

Rapport d'Étonnement - Mohammad Rezki

Mohammad Rezki

<https://discovery-report.vercel.app>



Sommaire

1	Résumé	7
1.1	Résumé (Français)	7
1.2	Abstract (English)	7
2	Introduction	9
2.1	Contexte	9
2.2	Présentation personnelle	9
2.2.1	Compétences clés apportées	10
2.3	Objectifs du rapport	10
2.4	Période couverte	10
3	L'Entreprise Fortinet	11
3.1	Historique et identité	11
3.2	Secteur d'activité	12
3.2.1	Positionnement concurrentiel	12
3.3	Gamme de produits	12
3.3.1	Produits principaux	12
3.3.2	Innovation : FortiAI	12
3.4	Organisation	13
3.4.1	Structure globale	13
3.4.2	Le site de Sophia-Antipolis	13
3.5	Défis et enjeux	13
3.5.1	Les grands défis de demain	13
3.5.2	Engagement environnemental	13
4	Intégration	15
4.1	Les premiers jours	15
4.1.1	Jour 1 : Arrivée chez Fortinet (27 octobre 2025)	16
4.1.2	L'équipe NOC/SOC	16
4.2	Première semaine : Installation	16
4.2.1	Configuration de l'environnement de travail	16
4.2.2	Outils et méthodologies découverts	17
4.3	Semaines 2-3 : Immersion dans les projets	17
4.3.1	Prise en main des projets existants	18
4.3.2	Premier projet : Knock Analytics Dashboard	18
4.4	Accompagnement et suivi	18
4.4.1	Le rôle du tuteur	18
4.4.2	Ressources d'apprentissage	19

4.5 Bilan de l'intégration	19
5 Étonnement et Analyse	21
5.1 Observations positives	21
5.1.1 Une culture DevOps mature	22
5.1.2 Autonomie et confiance	22
5.1.3 L'écosystème <i>Eat Your Own Dog Food</i>	22
5.2 Points de complexité	22
5.2.1 Courbe d'apprentissage importante	23
5.2.2 Documentation dispersée	23
5.3 Analyse SWOT	23
5.3.1 Représentation visuelle	23
5.3.2 Détail de l'analyse	23
5.4 Méthodologie de travail observée	25
5.4.1 Cycle de développement	25
5.4.2 Points appréciés	25
5.5 Synthèse des étonnements	25
6 Missions confiées	27
6.1 Vue d'ensemble	27
6.2 Axe 1 : CMM Dashboard Tooling	28
6.2.1 1. Introduction	28
6.2.2 2. Architecture Technique	28
6.2.3 3. Fonctionnalités Principales (Modules)	28
6.2.4 4. Points Forts & Valeur Ajoutée	35
6.2.5 Compétences développées (Dashboard)	38
6.3 Axe 2 : Lab Management	38
6.3.1 Contexte (Lab Management)	38
6.3.2 Objectifs	38
6.3.3 Analyse d'architecture	38
6.3.4 Réalisations	38
6.3.5 Compétences développées (Lab)	39
6.4 Axe 3 : Innovation & Knowledge Sharing	39
6.4.1 Projet MCP (Model Context Protocol)	39
6.4.2 Knowledge Sharing	40
6.5 Synthèse des missions	40
6.5.1 État d'avancement	41
7 Propositions d'amélioration	43
7.1 Introduction	43
7.2 Proposition 1 : Unification des outils de reporting	44
7.2.1 Constat (Reporting)	44
7.2.2 Proposition (Reporting)	44
7.2.3 Statut	44

7.3 Proposition 2 : Centralisation de la documentation	45
7.3.1 Constat (Documentation)	45
7.3.2 Proposition (Centralisation)	45
7.4 Proposition 3 : Automatisation du cycle de vie Lab	45
7.4.1 Constat (Lab)	46
7.4.2 Proposition (Automatisation)	46
7.5 Proposition 4 : Tests automatisés pour les scripts	46
7.5.1 Constat (Tests)	46
7.5.2 Proposition (Tests)	46
7.6 Proposition 5 : Documentation du projet MCP	47
7.6.1 Constat (MCP)	47
7.6.2 Proposition (Doc MCP)	47
7.7 Synthèse des propositions	48
8 Conclusion	49
8.1 Bilan personnel	49
8.1.1 Ce que j'ai appris	50
8.1.2 Ce qui m'a marqué	50
8.2 Projection vers le métier d'ingénieur	50
8.2.1 Vision du métier	50
8.2.2 Mes aspirations	51
8.3 Défis de demain	51
8.3.1 Pour l'entreprise	51
8.3.2 Pour moi	51
8.4 Remerciements	51
8.5 Mot de la fin	52
9 Glossaire	53
9.1 Termes techniques	53
9.2 Produits Fortinet mentionnés	54
10 Bibliographie	55
10.1 Sources officielles	55
10.2 Documentation technique	55
10.3 Intelligence Artificielle et Innovation	55
10.4 Méthodologie et analyse	55
10.5 Réglementation	55
10.6 Rapports sectoriels	56
11 À propos de ce document	57

Résumé

Ce chapitre contient le résumé exécutif de ce rapport d'étonnement, en version française et anglaise.

1.1 Résumé (Français)

Ce rapport d'étonnement présente les observations et analyses d'un étudiant ingénieur CESI lors de ses premiers mois d'alternance chez Fortinet, leader mondial de la cybersécurité, sur le site de Sophia-Antipolis.

L'intégration au sein de l'équipe NOC/SOC (CSE-INTL-CMM) a révélé une organisation caractérisée par une maturité DevOps remarquable, une autonomie accordée aux nouveaux collaborateurs et une culture du “eat your own dog food” où les produits Fortinet sont utilisés en interne.

Trois missions principales ont été confiées :

- La création d'un dashboard hebdomadaire de rendu de l'activité (Redmine API),
- L'automatisation de la gestion du laboratoire virtualisé (vSphere/NetBox),
- Et l'exploration de technologies avancées comme le protocole MCP pour l'intégration de l'intelligence artificielle.

L'analyse SWOT met en évidence les forces de l'entreprise (leadership marché, innovation IA) tout en identifiant des axes d'amélioration (centralisation de la documentation, automatisation des processus).

Dans un premier temps, nous introduirons le contexte de cette alternance et les objectifs personnels, voir la section *Introduction*.

Ensuite, nous présenterons l'entreprise Fortinet et son positionnement dans le secteur de la cybersécurité, voir la section *L'Entreprise Fortinet*.

Nous continuerons avec la description de mon intégration au sein de l'équipe NOC/SOC à Sophia-Antipolis, voir la section *Intégration*.

Nous partagerons mes étonnements et observations avec un regard neuf, voir la section *Étonnement et Analyse*.

Puis nous détaillerons les missions confiées et les réalisations, voir la section *Missions confiées*.

Cinq propositions concrètes seront formulées pour contribuer à l'efficacité de l'équipe, notamment l'unification des outils de reporting et l'extension de l'automatisation du laboratoire. Voir la section *Propositions d'amélioration*.

1.2 Abstract (English)

This discovery report presents the observations and analyses of a CESI engineering student during the first months of a work-study program at Fortinet, a global leader in cybersecurity, at the Sophia-Antipolis site.

Integration within the NOC/SOC team (CSE-INTL-CMM) revealed an organization characterized by remarkable DevOps maturity, significant autonomy for new employees, and a “eat your own dog food” culture where Fortinet products are widely used internally.

Three main missions were entrusted:

- The creation of a comprehensive **CMM Dashboard** (Knock Analytics) for weekly activity reporting,
- The automation of the virtualized laboratory management (vSphere/NetBox),
- And the exploration of advanced technologies such as the **MCP protocol** for AI integration.

The SWOT analysis highlights the company's strengths (market leadership, AI innovation) while identifying areas for improvement (centralization of documentation, process automation).

First, we will introduce the context of this work-study program and personal objectives, see section [*010_introduction:Introduction*](#).

Then, we will present Fortinet and its positioning in the cybersecurity sector, see section [*L'Entreprise Fortinet*](#).

We will continue with the description of my integration within the NOC/SOC team at Sophia-Antipolis, see section [*Intégration*](#).

We will share my surprises and observations with a fresh perspective, see section [*Étonnement et Analyse*](#).

Then we will detail the assigned missions and achievements, see section [*Missions confiées*](#).

Five concrete proposals will be formulated to contribute to the team's efficiency, in particular the **unification of reporting tools** and the extension of laboratory automation. See section [*Propositions d'amélioration*](#).

Mots-clés / Keywords: Cybersécurité, Fortinet, NOC/SOC, DevOps, Automatisation, SWOT, Alternance

Cybersecurity, Fortinet, NOC/SOC, DevOps, Automation, SWOT, Work-study program

Introduction

Ce chapitre présente le contexte de cette alternance, mes objectifs et la période couverte par ce rapport d'étonnement.



2.1 Contexte

Ce rapport d'étonnement est rédigé dans le cadre de mon alternance au sein de **Fortinet**, leader mondial de la cybersécurité. Conformément aux exigences du cursus **Ingénieur CESI**, ce document vise à capturer mes premières impressions, observations et analyses en tant que nouveau collaborateur.

L'exercice du rapport d'étonnement revêt une importance particulière : il permet de valoriser le regard neuf d'un nouvel arrivant, capable d'identifier des éléments que les collaborateurs expérimentés pourraient ne plus remarquer.

