CYCLE DE FORMATION

Architecte Technique en Informatique et Réseaux

Titre RNCP - Niveau 7

PROJET DE FIN D'ETUDES

Sujet :

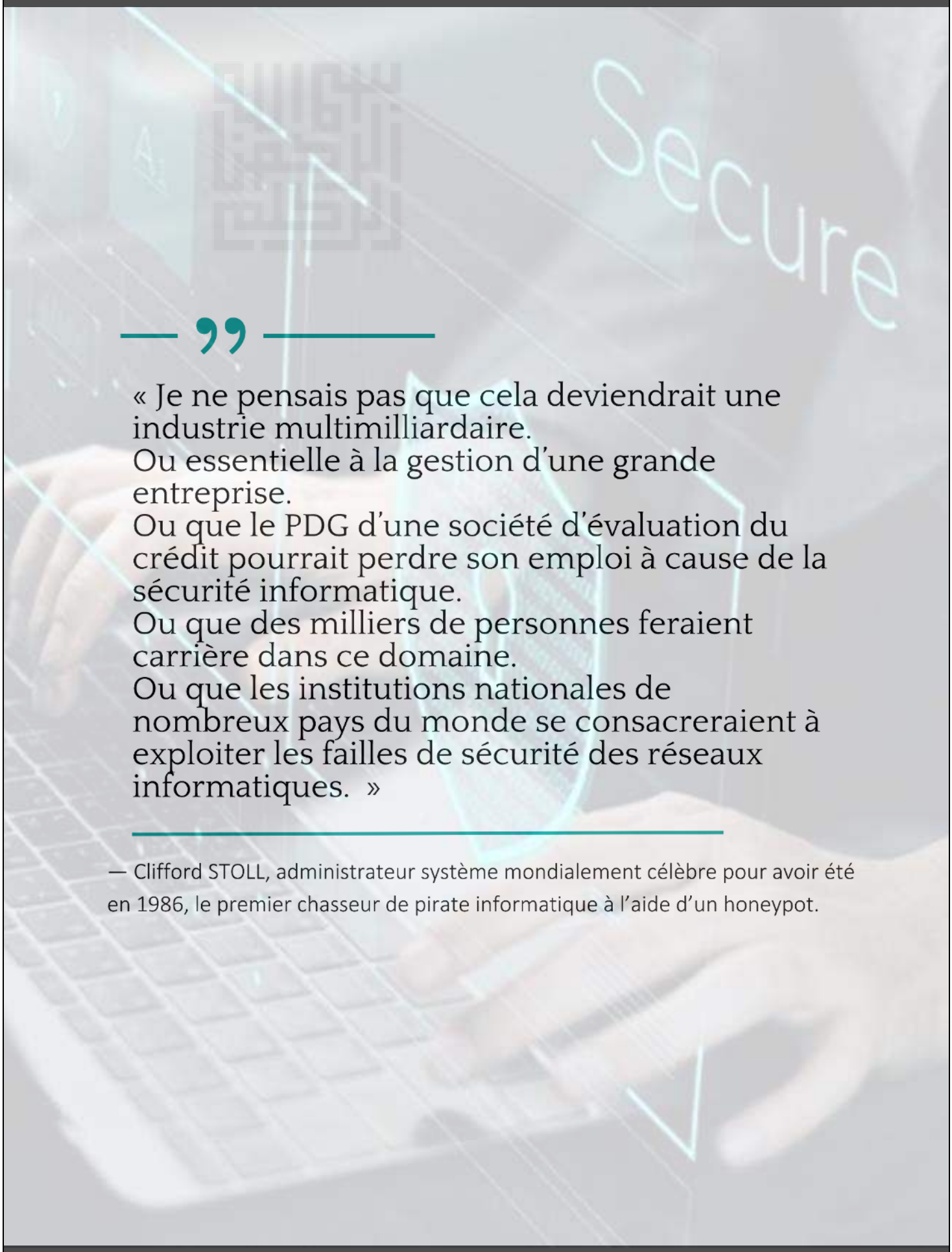
Conception et déploiement d'une architecture sécuritaire multicouche pour la surveillance du réseau et la détection d'intrusion

SOUTENU par : **Nicolas BODAINE**

ENTREPRISE : **EasyFormer**

Sous le tutorat de M. **Yann BENHAMRON**

Période du **1/09/2022** au **31/08/2024**



« Je ne pensais pas que cela deviendrait une industrie multimilliardaire.
Ou essentielle à la gestion d'une grande entreprise.
Ou que le PDG d'une société d'évaluation du crédit pourrait perdre son emploi à cause de la sécurité informatique.
Ou que des milliers de personnes feraient carrière dans ce domaine.
Ou que les institutions nationales de nombreux pays du monde se consacreraient à exploiter les failles de sécurité des réseaux informatiques. »

— Clifford STOLL, administrateur système mondialement célèbre pour avoir été en 1986, le premier chasseur de pirate informatique à l'aide d'un honeypot.

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

Versions du document		
Numéro	Date	Commentaire
1	14/07/2024	Rédaction terminée, document envoyé pour relecture et validation
2	20/07/2024	Document validé pour la soutenance

I. AVANT-PROPOS

A. PRESENTATION DU DOCUMENT

Ce document est mon mémoire de fin d'études destiné à être soutenu devant un jury composé de professionnels du métier pour l'obtention du diplôme d'*Architecte Technique en Informatique et Réseaux*.

J'y présente un projet enrichissant en architecture de sécurité réseau que j'ai eu la chance de mettre en place cette année au sein de mon entreprise d'accueil.

J'atteste que ce document est le fruit de mon travail et de mes efforts personnels.

Nicolas BODAINE

B. REMERCIEMENTS

Je souhaite exprimer ma profonde gratitude à tous les enseignants que j'ai eu durant mes études pour les précieuses connaissances qu'ils m'ont transmises.

Un grand merci aussi au personnel administratif des établissements scolaires et organismes de formation dans lesquels j'ai étudié pour leur gestion impeccable et leur professionnalisme.

Mes collègues de travail méritent également des remerciements pour leur bienveillance au quotidien et le partage de leurs expériences enrichissantes.

Un remerciement particulier à ma famille, dont le soutien et les encouragements ont été essentiels à mon parcours.

Enfin, un remerciement aux membres du jury, qui vont prêter leur oreille experte à la soutenance de ce mémoire.

C. PRESENTATION PERSONNELLE

1. Mon parcours scolaire, mes diplômes et certifications

Mon attrait pour la technologie s'est révélé très tôt dans mon parcours scolaire. Après le collège, je me suis orienté vers un Brevet d'Etudes Professionnelles dans les **Métiers de l'Electronique**[1] que j'ai obtenu en 2008, suivi d'un Bac Professionnel orienté **Systèmes Electroniques Numériques**[2] (SEN). Quelques années plus tard, j'ai décroché le Titre Professionnel de **Technicien Supérieur Systèmes et Réseaux**[3] (TSSR) avec les compliments d'un des membres du jury.

[1] Plus d'informations sur ce BEP sur : https://www.intercariforef.org/formations/certification-21889.html
[2] Plus d'informations sur ce Bac Pro de niveau 4 au RNCP sur : https://www.francecompetences.fr/recherche/rncp/4089/
[3] Plus d'informations sur ce titre professionnel de niveau 5 au RNCP sur : https://www.francecompetences.fr/recherche/rncp/31115/

Cela m'a motivé à continuer mes études afin de décrocher le diplôme **d'Analyste en Génie Informatique et Réseaux**[4] (AGIR) à l'Institut National Supérieur des Technologies Avancées (INSTA)[5], mais cette fois-ci en alternance dans un groupement d'associations à but non lucratif exerçant ses activités dans le milieu de la restauration et de la formation professionnelle.

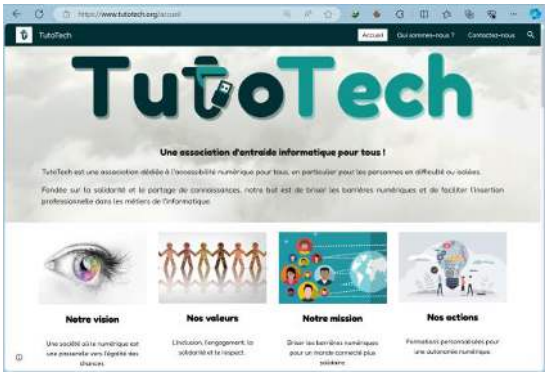
J'ai obtenu mon diplôme avec la mention « Très bien ». J'ai donc décidé de poursuivre mes études et de viser l'obtention du diplôme d'**Architecte Technique en Informatique et Réseaux**[6], toujours à l'INSTA, mais en changeant d'entreprise pour intégrer le Réseau EasyFormer, lui aussi un groupement d'associations à but non lucratif exerçant ses activités dans le milieu de l'informatique et de la formation professionnelle et chez qui j'avais précédemment fait mon stage en TSSR un peu plus d'un an auparavant.

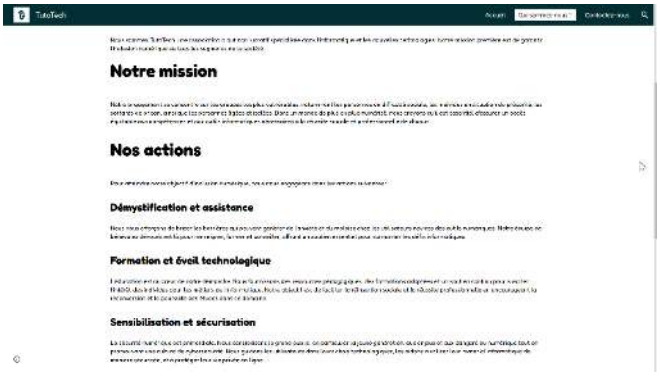
Appréciant particulièrement la cybersécurité défensive (*blue team*), j'ai en parallèle de mes études à l'INSTA, étudié le pare-feu de nouvelle génération « Stormshield Network Security » (SNS) et approfondi mes connaissances en sécurité réseau et *firewalling* pour finalement réussir à décrocher ces deux certifications : **Certified Stormshield Network Administrator** (CSNA) puis **Certified Stormshield Network Expert** (CSNE). Je me suis ensuite intéressé à la solution EDR (*Endpoint Detection and Response*) de Stormshield nommée « Stormshield Endpoint Security Evolution » et j'ai obtenu la certification **Certified Stormshield Endpoint Administrator** (CSEA). Mon prochain objectif à court terme est d'obtenir le niveau de certification supérieur : **Certified Stormshield Endpoint Expert** (CSEE).

[4] Plus d'informations sur ce titre professionnel de niveau 6 au RNCP sur : https://www.francecompetences.fr/recherche/rncp/29069/
[5] Plus d'informations sur l'école : https://www.insta.fr/Pourquoi-Choisir-INSTA/
[6] Plus d'informations sur ce titre professionnel de niveau 7 au RNCP sur : https://www.francecompetences.fr/recherche/rncp/29069/

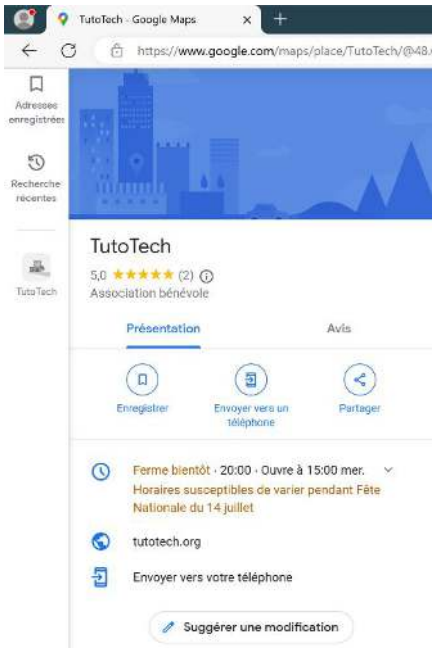
2. Mon engagement social

Je suis l'un des fondateurs de TutoTech[7], une association à but non lucratif d'entraide, d'enseignement et d'assistance informatique dont l'un des objectifs est d'assurer un accès équitable aux compétences et aux outils informatiques nécessaires à la réussite sociale et professionnelle de chacun. Je m'occupe de quasiment tout au sein de cette association : création et administration du site web, élaboration des graphismes, animation d'ateliers, visibilité sur les réseaux sociaux, établissement de partenariats, mentorat, etc.





Du fait de ma proximité avec le milieu de la formation professionnelle, il m'arrive aussi d'accompagner bénévolement des apprenants dans la rédaction des livrables qu'ils doivent rendre pour valider leur formation (dossier de projet, rapport de stage, dossier professionnel, mémoire, PFE, etc.). Voici ci-dessous l'avis[8] Google qui a été laissé par Maher S., l'un de mes apprenants qui a bénéficié d'un suivi particulier tout le long de sa formation AIS et qui a également contribué à la réalisation de mon PFE :



[7] Plus d'informations sur l'association sur : https://tutotech.org/
[8] Lien vers l'avis complet : https://maps.app.goo.gl/zirtj99WqQz7dHJk9

A l'avenir je souhaite faire évoluer le site web de l'association en y publiant des tutoriels informatiques qui seront libres de droit et me serviront également de supports de travaux pratiques à l'occasion de mes prestations de formation.

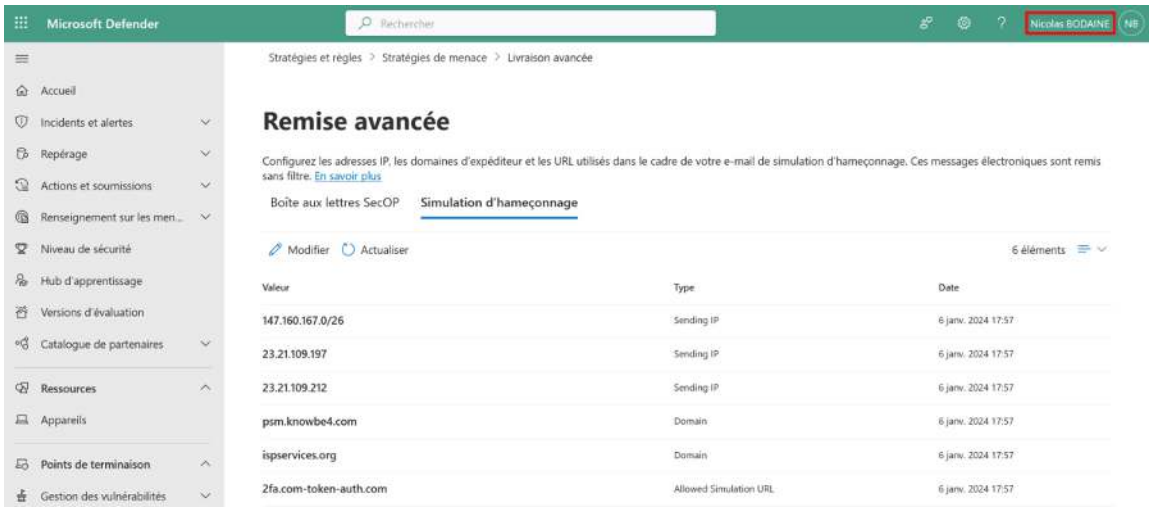
3. Mes missions au sein de l'entreprise

Depuis 2 ans, mes missions au sein du Réseau EasyFormer ont été diverses et variées allant de l'administration système/réseau/cloud à des prestations de formation, en passant par de la rédaction de documentation ou encore l'établissement de partenariats avec des sociétés de solutions informatiques. Mais j'ai principalement tenu ces deux rôles :

1) Administrateur des systèmes et réseaux informatiques

- Administration des systèmes, réseaux et des infrastructures cloud d'EasyFormer
- Audits de sécurité, supervision et établissement de rapports
- Sécurisation des serveurs et durcissement des configurations
- Sensibilisation des collaborateurs aux bonnes pratiques de sécurité
- Automatisation de tâches d'administration
- Rédaction de cahiers des charges pour des projets informatiques
- Documentation des processus, des configurations et des changements
- Mentorat pour les stagiaires intégrant l'équipe EasyFormer

Voici, pour illustrer l'un des exemples cités ci-dessus, une capture d'écran que j'ai effectuée lors de la configuration de notre *tenant* Microsoft 365 à l'occasion d'une simulation d'hameçonnage utilisant la plateforme KnowBe4 et destinée à sensibiliser mes collègues contre cette menace :

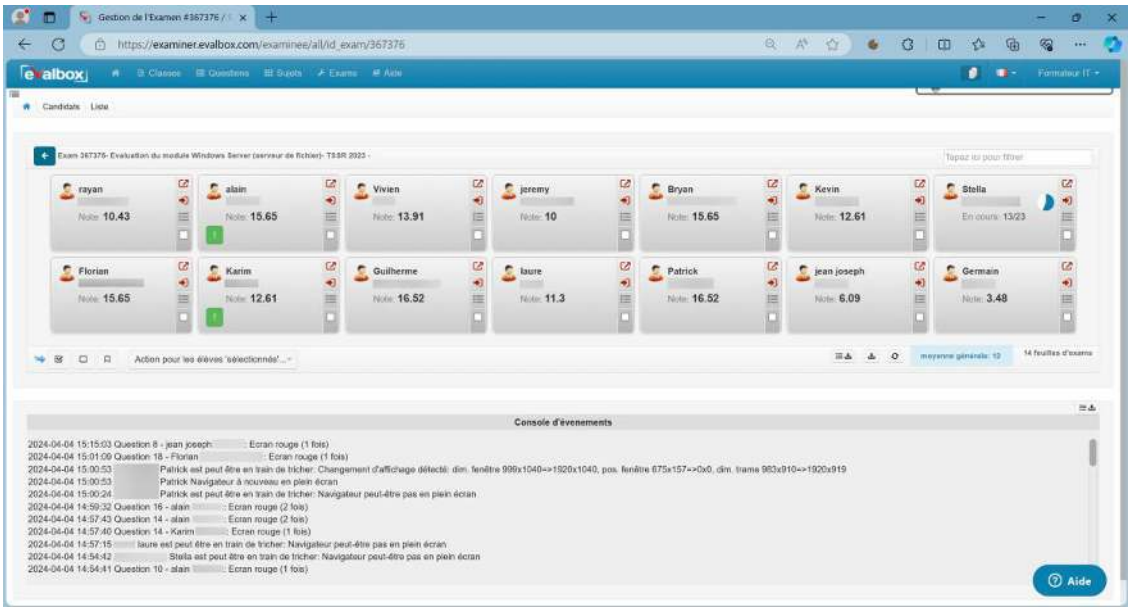


Au-delà de mes compétences purement techniques, je suis reconnu au sein de mon entreprise pour ma rigueur et mon travail soigné. Je suis donc régulièrement sollicité lorsqu'un travail rédactionnel exigeant est demandé (documentation de procédures, réalisation de supports de travaux pratiques, cahier des charges, etc.).

2) Formateur en informatique

- Animation de sessions de formation pour adultes en reconversion professionnelle dans des cursus informatiques TAI, TSSR, AIS et ASR dans divers domaines IT (supervision, cloud, firewalling, cybersécurité, virtualisation, automatisation, sauvegarde, réseaux, administration, accompagnement à la réalisation des livrables de fin d'étude, etc.)
- Veille technologique, révision des acquis et apprentissage continu en préparation des prestations de formation à venir
- Rédaction pédagogique IT (supports de cours, supports de travaux pratiques, évaluation, correction, QCM, fiches de révision)
- Ingénierie pédagogique (élaboration de programmes de formation, mise à jour des modules de formation)

Voici, pour illustrer l'une de mes missions en tant que formateur, une capture d'écran que j'ai effectuée en avril 2024 lors de l'évaluation d'une classe de TSSR via la plateforme EvalBox pour clôturer un module d'initiation au rôle « serveur de fichiers » de Windows Server :



Du fait de l'obtention de la certification de niveau « Expert » mentionnée ci-dessus et grâce à un partenariat conclu entre Stormshield et l'organisme de formation EasyFormers lié à mon entreprise d'accueil, je suis devenu instructeur officiel pour la marque Stormshield. J'anime désormais des sessions de formation CSNA et permets à mes étudiants de passer cette certification à tarif réduit.

D. PRESENTATION DE MON ENTREPRISE D'ACCUEIL

Le Réseau EasyFormer rassemble un collectif d'associations à but non lucratif (*EasyFormer*, *Alwayformer*, *Happyformer*, *Agencyformer*) et un organisme de formation (*EasyFormers*).

1. Activité

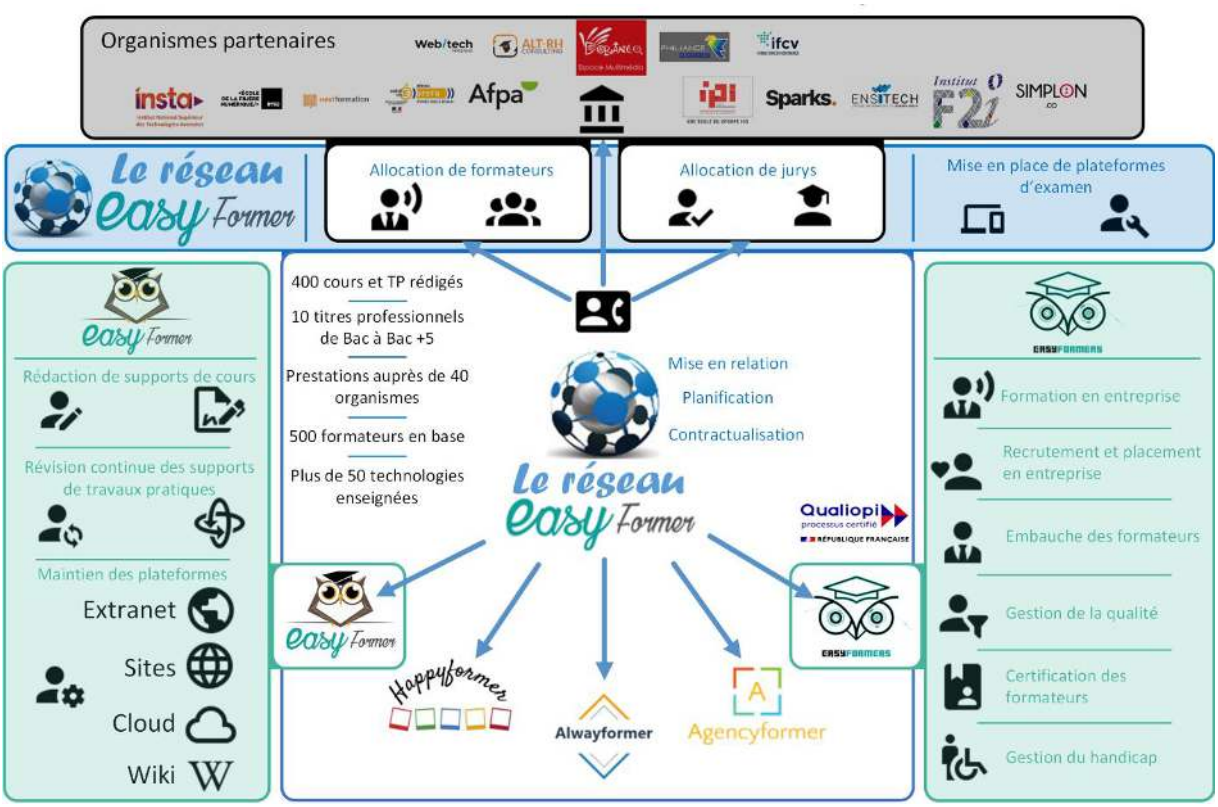


Illustration 1 : schéma fonctionnel du Réseau EasyFormer

Le Réseau EasyFormer exerce ses activités dans le domaine de l'informatique et de la formation professionnelle :

- Prestations de formation aux entreprises
- Mise en relation de formateurs auprès d'organismes de formation
- Placement de formateurs et gestion de leur planning
- Mise en relation des organismes de formation avec des jurys professionnels
- Rédaction pédagogique
- Ingénierie pédagogique
- Mise en place de plateformes techniques pour les centres d'examen
- Prêt de matériel informatique
- Prestations de services informatiques
- Conseil IT aux entreprises
- Mise en relation des apprenants auprès des entreprises
- Gestion des besoins pour les stages
- Conseil d'aides à l'embauche

2. Organigramme

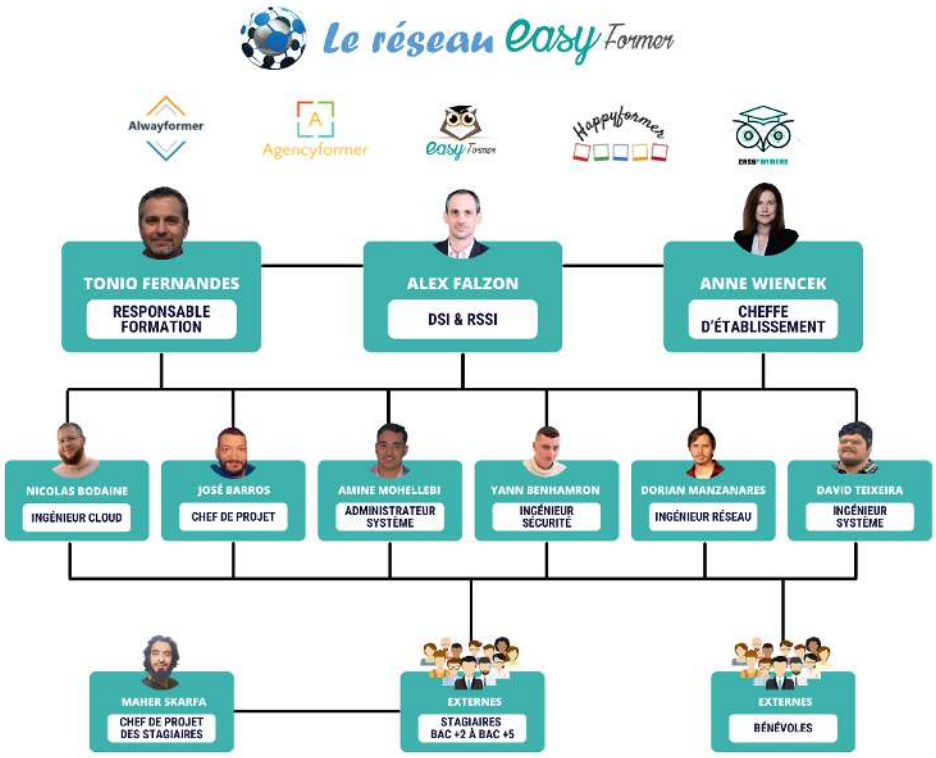


Illustration 2 : organigramme du Réseau EasyFormer en 2024

M^r^ FALZON est le directeur du système d'information et responsable de sa sécurité, chaque changement au sein de l'architecture doit lui être soumis avant validation. Il a également une seconde activité de formateur en informatique.

