMZ, MySQL, AD/DNS, VPN, etc.
- Détection de failles : VLANs mal cloisonnés, DMZ non protégée, base ouverte, logs absents…

Évaluation des risques

- Construction d'une matrice de risques complète (type de menace, impact, probabilité, type d'attaquant)
- Identification des vulnérabilités critiques : mauvaise segmentation, absence de supervision, mots de passe faibles…

Plan de remédiation

- Refonte de l'architecture :
  - Segmentation stricte des VLANs
  - Bastion d'administration Wallix
  - Double pare-feu FortiGate en haute disponibilité
  - Intégration de Cisco ISE pour l'accès réseau (802.1X, RADIUS, TACACS+)
- Mise en place d'une supervision centralisée via SIEM (Wazuh / ELK) et EDR/XDR
- Authentification forte (MFA) pour le VPN, le bastion, et les accès critiques

Conception d'un plan de continuité et PRA

- RTO < 4h, RPO < 15 min
- Sauvegardes locales + cloud via Veeam, chiffrées, testées mensuellement

- Procédures de restauration documentées (VM, bases, fichiers)
- Guide papier et numérique stocké hors réseau

Alignement avec les normes

- ISO 27001 : cloisonnement, journaux, MFA, sauvegarde
- RGPD : conservation limitée, traçabilité, bastion Wallix
- NIST CSF : Identify, Protect, Detect, Respond, Recover
- ANSSI : segmentation, gestion des incidents, sauvegardes hors ligne

Menace	Description	Note	Type d'attaquant	Probabilité	Impact	Risque global	Probabilité (Score)	# Impact (Score)	Score de Risque
Phishing	Courant, souvent automatisé ou lancé par des attaquants peu qualifiés.	C	Opportuniste / Externe	Élevée	Modéré	Moyen	5	2	10
Ransomware	Peut être lancé de manière opportuniste, mais les variantes modernes sont très ciblées.	B	Externe / Sophistiqué	Moyenne	Critique	Élevé	3	5	15
Attaque DDoS	Typiquement lancé de l'extérieur pour perturber la disponibilité.	D	Externe	Faible	Modéré	Faible	1	2	2
Mauvaise segmentation des VLANs	Exploité via un mouvement latéral après compromission interne.	A	Interne / Sophistiqué	Élevée	Critique	Élevé	5	5	25
Accès non sécurisé au Wi-Fi	Facile à exploiter à proximité (Wi-Fi ouvert ou mal protégé).	C	Opportuniste / Interne	Moyenne	Modéré	Moyen	3	2	6
Exposition des services de la DMZ	Point d'entrée direct depuis Internet.	A	Externe / Sophistiqué	Élevée	Critique	Élevé	5	5	25
Accès non restreint aux bases de données	Exploitable depuis l'intérieur ou via une escalade de privilèges.	B	Interne / Sophistiqué	Moyenne	Élevé	Élevé	3	4	12
Règles de pare-feu trop permissives	Facilite les déplacements latéraux ou l'exfiltration après compromission.	A	Interne / Sophistiqué	Élevée	Critique	Élevé	5	5	25
Absence de monitoring et logs centralisés	Rend difficile la détection d'abus internes ou externes.	B	Opportuniste / Interne	Moyenne	Élevé	Élevé	3	4	12
Failles dans les comptes administrateurs	Exploitable par erreur ou attaque ciblée.	B	Interne / Opportuniste / Sophistiqué	Moyenne	Critique	Élevé	3	5	15
Absence de plan de sauvegarde testé	Faute de l'organisation, aggravent l'impact d'un incident.	B	Interne / Opportuniste	Moyenne	Critique	Élevé	3	5	15
Mauvaise configuration des permissions Cloud	Très ciblé mais parfois causé par erreur humaine.	A	Sophistiqué / Opportuniste	Élevée	Critique	Élevé	5	5	25
Exposition de données sensibles sur le Cloud	Accès direct via erreurs de config ou attaques ciblées.	A	Externe / Sophistiqué	Élevée	Critique	Élevé	5	5	25
Absence de chiffrement des données stockées	Rend les données accessibles à tout utilisateur ou attaquant interne.	B	Interne / Opportuniste	Moyenne	Élevé	Élevé	3	4	12
Absence de journalisation et de monitoring Cloud	Difficulté à tracer les actions suspectes.	B	Opportuniste / Interne	Moyenne	Élevé	Élevé	3	4	12
Utilisation d'identifiants faibles ou partagés	Exploitable par n'importe quel attaquant avec peu de moyens.	A	Opportuniste	Élevée	Critique	Élevé	5	5	25
Manque de segmentation entre ressources Cloud	Permet une attaque latérale dans des environnements cloud.	B	Sophistiqué	Moyenne	Critique	Élevé	3	5	15
Absence de sauvegarde hors-ligne des données Cloud	Conséquence de mauvaise	B	Interne	Moyenne	Critique	Élevé	3	5	15