2.2 Présentation personnelle

Profil

Mohammad Rezki

Étudiant ingénieur en alternance - CESI École d'Ingénieurs Nice

Spécialisation : Informatique & Numérique

22 ans - Carros (06)

Passionné par la cybersécurité et l'automatisation, j'ai rejoint Fortinet avec l'objectif d'acquérir une expertise concrète dans ce domaine. Mon parcours inclut une expérience en support technique, en développement d'interfaces web internes, et en automatisation de documentation technique.

2.2.1 Compétences clés apportées

Le tableau ci-dessous résume les compétences techniques que j'apporte à l'équipe :

Domaine	Compétences
Systèmes & Sécurité	Windows, Linux, Docker, pare-feu, sécurisation des accès
Réseaux	TCP/IP, VLAN, DNS, DHCP, VPN, diagnostic réseau
Développement	Python, HTML/CSS/JS, PHP, documentation Sphinx
DevOps	Git, GitLab CI/CD, Docker, Power BI, SharePoint

2.3 Objectifs du rapport

Ce rapport vise à :

- Présenter l'entreprise** Fortinet et son positionnement sur le marché de la cybersécurité
- Décrire mon intégration** au sein de l'équipe NOC/SOC à Sophia-Antipolis
- Partager mes étonnements** et observations avec un regard neuf
- Analyser l'environnement** via une approche SWOT
- Proposer des pistes d'amélioration** dans mon domaine de compétence

2.4 Période couverte

Le tableau suivant détaille la période d'observation couverte par ce rapport :

Timeline
⌚ Début de l'alternance : 27 octobre 2025
⌚ Période d'observation : Octobre 2025 ⌚ Janvier 2026
⌚ Lieu : Fortinet, Sophia-Antipolis (France)

Ce document a été rédigé avec le souci de préserver la confidentialité des informations sensibles de l'entreprise, tout en offrant une vision authentique de mon expérience d'intégration.

L'Entreprise Fortinet

Ce chapitre présente Fortinet, son histoire, ses produits, son organisation et les défis auxquels l'entreprise fait face.



3.1 Historique et identité

Fortinet a été fondée en **2000** à Sunnyvale, en Californie, par les frères Ken et Michael Xie. Le nom *Fortinet* est une contraction de *Fortified Networks* (réseaux fortifiés), reflétant la mission fondamentale de l'entreprise : sécuriser les infrastructures numériques.

Le tableau suivant présente les étapes clés de l'évolution de Fortinet :

Chiffres clés (2024)

- **Présence mondiale** : Plus de 750 000 clients dans le monde
- **Effectifs** : ~14 000 collaborateurs
- **Chiffre d'affaires** : ~5,5 milliards USD
- **Position** : Leader du marché des pare-feux (UTM/NGFW)

3.2 Secteur d'activité

Fortinet opère dans le secteur de la **cybersécurité**, un domaine en constante évolution face aux menaces croissantes :

- Ransomwares et attaques ciblées
- Sécurisation des environnements cloud et hybrides
- Protection des infrastructures critiques (OT/IoT)
- Zero Trust Architecture

3.2.1 Positionnement concurrentiel

Le graphique suivant illustre le positionnement de Fortinet par rapport à ses principaux concurrents sur le marché de la cybersécurité.

Fortinet se différencie par son approche **Security Fabric** : un écosystème intégré où tous les produits communiquent entre eux pour offrir une protection unifiée.

3.3 Gamme de produits

Fortinet propose un portefeuille complet de produits de sécurité, couvrant l'ensemble des vecteurs d'attaque.

3.3.1 Produits principaux

Produit	Description	Usage
FortiGate	Pare-feu nouvelle génération (NGFW)	Protection périphérique
FortiManager	Gestion centralisée des équipements	Administration
FortiAnalyzer	Analyse et reporting sécurité	SIEM interne
FortiSIEM	Corrélation d'événements	SOC
FortiPAM	Gestion des accès privilégiés	Zero Trust

3.3.2 Innovation : FortiAI

Focus Innovation

FortiAI représente la nouvelle génération d'outils intégrant l'intelligence artificielle :

- Détection automatique des menaces
- Analyse comportementale
- Assistance aux opérateurs SOC

3.4 Organisation

L'entreprise est structurée pour assurer une présence mondiale tout en conservant des pôles d'expertise locaux forts.

3.4.1 Structure globale

L'organigramme ci-dessous schématise l'organisation géographique de Fortinet, du siège mondial jusqu'au site local de Sophia-Antipolis.

3.4.2 Le site de Sophia-Antipolis

Le centre **Sophia-Antipolis** joue un rôle stratégique pour la région EMEA; il héberge les pôles d'activités suivants:

- **Équipe Support technique Europe** pour l'assistance aux clients finaux
- **Équipe Consultants NOC/SOC Europe** pour l'aide aux projets avant-ventes
- **Équipe Certifications** pour la formation des clients finaux et des partenaires
- **Équipe Lab** pour la reproduction de cas clients ou la préparation de démonstrations.

3.5 Défis et enjeux

Dans un secteur en perpétuelle mutation, Fortinet doit relever plusieurs défis stratégiques.

3.5.1 Les grands défis de demain

1. **Transition vers le cloud** : Accompagner les clients dans leur migration tout en maintenant la sécurité
2. **Intelligence artificielle** : Intégrer l'IA dans les solutions de sécurité pour contrer des menaces de plus en plus sophistiquées
3. **Pénurie de talents** : Former et attirer les experts en cybersécurité
4. **Conformité réglementaire** : S'adapter aux évolutions (NIS2, DORA, RGPD)

3.5.2 Engagement environnemental

Fortinet s'engage dans une démarche **RSE** avec :

- Réduction de l'empreinte carbone des datacenters
- Optimisation énergétique des appliances (ASIC propriétaires)
- Programmes de recyclage des équipements

Intégration

Ce chapitre décrit mes premières semaines au sein de l'équipe NOC/SOC de Fortinet à Sophia-Antipolis.



4.1 Les premiers jours

L'arrivée dans une nouvelle entreprise est un moment clé. Voici le déroulement de mes premiers pas chez Fortinet.

4.1.1 Jour 1 : Arrivée chez Fortinet (27 octobre 2025)

Mon premier jour a été riche en découvertes et en rencontres. L'accueil a été structuré et bienveillant :

Étapes d'intégration - Jour 1

1. ☑ Récupération du badge visiteur (en attente du badge permanent)
2. ☑ Attribution du matériel informatique (laptop)
3. ☑ Création des accès aux systèmes internes
4. ☑ Présentation à l'équipe NOC/SOC
5. ☑ Tour des locaux et présentation de l'environnement

4.1.2 L'équipe NOC/SOC

J'ai été accueilli au sein de l'équipe **CSE-INTL-CMM** (Consulting Systems Engineer - International), sous la responsabilité de **Jean-Pierre Forcioli**.

Note

CMM signifie *Central Management & Monitoring*. Cela regroupe les produits Fortinet en charge de l'administration et la surveillance centralisées (FortiManager et FortiAnalyzer respectivement). Désormais, on parle plus d'activité NOC (Network Operations Center) et SOC (Security Operations Center) pour refléter les missions de l'équipe.

L'ambiance au sein de l'équipe est collaborative et technique. Dès le premier jour, j'ai pu échanger avec d'autres alternants et stagiaires sur leurs expériences.

4.2 Première semaine : Installation

Cette première semaine a été dédiée à la construction d'un socle technique solide pour la suite de l'alternance.

4.2.1 Configuration de l'environnement de travail

La première semaine a été consacrée à la mise en place de mon environnement technique :

Étape	Description	Durée
Installation laptop	Configuration Windows/Linux, VPN	1 jour
Accès GitLab	Clonage des dépôts de l'équipe	0.5 jour
Formation produits	Introduction FortiOS, FortiManager	2 jours
Certifications NSE	NSE 1, NSE 3, FCA	Semaine 1
Lab Setup	Configuration de l'environnement de test	Semaine 1

Certifications Fortinet obtenues

Formations complétées (Octobre 2025) :

- **Getting Started in Cybersecurity 3.0** (28/10/2025)
- **FortiGate 7.6 Operator** (29/10/2025)
- **FortiAnalyzer 7.6 Administrator** (29/10/2025)

Certifications et badges :

- **Fortinet Certified Associate (FCA) in Cybersecurity** (29/10/2025)
- **NSE 1** - Getting Started in Cybersecurity v3.0
- **NSE 3** - FortiGate Operator v7.6

4.2.2 Outils et méthodologies découverts

Le tableau ci-dessous résume les principaux outils et méthodologies utilisés par l'équipe :

Stack technique de l'équipe

Gestion de code

- GitLab interne (CI/CD pipelines)
- Branches et merge requests

Documentation

- Sphinx (génération de doc)
- SharePoint

Infrastructure Lab

- vSphere (virtualisation)
- NetBox (IPAM/DCIM)
- Docker (conteneurisation)

Développement

- Python (scripts, automatisation)
- Streamlit (dashboards)

4.3 Semaines 2-3 : Immersion dans les projets

Une fois l'environnement prêt, j'ai pu plonger dans le vif du sujet et contribuer aux projets de l'équipe.

4.3.1 Prise en main des projets existants

Rapidement, j'ai été impliqué dans des projets concrets de l'équipe :

4.3.2 Premier projet : Knock Analytics Dashboard

Dès la fin de la première semaine, j'ai commencé à travailler sur le **Dashboard Knock Analytics**, un outil interne permettant de visualiser les KPIs de l'équipe.