M^r^ FERNANDES s'occupe de la partie administrative, juridique et de la relation avec les différents centres de formation, ainsi que l'affectation des formateurs dans ces derniers. Il s'assure aussi de la qualité des prestations de formation.

M^me^ WIENCEK s'occupe de tout ce qui est en lien avec l'organisme de formation EasyFormers (certification Qualiopi, etc.).

M^r^ BARROS est chargé, en lien avec **M^r^ FERNANDES**, de la plupart des tâches administratives et juridiques en plus de la chefferie de projet. Il est aussi formateur IT.

M^r^ MANZANARES, **M^r^ BENHAMRON**, **M^r^ TEIXEIRA** et **moi-même** sommes chargés de l'infrastructure informatique et d'intervention techniques chez des clients. Nous sommes polyvalents bien que nous ayons chacun été affectés à un poste spécifique (système, réseau, cloud, cybersécurité). Nous sommes aussi formateurs IT. M^r^ BENHAMRON et moi-même sommes aussi chargés de la gestion de la documentation pédagogique et technique.

M^r^ MOHELLEBI est un alternant en 2^e^ année de BTS, il est régulièrement chargé de diverses tâches d'administration système et réseau par M^r^ FALZON dans le cadre de son apprentissage.

3. Architecture réseau

Le Réseau EasyFormer héberge sur son site de Cergy ses sites web, ses services extranet et une plateforme de partage de ressources (Nextcloud et NAS Synology) servant à collecter, stocker puis partager les supports de cours et les documentations fournis par les formateurs, alternants, stagiaires et apprenants.

Une plateforme collaborative d'intégration continue documentaire est également en cours de finalisation. Elle permettra de mieux gérer le versioning des supports pédagogiques :

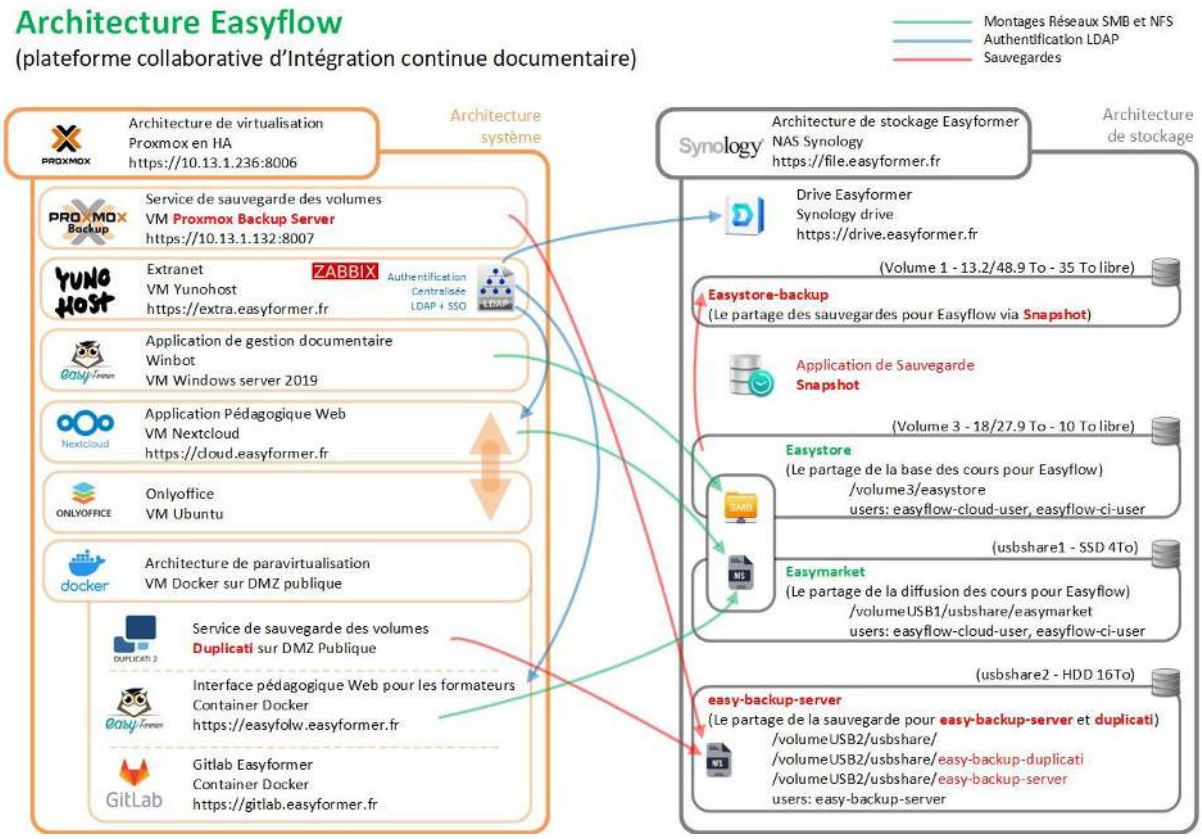


Illustration 3 : schéma fonctionnel de la plateforme EasyFlow

Pour la communication interne et la documentation technique, une base de connaissances collaborative (Wiki.js) est également en place et constamment mise à jour.

EasyFormer fournit aussi aux apprenants et leurs formateurs, des plateformes de virtualisation (ESXi et Proxmox) à vocation pédagogique pour la réalisation de projets de fin d'études et de travaux pratiques.

Le Réseau EasyFormer dispose aussi de services cloud : espace de stockage, messagerie et outils de productivité via un tenant Microsoft 365 (non représenté sur le schéma ci-dessous).

Voici le schéma logique du réseau informatique « on-premises » d'EasyFormer (**par mesure de sécurité les adresses IP réelles ont été modifiées**) :

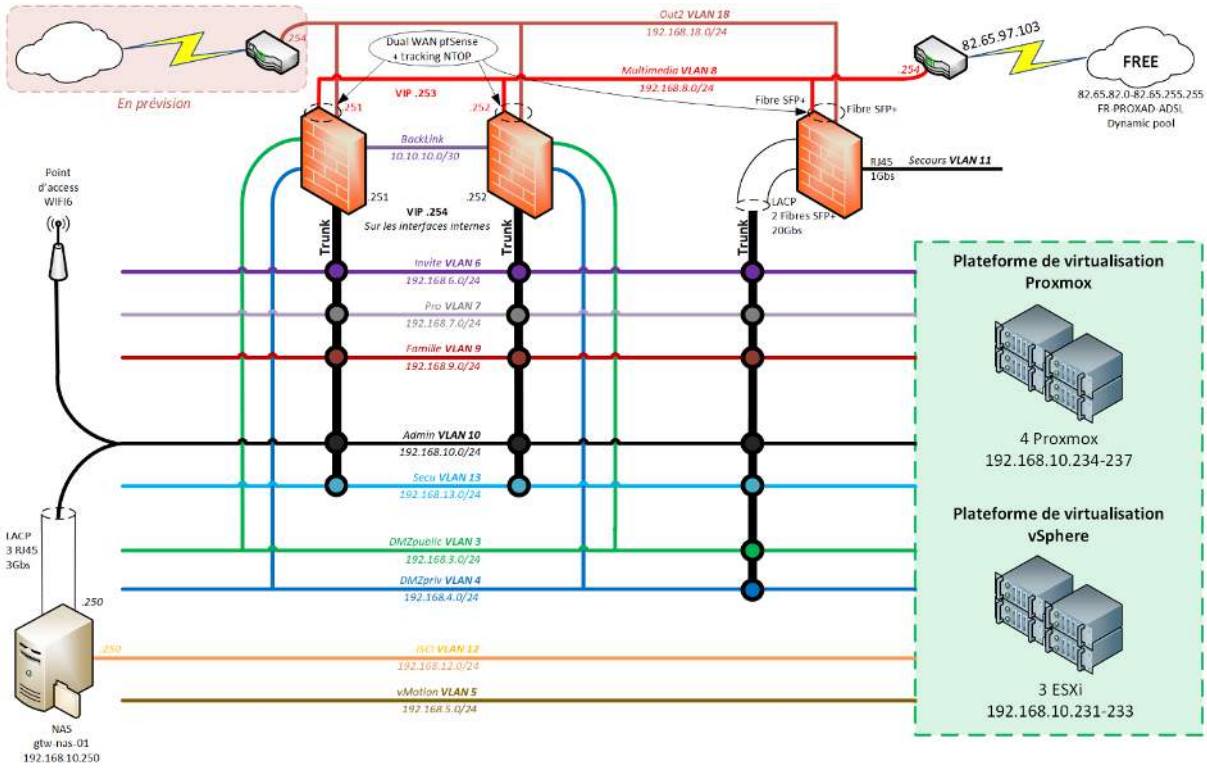


Illustration 4 : schéma logique de l'architecture Réseau EasyFormer

Voici maintenant le schéma physique du réseau informatique d'EasyFormer :

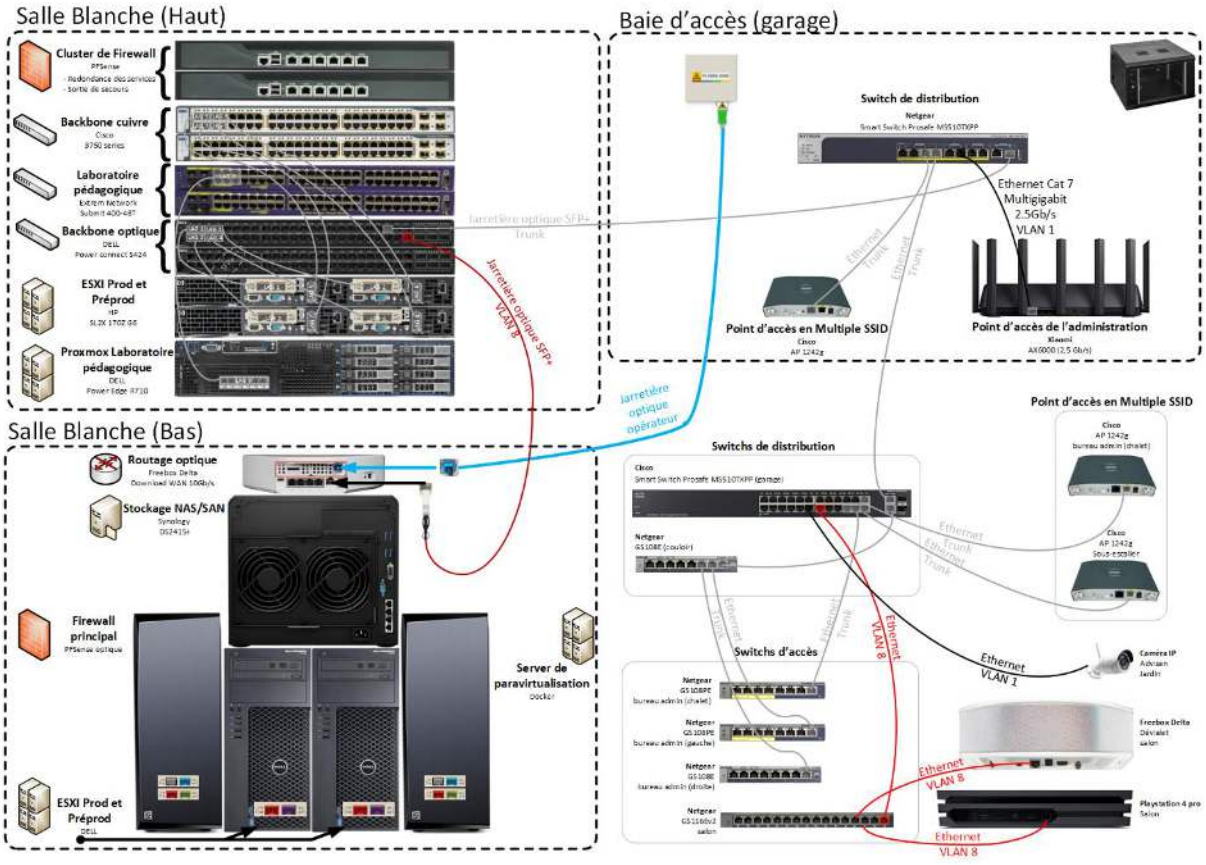


Illustration 5 : schéma physique de l'infrastructure informatique d'EasyFormer

Vous trouverez ci-dessous une photographie et le schéma des « salles blanches » dans lesquelles se trouvent une partie des équipements informatiques d'EasyFormer :

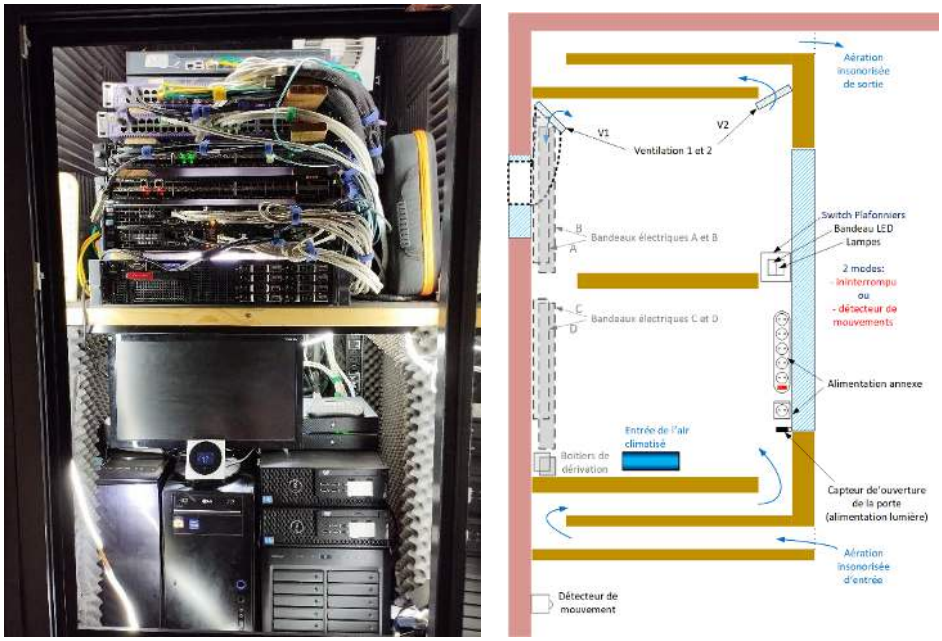


Illustration 6 : photo et schéma des salles blanches

Voici maintenant une photo plus agrandie des serveurs informatiques et équipements réseau (cluster de pare-feu pfSense, commutateurs Cisco, hyperviseurs, etc.) :

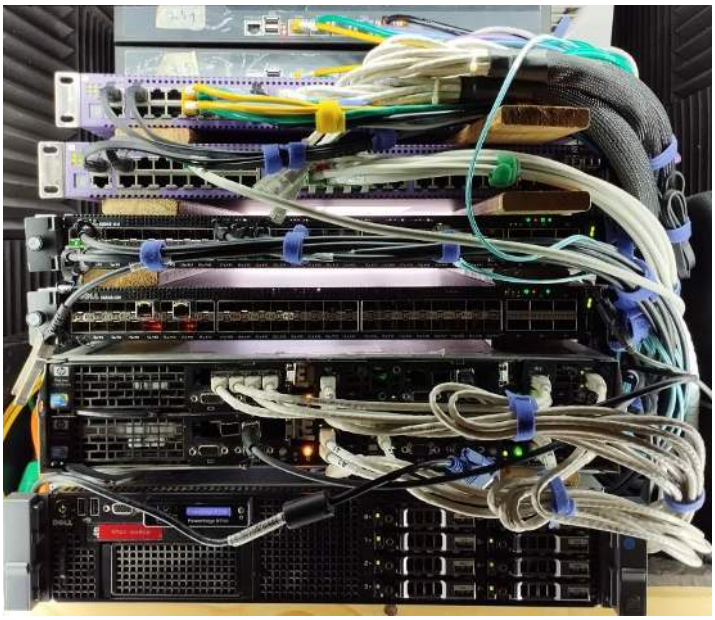


Illustration 7 : photo des équipements informatiques d'EasyFormer

II. INTRODUCTION

A. CONTEXTE MONDIAL ET FRANÇAIS DE LA CYBERMENACE

Nous constatons de jour en jour et d'années en années que **les attaques informatiques ne cessent d'augmenter**, de gagner en sophistication et qu'assurer la sécurité des systèmes et réseaux informatiques d'entreprise représente un véritable défi.

A l'échelle mondiale et pour la période allant de juin 2022 à juin 2023, Microsoft a publié un rapport[9] qui met en lumière l'état actuel du cybercrime mondial :

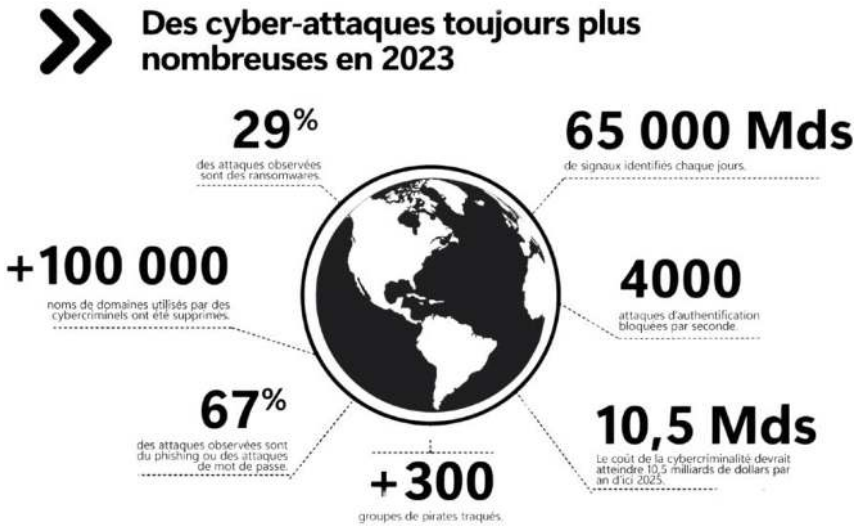


Illustration 8 : infographie basée sur les chiffres du rapport Microsoft Digital Defense 2023

Les chiffres-clés du rapport :

- **65 000 milliards de signaux de sécurité** analysés en 2023 soit une augmentation de 51% par rapport à 2022
- Les attaques de mots de passe ont été **multipliées par 10** vs. 2022
- **1700 attaques par déni de service distribué (DDoS)** contrecarrées chaque jour via les solutions Microsoft
- Des **cyber-attaques** toujours **plus nombreuses** en 2023

La France n'est évidemment pas épargnée par cette *cyber-insécurité* mondiale. Selon certaines estimations, le coût total des cyberattaques et autres actes malveillants en ligne **devrait atteindre 129**

[9] Microsoft Digital Defense Report 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

milliards de dollars américains dans le pays en 2024 (soit environ 119 milliards d'euros), contre près de 94 milliards de dollars l'an passé. »[10]

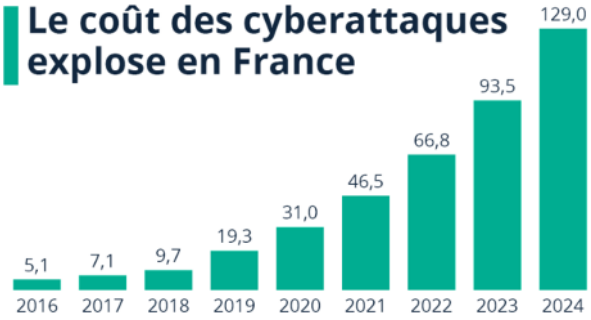


Illustration 9 : estimation du coût annuel de la cybercriminalité en France (en milliards de US $)

Même les entités publiques les plus importantes ne sont pas à l'abri. Pour preuve : cette carte interactive[11] de la France répertoriant les principales cyberattaques dont ont été victimes les administrations françaises ces dernières années :

Illustration 10 : carte des cyber-attaques auprès d'organismes publics français

Dans son rapport[12] annuel de 2023 sur les intentions des attaquants, leurs capacités et les opportunités qu'ils exploitent pour compromettre des systèmes d'information (SI), l'ANSSI nous confirme également cette tendance mondiale à l'augmentation des cyberattaques de tous types :

[10] Technology Market Insights de Statista, https://fr.statista.com/infographie/31783/cout-annuel-cybercriminalite-cyberattaques-en-france/
[11] OpenStreetMap, https://umap.openstreetmap.fr/en/map/attaques-cybersecurite-aupres-dorganismes-publics_821557#6/46.460/6.394
[12] Panorama de la cybermenace, https://cyber.gouv.fr/actualites/lanssi-publie-le-panorama-de-la-cybermenace-2023

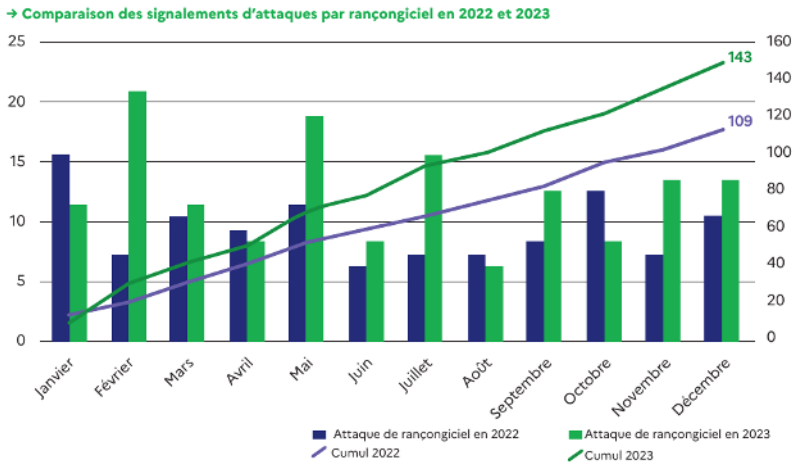


Illustration 11 : graphique basée sur les données de l'ANSSI concernant des signalements d'attaque par ransomware

D'autres chiffres et études sur le sujet nous apprennent également que **les professionnels de la cybersécurité seront de plus en plus prisés** pour défendre les entreprises face à toutes ces menaces.