Légende
25 =< A < 15
15 =< B < 10
10 =< C < 5
5 =< D < 0

1. Plan d'adressage IP (extrait)

VLAN	Nom	Adresse réseau	Plage DHCP / IP fixe
10	Admin	10.0.10.0/24	10.0.10.100 – 10.0.10.200
20	Développement	10.0.20.0/24	10.0.20.100 – 10.0.20.200
30	Commercial	10.0.30.0/24	10.0.30.100 – 10.0.30.200
40	Serveurs	10.0.40.0/24	IP fixes
99	Management	10.0.99.0/24	IP fixes
50	DMZ	192.168.50.0/24	IP fixes

2. Affectation des ports (switch)

- VLAN 10 : Ports 1–5 (Postes Admin)
- VLAN 20 : Ports 6–10 (Postes Dev)
- VLAN 30 : Ports 11–15 (Postes Commerciaux et Wi-Fi)
- VLAN 40 : Ports 16–18 (Serveurs internes)
- VLAN 99 : Ports 19–20 (Gestion)
- Trunk entre switch L3 et pare-feu : Port 24

3. Configuration pare-feu ASA / FortiGate (exemple résumé)

- ACL inter-VLAN : uniquement les flux nécessaires sont autorisés
  - VLAN 10 peut accéder à VLAN 40 (gestion serveurs)
  - VLAN 20 accès restreint à MySQL (port 3306)
  - VLAN 30 interdit d'accéder à VLAN 10 ou 40
- NAT DMZ → Internet activé uniquement pour Web / Mail
- VPN SSL avec MFA pour administrateurs distants

4. Configuration du bastion Wallix

- Authentification centralisée via ISE (RADIUS / TACACS+)
- MFA obligatoire pour tous les accès
- Enregistrement des sessions et des commandes exécutées

5. Configuration Cisco ISE / Authentification

- Affectation dynamique aux VLANs via 802.1X
- Profils utilisateurs : Admin / Utilisateur / Invité
- Intégration AD pour les comptes nominatifs

6. Configuration SIEM / EDR

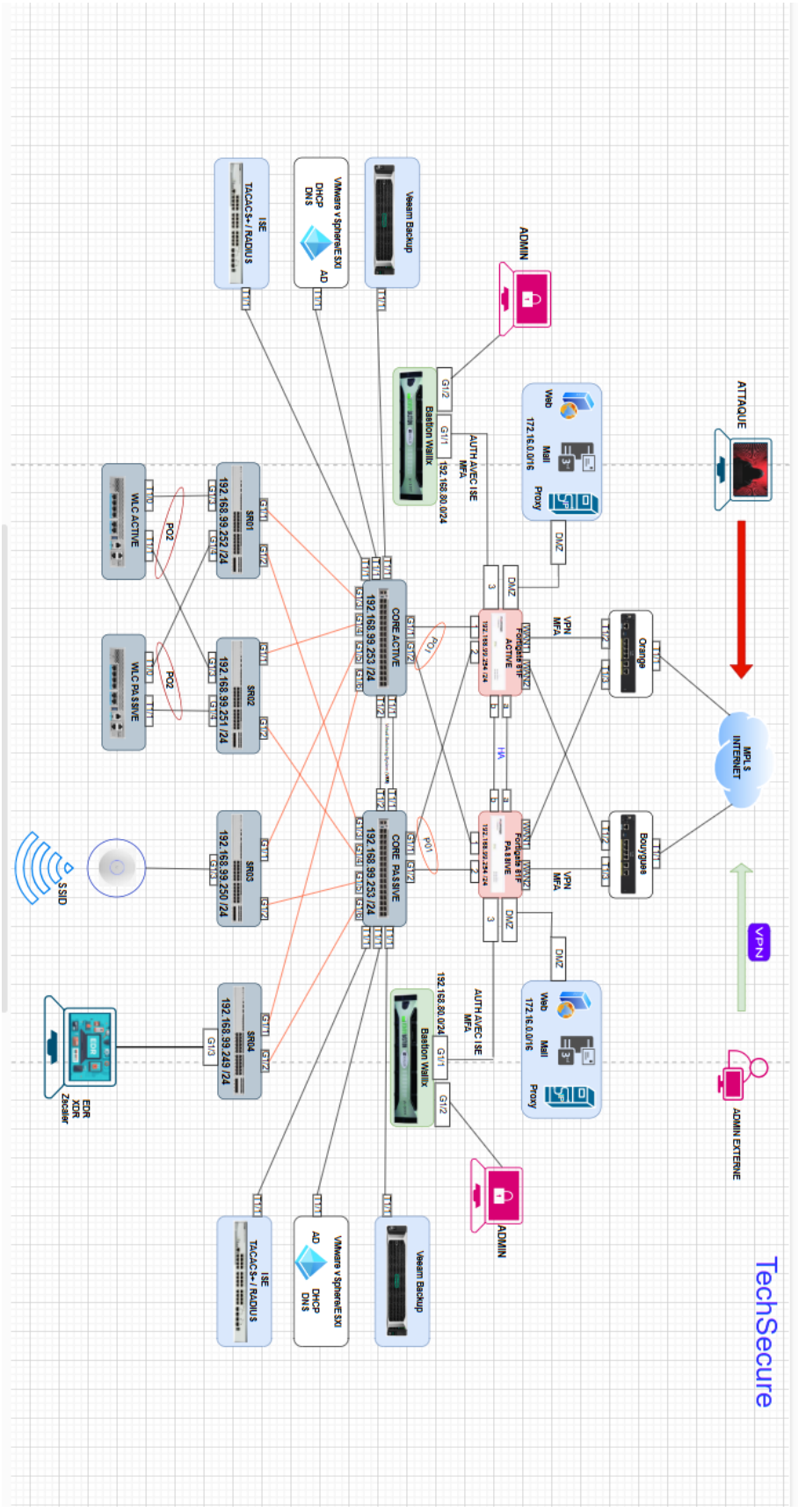
- Collecte des logs : FortiGate, Wallix, AD, Switchs, ISE
- Envoi vers serveur SIEM (ex : Wazuh / ELK)
- Déploiement EDR/XDR sur postes sensibles (Admin, Dev)