Mes premières contributions :

- Correction de bugs d'affichage
- Amélioration de la documentation
- Ajout de nouvelles visualisations

Le nouveau rapport hebdomadaire a été déployé avec succès, apportant une meilleure visibilité sur l'activité de l'équipe. Ci-après un exemple de rapport :



Fig. 1: Exemple de rapport hebdomadaire généré automatiquement (données anonymisées).

4.4 Accompagnement et suivi

L'autonomie n'exclut pas l'accompagnement. Un cadre de suivi a été mis en place dès le début.

4.4.1 Le rôle du tuteur

Jean-Pierre Forcioli m'a accompagné tout au long de cette phase d'intégration avec :

- **Points hebdomadaires** pour faire le bilan des avancées
- **Disponibilité** pour répondre à mes questions techniques
- **Autonomie progressive** dans la gestion de mes tâches
- **Feedback constructif** sur mon travail

4.4.2 Ressources d'apprentissage

L'entreprise met à disposition de nombreuses ressources :

Formation continue

- **Documentation interne** (CMM)
- **Plateforme NSE** (certifications Fortinet)
- **Knowledge sharing** entre équipes
- **Accès au lab** pour expérimenter

4.5 Bilan de l'intégration

Après les trois premières semaines, je me suis senti :

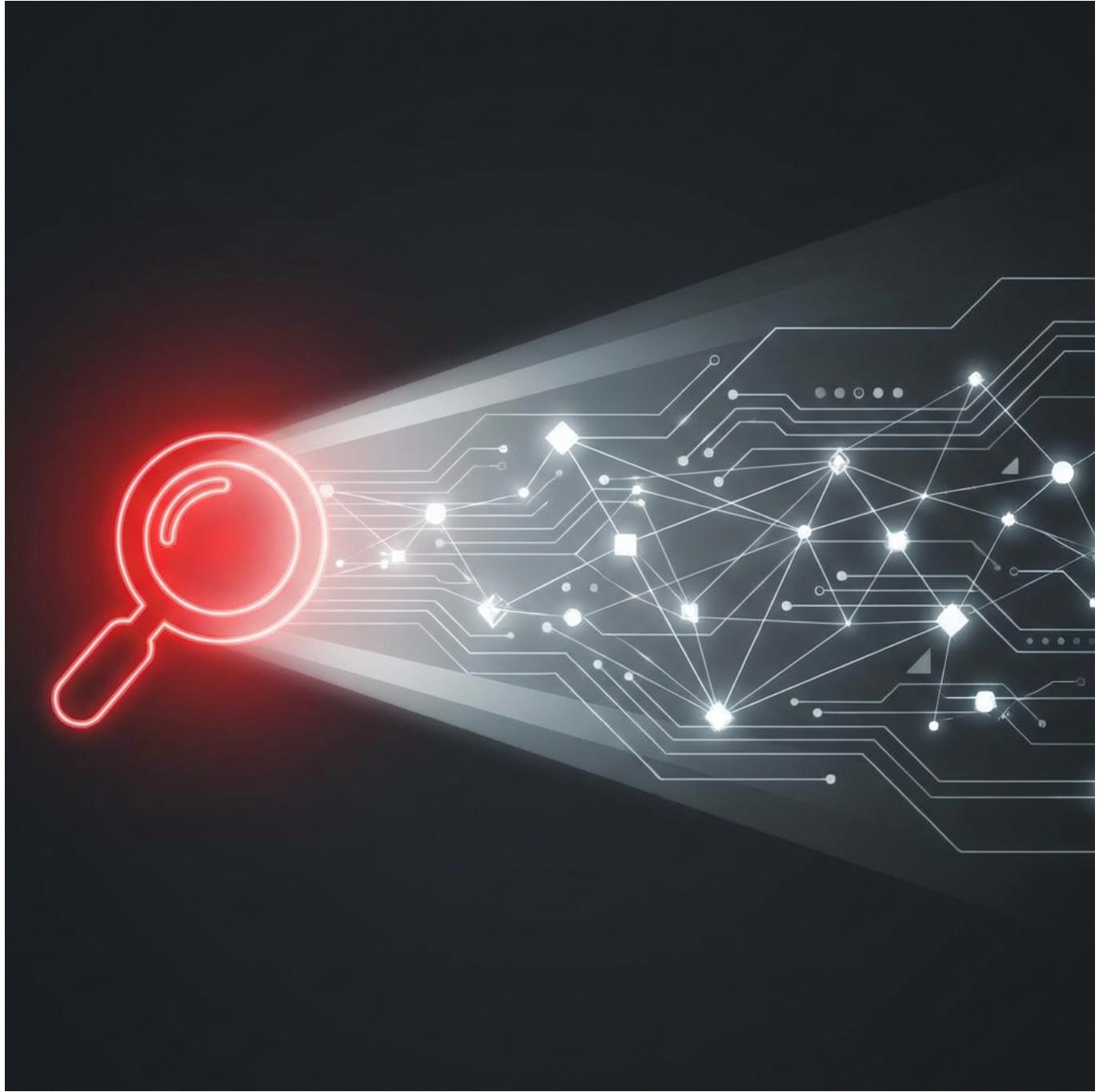
- **Accueilli** : L'équipe a pris le temps de m'intégrer
- **Outilisé** : Tous les accès et ressources nécessaires
- **Challengé** : Des projets concrets dès le départ
- **Accompagné** : Un suivi régulier par mon tuteur

Point fort

Ce qui m'a particulièrement marqué : la **confiance** accordée aux nouveaux arrivants. Dès les premiers jours, j'ai eu accès au code source, aux systèmes de production (en lecture), et j'ai pu proposer des modifications.

Étonnement et Analyse

Ce chapitre présente mes principales observations et étonnements avec un regard neuf sur l'organisation et les pratiques de l'équipe.



5.1 Observations positives

L'immersion dans l'équipe m'a permis de relever plusieurs points très positifs concernant l'organisation et les méthodes de travail.

5.1.1 Une culture DevOps mature

Premier étonnement majeur : le niveau de maturité des pratiques DevOps au sein de l'équipe.

Ce qui m'a surpris

Dès mon arrivée, j'ai découvert :

- **GitLab CI/CD** : Pipelines automatisés pour chaque projet
- **Infrastructure as Code** : Scripts Python versionnés, Docker
- **Documentation as Code** : Sphinx avec build automatique
- **Environnements séparés** : Dev ↗ Preprod ↗ Production

Venant du monde académique où les projets sont souvent gérés de manière plus artisanale, cette rigueur m'a impressionné.

5.1.2 Autonomie et confiance

Deuxième étonnement : le niveau d'autonomie accordé aux nouveaux arrivants.

Contrairement à mes attentes, je n'ai pas eu de période d'observation passive. Dès la première semaine :

- Accès complet aux dépôts de code
- Possibilité de proposer des modifications
- Participation aux discussions techniques

Cette approche *learning by doing* est très efficace mais demande une capacité d'adaptation rapide.

5.1.3 L'écosystème *Eat Your Own Dog Food*

Troisième étonnement : Fortinet utilise intensivement ses propres produits en interne.

Ce principe est illustré par l'architecture simplifiée suivante, montrant l'interconnexion des outils au sein du laboratoire.

Cette pratique permet aux équipes de :

- Comprendre les produits de l'intérieur
- Identifier les bugs avant les clients
- Proposer des améliorations concrètes

5.2 Points de complexité

Bien que mon intégration se soit bien passée, j'ai rencontré plusieurs défis liés à la richesse de l'environnement technique.

5.2.1 Courbe d'apprentissage importante

La richesse de l'écosystème Fortinet est aussi sa complexité :

Domaine	Éléments à maîtriser
Produits	FortiOS, FortiManager, FortiAnalyzer, FortiPAM, FortiAI...
Infra Lab	vSphere, NetBox, Docker
Outils internes	GitLab, Knock, Redmine, Teams
Documentation	Sphinx, CMM

Observation : Il faut accepter de ne pas tout comprendre immédiatement et progresser par couches successives.

5.2.2 Documentation dispersée

J'ai remarqué que la documentation est parfois répartie entre plusieurs sources :

- GitLab (README, docs techniques)
- SharePoint (procédures, guides)
- CMM (documentation officielle)
- Teams (discussions, décisions)

Cela peut rendre la recherche d'information plus longue pour un nouvel arrivant.

5.3 Analyse SWOT

L'analyse SWOT permet de synthétiser les observations en identifiant forces, faiblesses, opportunités et menaces.

5.3.1 Représentation visuelle

Le graphique en quadrants ci-dessous offre une vue synthétique des forces et faiblesses internes, ainsi que des opportunités et menaces externes.

5.3.2 Détail de l'analyse

Voici le détail de chaque quadrant de l'analyse SWOT.

Forces (internes, positives)

Fortinet dispose de nombreux atouts sur lesquels s'appuyer.

Points forts

1. **Leadership marché** : Fortinet est reconnu comme leader dans les pare-feux nouvelle génération

2. **Innovation continue** : FortiAI, intégration IA dans les produits
3. **Équipe technique experte** : Niveau technique élevé des CSE
4. **Culture DevOps** : Pratiques modernes de développement et déploiement
5. **Infrastructure lab** : Environnement de test complet et accessible

Faiblesses (internes, négatives)

Malgré ces forces, certains points méritent attention.