B. RESUME DU PROJET (ABSTRACT)

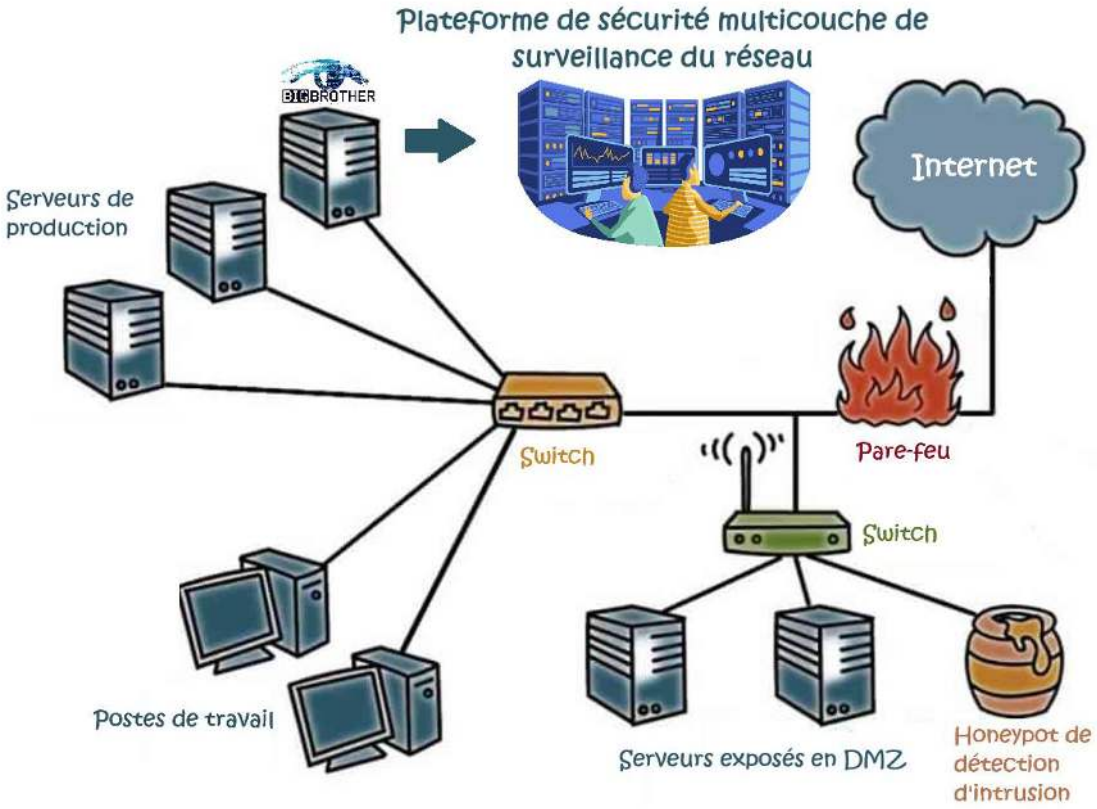


Illustration 12 : schéma conceptuel du projet de sécurisation du réseau

1. En français

Dans ce contexte d'augmentation des actes de cybermalveillance, j'ai choisis d'explorer pour mon projet de fin d'études une approche particulière pour renforcer la sécurité du système d'information de mon entreprise d'accueil, en me focalisant sur l'implémentation d'une solution avancée de détection d'intrusions : j'ai combiné l'usage d'**un outil de leurre de type « pot de miel »** (*Intrusion Detection Honeypot*, ou IDH) pour détecter les intrusions, avec une **plateforme multicouche de surveillance de la sécurité du réseau** (*Network Security Monitoring*, ou NSM) que j'ai intégrée au réseau informatique existant via la configuration de port d'écoute (*port mirroring*) pour la surveillance du trafic, le déploiement d'agents sur hôtes et la configuration de l'ingestion des journaux d'activité d'éléments stratégiques du SI.

Dans ce mémoire, je démontre comment mon entreprise a amélioré significativement sa capacité à détecter et à répondre aux incidents de sécurité en surveillant, enregistrant et analysant le trafic réseau tout en simulant un service réseau vulnérable pour tromper les attaquants.

J'ai donc mis en place cette configuration et conduit une série de tests pour évaluer l'efficacité du système face à diverses tentatives d'intrusion.

Ce mémoire décrit en détail les étapes de mise en œuvre, les défis rencontrés, et les résultats obtenus.

2. In english

Against this backdrop of increasing cyber-maliciousness, I chose to explore for my final year project a particular approach to strengthening the security of my host company's information system, focusing on the implementation of an advanced intrusion detection solution: I combined the use of a **honeypot decoy tool** (*Intrusion Detection Honeypot*, or IDH) to detect intrusions, with a multilayer **network security monitoring platform** (NSM) that I integrated into the existing IT network by configuring a port mirroring for traffic monitoring, deploying agents on hosts and configuring the ingestion of activity logs from strategic elements of the IS.

In this thesis, I demonstrate how my company has significantly improved its ability to detect and respond to security incidents by monitoring, recording and analyzing network traffic while simulating a vulnerable network service to fool attackers.

I therefore set up this configuration and conducted a series of tests to assess the system's effectiveness in the face of various intrusion attempts.

This thesis describes in detail the implementation steps, the challenges encountered, and the results obtained.

III. PHASE D'INITIALISATION DU PROJET

A. CONTEXTE ET PROBLEMATIQUE DU PROJET

L'organisation EasyFormer a été victime d'une attaque informatique il y a quelques temps.

Plus que jamais, il est important que chaque collaborateur adopte désormais les bons réflexes au quotidien : mots de passe robustes stockés dans la base de données chiffrée d'un gestionnaire de mots de passe, attention aux pièces jointes suspectes, sauvegardes régulières des données, etc.

Mais c'est aussi l'entreprise (EasyFormer) qui se doit d'**avoir des outils efficaces pour détecter les tentatives d'intrusions et empêcher les attaques avant qu'elles ne se produisent** car une seule faille peut mettre en péril des années de travail et nuire à la réputation de l'entreprise.

Prenant acte de ce contexte, le Réseau EasyFormer décida de chercher à **améliorer sa posture de sécurité**.

1. Etat des lieux, description de la situation actuelle

La première étape pour cela fut de faire un état des lieux de la situation : **quels sont les points forts et les points faibles du système d'information (SI) actuel ?**

Illustration 13 : compte-rendu graphique de l'état des lieux

Parmi les points faibles identifiés, nous avons relevé particulièrement la criticité de **l'absence de visibilité sur le trafic réseau** et **l'insuffisance des outils de sécurité actuellement en place**.

2. Brainstorming, ou « remue-méninges »

Nous avons ensuite organisé un *brainstorming*, ou « remue-méninges » en français, c'est-à-dire une réunion pendant laquelle nous avons récolté les idées des uns et des autres aussi nombreuses et originales soient-elles en prenant soin de respecter le principe même du brainstorming : **s'abstenir de toute critique envers les idées émises**.

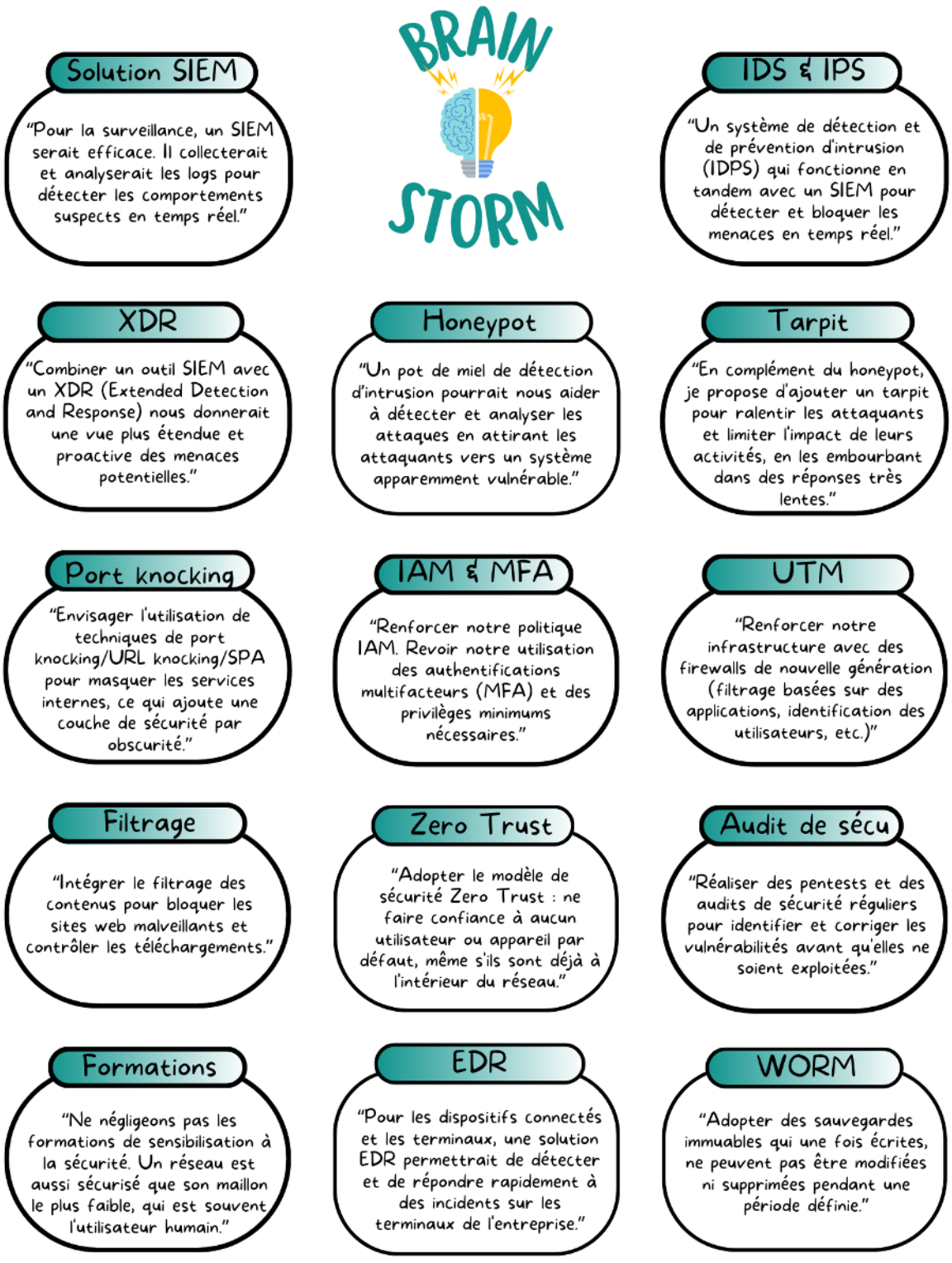


Illustration 14 : compte-rendu graphique du brainstorming

Parmi les idées exprimées qui ont été particulièrement discutées et ont eu le plus de succès lors de cette réunion, il y a la mise en place d'un **centre d'opérations de sécurité** (SOC), d'une plateforme **gestion des informations et des événements de sécurité** (SIEM), de **surveillance de la sécurité du réseau** (NSM), d'un système de **détection et prévention d'intrusion** (IDPS), et d'un **honeypot** (IDH).

B. L'ANALYSE FONCTIONNELLE DU BESOIN

L'analyse fonctionnelle du besoin (AFB) est une démarche méthodologique utilisée dans la gestion de projet pour **définir les besoins de l'utilisateur et les fonctions que le produit ou le service doit remplir pour répondre à ces besoins**. Elle se concentre sur ce que le système doit faire, sans s'attacher à la manière dont il doit le faire, permettant ainsi de séparer les exigences fonctionnelles des solutions techniques.

1. Méthode de questionnement « QQOQCCP »

Afin de bien **clarifier la problématique dans le but de recueillir le besoin**, nous avons utilisé l'analyse « QQOQCCP ».

Elle consiste à poser sept questions afin de compiler les informations essentielles à la résolution du problème : Quoi, Qui, Où, Quand, Comment, Combien et Pourquoi ? Ce questionnement systématique est un outil de décomposition très utile pour **obtenir une bonne vue d'ensemble**.

Quoi ? *(Quel est le problème ?)*	Le système d'information (SI) d'EasyFormer ne dispose **pas d'outils de sécurité efficaces** pour détecter les tentatives d'intrusions et empêcher les attaques avant qu'elles ne se produisent.
Qui ? *(Qui rencontre le problème défini plus haut ?)*	L'**équipe informatique** chargée de la sécurité du réseau d'EasyFormer.
Où ? *(Où se situe le problème ?)*	Dans le **réseau informatique** de l'organisation EasyFormer.
Quand ? *(Quand a lieu le problème ? À quelle fréquence ?)*	**En continu** car la surveillance et la détection doivent fonctionner 24h/24 et 7j/7 pour garantir une protection efficace du SI.
Comment ? *(Comment se manifeste le problème ?)*	Une **intrusion dans le SI non détectée** voire une **attaque informatique**.
Combien ? *(De quel budget/combien de temps dispose-t-on pour résoudre le problème ?)*	Le **moins cher** possible et **au plus tôt**.
Pourquoi ? *(Quel est l'objectif visé ?)*	Le but principal est de **renforcer la sécurité du réseau en détectant les activités** suspectes ou malveillantes, **en attirant les attaquants vers des cibles contrôlées** (les honeypots), et en réduisant ainsi le risque d'attaques réussies sur les actifs réels du réseau.

En posant les bonnes questions, cette technique a permis d'identifier clairement le besoin :

L'équipe IT d'EasyFormer a besoin**, au plus tôt et à moindre coût,** de mettre en place **une solution de surveillance du réseau informatique de type outil « SIEM/NSM » et de détection/prévention d'intrusion** afin de **renforcer sa posture de sécurité.** Elle souhaite également à l'occasion de la mise en place de ce système, **renforcer sa capacité de détection des intrus** à l'aide d'un **leurre de type « honeypot »**.

2. Méthode de la bête à cornes

Un diagramme de type « bête à cornes » a également été utilisé dans le cadre de l'AFB pour permettre d'identifier le besoin à satisfaire :

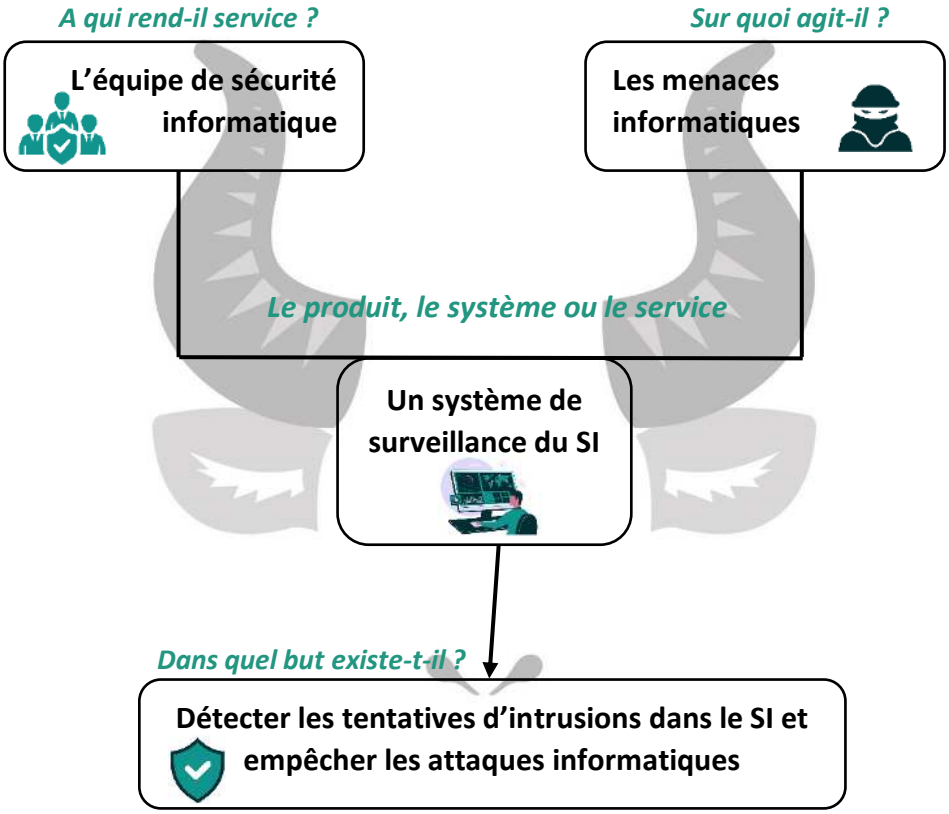


Illustration 15 : diagramme de la bête à corne

C. OBJECTIFS DU PROJET

L'objectif global identifié est de **rendre l'environnement informatique plus sûr**. Les bénéficiaires seront l'ensemble de l'entreprise, y compris l'équipe IT, les employés et la direction.

Amélioration de la sécurité globale	Réactivité accrue	Capacité de reporting et d'analyse
•Renforcer la capacité de détection et de prévention des intrusions afin de diminuer significativement les risques de cyberattaques et de compromission des données.	•Mettre en place un système permettant une réponse rapide et efficace aux incidents de sécurité, minimisant ainsi les dégâts potentiels et réduisant le temps de rétablissement après une attaque.	•Fournir des outils d'analyse et de reporting avancés pour permettre un suivi précis et continu de l'activité du réseau, des tentatives d'intrusion, et des performances des systèmes de sécurité.

D. PERIMETRE DU PROJET

Rappelons que le projet consiste en **l'implémentation, au sein des locaux d'EasyFormer, d'une solution de surveillance de la sécurité du réseau informatique et d'analyse des données, liée à un système de leurre (*honeypot*)** qui servira à **améliorer la posture de sécurité de l'entreprise en détectant les tentatives d'intrusion** et **en fournissant une analyse approfondie des menaces potentielles**, sans toutefois redéfinir entièrement l'architecture IT existante ni s'étendre au-delà des capacités actuelles de l'entreprise.

1. Périmètre inclus

Afin que toutes les parties prenantes aient une compréhension commune des livrables et prestations attendues nous avons déterminé avec précision le travail à réaliser (le périmètre projet) :

Infrastructure de surveillance et détection	Installation complète du système de surveillance et configurations nécessaires pour la détection d'intrusion, l'intégration du honeypot et l'ingestion des journaux des endpoints et du pare-feu pfSense déjà en place.
Tests et validation	Réalisation de tests de pénétration et autres évaluations de sécurité pour vérifier l'efficacité du système après sa mise en production.
Documentation	Création de manuels d'utilisation et de procédures d'intervention en cas d'incident de sécurité. Documentation détaillée des configurations et des architectures mises en place dans le wiki d'EasyFormer.
Formation	Animation d'une séance de formation à l'attention des collaborateurs afin de développer les compétences internes pour l'exploitation de la solution de sécurité.

2. Périmètre exclu

Afin de ne pas se retrouver avec un projet qui dérive sans fin et dans lequel on vient rajouter toujours plus de tâches à réaliser, nous avons également clarifié ce qui serait exclu du périmètre du projet :

Infrastructure IT non liée à la sécurité réseau	Il n'y aura pas d'amélioration ou de modification de l'infrastructure IT qui ne soit pas directement liées à la sécurité du réseau. Il n'y aura pas de mise à jour des équipements informatiques non associés aux objectifs de sécurité du projet.
Autres projets de sécurité	Il n'y aura pas d'intervention concernant les projets de sécurité informatique qui ne concernent pas la surveillance réseau ou la détection d'intrusions. Le projet n'inclut pas la mise en place de politiques de sécurité informatique globales, bien qu'il puisse recommander des modifications ou des ajouts.
Intégrations non prévues	Il n'y aura pas d'intégration avec des systèmes de sécurité non spécifiés dans le cahier des charges, ni de refonte de l'architecture réseau existante.
Portée et limites	Le projet se limite aux infrastructures réseau situées dans les locaux de l'entreprise. L'infrastructure cloud dont dispose EasyFormer n'est pas incluse. La protection contre toutes les formes de cyberattaques n'est pas garantie ; le focus est mis sur la détection d'intrusion et la réponse aux incidents. Les solutions de sécurité physique (comme les systèmes de surveillance par caméra, les contrôles d'accès physique) ne sont pas couvertes.
Exploitation et maintenance	L'exploitation quotidienne du système, sa maintenance et ses mises à jour devront par la suite être réalisées en interne par l'équipe IT d'EasyFormer mais pas forcément par le personnel qui a installé la solution.

E. GESTION DU PROJET

Pour assurer le bon déroulement des différentes étapes de réalisation d'un projet, il convient d'adopter une méthode de gestion de projet adaptée au type de projet.

1. Choix de la méthode de gestion de projet

Dans notre cas où le projet est prévisible, nous avons opté pour la méthode « en cascade » (*waterfall*) qui est une méthode de gestion dite « classique », « prédictive » ou encore « séquentielle » (par opposition aux méthodes « agiles »).

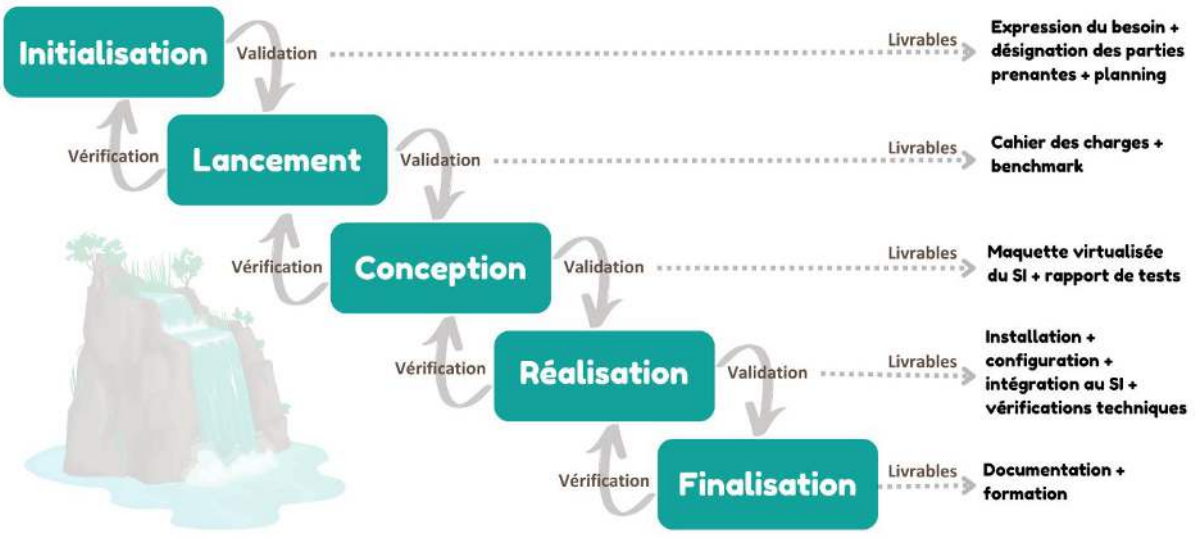


Illustration 16 : modèle de projet en cascade

C'est une méthode assez naturelle, simple à comprendre et à implémenter impliquant un déroulement en étapes, en séquences, en phases.

Elle convient aux projets où la qualité a plus d'importance que les coûts ou les délais et dont les besoins sont clairement définis et stables ce qui est particulièrement bien adapté pour la mise en place de notre solution.

Le modèle en cascade offre une structure hiérarchique. L'organisation du travail est découpée en plusieurs étapes qui se succèdent les unes aux autres et qui se terminent par un résultat. Lors du déroulement du processus, chaque étape ou phase doit être définie précisément c'est-à-dire les personnes participantes à ce projet et qui travaillent dessus doivent identifier les différents besoins pour mener à bien leur tâche à terme et quels sont les livrables attendus. Son résultat n'a de sens qu'une fois complétée.

Concernant la phase de validation, la première chose à faire est de vérifier que les entrants sont satisfaisants. Si ce n'est pas le cas, l'étape est refusée avec un retour à l'étape précédente. Dans le cas d'une erreur majeure détectée, il est possible de revenir à la première étape. Et si tout se passe bien le processus continue son exécution. Enfin, le cycle en cascade que j'ai établi, a permis à M^{r} Alex FALZON (le maître d'ouvrage, ou MOA) de savoir précisément ce qui va lui être livré et quand il pourra en prendre la livraison.

Comme toutes les méthodes, la cascade a ses avantages et ses inconvénients :

Avantages	Inconvénients
Structure simple et claire - Le projet est divisé en phases séquentielles et linéaires. - Chaque phase a des livrables attendus. - Les étapes claires permettent un meilleur contrôle de qualité et de progression.	**Faible adaptabilité aux changements** - Peu de flexibilité pour revenir en arrière une fois une étape complétée. - Peut être coûteux et chronophage pour intégrer les changements.
Planification détaillée - Planification initiale exhaustive, ce qui permet une meilleure estimation des coûts et des délais. - Les exigences doivent être clairement définies dès le début. - Suivi plus aisé pour les commanditaires.	**Dépendance aux étapes antérieures** - Les retards dans une phase affectent tout le projet. - Accumulation possible de problèmes non détectés jusqu'aux phases finales.
Documentation complète - Documentation détaillée à chaque étape, facilitant la maintenance et la gestion. - Favorise la communication et le transfert d'informations entre les équipes.	**Long délai de livraison** - Le produit final n'est livré qu'à la fin du projet, ce qui peut retarder la détection de problèmes. - Risque d'obsolescence si les exigences évoluent pendant la durée du projet.