7. Sauvegarde et PRA

- Sauvegardes chiffrées via Veeam Backup (local + cloud)
- Test mensuel de restauration
- Accès sécurisé aux sauvegardes depuis VLAN 99 uniquement

8. Interfaces de management

- Accès uniquement depuis VLAN 99
- Interfaces Web désactivées si possible, accès SSH restreint par ACL
- Journalisation de toutes les connexions sur SIEM


ISE
TACACS+ / RADIUS
VMware V SphereE.SXI
DHCP
DNS
AD
Veeam Backup
ADMIN
Bastion Wallix
AUTH AVEC ISE
MFA
Web
Mail
Proxy
DMZ
ATTAQUE
WLC ACTIVE
WLC PASSIVE
SR01
SR02
SR03
SR04
CORE ACTIVE
CORE PASSIVE
Fortigate HA
ACTIVE
PASSIVE
VPN
MFA
Orange
Bouygues
MPLS
INTERNET
SSID
EDR
XDR
Zbctler
ADMIN EXTERNE
TechSecure

2. Précisez les moyens utilisés :

Logiciels :

- PowerPoint (présentation audit)
- Google Sheets (matrice des risques)
- Obsidian (documentation structurée)
- Veeam (sauvegarde / restauration)
- Outils simulés : Cisco ASA, ISE, FortiGate, Wallix, Wazuh

Ressources :

- Configuration réseau en annexe
- Schéma d'architecture cible
- Éléments d'analyse (rapport PDF, slides, configuration)

3. Avec qui avez-vous travaillé ?

Projet réalisé en trinôme.
J'ai personnellement rédigé les parties suivantes :

- Contexte, analyse de l'existant, matrice des risques
- Alignement normatif (RGPD, ISO, NIST, ANSSI)
- Conclusion générale et présentation orale du livrable

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Audit sécurité + Refonte architecture TechSecure**

Période d'exercice ▸ **Du 19/05/2025 au 19/05/2025**

5. Informations complémentaires *(facultatif)*

L'analyse complète a été restituée à l'oral avec un support PowerPoint

La documentation est disponible en markdown, PDF, présentation et schémas en annexe.

Activité-type 2 — Concevoir et mettre en œuvre une solution technique

Exemple n°2 ▸ *Mise en place d'un réseau Wi-Fi sécurisé avec analyse de trames*

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

Ce projet visait à étudier en profondeur les aspects techniques et sécuritaires du Wi-Fi dans un environnement professionnel.
L'objectif était double :

- Mettre en place des environnements Wi-Fi sécurisés (WPA2, WPA3, transition)
- Capturer et analyser les trames échangées pendant les différentes phases de connexion

Les opérations réalisées :

- Recherche technique sur les normes Wi-Fi : IEEE 802.11 (b/g/n/ac/ax/be), bandes de fréquence (2.4/5/6 GHz), architecture client-serveur vs Ad-Hoc
- Étude comparative des sécurités Wi-Fi : WEP (obsolète), WPA2-PSK, WPA3-Personal (SAE), WPA3-Enterprise (EAP-TLS)
- Captures de trafic avec Wireshark :
    - dot11-sample.pcap (WPA2)
    - wpa3.pcapng (WPA3)
    - transition WPA2/WPA3, Mist 6GHz, Nokia mobile…
- Analyse fine des trames :
    - Beacon, Probe Request/Response
    - Authentication, Association
    - EAPOL : 4-Way Handshake complet
    - Deauthentication volontaire ou forcée
- Identification des menaces :
    - Capture de handshake
    - Attaques Deauth
    - Rogue AP, Evil Twin, KRACK…

2. Précisez les moyens utilisés :

Logiciels :

- Wireshark
- Airodump-ng, Airtool (pour captures en monitor mode)
- Obsidian (rédaction), PDF pour rendu

Matériel :

- Carte Wi-Fi compatible monitor mode
- Environnements de test (réseaux WPA2, WPA3, AP Mist sur 6 GHz)

Fichiers analysés :

- dot11-sample.pcap, wpa3.pcapng, mistap-5-6ghz.pcapng, etc.

dot11-sample.pcap
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
wlan.fc.type_subtype == 8 || wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5 || wlan.fc.type_subtype == 1 || eapol || wlan.fc.type_subtype == 12
Ajuster les colonnes de la liste des paquets au contenu
No. Time Source Destination Protocol Length Info
Frame 1: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ....
IEEE 802.11 Wireless Management
dot11-sample.pcap
Paquets : 227 · Affichés : 166 (73.1%)
Profil : Default