Points d'attention

1. **Complexité de l'écosystème** : Nombreux produits à maîtriser
2. **Documentation fragmentée** : Multiples sources d'information
3. **Courbe d'apprentissage** : Temps nécessaire pour être opérationnel

Opportunités (externes, positives)

Le contexte externe offre de nombreuses opportunités.

Tendances favorables

1. **Marché de la cybersécurité** : Croissance continue (+15%/an)
2. **Adoption cloud** : Besoin de sécurité cloud/hybride
3. **Réglementation** : NIS2, DORA créent de nouveaux besoins
4. **IA générative** : Opportunité d'intégration (ex: protocole MCP)
5. **Pénurie de talents** : Valorisation des profils formés

Menaces (externes, négatives)

Des risques externes sont également à surveiller.

Risques identifiés

1. **Concurrence intense** : Palo Alto, Cisco, CrowdStrike, Zscaler, Netskope, Cato
2. **Évolution rapide des menaces** : Nécessité d'adaptation constante
3. **Guerre des talents** : Difficulté de recrutement dans le secteur

5.4 Méthodologie de travail observée

L'organisation du travail au sein de l'équipe repose sur des processus clairs et efficaces, favorisant la qualité et la rapidité.

5.4.1 Cycle de développement

L'équipe suit une méthodologie **AGILE adaptée** dont les principales étapes sont décrites dans le diagramme suivant :

5.4.2 Points appréciés

Voici les aspects de la méthodologie que j'ai particulièrement appréciés.

- **Flexibilité** : Pas de rigidité excessive dans les processus
- **Communication** : Points réguliers, disponibilité des collègues
- **Qualité** : Revue de code systématique
- **Automatisation** : Réduction des tâches manuelles répétitives

5.5 Synthèse des étonnements

Le tableau ci-dessous résume mes principales observations.

Aspect	Attendu	Observé	Étonnement
Autonomie	Progressive	Immédiate	Positif
Complexité	Modérée	Élevée	Challengeant
DevOps	Basique	Très mature	Positif
Documentation	Centralisée	Dispersée	À améliorer
Ambiance	Formelle	Collaborative	Positif

Missions confiées

Ce chapitre détaille les missions qui m'ont été confiées durant cette alternance et les réalisations associées.



6.1 Vue d'ensemble

Mon alternance s'articule autour de **trois axes principaux**, définis avec mon tuteur Jean-Pierre Forcioli :

6.2 Axe 1 : CMM Dashboard Tooling

Cet axe constitue le cœur technologique de mon alternance. Il a consisté à transformer un ensemble de scripts disparates en une véritable suite logicielle unifiée : le **CMM Dashboard**.

6.2.1 1. Introduction

Le **CMM Dashboard** (Central Management & Monitoring) est une application web analytique développée pour piloter l'activité de l'équipe NOC/SOC. Elle centralise les données issues de l'outil de gestion Knock pour offrir une visualisation temps réel des KPIs, faciliter la génération de rapports hebdomadaires et suivre la performance commerciale et technique.

6.2.2 2. Architecture Technique

Le projet repose sur une stack moderne et modulaire, conçue pour la performance et la maintenabilité.

- **Technologie Principale** : Python avec le framework **Streamlit**.
- **Architecture** : Modulaire (un module par onglet fonctionnel) pour faciliter la maintenance.
- **Données** :
 - *Source* : API Knock (récupération des issues, projets, custom fields).
 - *Stockage Local* : Cache optimisé en CSV pour la performance, avec rafraîchissement planifié.
 - *Traitements* : Pandas pour le nettoyage, la transformation et l'analyse.
- **Génération de Documents** :
 - *HTML* : Moteur de template pour les rapports email interactifs.
 - *PPTX* : Librairie `python-pptx` pour la génération automatique des slides avec mise en page précise.

6.2.3 3. Fonctionnalités Principales (Modules)

L'application est structurée en plusieurs onglets thématiques accessibles via une navigation fluide. Visualisez chaque module ci-dessous :

3.1 Analyse Commerciale & Stratégique

Ce premier ensemble de modules permet le suivi de la performance commerciale et l'identification des tendances.

Executive Overview

Tableau de bord de direction offrant une vue synthétique de l'activité.

- **KPIs Clés** : Revenu total (Total Value), Closing Volume, Win Rate.
- **Comparaisons** : Analyse Year-on-Year (YoY) et Quarter-on-Quarter (QoQ).
- **Top 5 Deals** : Visualisation immédiate des opportunités majeures.

NOC/SOC Team FY 2024-2026

Central Management & Monitoring - 1596 issues

Closing Quarters: All

Current Quarter: Q1-2026

Last update: 2026-01-19 07:30

Executive Overview Sales Pipeline Products & Regions Trends & Analytics Detailed Data CSE Management Weekly Report Report Hub Automation Docs

Executive KPIs for Q1-2026

Total Issues 164 ↑ 15 vs prev Q	Total Deal Size \$98M ↓ -16,663,650 vs prev Q	Open Issues (Backlog) 0	Conversion Rate 9.1%
Average Deal Size \$597K	Pending Rate 77.4%	Closed Issues 15	Win Rate 0.0%

Quarter-over-Quarter Performance

Comparison of key metrics between the current and previous quarter.

Total Issues (Q1-2026 vs. Previous Q)	Total Deal Size (Q1-2026 vs. Previous Q)
Number of Issues 149 (Q4-2025) 164 (Q1-2026)	Deal Size in Million \$ 114.70 (Q4-2025) 98.03 (Q1-2026)

Sales Pipeline

Analyse détaillée du tunnel de vente et des opportunités en cours.

- Funnel de Vente** : Visualisation des étapes (New -> In Progress -> Closed).
- Répartition** : Suivi des dossiers gagnés, perdus, annulés.
- Prévisions** : Identification des dossiers à haut potentiel.

Products & Regions

Analyse dimensionnelle de l'activité.

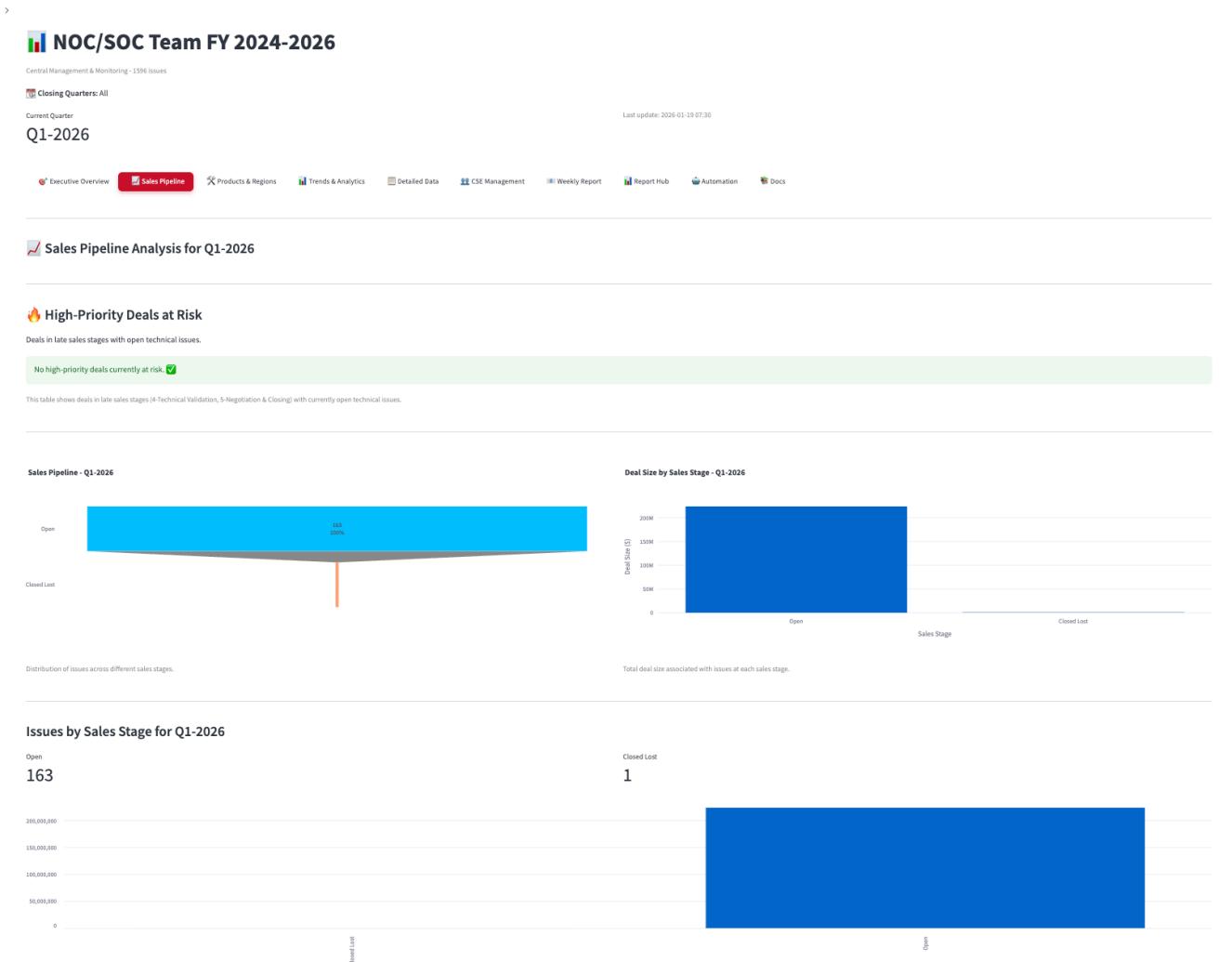
- Répartition Géographique** : Cartographie des revenus par région (EMEA, APAC...).
- Mix Produit** : Analyse de performance par ligne de produit.
- Verticales** : Segmentation par secteur client.