2. Choix de l'outil de gestion de projet

Afin de structurer le projet, j'ai choisi d'utiliser un outil très efficace pour cela : Microsoft Project.

Il m'a permis de planifier avec précision afin de communiquer clairement avec les parties prenantes.

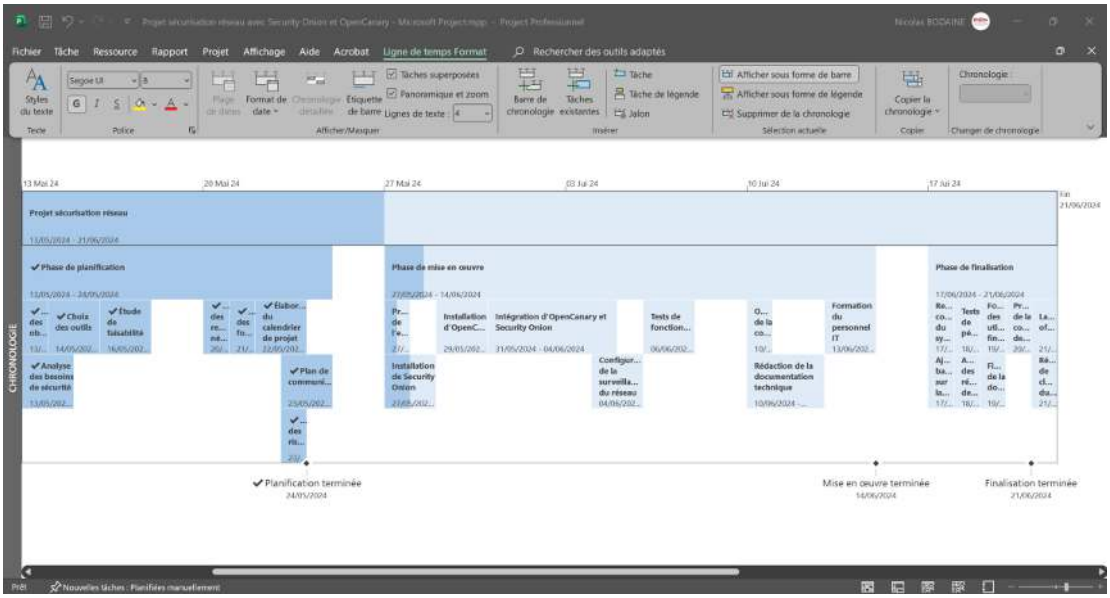


Illustration 17 : vue « ligne de temps » du projet dans MS Project

La fonctionnalité de rapport de Microsoft Project m'a été particulièrement utile. J'ai généré des rapports d'avancement hebdomadaires pour partager avec les parties prenantes, leur offrant une transparence complète sur l'état du projet.

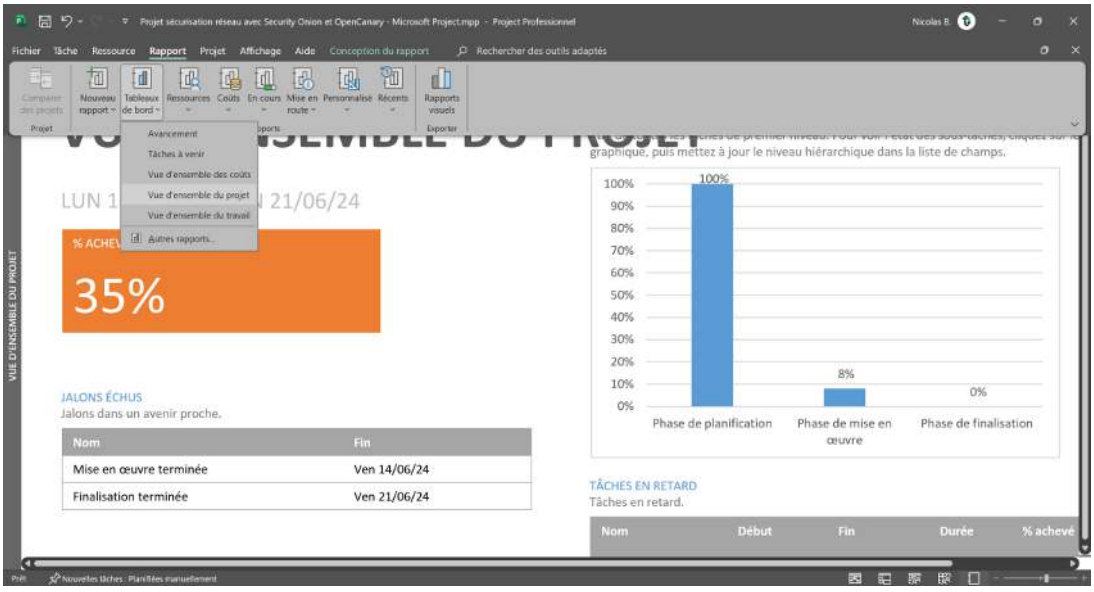


Illustration 18 : rapport « vue d'ensemble du projet » dans MS Project

3. Méthodologie de gouvernance

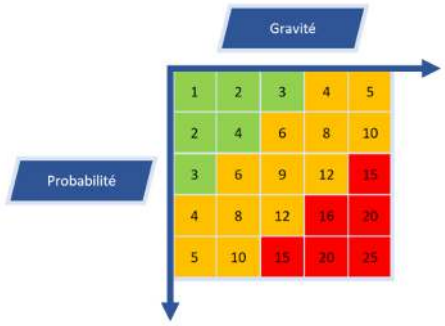
Afin de remonter les difficultés et de donner de la visibilité au projet, nous avons mis en place un système de réunions qui nous a permis d'assurer le bon avancement des réalisations.

La première réunion effectuée fut la réunion du comité de pilotage, aussi appelée « copil » qui a défini une stratégie d'orientation pour notre projet. Ensuite, la réunion de lancement de notre projet ou le « kick off » qui a réuni tous les contributeurs à ce projet et qui a servi à informer et à donner le contexte et les enjeux du projet. Une fois le projet lancé, des réunions périodiques ont été organisées toutes les semaines pour assurer le suivi et le bon déroulement du projet. Une réunion de clôture a été organisée une seule fois à la fin du projet et a permis un retour d'expérience ainsi qu'une reconnaissance du travail effectué par les différents contributeurs.

A. ANALYSE DES RISQUES

L'AMDEC (**A**nalyse des **M**odes de **D**éfaillance, de leurs **E**ffets et de leur **C**riticité) est une méthode structurée permettant d'identifier et d'évaluer les risques associés à différents aspects d'un projet. Cette méthode nous a permis d'allouer efficacement les ressources et de savoir où concentrer nos efforts.

Pour avoir une visualisation immédiate des niveaux de risque associés à chaque risque identifié, j'ai utilisé un tableau AMDEC dans lequel il y a une échelle de 3 couleurs et 2 critères pour évaluer la criticité d'un risque sur 25 points.

Explication des codes couleur du tableau AMDEC	
	Vert : **Risques acceptables** ayant une **faible criticité**, nécessitant une surveillance mais ne requérant pas d'actions immédiates.
	Orange : **Risques à surveiller** ayant une **criticité modérée**, nécessitant une planification des mesures de mitigation pour réduire leur probabilité d'occurrence ou leur impact.
	Rouge : **Risques inacceptables** ayant une **criticité élevée**, requérant une attention particulière et des actions prioritaires pour leur mitigation pour prévenir des impacts significatifs sur le projet.
Explication des critères du tableau AMDEC	
G pour **Gravité (1-5)** : Mesure l'impact du risque sur le projet (1 étant le moins grave, 5 le plus grave).	
P pour **Probabilité (1-5)** : Évalue la probabilité d'occurrence du risque (1 étant peu probable, 5 très probable).	
C pour **Criticité (1-25)** : Calculée en multipliant Gravité et Probabilité. Les scores plus élevés indiquent une nécessité plus urgente d'éliminer le risque.	

Risque	Mode de défaillance	Effet du risque	Criticité (GxP)	Mesures de mitigation
Risques internes				
Retard dans la mise en œuvre du projet	Le projet ne sera pas achevé dans les délais impartis	Insatisfaction commanditaire, réputation endommagée	4 (2x2)	Suivre l'avancement du projet et identifier les risques dès le début
Insuffisance de formation	Manque de compétences techniques de l'équipe IT	Mauvaise configuration	6 (3x2)	Prévoir un temps de formation et de documentation avant le début de la mise en œuvre
Problèmes de compatibilité avec les systèmes et outils existants	Risque de dysfonctionnement ou de limitation des fonctionnalités	Retard dans la mise en œuvre du projet, interruption des services	12 (4x3)	Évaluation approfondie des systèmes existants, faire des choix pertinents
Failles de sécurité non détectées	Configuration incorrecte ou incomplète	Intrusions non détectées menant à des fuites de données	16 (4x4)	Tests de pénétration réguliers, audits de sécurité, mise à jour et patchs systématiques
Surcharge du système	Capacité insuffisante pour gérer le trafic	Performances réseau dégradées, fausses alertes	8 (4x2)	Dimensionnement correct du système, surveillance des performances, ajustements réguliers
Perte de données	Défaillance du système de stockage des logs et des alertes	Perte d'informations cruciales pour l'analyse forensique	3 (3x1)	Solutions de sauvegarde et de récupération
Résistance au changement	Administrateurs réfractaires à adopter le nouvel outil de sécurité	Efficacité réduite du système de sécurité, risques accrus	20 (4x5)	Campagnes de sensibilisation, formation des administrateurs, communication sur les bénéfices du système
Risques externes				
Coupure du service au niveau du FAI	Impossibilité de travailler à distance, de faire des installations ou mises à jour de logiciels	Retard dans la mise en œuvre du projet, interruption des services	12 (4x3)	Système Dual WAN auprès d'un autre fournisseur d'accès à internet
Coupure de courant	Impossibilité de travailler	Retard dans la mise en œuvre du projet, interruption des services	15 (5x3)	Générateur de secours
Vol du matériel	Le matériel du projet peut être volé	Retard dans le projet. Augmentation des coûts. Interruption des services	10 (5x2)	Stocker le matériel dans un endroit sûr et sécurisé. Mettre en place un plan de réponse en cas de vol de matériel

B. BUDGET PREVISIONNEL

Avec une allocation budgétaire nulle, l'accent a été mis sur l'optimisation des ressources disponibles et l'utilisation de solutions gratuites.

J'ai commencé par distinguer les différentes ressources à disposition :

- Les **ressources matérielles** comme les hyperviseurs Proxmox, ESXi et les commutateurs au sein de l'organisation.
- Les **ressources informatiques** comme les logiciels gratuits disponibles et/ou des logiciels libres et open source.
- Les **ressources humaines** que sont les membres de l'équipe IT actuelle : salariés, alternants, stagiaires et bénévoles.

C. MACRO-PLANNING

Le macro-planning offre une **vue d'ensemble et à grande échelle du projet**. Il s'agit d'un planning qui définit les grandes phases du projet sur une échelle de temps. Il ne rentre pas dans le détail des tâches individuelles mais se concentre sur les objectifs majeurs et la durée globale du projet.

Phase	Durée (en semaines)	Activités principales
Initialisation	1	Analyse des besoins, objectifs et périmètre du projet, désignation des parties prenantes, identification des contraintes, affectation du budget, planification, identification des risques
Lancement	1.5	Rédaction d'un cahier des charges clarifiant les spécifications fonctionnelles et techniques attendues, études comparatives des solutions pouvant être retenues, choix des technos
Conception	1.5	Réflexion de conception technique et ingénierie réseau, planification détaillée des étapes du projet, autoformation du personnel technique, réalisation d'une maquette virtualisée du SI pour tests, validation des conceptions avec les parties prenantes
Réalisation	1	Installation et configuration des solutions, intégration dans le SI existant, test de vérification des fonctionnalités et résolution des problèmes le cas échéant
Finalisation	1	Transfert des connaissances par la rédaction de la documentation technique et la formation des collaborateurs, contrôle et suivi, retour d'expérience

D. PLANNING DETAILLE

Une fois le projet plus avancé (à la phase de conception) et l'ensemble des tâches identifiées, j'ai réalisé un planning détaillé du projet afin de représenter visuellement et précisément son état d'avancement.

Conscient de l'importance d'une planification minutieuse, j'ai décidé de décomposer le projet en 5 phases claires, en me basant sur un calendrier précis qui s'étendait sur 6 semaines du 13 mai au 21 juin 2024 :

- la phase d'**initialisation** (analyse des besoins, planification globale, budget)
- la phase de **lancement** (cahier des charges, benchmark)
- la phase de **conception** (réflexion de conception, planification détaillée)
- la phase de **réalisation** (installation, configuration, intégration, vérifications, optimisations)
- la phase de **finalisation** (documentation, formation, clôture)

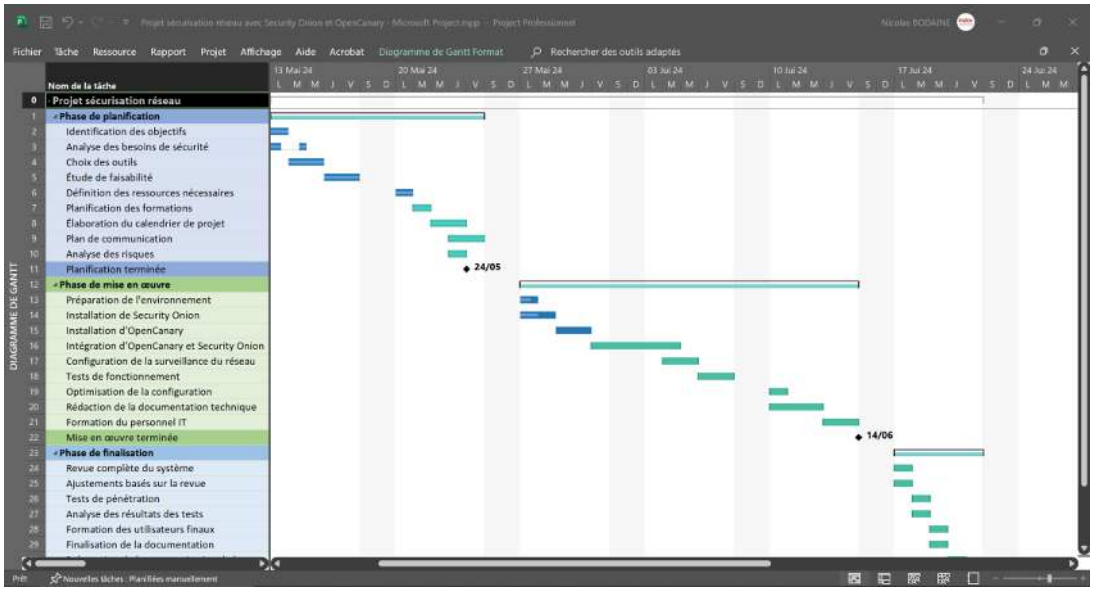


Illustration 19 : planning prévisionnel du projet (diagramme de Gantt)

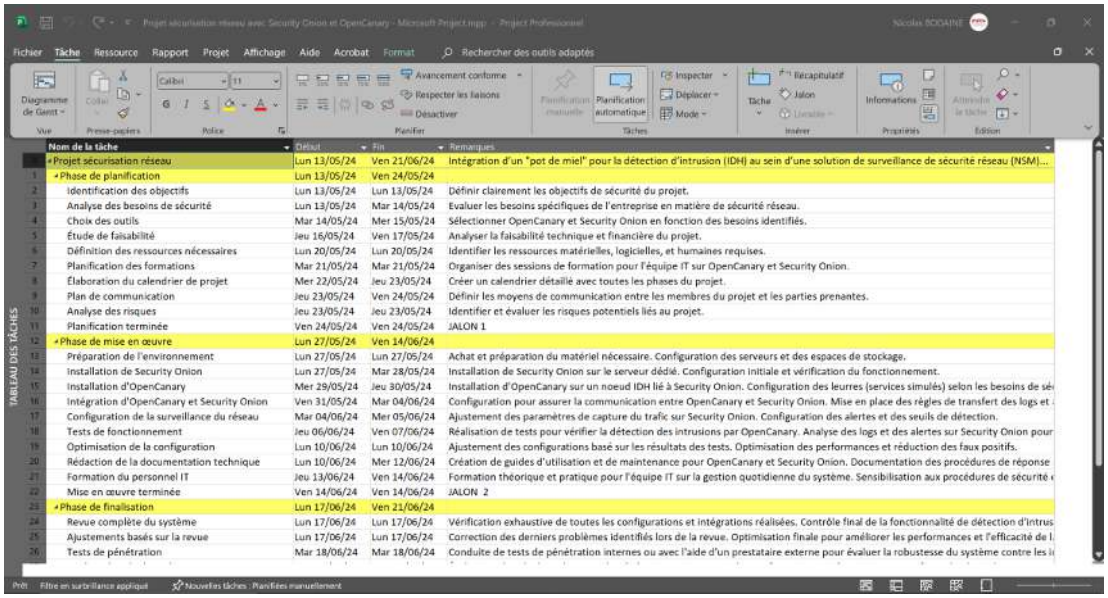


Illustration 20 : vue « tableau des tâches » du projet dans MS Project

E. PARTIES PRENANTES

Pour assurer la réussite du projet, il a fallu bien **identifier et impliquer toutes les parties prenantes**. La communication régulière avec celles-ci a permis que le projet avance selon les attentes.

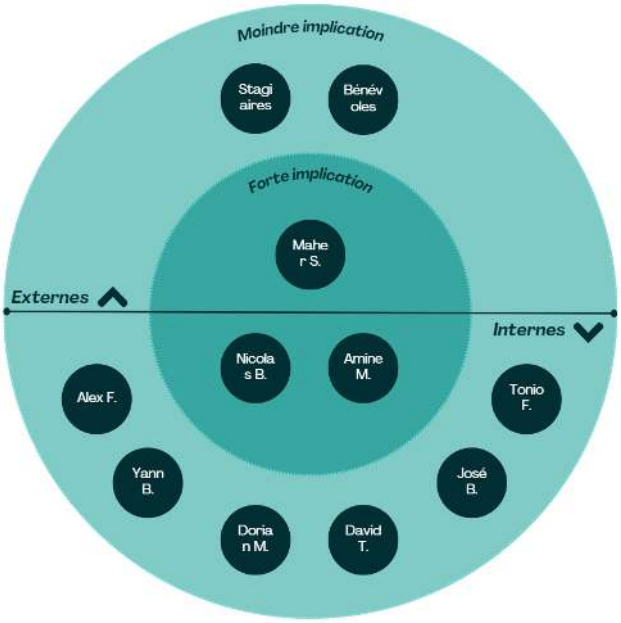


Illustration 21 : les parties prenantes du projet

1. Directeur du système d'information

Il s'agit de M[r] Alex FALZON, c'est le maître d'ouvrage (MOA). Son rôle a été de fournir une vision stratégique et des ressources pour le projet. C'est lui qui a défini le budget, la portée et les objectifs du projet. Il a aussi assuré le suivi de l'avancement et la réalisation des objectifs.

2. Équipe IT et sécurité

J'ai été le maître d'œuvre (MOE) et l'acteur le plus impliqué dans le projet. C'est moi qui ai réalisé la plupart des phases techniques, ainsi que les tests, la résolution des problèmes, la rédaction de la documentation et la formation post-déploiement. Maher SKARFA, un des stagiaires présents à ce moment, et Amine MOHELLEBI, notre apprenti en alternance, ont également été des acteurs bien impliqués dans ce projet. Dans une moindre mesure, il y a eu mes collègues de l'équipe IT qui ont pu nous aider et nous épauler en cas de besoin. J'ai pu également faire appel à des stagiaires qui étaient présents au sein de la structure EasyFormer, et des bénévoles - souvent d'anciens stagiaires.

Notre rôle a été de réaliser la partie technique du projet, incluant la planification, l'installation, la configuration et le déploiement de la solution de sécurité.

3. Service juridique

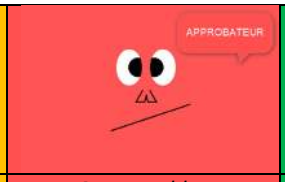
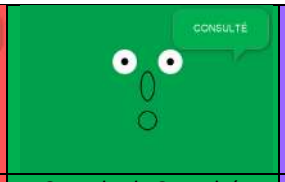
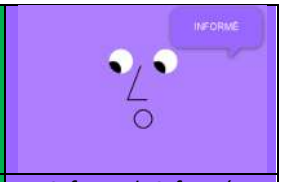
Il s'agit de Tonio FERNADES et de José BARROS. Leur rôle a été de s'assurer que le projet respecte toutes les réglementations en matière de sécurité des données et de confidentialité. Leur implication dans le projet a été de revoir et approuver toutes les documentations et pratiques pour leur conformité légale.

4. Responsable des opérations

Il s'agit de Mr Alex FALZON. Son rôle a été de veiller à ce que les opérations quotidiennes ne soient pas perturbées par l'intégration des nouvelles technologies de sécurité. Il a fourni des retours sur l'impact opérationnel des nouvelles installations et a participé aux phases de test pour garantir une intégration fluide.

F. ROLES ET RESPONSABILITES

La matrice RACI est un outil de gestion de projet qui permet de clarifier les rôles et les responsabilités des membres de l'équipe par rapport aux différentes tâches et activités du projet. L'acronyme RACI est décomposé comme suit avec les 4 responsabilités :

Légende				
Qui ?	***R**esponsible* : **R**esponsable, **R**éalisateur	***A**ccountable* : **A**pprobateur, **A**utorité	***C**onsulted* : **C**onsulté, **C**onsultant	***I**nformed* : **I**nformé
Rôle	Réaliser une tâche et être responsable de son achèvement	Déléguer la réalisation d'une tâche et approuver son achèvement	Fournir des conseils et renseignements avant la prise de décision et la réalisation d'une tâche	Être informé après une décision ou la réalisation d'une tâche

Le présent tableau de la matrice RACI a été présenté à Mr Alex FALZON (le MOA) qui a donné son approbation pour le projet :

Projet de sécurisation du SI	ACTEURS				
	Nicolas BODAINE	Maher SKARFA	Amine MOHELLEBI	Tonio FERNANDES	Alex FALZON
TACHES					
Phase d'initialisation du projet					
Analyse des besoins	R	I	I	C	A
Définition des objectifs et du périmètre du projet	I	I	I	C	R
Désignation des parties prenantes	C	I	I	I	R
Identification des contraintes	R	I	I	C	A
Identification des risques	R	I	I	C	A
Affectation du budget	I	I	I	A	R
Planification macro	R	I	I	I	A
Phase de lancement du projet					
Rédaction d'un cahier des charges	R	I	I	I	A
Etudes comparatives des solutions	R	I	I	I	C
Choix des technologies	C	I	I	C	R
Phase de conception du projet					
Réflexion de conception technique et ingénierie réseau	R	C	C	I	A
Planification détaillée des étapes du projet	R	C	C	I	A
Autoformation du personnel technique	R	R	R	I	I
Réalisation d'une maquette virtualisée du SI (pré-prod)	R	C	C	I	A
Validation des conceptions avec les parties prenantes	I	I	I	I	R
Phase de réalisation du projet					
Installation de la plateforme SIEM	R	R	I	I	A
Installation et configuration du honeypot	R	R	I	I	A
Configuration des règles de détection d'intrusion	R	R	I	I	A
Configuration de l'ingestion des journaux des points de terminaison du réseau	R	R	I	I	A
Configuration du port mirroring pour le sniffing réseau	C	C	C	I	RA
Test de vérification des fonctionnalités SIEM/NSM	R	C	C	I	A
Résolution des problèmes et correction des confs	R	C	C	I	A
Phase de finalisation du projet					
Rédaction de la documentation technique	R	C	C	I	A
Formation des collaborateurs aux nouveaux outils	R	I	I	I	A
Validation du projet	C	C	C	I	A

IV. PHASE DE LANCEMENT : CAHIER DES CHARGES DU PROJET

A. CONTRAINTES DU PROJET

Les contraintes suivantes ont dû être prises en compte dans la planification et l'exécution du projet :

1. Budget limité

Le budget alloué pour la mise en place de la solution complète a été de 0€. La solution doit être mise en place par moi-même dans le cadre de mon projet de fin d'études, aidé si besoin par notre équipe interne, ainsi que les stagiaires et bénévoles. Elle doit être virtualisée par les hyperviseurs déjà en production et aucun coût de licence payante n'a été autorisé. La solution doit être économiquement viable et adaptée à la taille et aux capacités de l'équipe IT de l'entreprise.