3. Avec qui avez-vous travaillé ?

Projet réalisé en autonomie dans le cadre de la formation.
Des échanges ont été menés avec d'autres étudiants pour comparer les captures et outils utilisés.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Sécurité réseau Wi-Fi & Analyse de trames**

Période d'exercice ▸ **Du 16/06/2025 au 20/06/2025**

5. Informations complémentaires *(facultatif)*

Les captures ont permis de visualiser des connexions réelles sur des réseaux modernes (WPA3, Wi-Fi 6E)

L'analyse de trames apporte une compréhension pratique du fonctionnement Wi-Fi et de ses failles potentielles (annexe en fin de dossier)

Ce projet est très utile pour anticiper des attaques sans fil ou auditer la robustesse d'un réseau d'entreprise

Activité-type 2 — Concevoir et mettre en œuvre une solution technique

Exemple n°3 ▸ ***Conception et sécurisation d'une maquette réseau avec redondance, HSRP et VLANs segmentés***

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

Dans le cadre d'un projet de fin de formation encadré par un formateur, j'ai conçu et déployé une infrastructure réseau physique sur équipements Cisco Catalyst. Ce projet simulait un environnement d'entreprise réparti sur deux bâtiments, avec des VLANs isolés, une redondance de cœur réseau, et une haute disponibilité via HSRP.

L'objectif était de construire une maquette représentative d'une architecture LAN professionnelle, avec redondance de l'interconnexion, gestion de la segmentation réseau et sécurisation des accès.

Travail réalisé :

Conception logique du réseau

- Élaboration d'un plan d'adressage IPv4 en /24
- Définition de 4 VLANs :
  - VLAN 10/20 pour l'entreprise A (bâtiment A)
  - VLAN 30/40 pour l'entreprise B (bâtiment B)
- Identification des liens critiques et des chemins de secours

Configuration des VLANs et du routage inter-VLAN

- Création des VLANs sur les switches
- Attribution des interfaces aux bons VLANs
- Activation du routage via ip routing
- Routage inter-VLAN implémenté localement sur les switches de cœur

Mise en place de la redondance

- Lien d'interconnexion via Port-Channel (agrégation de liens)
- Redondance de cœur réseau assurée par deux switches configurés en HSRP
- Attributions HSRP :
  - Switch 1 maître pour VLAN 10/20
  - Switch 2 maître pour VLAN 30/40

- Utilisation de standby, priority, preempt, show standby

Sécurisation des accès

- Activation du SSH version 2 uniquement sur les VLANs de gestion
- Mise en place d'ACLs pour limiter l'accès SSH à certaines IPs
- Désactivation des interfaces inutilisées via shutdown
- Protection Spanning Tree :
    - spanning-tree portfast
    - spanning-tree bpduguard enable sur les ports d'accès

Tests et vérifications

- Test de ping inter-VLAN
- Simulation de panne d'un switch cœur : basculement observé vers le routeur HSRP secondaire
- Analyse des logs via terminal CLI pour diagnostiquer les ports et les routes

2. Précisez les moyens utilisés :

Matériel réel :

- Switches Cisco Catalyst 2960-X et C9200
- Câblage cuivre RJ45
- Postes clients pour test de connectivité

Logiciels / Outils :

- Terminal SSH / Telnet
- IOS Cisco (CLI)
- Documentation Markdown
- Schéma de topologie réalisé sous Lucidchart

Commandes clés utilisées :

- vlan, interface vlan, ip routing
- standby, channel-group, spanning-tree, show, switchport, description

3. Avec qui avez-vous travaillé ?

Projet réalisé en binôme, sous la supervision d'un formateur référent. Chacun gérait une moitié de la topologie pour ensuite les interconnecter en fin de projet.

4. Contexte

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

Chantier, atelier, service ▸ **Projet de maquette réseau sur matériel réel**

Période d'exercice ▸ **Du 13/01/2025 au 17/01/2025**

5. Informations complémentaires *(facultatif)*

Ce projet m'a permis de manipuler des équipements réels dans des conditions proches de la production. J'ai pu consolider mes compétences en configuration Cisco, haute disponibilité, sécurisation des accès, et dépannage CLI.

La maquette est un excellent reflet des exigences d'un réseau LAN moderne, avec gestion fine des VLANs, performances stables et architecture tolérante aux pannes.

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

Exemple n°1 ▸ Évaluation des risques de sécurité et application des normes ISO 27000

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

Dans le cadre d'un atelier de cybersécurité avancée, j'ai participé à la préparation et la présentation structurée d'un panorama complet des normes ISO 27000, dans l'objectif de comprendre les enjeux réglementaires et stratégiques liés à la sécurité de l'information dans les organisations.
L'exercice était autant documentaire que pédagogique, visant à expliquer clairement comment ces normes s'articulent et s'appliquent dans des contextes réels (PME, grands groupes, hébergeurs, etc.).