Trends & Analytics

Analyse historique et tendances de fond.

- Évolution Temporelle** : Courbes de tendance sur plusieurs années.
- Saisonnalité** : Identification des pics de charge.

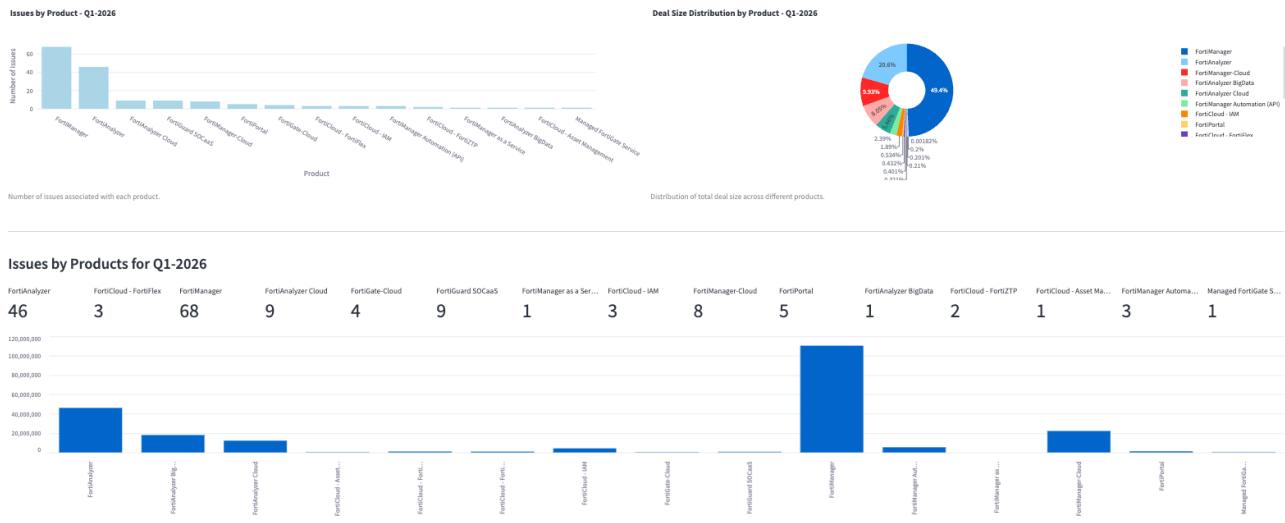
Rapport d'Étonnement - Mohammad Rezki, Release 1.0



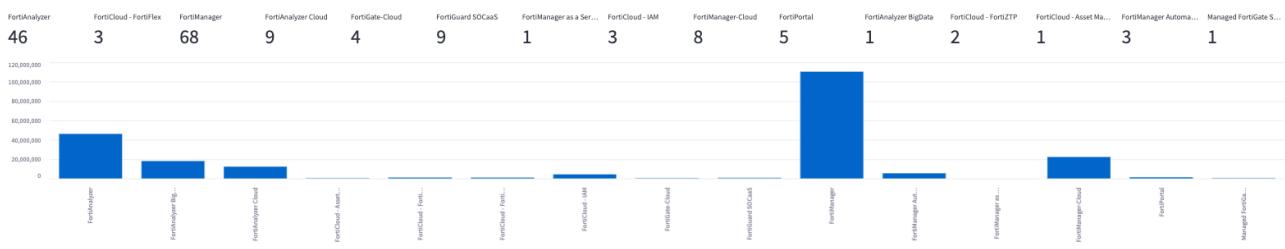
Rapport d'Étonnement - Mohammad Rezki, Release 1.0



Product & Region Performance for Q1-2026



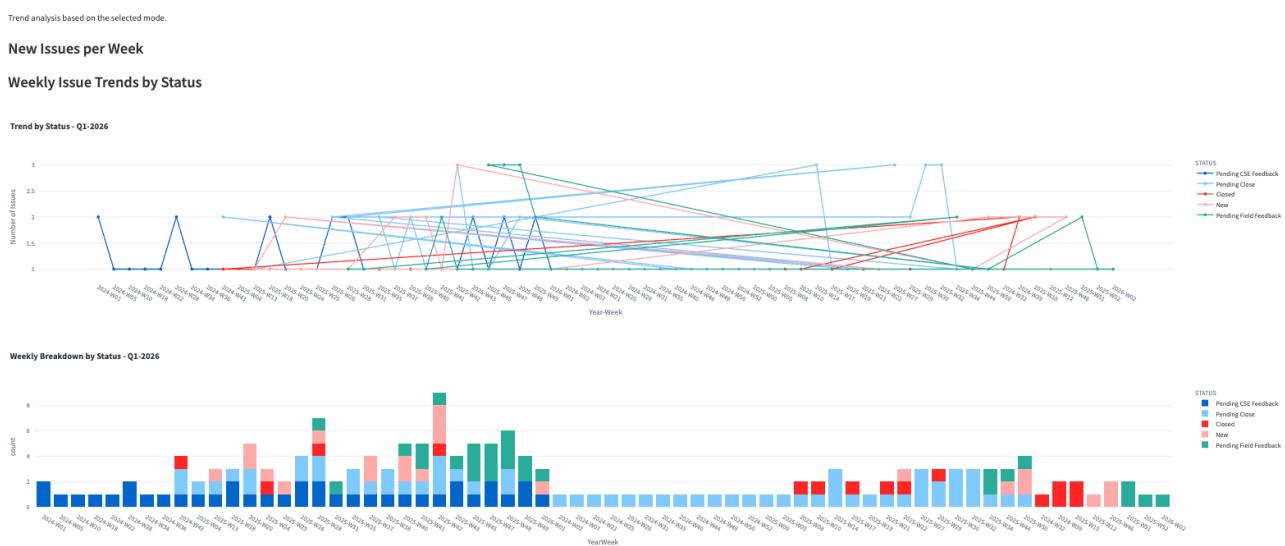
Issues by Products for Q1-2026



NOC/SOC Team FY 2024-2026



Trends & Performance Over Time for Q1-2026



3.2 Reporting & Opérations

Ces modules constituent le cœur opérationnel de l'outil, automatisant la production des rapports hebdomadaires.

Weekly Report

Le module critique pour le management : génération de rapports.

- **Génération Automatique** : Rapport HTML structuré en un clic.
- **Support PPTX** : Slides PowerPoint chartés, avec pagination intelligente.
- **Workflow** : Mode Brouillon vs Officiel pour validation.

The screenshot shows the 'Weekly Report Generator' section of the platform. At the top, there's a navigation bar with various tabs like Executive Overview, Sales Pipeline, Products & Regions, Trends & Analytics, Detailed Data, CSE Management, Weekly Report (which is highlighted in red), Report Hub, Automation, and Docs. Below the navigation, it says 'Central Management & Monitoring - 1596 issues'. It shows 'Closing Quarters: All' and 'Current Quarter: Q1-2026'. The date 'Last update: 2026-01-19 07:30' is also displayed. A 'Generate New Report' form is present, with fields for 'Week Number' (set to 4), 'Year' (set to 2026), and 'Publish Official' status (showing 'No draft found for Week 4'). There are dropdown menus for 'Automatic Report Generation' and 'View Last Cron Log', and a red 'Generate Weekly Report' button. Below this is a table titled 'Existing Reports' showing a list of files with columns for Filename, Type, Size, Modified, and Actions. The table lists several reports from different weeks, some in 'Official' status and others in 'Draft' status, with file sizes ranging from 139.8 KB to 289.1 KB.

Report Hub

Centre d'archivage et de gestion de l'historique.

- **Centralisation** : Accès à tous les rapports (Drafts/Officiels).
- **Actions** : Prévisualisation, Téléchargement (HTML/PPTX), Suppression.
- **Analytique** : Suivi de l'évolution des KPIs reportés.

Rapport d'Étonnement - Mohammad Rezki, Release 1.0

NOC/SOC Team FY 2024-2026

Central Management & Monitoring - 1596 issues

Closing Quarters: All

Current Quarter: Q1-2026

Last update: 2026-01-19 07:30

Executive Overview Sales Pipeline Products & Regions Trends & Analytics Detailed Data CSE Management Weekly Report Report Hub Automation Docs

Report Hub

Overview of all weekly reports - Draft vs Official

Total Weeks	Official	Draft Only
5	3	2

KPI Trends

Show Performance Graphs

Weekly Revenue (€)

WeekLabel	Revenue (€)
W50 2025	96M
W51 2025	94M
W1 2026	97M
W2 2026	95M
W3 2026	98M

Weekly Closing Volume

WeekLabel	Closing
W50 2025	100
W51 2025	100
W1 2026	100
W2 2026	100
W3 2026	100

Filters

Select Year: 2026

Filter by Quarter: Q1, Q2, Q3, Q4

Filter Mode: All Reports

All Reports

Expand All Weeks

Status	Count	Revenue	Actions			
Official	124	\$97M				
Draft	124	\$96M				
Week 3 - 2026 (Jan 12 - Jan 18)						
Week 2 - 2026 (Jan 05 - Jan 11)						
Week 1 - 2026 (Dec 29 - Jan 04)						

Rapport d'Étonnement - Mohammad Rezki, Release 1.0

3.3 Administration & Outils

Ces fonctionnalités permettent le pilotage de l'équipe et la maintenance des données du dashboard.