En tenant compte de ces ressources limitées, nous avons pensé à nous orienter vers des **solutions gratuites FOSS** (*Free & Open Source Software*) mais également des solutions propriétaires dont les éditeurs donnent des **licences gratuitement aux associations à but non lucratif**.

2. Délais à respecter

Le projet doit être pleinement opérationnel dans un délai de 45 jours à compter de la date de début. Ce délai comprend toutes les phases du projet : de la planification à la mise en service, en passant par le test du système. Un retard dans la livraison ne sera pas forcément critique mais le projet doit absolument être totalement terminé avant le mois d'août 2024.

3. Compétences techniques disponibles

L'équipe IT et moi-même disposons d'une expertise limitée en matière de SIEM, NSM et gestion des honeypots. J'aurai besoin d'un temps de formation et de documentation qui devra être pris en compte dans le planning.

4. Intégration avec les systèmes existants

La solution de surveillance et de détection d'intrusions doit être compatible avec l'infrastructure informatique existante chez EasyFormer. Des tests d'intégration approfondis devront être réalisés pour garantir que la nouvelle solution ne perturbe pas les opérations en cours.

5. Impact sur le réseau

La solution ne doit pas impacter négativement les performances du réseau existant.

6. Sécurité et confidentialité des données

Assurer que la mise en œuvre de ces outils n'introduise pas de vulnérabilités et protège les données sensibles de l'entreprise.

7. Evolutivité

La solution doit pouvoir évoluer facilement avec l'entreprise (ex. : volume de trafic, complexité des menaces) permettant à EasyFormer d'étendre sa couverture de surveillance à mesure que l'entreprise grandit.

B. SPECIFICATIONS FONCTIONNELLES

Généralement formulé sous formes d'exigences fonctionnelles, **les besoins fonctionnels sont l'expression de ce que le produit ou le service délivré par le projet devrait être ou faire**. Les besoins fonctionnels sont spécifiés par les représentants des utilisateurs et des bénéficiaires du produit/service délivré par le projet.

Le cahier des charges (CDC) est le document contractuel qu'il a fallu respecter lors de notre projet. Il permit à M^r^ Alex FALZON (le MOA) de nous faire savoir ce qu'il attendait de nous lors de la réalisation du projet.

Le cahier des charges fonctionnel ne se contente pas de lister les fonctionnalités du projet, il le spécifie, l'explique et le délimite ainsi que les conditions de sa réalisation. C'est le socle de travail qui a servi à cadrer notre projet de déploiement d'une architecture sécuritaire multicouche et qui décrit précisément les besoins et exigences auxquels nous avons dû répondre.

Son rôle a été essentiel, car ce fut **le lien factuel et concret qui a permis d'assurer la bonne compréhension** entre toutes les parties prenantes du projet.

1. Identification des besoins principaux

Après avoir précédemment pointé la problématique et réalisé l'analyse fonctionnelle des besoins, nous avons pu par la suite identifier les principaux besoins de manière plus claire et précise :

Détection d'intrusion	Capacité à détecter activement les tentatives d'accès non autorisées ou les comportements anormaux sur le réseau qui pourraient indiquer une tentative de compromission (= mettre en place une défense proactive contre les cybermenaces).
Réponse aux incidents	Fournir des mécanismes pour une réponse rapide et efficace aux incidents de sécurité détectés.
Enregistrement des événements	Collecte et archivage des logs pour toutes les activités détectées, offrant ainsi la possibilité d'effectuer des analyses forensiques en cas d'incident.
Alertes et notifications	Mise en place d'un système d'alertes en temps réel pour informer les responsables de la sécurité des éventuelles intrusions détectées, permettant une réaction rapide.
Visualisation et analyse	Outils pour visualiser les données de sécurité de manière intuitive, facilitant l'analyse des menaces et la prise de décision pour les actions correctives.
Simplicité d'utilisation et de gestion	Interface utilisateur conviviale pour la configuration, la surveillance, et la gestion des alertes sans nécessiter une expertise technique approfondie.
Formation du personnel	Assurer la formation nécessaire pour le personnel sur l'utilisation et la gestion du système.
Documentation	Fournir une documentation complète.

2. Fonctionnalités clés

La solution à mettre en place doit posséder ces différentes fonctionnalités :

Simulation de services vulnérables	Implémentation de faux services (comme SSH, HTTP, SMB) pour attirer les attaquants, agissant comme des leurres.
Configuration flexible	Possibilité de personnaliser les services à simuler en fonction du profil de l'entreprise.
Intégration des alertes	Capacité d'envoyer des notifications via email ou d'autres canaux de communication en cas de détection d'activité suspecte.
Surveillance de réseau (NSM)	Capture et analyse du trafic réseau pour identifier des signes d'activité malveillante.
Gestion des logs et événements (SIEM)	Agrégation et stockage sécurisé des logs provenant de différentes sources, y compris le honeypot.
Outils d'analyse	Suite d'outils pour l'analyse des données collectées, incluant des capacités de recherche avancée et de visualisation des menaces.
Support de la communauté	Accès à une large communauté d'utilisateurs et de développeurs pour le support et le partage des meilleures pratiques.

C. SPECIFICATIONS TECHNIQUES

Le cahier des charges technique se focalisera sur les exigences et contraintes techniques du produit.

1. Infrastructure et plateforme

Serveurs	Les caractéristiques minimales des solutions à mettre en place doivent permettre de les installer et les faire tourner sur nos hyperviseurs (CPU, RAM, espace de stockage, compatibilité)
Système d'exploitation	Utilisation de systèmes d'exploitation compatibles et sécurisés, préférentiellement Linux, pour l'hébergement de solutions.
Réseau	Configuration du réseau pour permettre la surveillance efficace et la simulation des services leurres sans impacter les performances du réseau existant.

2. Plateforme de surveillance de la sécurité du réseau

a) Définitions d'un système SIEM

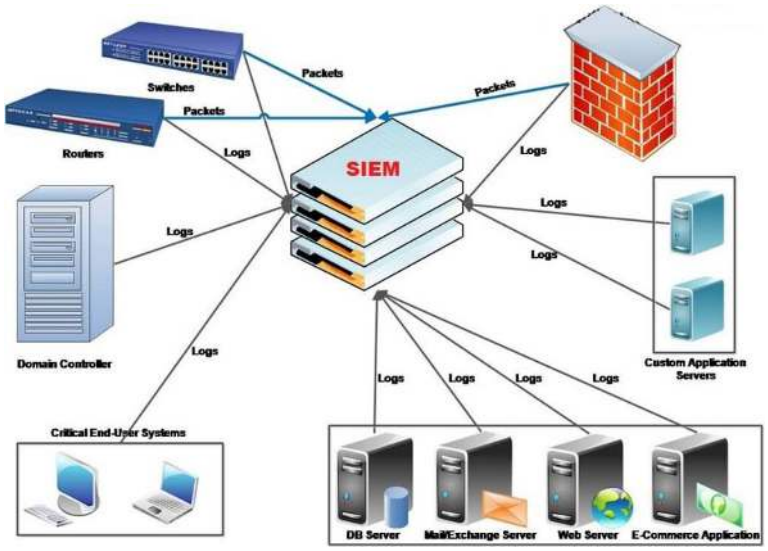


Illustration 22 : schéma représentant un système SIEM au sein d'un SI d'entreprise

Le célèbre cabinet d'analystes Gartner définit le SIEM de cette manière :

« Le SIEM est **un système d'enregistrement de sécurité configurable qui regroupe et analyse les données d'événements de sécurité provenant d'environnements sur site et dans le cloud**. Le SIEM aide à prendre des mesures pour atténuer les problèmes qui nuisent à l'organisation et à satisfaire aux exigences en matière de conformité et de rapports.

Le système de gestion des informations et des événements de sécurité (SIEM) doit permettre de :

- agréger et normaliser les données provenant de divers environnements informatiques et de technologies opérationnelles (OT)
- identifier et enquêter sur les événements de sécurité dignes d'intérêt
- soutenir les actions de réponse manuelles et automatisées
- maintenir les événements de sécurité actuels et historiques et établir des rapports à ce sujet »[13]

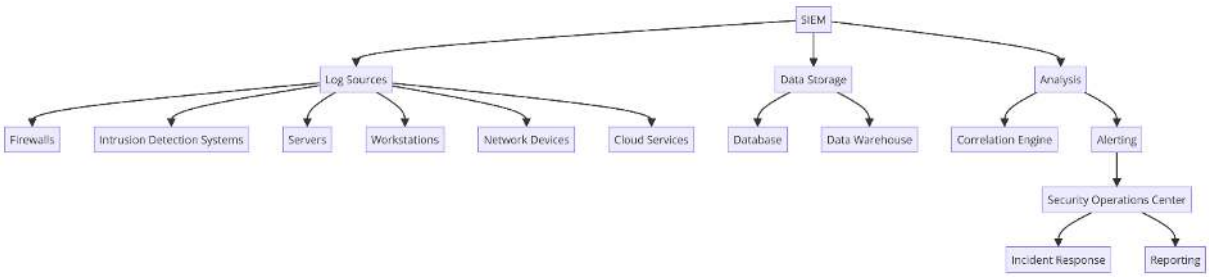


Illustration 23 : diagramme fonctionnel d'un système SIEM

IDC, un autre cabinet d'analystes mondialement réputé, les définit ainsi :

[13] Définition SIEM Magic Quadrant 2024 : https://www.gartner.com/doc/reprints?id=1-2HI8DCZY&ct=240508&st=sb

« Les solutions de gestion des informations et des événements de sécurité (SIEM) sont **des plateformes centrées sur les journaux, utilisées pour garantir la politique et la conformité, ainsi que pour lancer des enquêtes de sécurité**.

Les solutions SIEM comprennent des produits conçus pour agréger des données provenant de sources multiples afin d'identifier des modèles d'événements qui pourraient être le signe d'attaques, d'intrusions, d'abus ou de défaillances.

La corrélation d'événements simplifie et accélère la surveillance des événements réseau en regroupant les alertes et les journaux d'erreurs en un ensemble court et facile à comprendre.

Les produits peuvent également consolider et stocker les données de journalisation traitées par le SIEM.

Cette technologie comprend également des produits qui collectent et diffusent des informations sur les menaces, fournissent des services d'alerte précoce sur les menaces et peuvent fournir des informations sur les contre-mesures.

Les données provenant des produits SIEM sont fournies aux solutions de politique et de conformité pour l'établissement de rapports cohérents. Un SIEM doit prendre en compte différents journaux et flux, dispose de tableaux de bord spécifiquement utilisés pour les enquêtes sur les menaces et est capable d'établir des rapports de conformité. […] »

b) Fonctionnalités

Le logiciel SIEM comprend généralement plusieurs fonctionnalités conçues pour aider les organisations à gérer efficacement les événements de sécurité.

L'entreprise américaine Palo Alto, spécialisée dans les solutions de sécurité, a décrit les caractéristiques communes des systèmes SIEM dans un article de son encyclopédie de la cybersécurité en lige « Cyberpédia »[14] :

Fonctionnalité de sécurité	Description
Collecte et agrégation des journaux	Les données de journaux provenant de diverses sources, notamment les périphériques réseau, les serveurs, les applications et les dispositifs de sécurité, sont collectées et regroupées.
Surveillance et alertes en temps réel	Les événements de sécurité sont surveillés en temps réel et des alertes sont générées lorsque des incidents ou des menaces de sécurité potentielles sont détectés.
Analyses avancées et corrélation	Des algorithmes d'analyse et de corrélation avancés sont utilisés pour identifier les menaces de sécurité potentielles et les anomalies dans le comportement des utilisateurs.
Automatisation de la réponse aux incidents	Les flux de travail de réponse aux incidents sont automatisés, permettant aux équipes de sécurité de répondre rapidement et efficacement aux incidents de sécurité potentiels.
Analyse médico-légale (forensic)	Des capacités d'analyse médico-légale sont fournies, permettant aux équipes de sécurité d'enquêter sur les incidents de sécurité et de comprendre la cause profonde d'un événement de sécurité.

[14] Source : https://www.paloaltonetworks.com/cyberpedia/what-is-siem-software

Rapports et visualisation	Des rapports et des visualisations des événements et des tendances de sécurité sont générés, permettant aux équipes de sécurité de comprendre la situation de sécurité globale d'une organisation.
Conformité et piste d'audit	Des pistes d'audit et des journaux d'événements de sécurité sont fournis, aidant ainsi les organisations à répondre aux exigences de conformité réglementaire.
Intégration avec d'autres outils de sécurité	Une intégration avec d'autres outils de sécurité, tels que des systèmes de détection d'intrusion et des scanners de vulnérabilités, est possible pour fournir une solution de sécurité complète.

3. Système de pot de miel de détection d'intrusion

a) Définitions d'un honeypot

Dans la littérature, il y a diverses définitions pour les pots de miel selon le contexte d'utilisation. En effet, certains considèrent qu'un pot de miel est un outil pour attirer les attaquants alors que d'autres le considèrent plutôt comme un outil de détection d'intrusions.

Dans le reste de ce document nous adopterons la définition suivante donnée par le CIC :

« Dans la terminologie informatique, un pot de miel est **un piège destiné à détecter, dévier ou, d'une manière ou d'une autre, contrecarrer les tentatives d'utilisation non autorisée des systèmes d'information.** »[15].

Victor Garcia sur le site *Canadian Honeypot Security Research* présente la définition suivante :

« **Un pot de miel est une contre-mesure efficace visant à empêcher l'utilisation non autorisée de systèmes d'information critiques dans les réseaux** »[16].

D'après l'équipe de Security Onion, qui est une plateforme de surveillance de sécurité réseau, « un pot de miel de détection d'intrusion (IDH) est **une ressource de sécurité placée à l'intérieur du périmètre de votre réseau qui génère des alertes lorsqu'elle est sondée ou attaquée**. Ces systèmes, services et jetons s'appuient sur la tromperie pour attirer les attaquants et les convaincre d'interagir. À l'insu de l'attaquant, vous êtes alerté lorsque l'interaction se produit et vous pouvez commencer à enquêter sur la compromission. »[17]

Le NIST américain quant à lui définit le honeypot ainsi : « **Un système (par exemple, un serveur Web) ou une ressource système (par exemple, un fichier sur un serveur) conçu pour attirer les pirates et les intrus potentiels**, comme le miel attire les ours. »[18]

b) Principe de fonctionnement des honeypots

« Les honeypots sont des systèmes de sécurité qui n'ont aucune valeur de production. Dès lors, **aucun utilisateur ni aucune autre ressource ne devrait en principe avoir à communiquer avec lui**.

[15] Canadian Institute for Cybersecurity (CIC), https://www.unb.ca/cic/research/honeynet.html
[16] Canadian Honeypot Security Research, http://www.honeynet.org
[17] Source : https://www.youtube.com/watch?v=NzUhfARVfJk
[18] Source : https://csrc.nist.gov/glossary/term/honeypot

L'activité ou le trafic attendu sur le honeypot étant nul à la base, on en déduit *a contrario* que **toute activité enregistrée par cette ressource est suspecte par nature**.

Ainsi, tout trafic, tout flux de données envoyé à un honeypot est probablement un test, un scan ou une attaque. Tout trafic initié par un honeypot doit être interprété comme une probable compromission du système et signifie que l'attaquant est en train d'effectuer des connexions par rebond.

Généralement, un honeypot se comporte telle une boîte noire, enregistrant passivement toute l'activité et tout le trafic qui passe par lui, sur la base du principe de fonctionnement précédent. »[19]

c) Histoire du concept

En 1986, alors qu'il était employé comme administrateur système au *Lawrence Berkeley National Laboratory*, Clifford STOLL a enquêté sur un pirate informatique tenace – identifié plus tard comme la recrue du KGB Markus HESS – qui a volé des mots de passe, piraté plusieurs comptes informatiques et tenté de violer la sécurité militaire américaine. Après avoir identifié l'intrusion, STOLL a mis en place un *honeypot* pour HESS, le traquant finalement et transmettant les détails aux autorités. Il est reconnu comme l'un des premiers exemples de criminalistique numérique.

La liste suivante résume quelques événements clés de l'histoire des pots de miel :

- 1990/1991 – Premiers travaux publics documentant les concepts de pots de miel « *The Cuckoo's Egg* » de Clifford STOLL et « *An Evening With Berferd* » de Bill CHESWICK.
- 1997 : La version 0.1 de *Deception Toolkit* de Fred COHEN est publiée, l'une des premières solutions *honeypot* disponibles pour la communauté de la sécurité.
- 1998 : Début du développement de *CyberCop Sting*, l'un des premiers pots de miel commerciaux vendus au public.
- 2008 : la section canadienne *Honeynet* a été fondée à l'Université du Nouveau-Brunswick.

d) Types de honeypots

Il existe deux types de honeypot : les **honeypots de production** et les **honeypots de recherche**.

Le honeypot de production sera utilisé afin de pouvoir **détecter les attaques** venant de l'extérieur.

L'objectif du honeypot de recherche sera quant à lui d'**étudier le comportement des attaquants** dans le but de comprendre les techniques utilisées lors d'une attaque. Les informations sont ensuite stockées (adresse IP, type d'attaque...) pour être analysées.

Le projet canadien Honeynet[20] est un réseau constitué de ce type de honeypots de recherche et est déployé à l'échelle mondiale.

Honeynet a publié en 2018 un article : « Connaissez votre ennemi : analyse des attaques Internet sur 24 heures » dans lequel il y est démontré que de nombreux robots et botnets (réseaux de machines « zombies » compromises) sévissent sur Internet en lançant de nombreuses attaques automatisées.

[19] Barel, Marie. "HONEYPOT, UN «POT-POURRI»… JURIDIQUE." (2004).
[20] Page de présentation du projet : https://www.honeynet.org/about/ ; https://www.unb.ca/cic/research/honeynet.html

Dans le cadre de leur étude, ils ont mis en place et décidé d'observer ce qui arrive à un serveur connecté à Internet (depuis le cloud AWS). Il ressort de l'étude que des protocoles comme SSH, SIP et HTTP ont été particulièrement ciblés par les attaquants :

Table 1.1: Overview of the Layer 7 Traffic Captured (24-hour capture)

Ports	Protocols	Number of Interactions
22	SSHv2	255796
53	DNS	28713
22	SSH	15206
80	HTTP	245
67	DHCP	114
5060	SIP	28
389	CLDAP	1

e) Avantages et inconvénients

Avantages	Inconvénients
Obtenir des données très pertinentes. Comme un honeypot en fonctionnement normal n'assume aucune fonction, chaque activité dans ce système de contrôle représente une attaque potentielle.	Si l'appât est trop peu attractif ou difficile à atteindre, le risque est de n'avoir aucune attaque et donc un retour nul sur les investissements financiers et humains pour la mise en place de ce système de sécurité.
Gaspiller le temps et les ressources des pirates.	Un honeypot ne fournit pas toujours des informations exploitables.

f) Attaques sur les honeypots

Le potentiel gain de données pertinentes via les honeypots pour les entreprises se caractérise aussi par un risque supplémentaire.

Comme le système de diversion leurre ponctuellement les pirates, **il existe toute de même un risque que ces derniers causent plus de dégâts sur le réseau lors d'une effraction du honeypot**.

Toutefois, il est possible de réduire ce risque par une séparation maximale entre les systèmes en production et l'honeypot ainsi qu'en maintenant une surveillance constante de toutes les activités dans les systèmes de leurre.

Il est enfin important de limiter les dégâts à l'extérieur : pour empêcher l'utilisation d'un honeypot comme point de départ d'attaques de hackers sur d'autres systèmes, **les connexions sortantes doivent être réduites à son minimum**.[21]

[21] *Cf* article « Qu'est-ce qu'un honeypot ? » (2017) : https://www.ionos.fr/digitalguide/serveur/securite/honeypot-securite-informatique-via-des-leurres/

Un exemple de type d'attaque sur les pots de miel est ce PoC d'injection de commandes dans les terminaux Windows connectés aux pots de miel :

L'attaque suppose que l'analyse des logs est faite dans un terminal (ici, celui de Windows 10) au sein duquel on va introduire des séquences d'échappement. Pour cela, **on envoie un fichier vers le pot de miel… et on espère qu'un analyste le consulte avec la commande « cat »**.

En fonction du système cible, on peut insérer des données dans le presse-papiers, ouvrir des liens, suivre les mouvements de la souris, etc. Voire exécuter des processus (cf. faille CVE-2022-44702).

Pour masquer ces actions, on peut déclencher, à leur suite, une forme de dépassement de tampon : afficher une très longue suite de caractères, de sorte qu'on perd le début du log.

On admettra qu'un tel scénario d'*empoisonnement* de pot de miel implique une configuration spécifique. Et qu'on peut l'éviter de bien des manières. Par exemple en utilisant la commande « file » (qui révèle la nature du fichier) ou l'argument « -v » (qui affiche des caractères non imprimables).[22]

D. COMPARAISON ET CHOIX DES SOLUTIONS

Afin de permettre à M^r^ Alex FALZON de prendre une décision éclairée dans le but de proposer les meilleures solutions pour le Réseau EasyFormer, j'ai réalisé un « *benchmark* », une étude comparative de différents systèmes SIEM et solutions de *honeypot* afin d'identifier les performances et fonctionnalités de chacun d'eux tout en considérant le budget très limité dont nous disposions et les besoins spécifiques du projet.

1. Etude comparative de systèmes SIEM

a) Classement auprès des spécialistes

Afin d'avoir une bonne vue d'ensemble des systèmes de *gestion des informations et des événements de sécurité* (SIEM) et d'identifier les acteurs importants du marché, j'ai consulté trois rapports spécialisés SIEM rédigés par des cabinets d'analystes très réputés : Forrester, IDC et Gartner.

FORRESTER

Dans le rapport[23] *The Forrester Wave* du 4^e^ trimestre 2022 sur les plateformes d'analyse de sécurité j'ai pu constater que **Microsoft**, **Splunk** et **Elastic** ont été placés en tant que leaders sur le marché des fournisseurs de solutions SIEM :

[22] Cf article « Cybersécurité : gare au détournement des pots de miel » : https://www.silicon.fr/cybersecurite-detournement-pots-miel-470912.html
[23] The Forrester Wave: Security Analytics Platforms, Q4 2022 : https://reprints2.forrester.com/#/assets/2/682/RES176427/report

Illustration 24 : The Forrester Wave : Security Analytics Platforms, Q4 2022

Dans le rapport[24] *IDC MarketScape* évaluant les fournisseurs SIEM dans le monde en 2022, celui-ci a également placé **Splunk** en tant que leader du marché :

Illustration 25 : IDC MarketScape : Worldwide SIEM 2022 Vendor Assessment

Dans le rapport[25] *Magic Quadrant* de Gartner sorti en 2024, la solution SIEM proposée par **Elastic** s'y trouve mais plus bas, parmi les « précurseurs ». Quant à

[24] IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment : https://idcdocserv.com/US49029922e_Splunk
[25] Magic Quadrant, Gartner, mai 2024 : https://www.gartner.com/doc/reprints?id=1-2HI8DCZY&ct=240508&st=sb

Splunk Enterprise Security, il y est nommé leader pour la dixième fois consécutive. La solution **Microsoft Sentinel** est aussi parmi les leaders.