Tâches principales :

- Veille documentaire sur les normes :
  - ISO 27001 (Système de Management de la Sécurité de l'Information)
  - ISO 27002 (Mesures de sécurité – guide de mise en œuvre)
  - ISO 27005 (Gestion des risques liés à la sécurité)
  - ISO 27701 (Protection des données personnelles, extension RGPD)
  - ISO 27017 / 27018 (Sécurité du Cloud / Vie privée en Cloud)
- Lecture croisée et synthèse : lecture de sources officielles + vulgarisation + comparaison structurée
- Organisation du contenu :
  - Création d'un plan détaillé en 3 parties avec alternance d'intervenants
  - Préparation d'un discours pédagogique, adapté à un public non spécialiste
  - Ajout de cas concrets (Carrefour certifié 27001, Azure compliant, Google Cloud)
- Analyse appliquée :
  - Application fictive des normes dans un scénario d'entreprise
  - Construction d'un raisonnement : quels risques → quelle norme → quel contrôle
  - Mise en lien avec mes expériences antérieures (PRA, segmentation réseau, MFA…)

2. Précisez les moyens utilisés :

Sources :

- Extraits des normes ISO accessibles publiquement
- Sites de l'ANSSI, CNIL, et des éditeurs de cloud
- Études de cas (Carrefour, Microsoft Azure, Google Cloud)

Supports produits :

- Fichier Markdown structuré (≈ 15 minutes par intervenant)
- Slides synthétiques
- Plan de présentation minuté

Logiciels utilisés :

- Obsidian (rédaction)
- Google Drive / Docs (partage)
- PowerPoint (présentation orale)

3. Avec qui avez-vous travaillé ?

Travail en trinôme.
J'ai assuré personnellement :

- La rédaction intégrale du contenu lié aux normes 27002, 27005 et 27701
- La mise en forme pédagogique de ces parties
- La prise de parole orale sur ces thématiques
- L'animation des échanges avec les autres membres pour harmoniser le propos et éviter les redondances

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Normes ISO 27000**

Période d'exercice ▸ **Du 27/05/2024 au 31/05/2024**

5. Informations complémentaires *(facultatif)*

Cette présentation m'a permis d'acquérir une compréhension transversale des normes ISO appliquées à la cybersécurité

Elle a renforcé ma capacité à :

- Faire de la veille réglementaire
- Expliquer clairement des concepts complexes
- Faire le lien entre théorie et application concrète

Ce projet m'a aussi préparé à justifier des choix techniques dans mes projets réels (MFA, segmentation, logs, PRA, RGPD)

Cette compétence de communication cyber est précieuse en entreprise pour sensibiliser, cadrer les audits ou accompagner des DSI dans leur stratégie de mise en conformité

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

Exemple n°2 ▸ ***Analyse de vulnérabilités et sécurisation d'infrastructures avec OpenVAS***

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

Dans le cadre d'un projet pratique, j'ai été chargé de simuler un environnement d'entreprise avec des machines vulnérables pour y appliquer une analyse complète des vulnérabilités via OpenVAS, suivi d'un processus de correction.

L'objectif : reproduire un cycle réel de gestion des vulnérabilités, de la détection à la remédiation.

Étapes réalisées :

- Installation d'un serveur OpenVAS (Greenbone) sur une VM Debian 12
- Création d'un parc de machines vulnérables volontairement non mises à jour :
  - Windows 10 (sans patch)
  - Debian 11 avec Apache / Nginx / FTP / MariaDB
- Scan CVE ciblé : basé uniquement sur les vulnérabilités connues
  - Aucun résultat critique initial
- Scan complet : analyse active de tous les services ouverts
  - 4 vulnérabilités détectées dont 2 critiques
- Comparaison des résultats :
  - Mise en évidence de vulnérabilités non détectées par le simple scan CVE
- Remédiation :
  - Mise à jour des systèmes
  - Désactivation de services non nécessaires
  - Renforcement des configurations (FTP, bases de données)
- Re-scan post-correction :
  - Réduction des vulnérabilités critiques
  - Détection de nouvelles failles mineures introduites par les mises à jour

2. Précisez les moyens utilisés :

- Systèmes :
  - Debian 12 (serveur)
  - Windows 10 + Debian 11 (machines cibles)
- Outils :
  - OpenVAS (scanner de vulnérabilités)
  - Base CVE, NVD, MITRE
  - Interfaces Web et ligne de commande
- Documentation :
  - Markdown (rapports de scans)
  - Tableaux comparatifs

3. Avec qui avez-vous travaillé ?

Projet réalisé en trinôme.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Analyse de vulnérabilités avec OpenVAS**

Période d'exercice ▸ **Du 16/12/2024 au 20/12/2024**

5. Informations complémentaires *(facultatif)*

J'ai proposé une intégration future avec un SIEM (Wazuh, ELK, Splunk) pour :

- Centralisation des alertes
- Suivi dans le temps
- Détection temps réel

Ce projet m'a permis de maîtriser le processus complet de gestion de vulnérabilités :

- Découverte → Analyse → Correction → Vérification

J'ai également renforcé mes compétences en administration système, lecture de rapports CVE, et prise de décision sécuritaire