CSE Management

Outil de pilotage de la charge d'équipe.

- Charge Individuelle** : Dossiers gérés par ingénieur.
- Performance** : Temps de traitement, complexité.



Priority Alerts & Tactical View for Q1-2026

Tickets requiring immediate attention to unblock commercial or technical situations.

High-Value Issues Need Attention

ID	PRODUCT	DEAL_SIZE	STATUS	UPDATED_ON
941	85233	FortiManager	18,019,511 Pending CSE Feedback	2025-07-30 20:24:38+00:00
924	85844	FortiManager	18,019,511 Pending CSE Feedback	2025-09-10 18:44:23+00:00
1,083	85244	FortiAnalyzer	18,019,511 Pending CSE Feedback	2025-08-01 09:19:16+00:00
843	89357	FortiManager	7,431,168 Pending Close	2025-11-25 10:10:33+00:00
1,335	89598	FortiAnalyzer	7,431,168 Pending Field Feedback	2026-01-14 11:27:11+00:00
1,552	86349	FortiAnalyzer Cloud	5,726,201 Pending Close	2025-09-18 07:50:16+00:00
460	76501	FortiAnalyzer	3,696,803 Pending Close	2025-03-07 06:57:54+00:00

Automation

Supervision des automates de gestion.

- Cycle de Vie** : Scripts de détection (inactivité 15j/30j).
- Actions** : Warnings automatiques, clôtures.
- Logs** : Visualisation des journaux d'exécution.

The screenshot shows the 'Issue Lifecycle Automation' section of the dashboard. It includes a note about scanning stale issues and performing actions like posting reminders or closing tickets. It also features a 'Configure Schedule' dropdown set to 'Daily/Weekly' and a 'View Last Cron Log' button.

Manual Execution

Trigger an immediate run (Dry Run Recommended first).

Dry Run (Simulation) ⓘ

Use Local CSV Cache ⓘ

Script location: /var/knock_tooling/automation/archive/com_update_1.4.py

Actions

Run Automation Now

Data Management

Gestion de la fraîcheur des données.

- **On-Demand** : Mise à jour manuelle immédiate.
- **Scheduled** : Cron job quotidien (08:00) pour le cache CSV.
- **Logs** : Suivi des mises à jour.

Filtres & Analyse

Contrôle global des données visualisées (Sidebar).

- **Filtres Dynamiques** : Sélection par Années, Statut, Quarter.
- **Dimensions** : Filtrage par Région, Produit et Phase.
- **Mode** : Bascule “Full Analysis” vs “Quarterly Focus”.

6.2.4 4. Points Forts & Valeur Ajoutée

Ce projet apporte une valeur immédiate et mesurable à l'équipe.

- **Gain de Temps** : La génération automatique des rapports (HTML + PPTX) réduit une tâche de 2h à quelques secondes.
- **Fiabilité** : Les données proviennent directement de la source (Knock) sans manipulation manuelle Excel.
- **Visibilité** : Accès temps réel aux KPIs critiques pour la prise de décision.
- **Flexibilité** : L'architecture modulaire permet d'ajouter rapidement de nouvelles analyses.

Rapport d'Étonnement - Mohammad Rezki, Release 1.0

Scheduled CSV Refresh

Server Time: 13:11

Enable CSV Refresh

Days of Week

Monday Tuesday Wednesday
Thursday Friday Saturday Sunday

Hour Minute

07 30

17 Next run: Tomorrow at 07:30

Apply CSV Schedule

Debug Logs (CSV)

Last 50 lines of CSV refresh log:

```
2026-01-17 07:30:01 - INFO: Fetching data for years:  
2026-01-17 07:30:01 - INFO: Running Python script wit  
2026-01-17 07:30:01,918 - INFO - --- Début du script  
2026-01-17 07:30:01,918 - INFO - Chargement de la con  
2026-01-17 07:30:01,918 - INFO - Connexion à l'API Kn  
2026-01-17 07:30:01,918 - INFO - Connexion réussie.  
2026-01-17 07:30:01,918 - INFO - Années à récupérer :  
2026-01-17 07:30:50,777 - INFO - 1613 tickets récupér  
2026-01-17 07:30:50,777 - INFO - Conversion des donné  
2026-01-17 07:30:50,852 - INFO - 5 tickets convertis  
2026-01-17 07:30:50,852 - INFO - Sauvegarde du ficher  
2026-01-17 07:30:50,854 - INFO - CSV régénéré avec su  
2026-01-17 07:30:50,854 - INFO - --- Fin du script --  
2026-01-17 07:30:50 - SUCCESS: CSV refresh completed  
2026-01-17 07:30:50 - INFO: CSV refresh finished.  
2026-01-17 07:30:50 - INFO: Cleaning up lock file...
```

Mode serveur: refresh via webhook (peut prendre 2 min).

Data Management

Start Year for Data Fetching: 2024

End Year for Data Fetching: 2026

On Demand Refresh

Scheduled CSV Refresh

Debug Logs (CSV)

Mode serveur: refresh via webhook (peut prendre 2 min).

Filters

Years: 2024, 2025, 2026

Status: Closed, New, Pending CSE Fee..., Pending Close, Pending Field Fe..., Pending SME Fe..., Pending Valid SF...

Closing Quarter: (Non défini), Q1-2017, Q1-2020, Q1-2021, Q1-2022, Q1-2023, Q1-2024, Q1-2025, Q2-2026, Q2-2027, Q2-2028, Q2-2029, Q2-2030, Q3-2019, Q3-2020, Q3-2021, Q3-2022, Q3-2023, Q3-2024, Q3-2025, Q3-2026, Q3-2027, Q3-2028, Q4-2019, Q4-2020, Q4-2021, Q4-2022, Q4-2023, Q4-2024, Q4-2025, Q4-2026, Q4-2027, Q4-2028, Q4-2029

Regions: T, ANZ, APAC, EMEA, Japan

Products: FortiAnalyzer, FortiAnalyzer Big..., FortiAnalyzer Cl..., FortiCloud - Asset..., FortiCloud - Forti..., FortiCloud - Forti..., FortiCloud - OU, FortiGate-Cloud, FortGuard SOC..., FortiManager, FortiManager Au..., FortiManager Cl..., Managed FortiG...

NOC/SOC Team FY 2024-2026

Central Management & Monitoring - 1596 issues
Closing Quarters: All
Current Quarter: Q1-2026
Last update: 2026-01-19 07:30

[Executive Overview](#) [Sales Pipeline](#) [Products & Regions](#) [Trends & Analytics](#) [Detailed Data](#) [CSE Management](#) [Weekly Report](#) [Report Hub](#) [Automation](#) [Docs](#)

Documentation

No documentation folder found.

6.2.5 Compétences développées (Dashboard)

Ce travail m'a permis de développer les compétences suivantes.

Compétence	Niveau acquis
Python (Pandas, Streamlit)	4/5
Analyse de données	3/5
CI/CD (GitLab)	4/5
Documentation technique	4/5

6.3 Axe 2 : Lab Management

Cet axe concerne l'amélioration de la gestion du laboratoire virtualisé de l'équipe.

6.3.1 Contexte (Lab Management)

L'équipe dispose d'un **laboratoire virtualisé** (vSphere) pour les tests et démonstrations. La gestion des VMs et des adresses IP était partiellement manuelle.

6.3.2 Objectifs

Les objectifs fixés pour ce chantier sont :

1. **Étudier les options d'automatisation** de création de VMs
2. **Intégrer NetBox** comme source de vérité (IPAM)
3. **Documenter les bonnes pratiques**

6.3.3 Analyse d'architecture

J'ai réalisé une étude comparative de **trois approches d'intégration** NetBox/vSphere :

Approche	Avantages	Inconvénients	Cible
Observation	Liberté totale	Données "sales"	R&D, Tests
Orchestration	Hygiène parfaite	Rigide	Formation
Hybride	Flexible	Deux systèmes	Recommandée

6.3.4 Réalisations

Voici les principaux livrables de cet axe de travail.

Livrables

1. **Document d'architecture** : Analyse SWOT des 3 approches
2. **Analyse des options** : Comparaison Ansible/Scripts Python
3. **Intégration NetBox** : Synchronisation des assets
4. **Documentation Sphinx** : Guide complet du lab

6.3.5 Compétences développées (Lab)

Ce travail m'a permis de développer les compétences suivantes.

Compétence	Niveau acquis
vSphere Administration	3/5
Scripts Python	4/5
NetBox (IPAM/DCIM)	4/5
Architecture système	3/5

6.4 Axe 3 : Innovation & Knowledge Sharing

Cet axe regroupe les travaux exploratoires et le partage de connaissances au sein de l'équipe.

6.4.1 Projet MCP (Model Context Protocol)

Le projet MCP représente la composante innovation de mon alternance.

Contexte (MCP)

Le **MCP (Model Context Protocol)** est un protocole émergent permettant de connecter des LLM (Large Language Models) à des outils externes.

Objectif du PoC

Connecter **Claude Desktop** (Anthropic) à **FortiManager** pour permettre la gestion conversationnelle des équipements Fortinet.