Illustration 26 : Magic Quadrant for Security Information and Event Management

Il ressort de ces 3 rapports que la solution **Splunk Enterprise Security** est parmi les meilleures du marché.

b) Fonctionnalités

Une étude minutieuse des différentes fonctionnalités que proposent les solutions de sécurité envisagées a également été réalisée :

Critères	Security Onion SOLUTIONS **Security Onion**	splunk> a cisco company Enterprise Security **Splunk ES**	elastic stack **Elastic Stack (ELK)**	ALIEN VAULT OSSIM **AlienVault OSSIM**
Capacités IDR (*Incident Detection and Response*)	Complètes, avec IDS/IPS, analyse de logs, et chasse aux menaces	Avancées, avec une forte analyse de données et de menaces	Personnalisables, dépendent de l'intégration et des plugins	Complètes, bien intégrées mais avec des fonctionnalités potentiellement limitées comparées à des solutions commerciales
Analyse des logs	Haute capacité, supporte divers formats	Excellente, avec des outils puissants pour l'analyse de données	Haute, personnalisable avec Logstash et Kibana	Bonne, supporte de nombreux formats mais peut être moins intuitive que Splunk
Intégration des données	Excellente, flexible pour différents formats et sources	Excellente, avec une large gamme de connecteurs et d'APIs	Excellente, très flexible avec Beats et Logstash	Bonne, supporte de nombreuses sources mais peut nécessiter plus de configuration manuelle
Facilité d'utilisation	Moyenne, nécessite une certaine expertise pour la configuration et l'optimisation	Haute, interface utilisateur intuitive et documentation complète	Moyenne à haute, dépend de la complexité de la configuration	Moyenne, interface utilisateur conviviale mais avec une courbe d'apprentissage pour la configuration
Support	Support « premium » (payant)[26] et communautaire	Professionnel (payant) et communautaire	4 niveaux de support technique Elastic (payant) + support communautaire	Professionnel (payant pour la version premium) et communautaire
Coût	Open source, coût lié au matériel et au support si nécessaire	Elevé, basé sur le volume de données et les fonctionnalités mais programme de don aux associations[27]	Principalement open source, coûts associés aux fonctionnalités premium d'Elastic	Open source, coûts pour les fonctionnalités avancées et le support professionnel

[26] Page de support SOS : https://securityonionsolutions.com/support
[27] Page de l'offre aux associations : https://www.splunk.com/en_us/about-us/splunk-pledge/nonprofit-license-application.html

c) Tarifs

Trois des solutions envisagées sont des logiciels libres et open source n'imposant pas de payer pour les utiliser. Il n'y a que Splunk qui est payant mais il offre une licence gratuite (10 Go de trafic) aux associations à but non lucratif :

Illustration 27 : page web mentionnant le don de licence Splunk aux associations

Toutes les solutions envisagées respectent donc le budget alloué pour la réalisation de ce projet.

d) Solution retenue

Après avoir entendu nos avis et le résultat de nos recherches, M^{r} Alex FALZON a décidé d'opter pour la solution **Security Onion** pour plusieurs raisons :

La culture d'entreprise de type association à but non lucratif du Réseau EasyFormer privilégie les FOSS (Free & Open Source Softwares)	Malgré le don de licence Splunk pour les associations, le Réseau EasyFormer n'avait pas envie de s'enfermer dans une solution propriétaire et devenir dépendant envers l'éditeur
Pas de possibilité de profiter d'une seconde licence Splunk gratuite en cas d'expansion (donc éventuel coût conséquent à venir)	L'équipe interne est techniquement assez compétente pour prendre en main la solution Security Onion

Grâce à ce benchmark nous avons pu conclure que la solution choisie pourra s'intégrer complètement dans l'environnement existant et qu'elle est bien adaptée aux besoins de l'organisation EasyFormer, tant pour aujourd'hui que pour l'avenir.

2. Présentation de la solution retenue

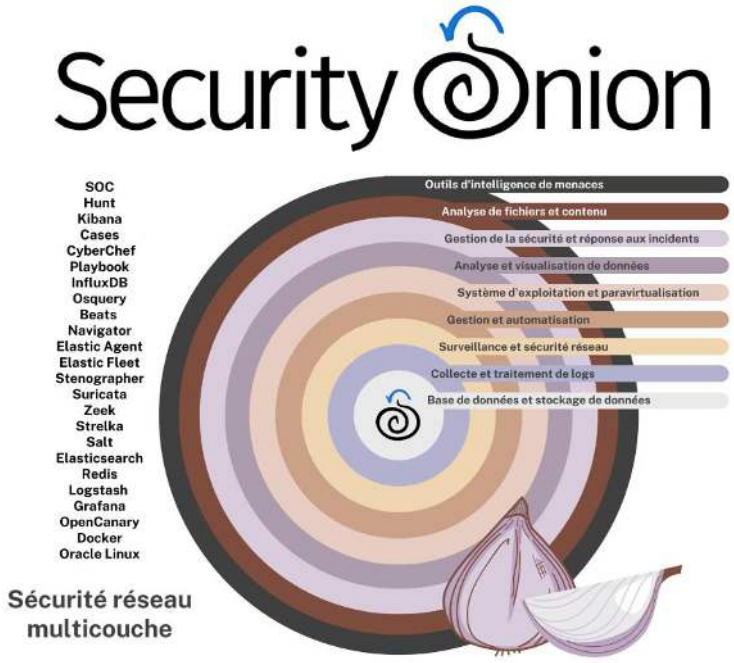


Illustration 28 : diagramme illustrant la sécurité multicouche de Security Onion

Security Onion est **une plate-forme (sous la forme d'une distribution GNU/Linux) gratuite, libre et open source pour la recherche de menaces (*threat hunting*), la surveillance de la sécurité du réseau (NSM) et la gestion des journaux**.

L'objectif principal de Security Onion est de fournir une solution tout-en-un pour la surveillance de la sécurité réseau, permettant aux organisations de détecter, d'analyser et de répondre aux incidents de sécurité.

Security Onion fournit une visibilité sur le trafic réseau et le contexte autour des alertes et des événements anormaux, mais cela nécessite tout de même d'examiner les alertes et surveiller l'activité du réseau.

Il est à noter que Security Onion ne se présente pas (encore ?) comme une solution SIEM mais en possède les principales fonctionnalités. Ses éditeurs ont jusqu'à la version 2.3 parlé de « plateforme pour la NSM et l'ESM ».

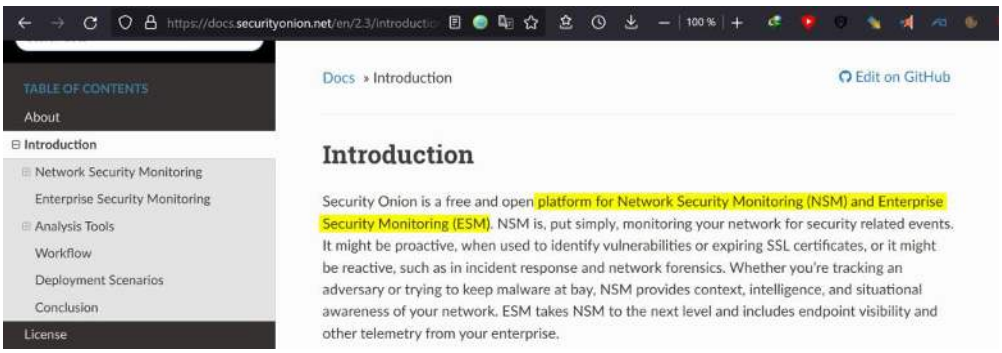


Illustration 29 : présentation de la solution SO dans la documentation v.2.3 (désormais supprimée)

La NSM (*Network Security Monitoring*), « surveillance de la sécurité du réseau » est **une discipline mêlant les aspects instrumentation réseau (collecte de trafic) et détection d'intrusions**, essentiellement via des NIDS (*Network Intrusion Detection Systems*) type Snort.[28]

L'ESM (*Enterprise Security Monitoring*), « surveillance de la sécurité de l'entreprise » est **un processus qui implique la collecte, l'analyse et la gestion des données de sécurité générées par diverses sources (hôtes, réseau) dans un environnement informatique d'entreprise**. L'objectif principal de l'ESM est d'identifier, de surveiller et de répondre aux menaces potentielles, aux incidents de sécurité et aux vulnérabilités qui pourraient affecter les systèmes et les réseaux d'une organisation.

Depuis la version 2.4, ses éditeurs ont retiré ces termes NSM et ESM pour présenter leur solution et ont préféré se focaliser sur la description de ses fonctionnalités et nombreux outils de sécurité et d'analyse.

Illustration 30 : présentation de la solution SO dans la documentation v.2.4

Security Onion adopte donc **une approche multicouche pour sécuriser le réseau**, en combinant plusieurs outils pour offrir une défense en profondeur :

Voici ses différentes couches de sécurité :

[28] Source : https://connect.ed-diamond.com/GNU-Linux-Magazine/glmf-175/introduction-au-network-security-monitoring-nsm

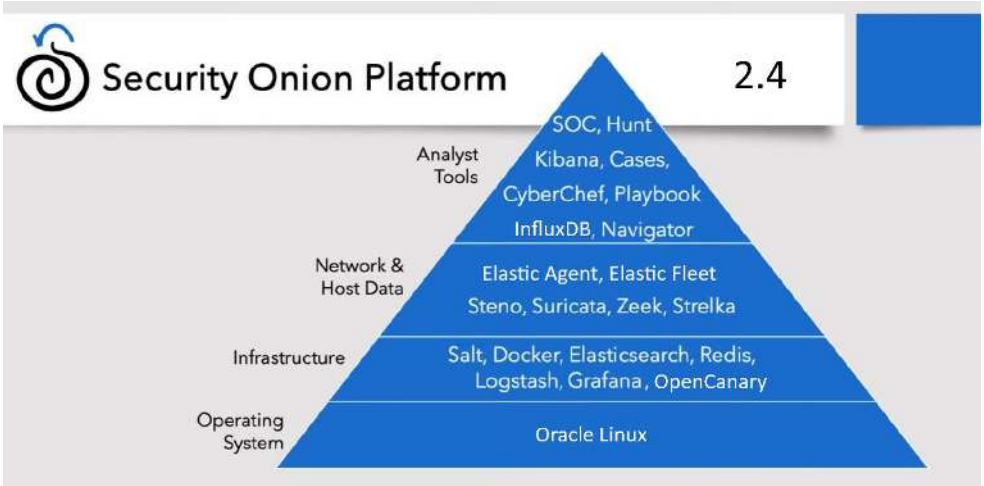


Illustration 31 : diagramme illustrant la pile technologique de Security Onion

a) Détection des intrusions (IDS)

En utilisant des règles prédéfinies et des mécanismes de détection d'anomalies, Security Onion peut aider à identifier des comportements suspects sur le réseau, indiquant potentiellement des activités malveillantes.

- **Suricata** et **Zeek** analysent le trafic réseau en temps réel pour détecter des modèles de menaces connus et inconnus.
- **Suricata** utilise des règles pour identifier des signatures spécifiques de menaces.
- **Zeek** fournit une analyse comportementale pour détecter des activités anormales.
- **OpenCanary** est un honeypot de détection d'intrusion qui imite des services. Les tentatives de connexion à ces services génèrent automatiquement des alertes.
- L'interface **Playbooks** permet de configurer des règles de détection basées sur le standard Sigma.

b) Surveillance et enregistrement

Security Onion inclut ces outils pour la surveillance du réseau et la capture des données :

- **Zeek** collecte et enregistre des métadonnées détaillées sur le trafic réseau, permettant une analyse approfondie des événements.
- **Logstash** collecte et transforme les données de journaux provenant de différentes sources.
- **Stenographer** capture les paquets.
- **Elastic Agent** collecte les journaux d'évènement sur les point de terminaison.
- **Elastic Fleet** permet la gestion centralisée.

c) Analyse et visualisation

Il intègre des outils comme Elasticsearch, Logstash et Kibana (stack ELK) pour la gestion et l'analyse des journaux, facilitant ainsi la corrélation des informations à partir de différentes sources de données.

- **Elasticsearch** indexe les données collectées, facilitant les recherches rapides et l'analyse.
- **Kibana** offre une interface web pour visualiser les données sous forme de tableaux de bord interactifs.
- **Strelka** analyse les fichiers.
- **Osquery** permet de faire des requêtes en direct sur la masse de données récoltée.

d) Gestion des incidents

- **TheHive** centralise les alertes et incidents, permettant une gestion efficace et collaborative.
- **Cortex** enrichit les incidents avec des informations supplémentaires pour faciliter l'analyse et la réponse.

Avec toutes les sources de données mentionnées ci-dessus, une quantité incroyable de données est disponible à portée de main. Heureusement, Security Onion intègre une console pour vous aider à donner un sens à ces données. **Security Onion Console (SOC)** est la première chose que vous voyez lorsque vous vous connectez à Security Onion.

Il comprend l'interface « Alertes » qui permet de voir toutes vos alertes NIDS depuis Suricata. Elle comprend également l'interface « Dashboards » qui vous donne un bon aperçu non seulement des alertes NIDS/HIDS, mais également des journaux de métadonnées réseau de Zeek ou Suricata et de tout autre journal que vous pourriez collecter.

3. Choix du pot de miel de détection d'intrusion

a) Popularité

En l'absence de rapports comparatifs sur les honeypots similaires à ceux que nous avons consulté pour les SIEM, il nous est paru pertinent d'effectuer une recherche sur la popularité à l'échelle mondiale des différentes solutions envisagées à l'aide du moteur de recherche Google Trends :

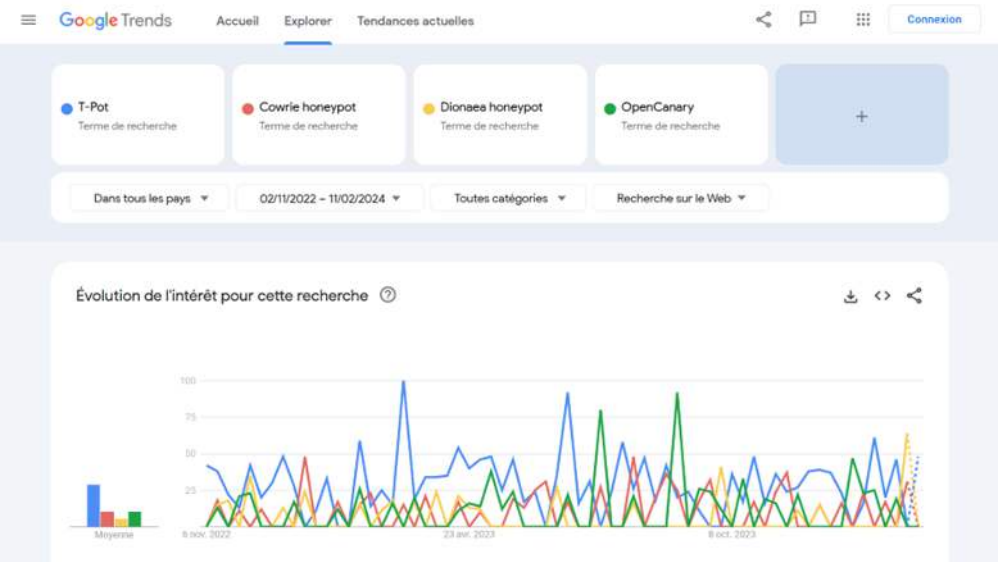


Illustration 32 : étude de popularité avec Google Trends effectuée le 11/02/2024

Les résultats de cette requête reflètent la proportion de recherches Google portant sur les mots clé « T-Pot », « Cowrie honeypot », « Dionaea honeypot », et « OpenCanary » dans tous les pays du monde et pour la période des 2 années précédentes, par rapport à la région où le taux d'utilisation de ce mot clé est le plus élevé (valeur de 100). Ainsi, une valeur de 50 signifie que le mot clé a été utilisé moitié moins souvent dans la région concernée.

Il ressort de l'étude comparative que la solution T-Pot (en bleu sur le graphique) est légèrement plus populaire que ses concurrentes sur ces 2 dernières années.

b) Fonctionnalités

Critères	T-Pot	OpenCanary	Cowrie	Dionaea
Open Source / Logiciel Libre	Oui (GPLv3)	Oui (licence BSD)	Oui (GPLv3)	Oui (GPLv3)
Facilité de déploiement	Elevée (distribution intégrée)	Moyenne (configuration nécessaire)	Moyenne (configuration nécessaire)	Moyenne (configuration nécessaire)
Diversité des protocoles	Très élevée (multiples honeypots intégrés)	Élevée (configurable pour plusieurs protocoles)	Limitée (principalement SSH et Telnet)	Élevée (capture des malwares via vulnérabilités de protocole)
Efficacité de la détection	Très élevée (diversité des honeypots)	Élevée (détection configurable)	Élevée (bonne pour SSH/Telnet)	Élevée (spécialisée dans la capture de malwares)
Personnalisation	Élevée (peut intégrer de nouveaux honeypots)	Très élevée (hautement configurable)	Élevée (scripts et interactions personnalisables)	Moyenne (quelques options de configuration)
Communauté et support	Élevée (bien soutenu par une communauté active)	Élevée (bonne documentation, communauté active)	Élevée (communauté active, bonne documentation)	Moyenne (communauté plus petite mais dédiée)
Fonctionnalités uniques	Intégration de multiples honeypots pour une couverture étendue	Flexibilité dans la simulation de services variés	Simulation interactive SSH/Telnet de haute fidélité	Spécialisé dans la capture de malwares avec simulation de vulnérabilités

c) Solution retenue

OpenCanary

La solution retenue a été OpenCanary pour les raisons suivantes :

La culture d'entreprise de type association à but non lucratif privilégie les FOSS (Free & Open Source Softwares)	OpenCanary se déploie facilement grâce à l'assistant d'installation inclus dans l'ISO de Security Onion
OpenCanary a fait ses preuves et est reconnu pour comme étant un honeypot efficace	OpenCanary s'intègre parfaitement pour la détection d'intrusion au sein de la plateforme Security Onion précédemment sélectionnée

V. PHASE DE CONCEPTION

A. PERIODE D'AUTOFORMATION

Afin de bien appréhender le projet nous avons dédié un temps à l'autoformation et la documentation, car Security Onion est une solution complexe rassemblant de nombreux outils eux aussi complexes.

Pour ma part, ayant trouvé peu de ressources sur cette technologie, je me suis plutôt orienté vers la documentation officielle et la chaine YouTube de Security Onion sur laquelle j'ai trouvé de nombreuses conférences instructives et tutoriels efficaces.

B. OU PLACER LE SERVEUR SECURITY ONION ?

1. Choix de la virtualisation dans un Proxmox

Même si l'équipe de Security Onion préconise d'utiliser du matériel dédié plutôt qu'une VM (machine virtuelle), par manque de budget nous n'avons eu le choix que de virtualiser la machine hébergeant le serveur Security Onion sur l'un des hyperviseurs disponibles. Nous avons opté pour le cluster de Proxmox car les ESXi du Réseau EasyFormer ont vocation à être abandonnés suite aux changements de politique après le rachat de VMware par Broadcom.

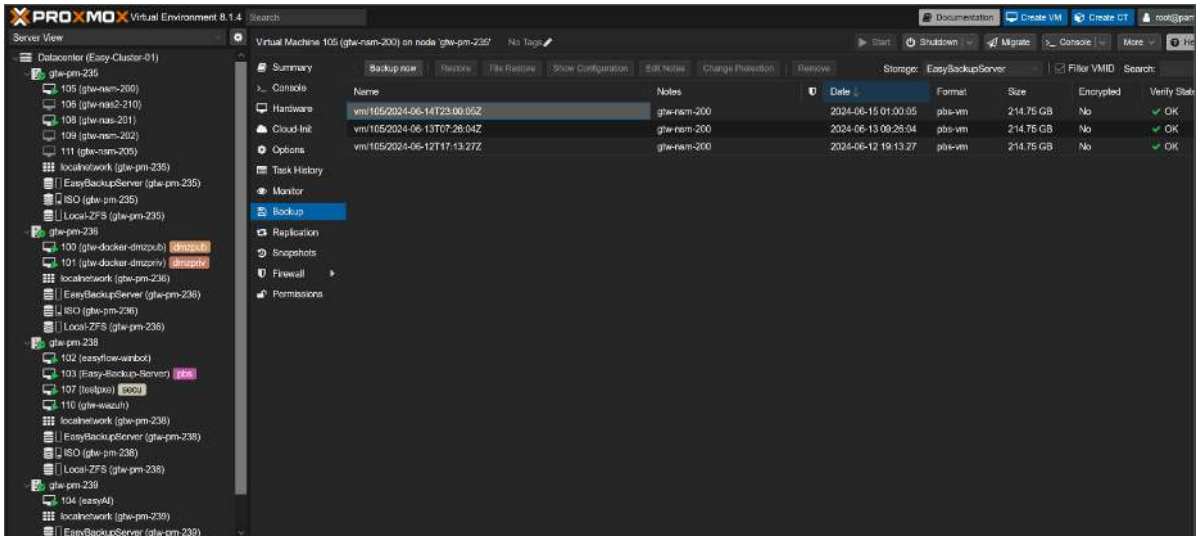


Illustration 33 : interface web d'administration des hyperviseurs Proxmox

2. Interface réseau d'administration

Dans son guide « Recommandations relatives à l'administration sécurisée des systèmes d'information »[29], l'ANSSI préconise de dédier un réseau de communication sur lequel transitent les **flux internes au SI d'administration** et les **flux d'administration à destination des ressources administrées**. De ce fait l'interface d'administration de notre plateforme Security Onion a été reliée au VLAN d'administration du réseau EasyFormer pour respecter cette bonne pratique.

3. Interface(s) réseau de surveillance

La plateforme Security Onion fonctionne avec au minimum deux interfaces réseau : une pour l'administration de Security Onion et une autre pour le *sniffing*/*monitoring* (« reniflage/surveilllance »).

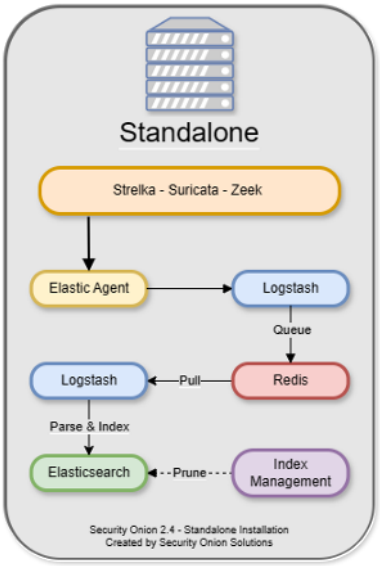
[29] Recommandations relatives à l'administration sécurisée des systèmes d'information, chapitre 5 « Réseau d'administration » : https://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/

Rien n'empêche d'ajouter d'autres interfaces dédiées au *monitoring* mais pour ce premier déploiement, il nous est paru prudent de ne pas complexifier la partie réseau. De ce fait le serveur Security Onion a été déployé avec une seule interface de *monitoring*.

Après en avoir discuté ensemble, Mr Alex FALZON a décidé d'utiliser cette première interface de *sniffing* (« reniflage ») pour surveiller son VLAN « DMZ publique » car les machines s'y trouvant sont directement exposées sur Internet et il y a potentiellement plus de risque qu'elles soient attaquées et compromises.

C. QUELLE ARCHITECTURE DE DEPLOIEMENT CHOISIR ?

1. Choix du déploiement standalone



Il y a plusieurs moyens de déployer Security Onion, l'un d'entre eux est le déploiement **Standalone** (autonome) avec tous les composants de Security Onion sur un seul serveur.

Ce type de déploiement est destiné notamment aux environnements à faible débit.

Dans un déploiement Standalone, l'agent Elastic envoie les journaux à Logstash, qui les envoie à Redis pour mise en file d'attente. Un deuxième pipeline Logstash extrait les journaux de Redis et les envoie à Elasticsearch, où ils sont analysés et indexés[30].

EasyFormer étant une petite structure, ce déploiement fut privilégié mais il n'est pas impossible de passer à un type de déploiement **Distributed** (distribué) plus tard si des besoins d'évolution se faisaient sentir.

D. QUELLE METHODE DE PORT MIRRORING CHOISIR ?

La question s'est posée de choisir quelle configuration réseau pour permettre la capture du trafic : mode *promiscuous* ou via un TAP réseau ?

Les recommandations que nous trouvons dans la documentation de Security Onion préconisent d'utiliser un TAP réseau dans la mesure du possible plutôt qu'un *port mirroring* de type SPAN.

[30] Documentation sur les types de déploiement : https://docs.securityonion.net/en/2.4/architecture.html

Best Practices

Security Onion provides lots of options and flexibility, but for best results we recommend the following best practices.

Installation

- Download and verify our ISO image as shown in the Download section.
- For production deployments, prefer dedicated hardware to VMs when possible (see the Hardware Requirements section).
- If VMs must be used, ensure that resources are properly dedicated to VMs to avoid resource contention.
- Use local storage and avoid NFS, NAS, iSCSI, etc.
- Adequately spec your hardware to meet your current usage and allow for growth over time.
- Prefer taps to span ports when possible.
- Make sure that any network firewalls have the proper firewall rules in place to allow ongoing operation and updates (see the Firewall section).