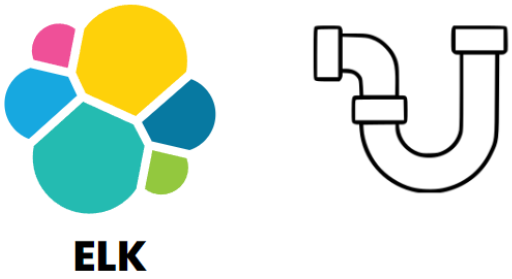
Activité-type 3 — Participer à la gestion de la cybersécurité

Exemple n°3 ▸ Mise en place d'une supervision centralisée d'un serveur vulnérable avec Filebeat, Logstash et Kibana

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

Dans le cadre d'un atelier avancé en cybersécurité, j'ai conçu une infrastructure de supervision centralisée pour un serveur volontairement exposé à des vulnérabilités connues, dans un objectif de détection, d'analyse, de visualisation et de durcissement progressif.

Ce projet m'a permis de mettre en œuvre la stack ELK complète (Elasticsearch, Logstash, Kibana), avec Filebeat en agent de collecte local.
J'ai également travaillé sur la sécurisation de l'environnement, la gestion de certificats, la structuration des logs et la création de dashboards analytiques.



Mise en place de l'infrastructure

- Création de 3 machines virtuelles Debian 12 :
  - Serveur log-central pour Elasticsearch + Kibana
  - Serveur log-process pour Logstash
  - Serveur web-vuln (machine vulnérable avec Apache2, FTP, MySQL)
- Configuration réseau entre les 3 machines via un pont local

Installation et configuration de la stack ELK

- Elasticsearch :
  - Installation depuis dépôt officiel Elastic
  - Configuration en mode standalone sur port 9200
  - Ouverture et sécurisation du port avec ufw
- Kibana :

- Interface Web sur port 5601
- Liaison avec Elasticsearch via configuration kibana.yml
- Génération de certificats SSL/TLS auto-signés pour sécuriser les accès

- Logstash :
  - Mise en place d'un pipeline dédié (pipeline.conf)
  - Parsing JSON et extraction des champs critiques
  - Filtres grok pour structuration fine des logs Apache et FTP
  - Redirection vers Elasticsearch

Collecte des logs avec Filebeat

- Installation de Filebeat sur la machine web-vuln
- Configuration du fichier filebeat.yml pour surveiller :
  - /var/log/apache2/access.log
  - /var/log/apache2/error.log
  - /var/log/vsftpd.log
  - /var/log/mysql/error.log
- Envoi des logs en sortie vers Logstash (port 5044)
- Tests de transmission et visualisation dans Kibana

Sécurisation et durcissement du serveur vulnérable

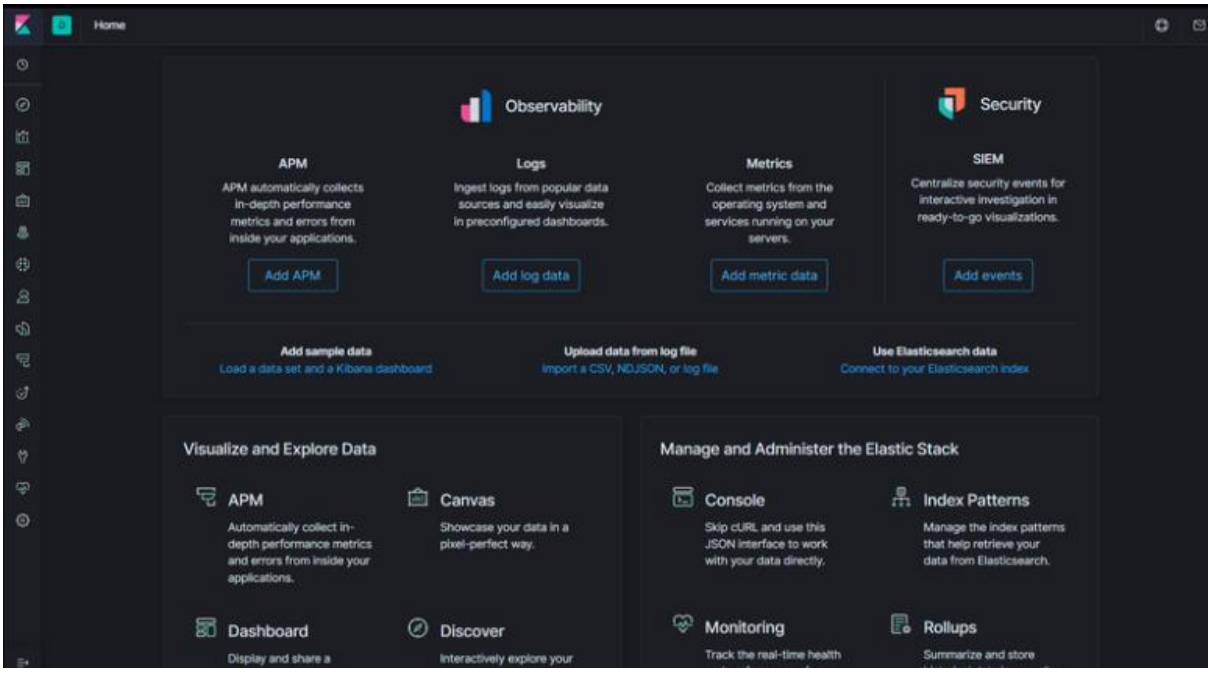
- Apache2 :
  - Version volontairement vulnérable installée dans un premier temps
  - Analyse des logs avec recherche de :
    - Requêtes 404 fréquentes
    - Méthodes HTTP interdites (PUT, DELETE)
    - User-Agents suspects (ex : scanners automatisés)
  - Durcissement : désactivation des modules non nécessaires, mise à jour de sécurité
- FTP (vsFTPd) :
  - Analyse des connexions anonymes
  - Restrictions appliquées (connexion TLS obligatoire, logs activés)
- MySQL :
  - Vérification des erreurs fréquentes, tentatives de login
  - Suppression des comptes sans mot de passe, durcissement via mysql_secure_installation