Architecture cible

Le schéma suivant illustre l'architecture envisagée pour le projet MCP.

Travaux réalisés

Voici les principales étapes réalisées sur ce projet.

- Étude du protocole MCP et de l'API FortiManager
- Mise en place d'un environnement de test (FortiPoc)
- **Test de connexion** : Cible FMG v7.6 (IP : 10.210.34.120)
- Documentation des limitations rencontrées

Difficultés rencontrées

Plusieurs obstacles techniques ont été identifiés, notamment liés à la licence.

Blocages techniques

- **Version FMG** : La version “Development” utilisée ne dispose pas de shell accessible pour le debug
- **Licence** : Problèmes d’activation limitant les fonctionnalités API
- **Compatibilité** : Ajustements nécessaires pour le format JSON-RPC
- **CORS** : Configuration des headers manquante sur le serveur de dev

6.4.2 Knowledge Sharing

En parallèle, je participe à l’initiative de **partage de connaissances** :

- Contribution à la documentation **CMM**
- Rédaction de guides techniques (Sphinx)
- Présentations internes sur mes travaux

Certifications Fortinet obtenues :

Je profite également de l'accès aux ressources de formation pour passer les certifications officielles Fortinet (NSE).

- **Fierce FortiGate** (NSE 1, 2, 3) : Fondamentaux de la cybersécurité
- **Fortinet Certified Fundamentals** (FCF) : Certifié
- **Fortinet Certified Associate** (FCA) : En cours de préparation)

6.5 Synthèse des missions

Le diagramme ci-dessous illustre la répartition de mon temps entre les différents axes.

6.5.1 État d'avancement

Voici l'état d'avancement de chaque mission à ce jour.

Mission	Statut	Progression
Dashboard Knock	En production	90%
Weekly Report	En production	85%
Lab Automation	En développement	60%
Projet MCP	PoC en cours	40%
Documentation	Continu	-

Propositions d'amélioration

Ce chapitre propose des pistes d'amélioration concrètes basées sur mes observations.



7.1 Introduction

Fort de mes observations et de mon expérience de ces premiers mois, je propose ici des pistes d'amélioration concrètes, dans mon domaine de compétence, pour contribuer à l'efficacité de l'équipe.

Approche

Ces propositions sont formulées avec humilité, en tant que regard neuf sur l'existant. Elles visent à apporter de la valeur tout en respectant les contraintes et l'historique de l'équipe.

7.2 Proposition 1 : Unification des outils de reporting

Cette proposition vise à simplifier les outils de suivi de l'équipe.

7.2.1 Constat (Reporting)

Actuellement, plusieurs outils coexistent pour le reporting :

- Dashboard Knock Analytics (visualisation temps réel)
- Scripts de génération de rapports hebdomadaires
- Exports manuels vers Excel

7.2.2 Proposition (Reporting)

L'idée est de regrouper ces outils en un dashboard uniifié.

Avantages :

Cette solution présente plusieurs bénéfices.

- Point d'entrée unique pour l'équipe
- Cohérence des données et des calculs
- Maintenance simplifiée (un seul code base)
- Meilleure expérience utilisateur

Effort estimé : 2-3 semaines de développement

7.2.3 Statut

Cette proposition a été largement implémentée durant le mois de janvier 2026.

Réalisation concrète

Le **CMM Dashboard** présenté dans le chapitre *Missions* concrétise cette vision. L'unification est effective (Executive Overview, Weekly Report HTML/PPTX, Pipeline...).

7.3 Proposition 2 : Centralisation de la documentation

Cette proposition vise à améliorer l'accès à la documentation.

7.3.1 Constat (Documentation)

La documentation est actuellement répartie entre :

- GitLab (README, docs techniques)
- SharePoint (procédures)
- Teams (discussions, fichiers)
- Sphinx (documentations formelles)

Cela peut créer de la confusion pour un nouvel arrivant.

7.3.2 Proposition (Centralisation)

Créer un **portail documentaire unique** basé sur Sphinx, avec :

| Quick Start | Guide d'intégration nouveaux arrivants | | Procédures | Toutes les procédures opérationnelles | | Technique | Documentation des projets | | Formation | Liens vers les ressources NSE |

Structure proposée :

```
docs/
├── index.md (portail d'accueil)
├── quickstart/
│   ├── onboarding.md
│   └── tools.md
├── procedures/
│   ├── lab/
│   └── support/
└── projects/
    ├── knock/
    ├── lab-management/
    └── mcp/
```

Effort estimé : 1-2 semaines (réorganisation)

7.4 Proposition 3 : Automatisation du cycle de vie Lab

Cette proposition s'attaque à la lourdeur administrative de la gestion du lab pour fluidifier l'expérience utilisateur.

7.4.1 Constat (Lab)

La gestion des VMs dans le lab implique plusieurs étapes manuelles :

- Réservation d'IP dans NetBox
- Création de la VM dans vSphere
- Configuration réseau
- Mise à jour DNS

7.4.2 Proposition (Automatisation)

Développer un **pipeline automatisé complet** :

Fonctionnalités clés :

- Interface web simple pour les demandes
- Validation automatique des ressources disponibles
- Provisioning en 5-10 minutes
- Notification par email/Teams

Effort estimé : 4-6 semaines

7.5 Proposition 4 : Tests automatisés pour les scripts

Pour garantir la qualité du code, la mise en place d'environnements de pré-production (staging) et production est essentielle. Mais pour aller plus loin et appliquer les bonnes pratiques, il est nécessaire d'ajouter des tests unitaires à chaque projet.

7.5.1 Constat (Tests)

Les scripts Python du Dashboard et du reporting ne disposent pas de tests unitaires formalisés.

7.5.2 Proposition (Tests)

Mettre en place une **suite de tests automatisés** :

```
# Exemple de structure de tests
tests/
├── test_data_parsing.py      # Tests du parsing CSV
├── test_kpi_calculations.py # Tests des calculs KPIs
├── test_report_generation.py # Tests de génération
└── conftest.py               # Fixtures partagées
```

Intégration CI/CD :

Voici un exemple de configuration GitLab CI/CD pour automatiser les tests.

```
# .gitlab-ci.yml (extrait)
test:
  stage: test
  script:
    - pip install pytest
    - pytest tests/ --verbose
  coverage: '/TOTAL.*\s+(\d+%) /'
```

Avantages :

Les tests automatisés offrent plusieurs bénéfices.

- Détection précoce des régressions
- Documentation vivante du comportement attendu
- Confiance lors des modifications

Effort estimé : 1-2 semaines

7.6 Proposition 5 : Documentation du projet MCP

Cette proposition concerne la documentation du projet innovant MCP.

7.6.1 Constat (MCP)

Le projet MCP est innovant mais peu documenté. Les difficultés rencontrées (versions FMG, configuration JSON-RPC) pourraient bloquer de futurs développeurs.

7.6.2 Proposition (Doc MCP)

Créer une **documentation complète** du PoC MCP :

1. **Guide d'installation** : Étapes détaillées pour reproduire l'environnement
2. **Troubleshooting** : Problèmes connus et solutions
3. **Architecture** : Diagrammes et flux de données
4. **API Reference** : Endpoints FortiManager utilisés

Valeur ajoutée

Cette documentation pourrait être partagée avec la communauté (GitHub) pour favoriser l'adoption du protocole MCP avec les produits Fortinet.

Effort estimé : 1 semaine

7.7 Synthèse des propositions

Le tableau ci-dessous résume l'ensemble des propositions avec leur impact et effort estimés.

#	Proposition	Impact	Effort	Priorité
1	Unification reporting	High	Moyen	Haute
2	Centralisation docs	Medium	Faible	Moyenne
3	Automatisation Lab	High	Élevé	Haute
4	Tests automatisés	Medium	Faible	Moyenne
5	Doc MCP	Low	Faible	Basse

Engagement

Je m'engage à contribuer activement à la réalisation de ces propositions dans la suite de mon alternance, en coordination avec mon tuteur et l'équipe.

Conclusion

Ce chapitre dresse le bilan de cette expérience et ouvre des perspectives pour la suite.



8.1 Bilan personnel

Ces premiers mois d'alternance chez Fortinet ont été riches en apprentissages et en découvertes. Le regard neuf que j'ai pu porter sur l'entreprise m'a permis d'identifier à la fois les forces remarquables de l'organisation et les axes d'amélioration possibles.

8.1.1 Ce que j'ai appris

Cette alternance m'a permis d'acquérir de nombreuses compétences.

Compétences techniques

- **Développement** : Python avancé (Pandas, Streamlit), CI/CD avec GitLab
- **Infrastructure** : Virtualisation (vSphere), IPAM (NetBox), Conteneurisation (Docker)
- **Cybersécurité** : Écosystème Fortinet, FortiManager API, concepts NGFW
- **Documentation** : Sphinx, Mermaid, bonnes pratiques de rédaction technique

Au-delà des aspects techniques, j'ai également développé des compétences transversales.

Compétences transversales

- **Autonomie** : Capacité à avancer sur des projets avec un cadrage minimal
- **Communication** : Interaction avec différents profils (CSE seniors, management)
- **Adaptation** : Gestion de la complexité et de l'incertitude
- **Esprit critique** : Analyse objective des situations

8.1.2 Ce qui m'a marqué

Plusieurs aspects de cette expérience resteront gravés dans ma mémoire.