Illustration 34 : page de documentation préconisant l'usage d'un TAP réseau pour le sniffing

1. Surveillance du trafic via un TAP réseau

Un **TAP réseau** (*Test Access Point*) est **un dispositif physique qui se connecte directement entre deux points réseau, comme entre un switch et un routeur. Il copie le trafic passant entre ces deux points vers un port de monitoring ce qui permet de surveiller et d'analyser le trafic réseau de manière passive sans interférer avec celui-ci**.

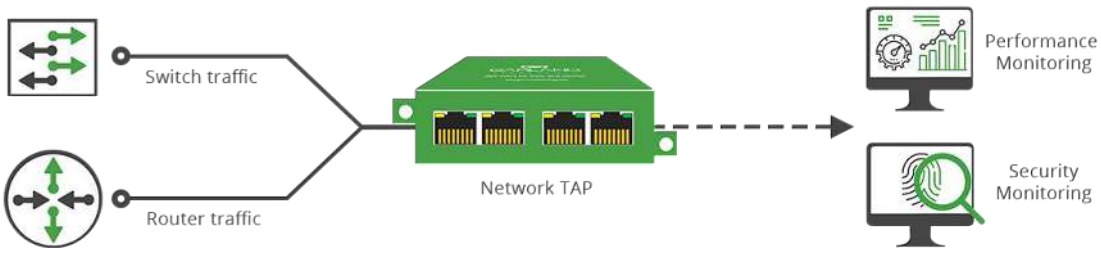


Illustration 35 : représentation graphique du fonctionnement d'un TAP réseau

Voici à quoi ressemblerait ce type de configuration :

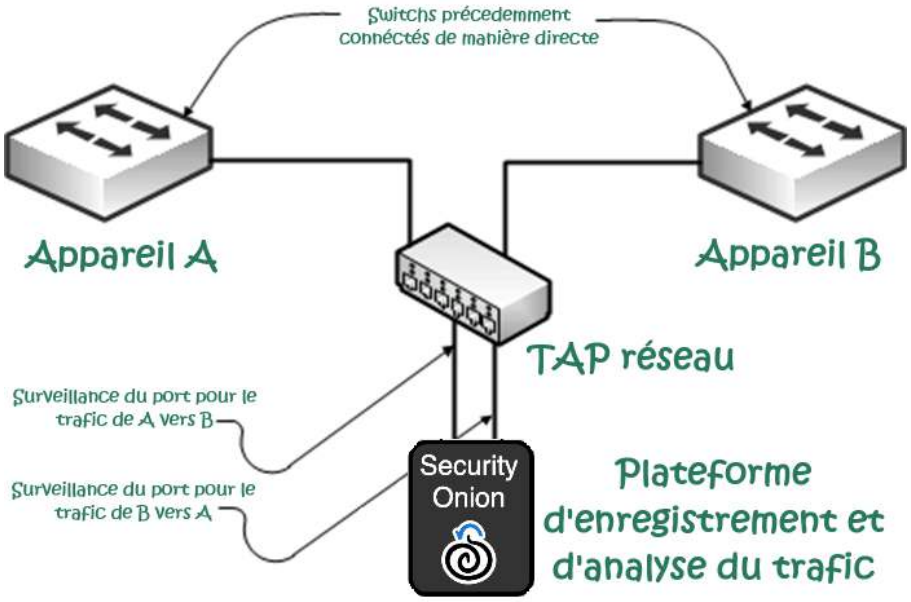


Illustration 36 : schéma d'un déploiement de SO avec un TAP réseau

Nous pouvons expliquer le schéma ci-dessus pour comprendre le fonctionnement d'un TAP réseau :

Connexion des dispositifs

Les dispositifs A et B (qui pourraient être des switches, des routeurs ou d'autres équipements réseau) sont normalement connectés directement entre eux. Le schéma montre une connexion qui était précédemment directe entre ces deux dispositifs.

Insertion du TAP réseau

Un TAP réseau est inséré entre les dispositifs A et B. Cela se fait en connectant le dispositif A au TAP et le dispositif B au TAP, comme indiqué sur le schéma. Ainsi, tout le trafic entre A et B passe désormais par le TAP réseau.

Fonctionnement du TAP

Le TAP réseau copie passivement tout le trafic qui passe entre les dispositifs A et B. Il fait cela sans modifier le trafic ou introduire des délais significatifs, ce qui est essentiel pour la performance et la fiabilité du réseau.

Port de monitoring

Le TAP a des ports de monitoring spécifiques pour capturer le trafic dans les deux directions :

- Un port de monitoring pour le trafic allant de A vers B.
- Un autre port de monitoring pour le trafic allant de B vers A.

Analyse du trafic

Ces ports de monitoring sont connectés à un dispositif d'analyse, ici représenté par Security Onion qui reçoit les copies du trafic réseau provenant des ports de monitoring du TAP et peut analyser ce trafic en temps réel ou l'enregistrer pour une analyse ultérieure.

2. Surveillance du trafic via un port SPAN

Un **port SPAN** (*Switched Port ANalyzer*) est configuré sur un switch réseau **pour rediriger le trafic d'un ou plusieurs ports spécifiés (ou VLANs) vers un port de monitoring désigné**. **Cela se fait au niveau du logiciel du switch**, ce qui peut parfois influencer la performance du switch lui-même. Il est possible de faire cela sur Proxmox de différentes manières (avec OpenVSwitch par exemple).

3. Avantages et inconvénients

Méthode	Avantages	Inconvénients
TAP	• **Ne consomme pas de ressources** supplémentaires sur les équipements réseau, car il agit comme un dispositif passif. • **Fournit une copie exacte du trafic**, incluant toutes les erreurs et les paquets corrompus, ce qui est essentiel pour des analyses détaillées et pour la détection de problèmes spécifiques.	**Plus coûteux** en raison du besoin de matériel supplémentaire et de l'intervention physique pour l'installation.
SPAN	**Moins coûteux** à mettre en œuvre car il utilise les capacités existantes du switch et peut être configuré via le logiciel du switch sans coût supplémentaire pour l'équipement.	• **Peut affecter les performances** du switch si la charge de trafic est élevée, car il nécessite que le switch traite et redirige le trafic supplémentaire vers le port de monitoring. • Peut occasionnellement **manquer de capturer certains paquets**, surtout en cas de forte charge réseau. Les erreurs de paquets ne sont généralement pas transmises au port de monitoring.

4. Choix de la méthode de port mirroring SPAN

En fonction de notre budget limité, nous avons opté pour la solution logicielle de type SPAN qui n'implique pas l'acquisition de nouveau matériel.

Il existe dans la documentation[31] une section dédiée à la configuration des cartes réseau pour l'analyse de trafic dans Proxmox :

- La première option consiste à détecter le trafic provenant d'une carte réseau physique « Passthrough » qui a été transmis à la machine virtuelle.
- La deuxième option consiste à détecter le trafic provenant d'une carte réseau virtuelle Proxmox.

[31] Page de documentation de Security Onion pour Proxmox : https://docs.securityonion.net/en/2.4/proxmox.html#nic

Une fois la carte réseau physique transmise à la machine virtuelle Security Onion, Security Onion a été en mesure de configurer correctement sa carte réseau pour le « reniflage ».

E. OU PLACER LE HONEYPOT ?

1. Choix de la virtualisation dans un Proxmox

Pour les raisons budgétaires exposées précédemment, nous avons également virtualisé la machine hébergeant le serveur leurre « honeypot » dans un hyperviseur Proxmox.

2. Choix du segment réseau DMZ

Dans la documentation de Security Onion, les éditeurs déconseillent d'exposer le honeypot sur Internet. Ce n'est pas un honeypot de recherche mais un honeypot de production destiné à détecter les intrusions sur le réseau interne. Nous avons donc décidé de le placer dans la DMZ publique car c'est ce segment réseau qui est le plus susceptible d'être attaqué depuis l'extérieur.

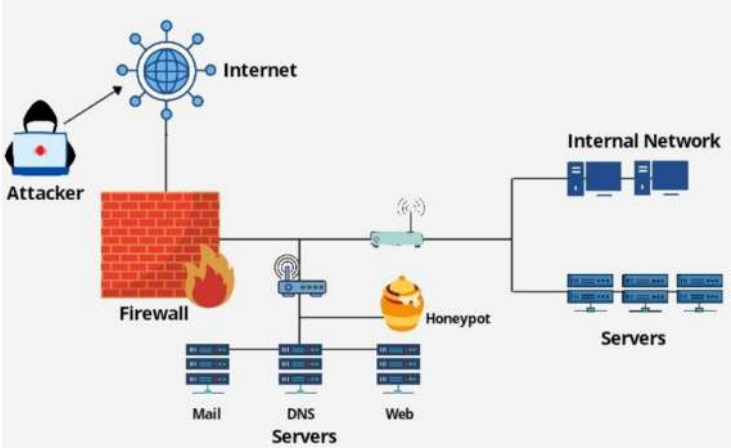


Illustration 37 : schéma d'un honeypot en DMZ

Il est à noter que placer le honeypot dans un réseau interne sur lequel il y a des serveurs de production aurait aussi été un choix pertinent.

VI. PHASE DE REALISATION

Les détails des procédures techniques (installations et configurations) ont été placés en IX pour respecter la consigne de limitation du nombre de pages de ce mémoire.

A. LES INSTALLATIONS

1. Installation de Security Onion

Tout d'abord, j'ai téléchargé l'ISO de la dernière version de Security Onion depuis le site officiel. Ensuite, j'ai créé une machine virtuelle (VM) dans Proxmox. J'ai inséré l'ISO dans le lecteur virtuel de

la VM et démarré cette dernière. L'installation s'est déroulée via une interface graphique minimale, où j'ai pu configurer les interfaces réseau d'administration et de surveillance.

2. Installation du honeypot OpenCanary

Pour l'installation du honeypot, je me suis appuyé sur la documentation officielle. J'ai utilisé l'assistant d'installation de l'ISO de Security Onion pour ajouter un nœud IDH (Intrusion Detection Honeypot) à notre plateforme Security Onion.

J'ai donc créé une nouvelle VM dans notre hyperviseur Proxmox avec Oracle Linux, hébergeant un service OpenCanary et fonctionnant dans un container Docker.

B. LES CONFIGURATIONS

1. Autorisation de la communication entre le nœud IDH et le manager

Après avoir installé notre nœud IDH, nous avons dû autoriser la connexion entre ce nœud et le *manager* Security Onion. Cela consistait à mettre en place des règles de *firewalling*. Après avoir effectué cette configuration, nous avons bien retrouvé notre nœud IDH dans la section « Grid » de l'interface web de Security Onion avec son statut de connexion « OK ».

2. Configuration des services leurres d'OpenCanary

Nous avons ensuite configuré les services leurres qui devaient tourner sur le nœud IDH. Une fois la configuration effectuée, la page web de connexion du faux NAS Synology simulé par OpenCanary ressemblait à l'originale.

3. Création des utilisateurs de Security Onion

Ensuite, nous avons créé des utilisateurs supplémentaires dans Security Onion, en nous assurant de créer des comptes nominatifs pour pouvoir attribuer chaque action effectuée à un individu spécifique si nécessaire. Nous leur avons également attribué les permissions appropriées.

4. Importation de règles Sigma de détection d'intrusion

Nous avons intégré des règles Sigma dans notre plateforme Security Onion pour identifier les tentatives de connexion sur notre nœud OpenCanary utilisant des protocoles surveillés, comme les connexions SSH ou les requêtes HTTP POST.

5. Déploiement des agents Elastic pour la collecte des journaux des points de terminaison

Nous avons déployé et configuré les agents Elastic pour collecter les journaux de notre pare-feu pfSense et des points de terminaison Linux et Windows. Voici les étapes principales :

a) Configuration du pare-feu de Security Onion

Ajustement du pare-feu de Security Onion pour accepter les connexions des agents Elastic et spécification des adresses IP autorisées.

b) Téléchargement et installation des agents Elastic

Téléchargement des agents Elastic depuis Security Onion et installation des agents sur les points de terminaison.

c) Configuration DNS sur le pfSense

Configuration du DNS pour que le serveur Security Onion soit accessible par son nom d'hôte.

d) Configuration des politiques des agents Elastic dans Elastic Fleet

Utilisation d'Elastic Fleet pour attribuer des politiques aux agents. Modifications des politiques pour collecter les journaux d'événements réseau, des processus système, etc.

e) Intégration pfSense

Activation de l'intégration Elastic pour pfSense. Configuration de Security Onion pour écouter le port UDP 9001. Mise à jour du pare-feu pour accepter le trafic syslog de pfSense. Activation de la journalisation distante dans pfSense et envoi des journaux à Security Onion.

6. Mise à jour de Security Onion vers la version 2.4.70

Lors de la sortie de Security Onion version 2.4.70 nous avons effectué avec succès la mise à jour depuis la version 2.4.60.

C. VERIFICATIONS DU BON FONCTIONNEMENT

Afin de vérifier le bon fonctionnement de nos configurations, nous avons effectué des tests.

1. Vérification du bon fonctionnement des Agents Elastic déployés

a) Vérification de l'ingestion des journaux Windows et Linux

Une fois les agents Elastic déployés sur nos hôtes Windows et Linux, nous pouvons utiliser le filtre prédéfini « Host Overview » par exemple :

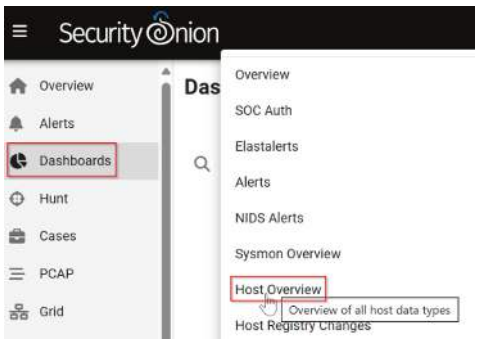


Illustration 38 : requête OQL prédéfinie « Host Overview »

Pour retrouver nos machines :

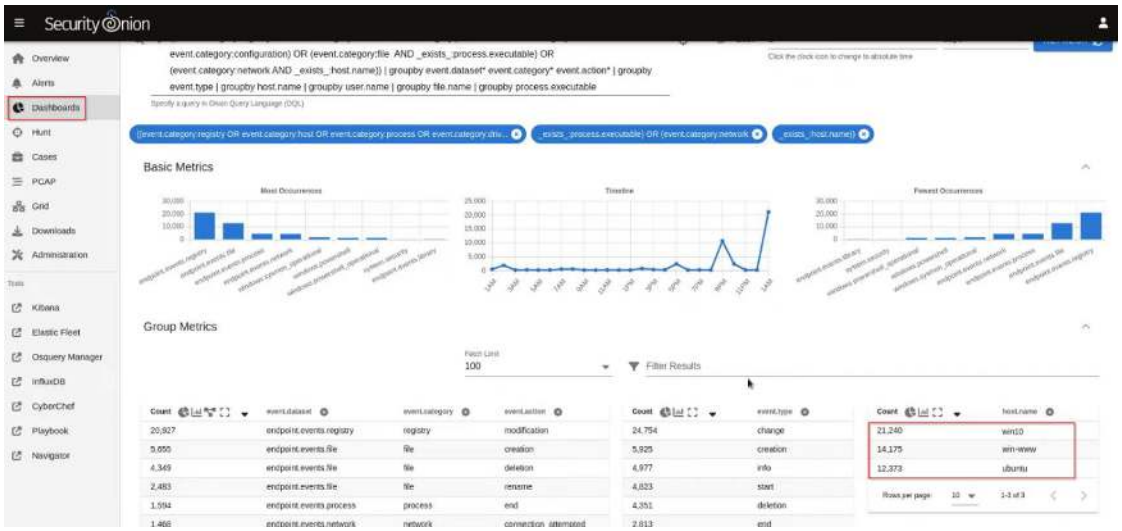


Illustration 39 : interface « Dashboards » avec présence des hôtes surveillés par les agents Elastic

Les tableaux de bord étant hautement interactifs, il est ensuite possible de faire un clic droit sur un élément, par exemple un nom d'utilisateur, et sélectionner « Include » pour l'ajouter au filtre d'affichage des données.

b) Vérification de l'ingestion des journaux pfSense

Après avoir configuré l'ingestion des journaux du pfSense nous sommes retournés dans la console Security Onion, et avons ouvert l'entrée de menu « Hunt ».

En laissant le filtre par défaut « ** | groupby event.module* event.dataset* » nous avons remarqué que nous recevions désormais des journaux pour l' « *event.module* » pfSense, tous regroupés dans un ensemble de données appelé « pfSense.log ».

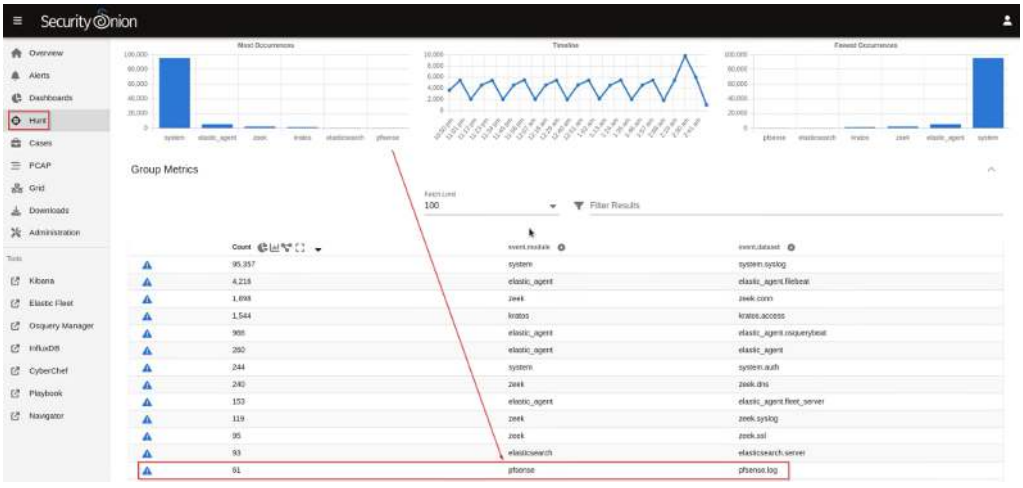


Illustration 40 : présence des journaux de pfSense dans l'interface « Hunt » de la SOC

Ceci prouve que l'ingestion des journaux du pfSense est fonctionnelle.

2. Vérification de détection d'intrusion en cas de scan réseau

Nous avons également effectué un scan de réseau pour tester la détection. Depuis un poste Windows sur le réseau j'ai utilisé le tool « Network scan » du logiciel MobaXterm :

Illustration 41 : interface de l'outil « Network scan » après un scan d'un segment du réseau EasyFormer

Nous avons ensuite constaté que le NIDPS Suricata inclus dans SO a bien remonté une alerte :

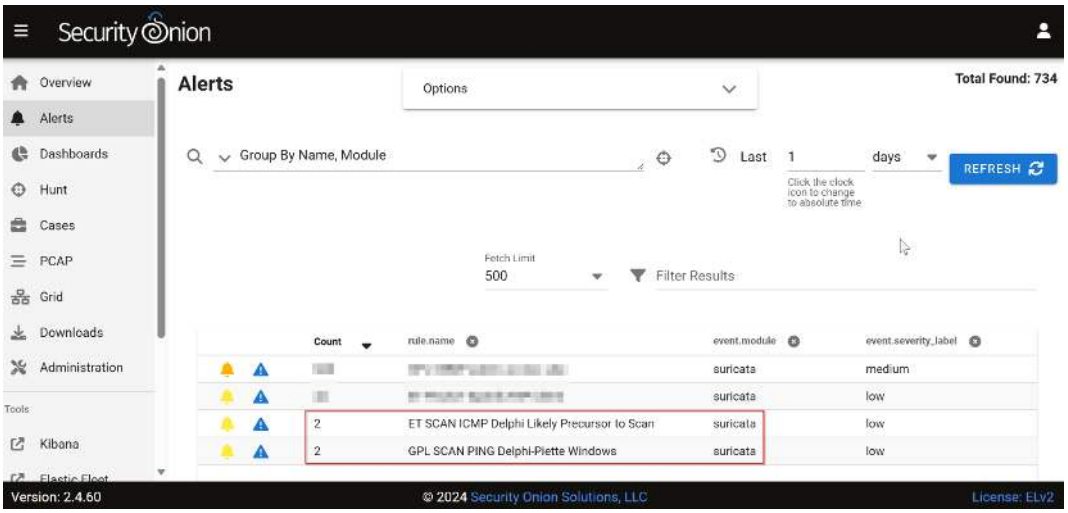
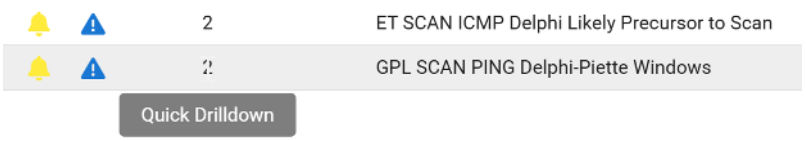


Illustration 42 : présence d'une alerte de Suricata générée suite au scan réseau

En cliquant sur le chiffre dans la colonne « Count » nous pouvons directement aller à l'action « Quick Drilldown » (recherche en profondeur rapide) :



Nous atterrissons sur une page où les événements ont été automatiquement filtrés avec la requête « *rule.name:"ET SCAN ICMP Delphi Likely Precursor to Scan"* ». Si nous cliquons sur la flèche à gauche de la ligne d'un de ces événements, le journal complet de l'événement s'affiche :

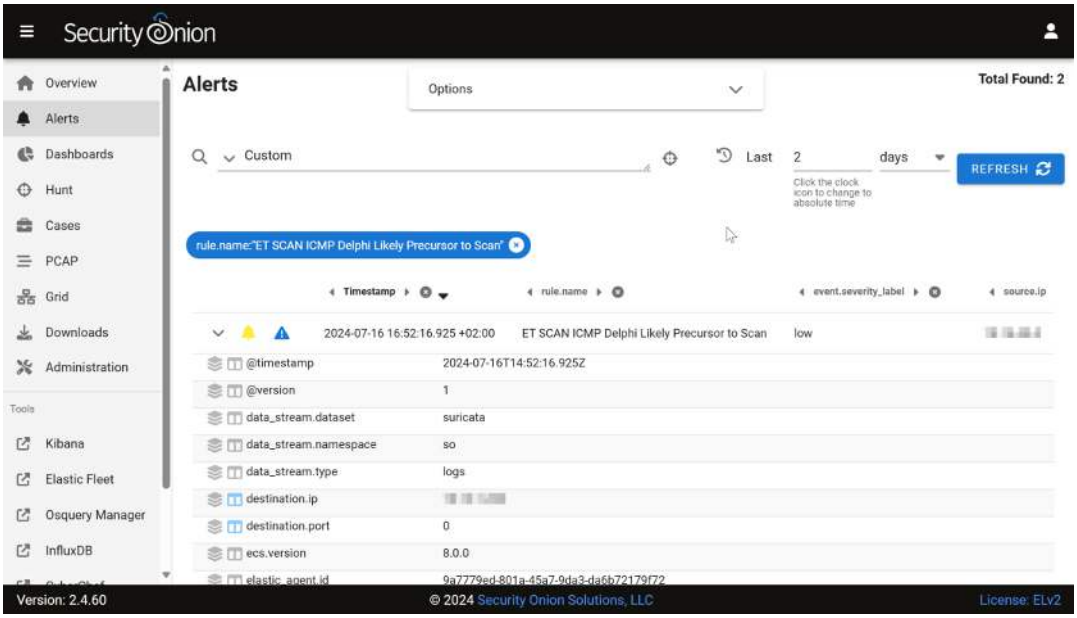


Illustration 43 : extrait du journal d'évènement lié au scan réseau

3. Vérification de la génération d'alerte en cas d'activation d'une règle Sigma

Nous avons tenté des connexions en HTTP, FTP et SSH au honeypot et celles-ci ont bien déclenché des alertes :

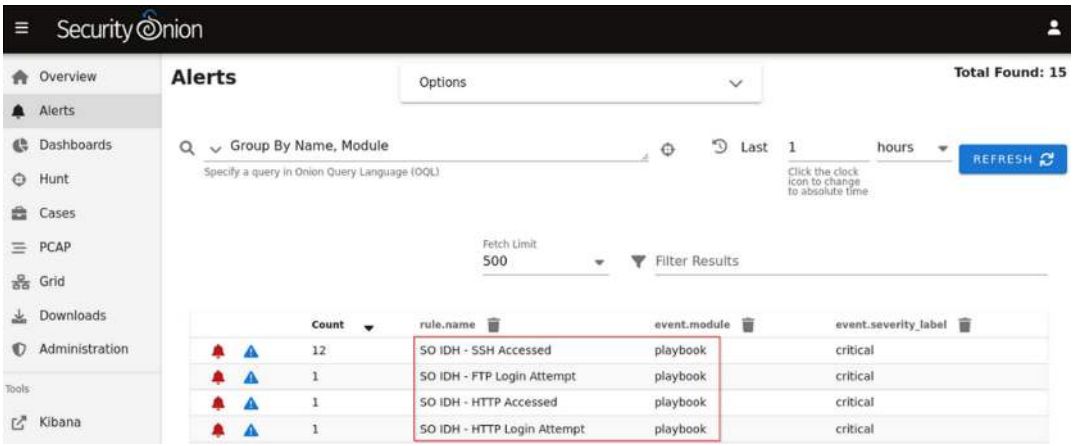


Illustration 44 : présence d'une alerte de type Playbook générée suite au scan réseau

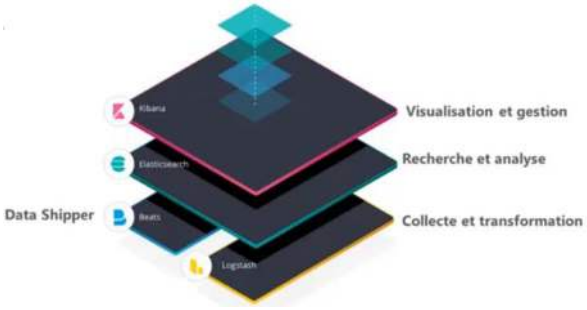
Les règles Sigma ont bien été appliquées et l'IDH a prouvé son efficacité.