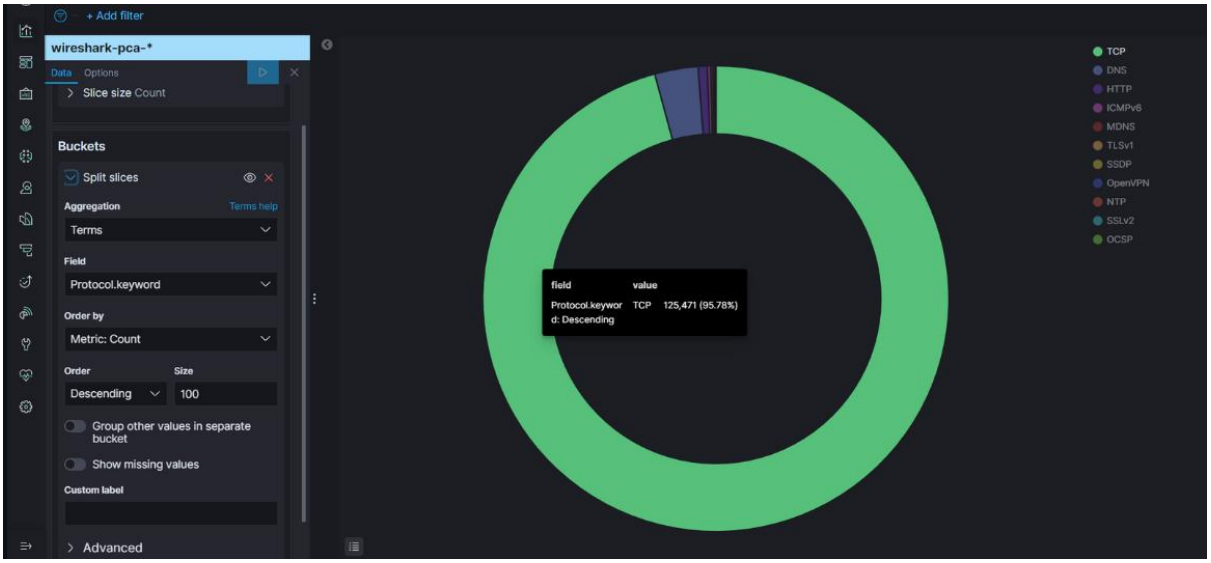
Visualisation et analyse dans Kibana

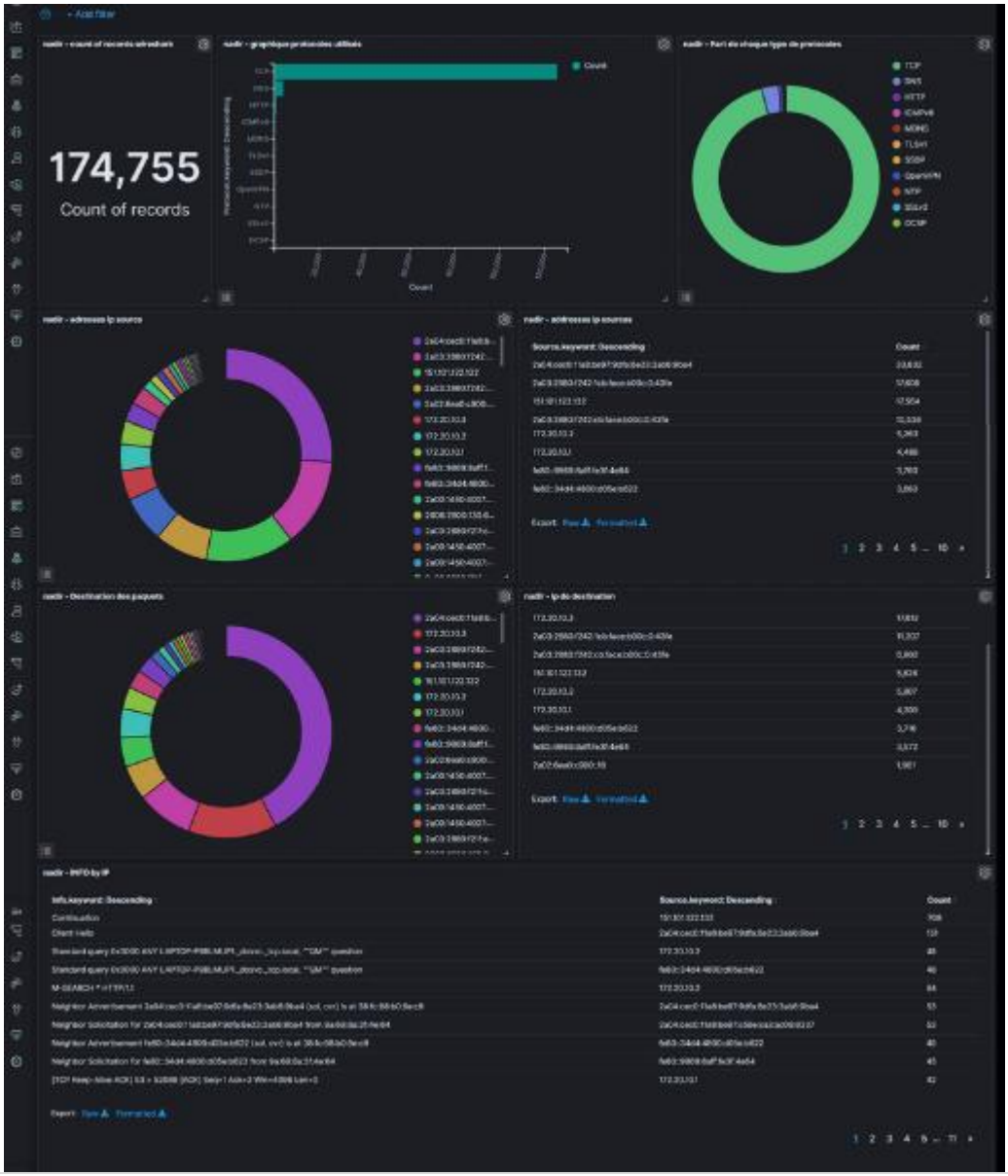
- Création de dashboards personnalisés :
  - Histogrammes des requêtes Apache par IP, par statut (200, 404, 500)
  - Top IPs FTP entrantes
  - Journaux d'erreurs MySQL
- Création de filtres dynamiques :
  - Recherches par User-Agent
  - Recherche de chaînes suspectes dans les URLs
- Visualisation du trafic journalier et corrélation de pics anormaux avec les logs

Vérifications et évolutions proposées

- Tests de résilience en arrêtant Logstash ou Filebeat → détection immédiate d'erreurs dans Kibana
- Proposition d'évolution : intégration d'alerting avec Watcher ou ELK + Elastalert
- Possibilité future : connecter cette stack à un SIEM centralisé type Wazuh ou Splunk




+ Add filter
wireshark-pca-*
Data
Options
Slice size Count
Buckets
Split slices
Aggregation
Terms help
Terms
Field
Protocol.keyword
Order by
Metric: Count
Order
Size
Descending
100
Group other values in separate bucket
Show missing values
Custom label
Advanced
field
value
Protocol.keywor d: Descending
TCP
125,471 (95.78%)
TCP
DNS
HTTP
ICMPv6
MDNS
TLSv1
SSDP
OpenVPN
NTP
SSLv2
OCSP



2. Précisez les moyens utilisés :

OS / Infrastructure : 3x Debian 12, réseau local virtuel

Outils utilisés :

- Filebeat (agent collecte)
- Logstash (filtrage, parsing)
- Elasticsearch (indexation)
- Kibana (visualisation)
- OpenSSL (génération de certificats auto-signés TLS)
- Apache2, vsFTPd, MySQL (cibles vulnérables)

Langages et fichiers :

- YAML (filebeat.yml)
- CONF (logstash pipeline.conf)
- JSON (logs)