1. **La confiance accordée** : Dès le départ, j'ai été traité comme un membre à part entière de l'équipe
 2. **La qualité technique** : Le niveau d'exigence et de maturité des pratiques
 3. **L'innovation** : La volonté d'explorer de nouvelles technologies (IA, MCP)
 4. **L'entraide** : La disponibilité des collègues pour partager leurs connaissances
-

8.2 Projection vers le métier d'ingénieur

Cette expérience confirme et affine ma vision de mon futur métier.

8.2.1 Vision du métier

Cette expérience chez Fortinet m'a permis de mieux cerner le métier d'**ingénieur en cybersécurité** :

8.2.2 Mes aspirations

À la lumière de cette expérience, je souhaite :

1. **Approfondir mes compétences** en automatisation et DevSecOps
 2. **Explorer l'IA appliquée** à la cybersécurité (détection, réponse)
 3. **Contribuer à l'innovation** (projets comme le MCP)
 4. **Partager mes connaissances** via la documentation et la formation
-

8.3 Défis de demain

L'avenir se prépare dès aujourd'hui, tant pour l'entreprise que pour ma propre trajectoire professionnelle.

8.3.1 Pour l'entreprise

Fortinet fait face à des défis majeurs que j'ai pu observer :

- **Concurrence accrue** sur le marché de la cybersécurité
- **Évolution des menaces** (IA offensive, attaques sophistiquées)
- **Transition cloud** des clients
- **Attractivité des talents** dans un marché tendu

8.3.2 Pour moi

Mes défis pour la suite de l'alternance

1. **Finaliser les projets en cours** : Dashboard unifié, Lab automation
2. **Poursuivre les certifications** : NSE 4+ (déjà obtenu : FCA, NSE 1, NSE 3)
3. **Contribuer à l'équipe** de manière significative
4. **Préparer mon projet de fin d'études** en lien avec ces missions

8.4 Remerciements

Je tiens à remercier chaleureusement :

- **Jean-Pierre Forcioli**, mon tuteur, pour son accompagnement, sa patience et sa confiance
- **L'équipe NOC/SOC** de Sophia-Antipolis pour son accueil et sa disponibilité
- **Les autres alternants et stagiaires** pour les échanges et le soutien mutuel

- **Fortinet** pour cette opportunité d'apprentissage dans un environnement stimulant
-

8.5 Mot de la fin

Note

Le rapport d'étonnement n'est pas un exercice de critique, mais une invitation à regarder avec des yeux neufs et à contribuer avec enthousiasme.

Cette alternance chez Fortinet représente une étape clé de ma formation d'ingénieur. Les compétences acquises, les projets réalisés et les relations nouées constituent un socle solide pour la suite de mon parcours professionnel.

Je suis impatient de poursuivre cette aventure et de continuer à apporter ma contribution à l'équipe.

Contact

Mohammad Rezki

Alternant Ingénieur - CESI École d'Ingénieurs

Fortinet, Sophia-Antipolis

Promotion 2026

Glossaire

9.1 Termes techniques

Terme	Définition
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information - Autorité française en cybersécurité
API	Application Programming Interface - Interface de programmation permettant la communication entre logiciels
CI/CD	Continuous Integration / Continuous Deployment - Pratiques DevOps d'automatisation du développement et déploiement
CSE	Customer Support Engineer - Ingénieur support technique chez Fortinet
DCIM	Data Center Infrastructure Management - Gestion de l'infrastructure des centres de données
DevOps	Méthodologie combinant développement (Dev) et opérations (Ops) pour accélérer les livraisons
DORA	Digital Operational Resilience Act - Réglementation européenne sur la résilience numérique
EMEA	Europe, Middle East and Africa - Région géographique couverte par Fortinet Sophia
IPAM	IP Address Management - Gestion centralisée des adresses IP
JSON-RPC	Protocole d'appel de procédure distante utilisant le format JSON
LLM	Large Language Model - Modèle de langage de grande taille (ex: ChatGPT, Claude)
MCP	Model Context Protocol - Protocole de connexion entre LLM et outils externes
NetBox	Outil open-source de gestion d'infrastructure réseau (IPAM/DCIM)
NGFW	Next-Generation Firewall - Pare-feu nouvelle génération
NIS2	Network and Information Security Directive 2 - Directive européenne sur la cybersécurité
NOC	Network Operations Center - Centre d'opérations réseau
NSE	Network Security Expert - Programme de certification Fortinet
PoC	Proof of Concept - Démonstration de faisabilité
RGPD	Règlement Général sur la Protection des Données
RSE	Responsabilité Sociétale des Entreprises
SIEM	Security Information and Event Management - Gestion des événements de sécurité
SOC	Security Operations Center - Centre d'opérations de sécurité
Sphinx	Générateur de documentation technique en Python
Streamlit	Framework Python pour créer des applications web de visualisation de données
SWOT	Strengths, Weaknesses, Opportunities, Threats - Matrice d'analyse stratégique
UTM	Unified Threat Management - Gestion unifiée des menaces
VLAN	Virtual Local Area Network - Réseau local virtuel
VM	Virtual Machine - Machine virtuelle
vSphere	Plateforme de virtualisation VMware
Zero Trust	Modèle de sécurité "ne jamais faire confiance, toujours vérifier"

9.2 Produits Fortinet mentionnés

Produit	Description
FortiGate	Pare-feu nouvelle génération (NGFW) - Produit phare de Fortinet
FortiManager	Console de gestion centralisée des équipements Fortinet
FortiAnalyzer	Plateforme d'analyse des logs et de reporting sécurité
FortiAI	Solution d'intelligence artificielle pour la cybersécurité
FortiPAM	Gestion des accès privilégiés (Privileged Access Management)
FortiSIEM	Solution de corrélation d'événements de sécurité
FortiMonitor	Outil de monitoring d'expérience digitale
FortiOS	Système d'exploitation des équipements Fortinet
FortiPoc	Plateforme de démonstration et de formation
Security Fabric	Architecture intégrée de sécurité Fortinet

Bibliographie

10.1 Sources officielles

1. **FORTINET INC.** *About Fortinet - Company Overview*. [En ligne]. Disponible sur : <https://www.fortinet.com/corporate/about-us/about-us.html>. Consulté le 15 janvier 2026.
2. **FORTINET INC.** *FortiOS Documentation*. [En ligne]. Fortinet Document Library. Disponible sur : <https://docs.fortinet.com/>. Consulté le 10 janvier 2026.
3. **FORTINET INC.** *Network Security Expert (NSE) Certification Program*. [En ligne]. Disponible sur : <https://training.fortinet.com/>. Consulté le 5 novembre 2025.

10.2 Documentation technique

4. **NETBOX COMMUNITY.** *NetBox Documentation*. [En ligne]. Read the Docs. Disponible sur : <https://docs.netbox.dev/>. Consulté le 12 novembre 2025.
5. **VMWARE INC.** *vSphere Documentation*. [En ligne]. VMware Docs. Disponible sur : <https://docs.vmware.com/en/VMware-vSphere/>. Consulté le 8 novembre 2025.
6. **DOCKER INC.** *Docker Documentation*. [En ligne]. Disponible sur : <https://docs.docker.com/>. Consulté le 15 novembre 2025.
7. **SPHINX TEAM.** *Sphinx Documentation Generator*. [En ligne]. Disponible sur : <https://www.sphinx-doc.org/>. Consulté le 20 novembre 2025.

10.3 Intelligence Artificielle et Innovation

8. **ANTHROPIC.** *Model Context Protocol (MCP) Specification*. [En ligne]. GitHub. Disponible sur : <https://github.com/anthropics/anthropic-cookbook>. Consulté le 31 décembre 2025.
9. **FORTINET INC.** *FortiAI - AI-Powered Security Operations*. [En ligne]. Disponible sur : <https://www.fortinet.com/products/fortiai>. Consulté le 5 janvier 2026.

10.4 Méthodologie et analyse

10. **HUMPHREY A.** *SWOT Analysis for Management Consulting*. SRI International, Stanford Research Institute, 1960-1970.

10.5 Réglementation

11. **JOURNAL OFFICIEL DE L'UNION EUROPÉENNE.** *Directive (UE) 2022/2555 (NIS2)*. [En ligne]. EUR-Lex. Disponible sur : <https://eur-lex.europa.eu/>. Consulté le 10 janvier 2026.

12. **ANSSI.** *Guide d'hygiène informatique.* [En ligne]. Agence Nationale de la Sécurité des Systèmes d'Information. Disponible sur : <https://www.ssi.gouv.fr/>. Consulté le 12 janvier 2026.

10.6 Rapports sectoriels

13. **GARTNER INC.** *Magic Quadrant for Network Firewalls.* 2024. [Rapport payant].
14. **CYBERSECURITY VENTURES.** *Cybersecurity Market Report.* 2024. [En ligne]. Disponible sur : <https://cybersecurityventures.com/>. Consulté le 8 janvier 2026.
-

Note

Les URLs internes GitLab de Fortinet n'ont pas été incluses dans cette bibliographie pour des raisons de confidentialité.

À propos de ce document

Ce rapport d'étonnement a été rédigé dans le cadre de l'alternance au sein de **Fortinet** (Sophia-Antipolis), conformément aux exigences du cursus **Ingénieur CESI**.

- **Auteur** : Mohammad Rezki
- **Période couverte** : Octobre 2025 - Janvier 2026
- **Tuteur entreprise** : Jean-Pierre Forcioli
- **École** : CESI École d'Ingénieurs