- GROK (regex)

3. Avec qui avez-vous travaillé ?

Projet réalisé individuellement.

J'ai présenté les résultats lors d'un échange oral avec un formateur et fourni un rapport complet illustré avec dashboards et configurations.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ ***La Plateforme***

Chantier, atelier, service ▸ **Supervision de services vulnérables avec la stack ELK**

Période d'exercice ▸ **Du 11/12/2023 au 15/12/2023**

5. Informations complémentaires *(facultatif)*

Ce projet m'a permis de comprendre la chaîne complète de supervision moderne : collecte, traitement, structuration, visualisation.

Il montre ma capacité à déployer des outils complexes, à les configurer avec rigueur et à en extraire des insights opérationnels.

Cette expérience sera directement transposable à un environnement professionnel nécessitant de la supervision, de la journalisation centralisée, ou de l'analyse des comportements système.

Il peut aussi servir de base à une intégration avec un SOC ou une plateforme XDR.

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Technicien Assistant Informatique	**Afpa, La Ciotat**	**2023**
Bac Scientifique spécialité Science de la Vie et de la Terre	**Lycée Denis Diderot, Marseille**	**2014**
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.

Déclaration sur l'honneur

Je soussigné(e) Meihdi Dif,

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 25/07/2025

pour faire valoir ce que de droit.

Signature : Meihdi DIF

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé
Cliquez ici pour taper du texte.

ANNEXES

(Si le RC le prévoit)