4. Analyse d'un journal d'évènement

En utilisant les requêtes (= filtres d'affichage), un analyste de sécurité peut filtrer rapidement les événements de sécurité pertinents et identifier les tentatives d'attaque sur leurs systèmes.

a) Qu'est-ce qu'une requête OQL ?

Rappelons tout d'abord qu'Elasticsearch est le moteur de recherche et d'analyse de texte qui est utilisé dans Security Onion pour stocker, rechercher et analyser les données en temps réel.



Les **requêtes OQL** (pour *Onion Query Language*, « Langage de Requête Onion ») sont, dans Security Onion, **des expressions qui définissent les critères de recherche et les filtres à appliquer pour extraire des informations à partir des données stockées dans Elasticsearch**. Une requête OQL permet à un utilisateur d'interroger et d'explorer les données indexées dans Elasticsearch.

Elles permettent d'effectuer des recherches complexes, des agrégations, des suggestions et des opérations de mise en évidence, entre autres.

b) Focus sur une tentative de connexion en HTTP à l'IDH

Après mes tentatives de connexion à l'IDH OpenCanary, je peux vérifier les journaux d'OpenCanary (via les menus « Dashboards », « Hunt » ou « Kibana ») en utilisant la requête OQL « *event.module: opencanary* » ou « *event.dataset: idh* » par exemple :

source.ip	source.port	destination.ip	destination.port	log.id.uid	network.community_id	event.dataset
[redacted]	56720		80			idh
[redacted]	56720		80			idh
[redacted]	56704		80			idh
[redacted]	51613		80			idh
[redacted]	51419		21			idh
[redacted]	51421		21			idh
[redacted]	51392		22			idh
[redacted]	51392		22			idh
[redacted]	51392		22			idh
[redacted]	53868		80			idh

Rows per page: 10 1-10 of 34

Illustration 45 : interface de la SOC après l'application d'un filtre des évènements liés à l'IDH

Si je développe un événement relatif à ma tentative de connexion en HTTP à l'IDH avec le nom d'utilisateur « nicolas.bodaine » et le mot de passe « test » ❶, je constate que beaucoup d'informations intéressantes ont été loguées et sont remontée dans la SOC :

❺ : l'heure à laquelle l'évènement s'est produit

❾ : l'adresse IP source

❷ : l'adresse IP de destination

❸ : le port de destination

❹ : le nom de l'hôte sur lequel la tentative de connexion a eu lieu

❼ : avec quel nom d'utilisateur l'attaquant a essayé de se connecter

❻ : il y a même le mot de passe qu'il a utilisé

❽ : et le message de log structuré au format JSON

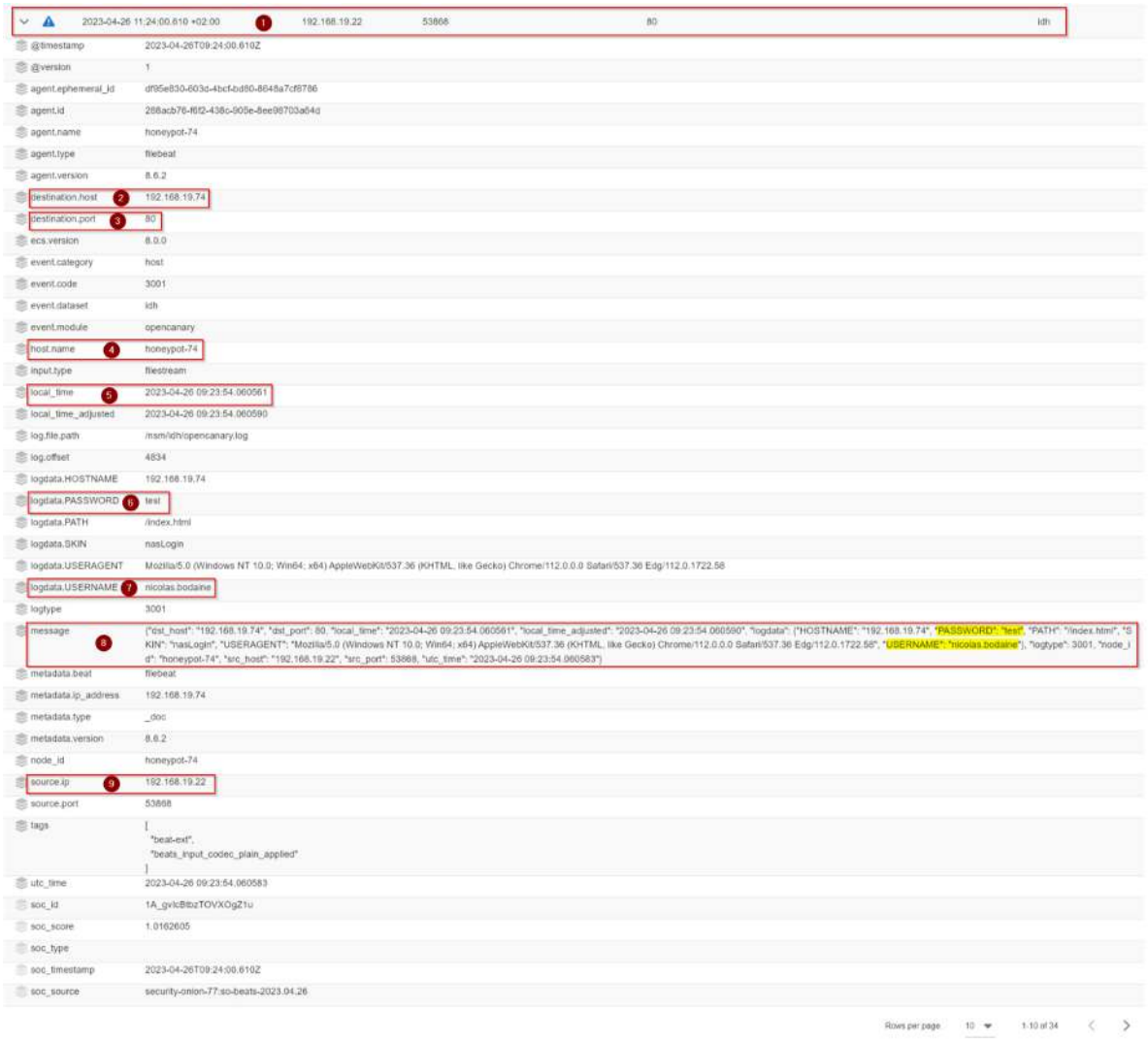


Illustration 46 : journal d'évènement complet lié à une tentative de connexion en HTTP à l'IDH

VII. PHASE DE FINALISATION

A. REDACTION DE LA DOCUMENTATION TECHNIQUE

Suite à la mise en production de la plateforme, j'ai rédigé un article dans notre Wiki interne pour documenter ce qui a été réalisé et transmettre à mes collègues des informations pertinentes sur la plateforme de sécurité.

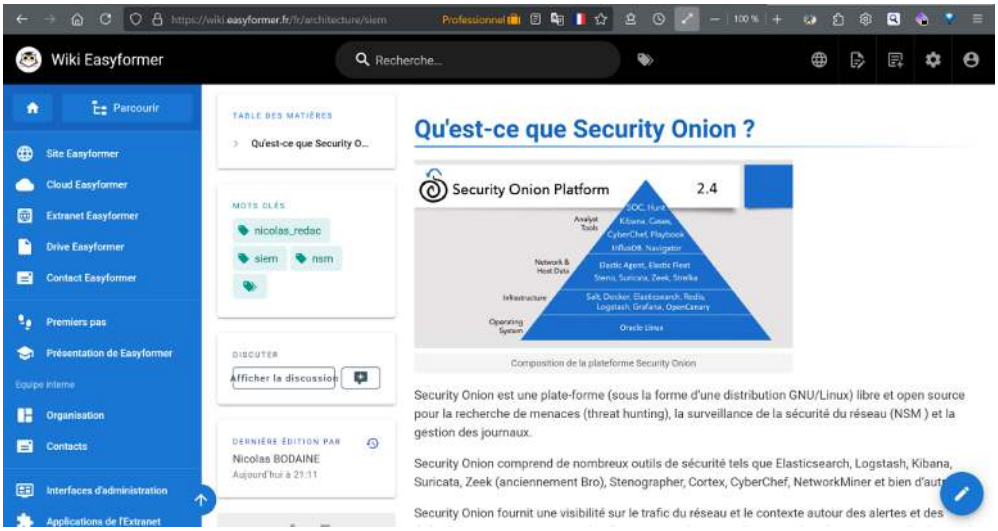


Illustration 47 : extrait de l'article sur Security Onion rédigé dans le wiki d'EasyFormer

B. FORMATION DU PERSONNEL

Après avoir terminé la mise en production et la rédaction de la documentation, j'ai prodigué à mes collègues une réunion de formation sur la Solution Security Onion :

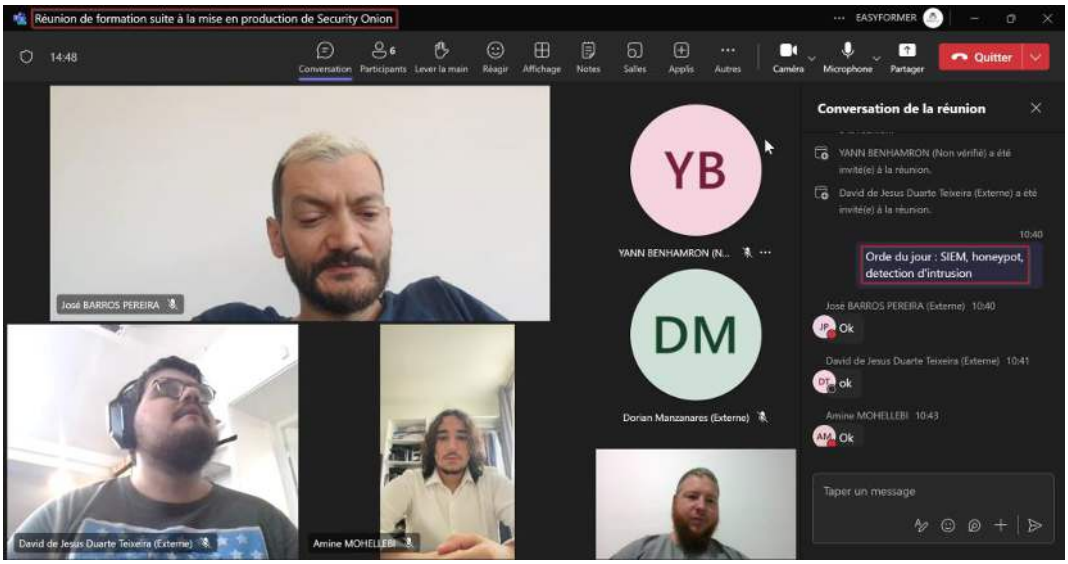


Illustration 48 : capture d'écran prise lors de la réunion de formation aux nouveaux outils déployés

C. RETOUR D'EXPERIENCE

OBJECTIFS

Le projet consistait à rendre l'environnement informatique plus sûr. Les livrables incluaient la mise en place d'une plateforme de surveillance de la sécurité du réseau de type SIEM et d'un *honeypot* intégrés dans le réseau et pleinement fonctionnels fournissant une capacité de détection d'intrusion, d'analyse et de reporting.

≠

REALITE

La plateforme SIEM et son *honeypot* ont été configurés et intégrés dans le réseau existant avec succès. Les principaux résultats sont que la sécurité du réseau a été améliorée en fournissant aux analystes d'EasyFormer divers outils de détection d'intrusion. Parmi les défis rencontrés, on peut citer la complexité de la solution Security Onion.

CE QUE NOUS AVONS APPRIS

CE QUI A FONCTIONNE	CE QUI N'A PAS FONCTIONNE
La plateforme Security Onion a été déployée et permet d'analyser les différentes données sur les éléments du réseau. Les systèmes de détection d'intrusion (Suricata par ex.) réagissent aux scans réseau. Les ingestions de journaux des endpoints via les Agents Elastic sont fonctionnelles. Le honeypot OpenCanary est fonctionnel et fait remonter des alertes dans la SOC.	La complexité de la solution Security Onion a entraîné des erreurs dans le déploiement de la plateforme. Le temps d'apprentissage a été sous-évalué et a entraîné des retards. Notamment à cause des changements majeurs de la version 2.4, des bugs non corrigés et du manque de ressources sur le sujet.

ANALYSE DES ECARTS

Les écarts entre les résultats escomptés et la réalité sont dus à une sous-estimation des ressources, à des défis techniques imprévus ayant entrainé des retards dans la livraison du projet.

AMELIORATION

Pour des projets futurs, nous pourrions bénéficier d'une évaluation plus détaillée des compétences requises pour chaque tâche, permettant une allocation plus efficace des ressources. De plus, la mise en place d'un processus formel de revue technique avant le lancement du projet pourrait aider à identifier et à résoudre les problèmes potentiels plus tôt. Il serait également utile d'accorder plus de temps à la phase de test pour s'assurer que toutes les fonctionnalités fonctionnent comme prévu.

EXPERIMENTER

Mettre en place un processus de revue technique avant le début du projet. Cela impliquerait que toutes les décisions techniques importantes soient examinées par des spécialistes pour identifier les problèmes potentiels avant le lancement du projet.

D. AXES D'AMELIORATION

1. Configurer des notifications aux administrateurs en cas d'alerte

Il est possible, avec ElastAlert[32], de configurer un système d'alerte en cas d'activité suspecte pour notifier les administrateurs via e-mail, Telegram, Teams, Discord, ou d'autres canaux de communication.

2. Utiliser l'automatisation pour déployer les agents Elastic

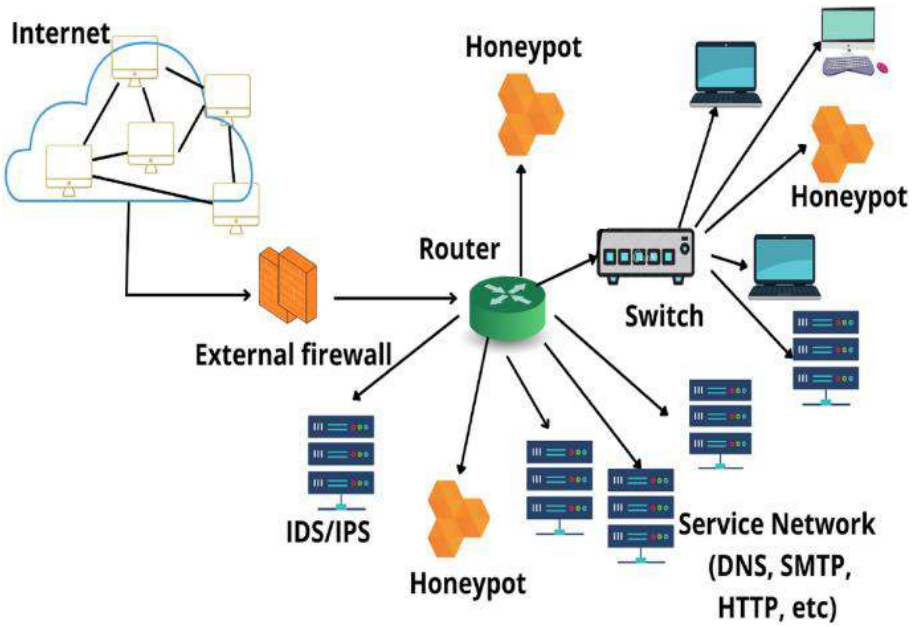
Il serait pertinent d'automatiser le déploiement des Agents Elastic sur les endpoints via Ansible par exemple.

3. Mettre en place des Canary Tokens pour renforcer la détection d'intrusion

Le **Canary Token**[33] est **une méthode de détection de menaces qui peut alerter les administrateurs lorsqu'un certain fichier, email, ou document est accédé**. Cela fonctionne en générant un *token* unique qui, lorsqu'il est utilisé ou consulté, envoie un signal d'alerte.

4. Créer un réseau de honeypots distribués

Il pourrait être pertinent d'ajouter des honeypots répartis à travers les différents segments du réseau, permettant de détecter et d'analyser une plus large gamme d'attaques.



[32] Pages de documentation ElastAlert : https://docs.securityonion.net/en/2.4/elastalert.html#elastalert et https://elastalert.readthedocs.io/en/latest/
[33] Pour approfondir le sujet : https://www.globalsecuritymag.fr/Comment-utiliser-les-Canary-Tokens,20200821,102000.html

VIII. CONCLUSION

A. EN FRANÇAIS

Ce projet a marqué une étape clé dans le renforcement de la sécurité du réseau d'EasyFormer. L'intégration de la solution NSM/SIEM Security Onion, l'installation du honeypot OpenCanary pour la détection d'intrusion, ainsi que la configuration de l'ingestion des journaux du pare-feu pfSense et des différents endpoints avec des agents Elastic, ont permis d'améliorer de manière considérable la capacité de l'entreprise à identifier, analyser et réagir aux menaces de sécurité.

Ce projet m'a également permis de découvrir de nouvelles technologies et d'apprendre énormément sur les pratiques de sécurité réseau.

Cette expérience m'a conforté dans mon choix de carrière et m'a motivé à poursuivre dans cette voie. Chaque défi relevé et chaque problème résolu ont renforcé mon enthousiasme pour ce domaine. J'ai découvert que j'apprécie particulièrement l'aspect technique et stratégique de l'installation d'infrastructures.

La réussite de ce projet d'infrastructure informatique m'a apporté une immense satisfaction personnelle. Voir le système fonctionner de manière optimale et répondre aux besoins de l'entreprise a été extrêmement gratifiant. Les retours positifs des utilisateurs et l'amélioration de l'efficacité opérationnelle ont renforcé mon sentiment d'accomplissement.

B. IN ENGLISH

This project marked a key step in strengthening EasyFormer's network security. The integration of the NSM/SIEM Security Onion solution, the installation of the OpenCanary honeypot for intrusion detection, as well as the configuration of log ingestion for the pfSense firewall and the various endpoints with Elastic agents, considerably improved the company's ability to identify, analyze and react to security threats.

The project also enabled me to discover new technologies and learn a great deal about network security practices.

The experience reinforced my career choice and motivated me to continue in this direction. Every challenge I faced and every problem I solved reinforced my enthusiasm for this field. I discovered that I particularly enjoy the technical and strategic aspects of infrastructure installation.

The success of this IT infrastructure project gave me immense personal satisfaction. It was extremely gratifying to see the system running optimally and meeting the company's needs. The positive feedback from users and the improved operational efficiency reinforced my sense of achievement.

IX. ANNEXES : PROCEDURES TECHNIQUES

J'ai présenté ci-dessous mes réalisations techniques en utilisant des captures d'écran. Par souci de sécurité **les adresses IP réelles ont été floutées ou masquées**.

A. LES INSTALLATIONS

1. Installation de la plateforme Security Onion

Pour installer Security Onion nous avons utilisé la plateforme de virtualisation Proxmox VE du Réseau EasyFormer. Il s'agit de quatre serveurs DELL mis en cluster pour un total de ressources disponibles de 64 vCPU, 440 Go de RAM et 95 To de stockage.

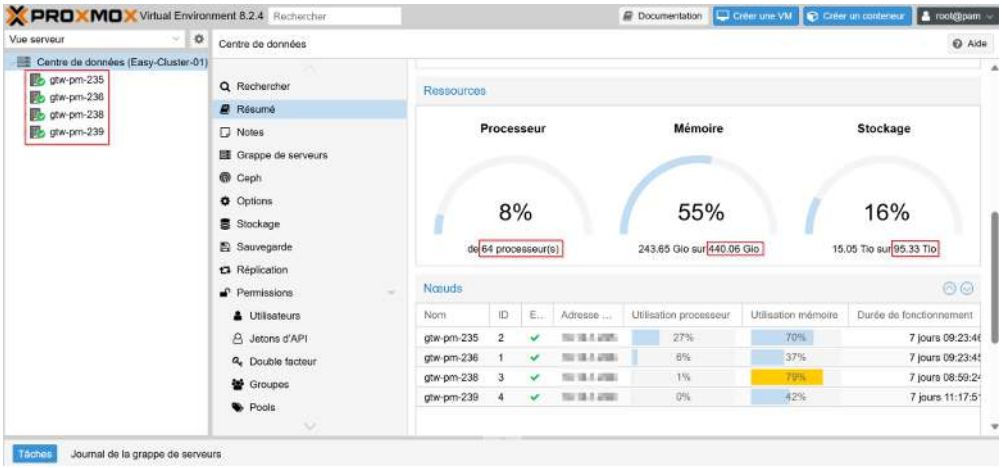


Illustration 49 : spécifications du cluster Proxmox

L'installation de la plateforme Security Onion n'a pu être correctement effectuée qu'après plusieurs tentatives à cause de bugs et mauvaises configurations. Ci-dessous un exemple des nombreux messages d'erreur rencontrés :

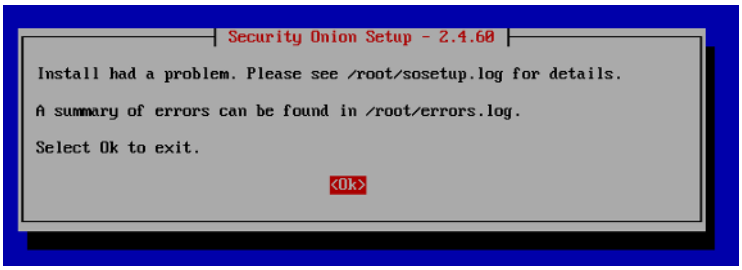


Illustration 50 : message d'erreur obtenu lors de l'installation de Security Onion

Sur la capture de l'interface web du cluster Proxmox ci-dessous, vous pouvez constater la présence de trois instances de Security Onion et de deux honeypot OpenCanary ce qui prouve nos nombreux tests et essais :

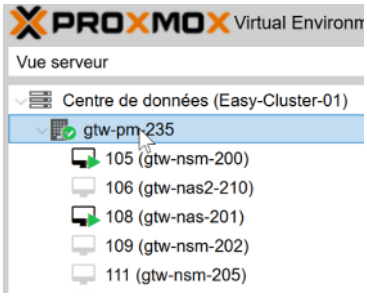


Illustration 51 : instances multiples de SO et OpenCanary dans Proxmox

Je passerai rapidement sur la procédure d'installation, qui bien que comportant de nombreuses et longues étapes de configuration, reste assez classique :

a) Téléchargement de l'ISO de Security Onion

Nous avons tout d'abord téléchargé l'ISO de la dernière version en date de Security Onion depuis le site officiel. A savoir que la version 2.4 de Security Onion a apporté des changements radicaux comparée à la version 2.3 précédente : par exemple ce n'est plus le même OS sous-jacent (Oracle Linux contre CentOS précédemment), des outils ont été supprimés car considérés en double usage (Wazuh notamment), et d'autres changements majeurs.

Fait étonnant : les changements opérés dans cette version sont tellement importants que l'équipe de Security Onion recommande officiellement de réinstaller une instance depuis l'ISO de la version 2.4 plutôt que de procéder à une mise à jour depuis la version 2.3 !

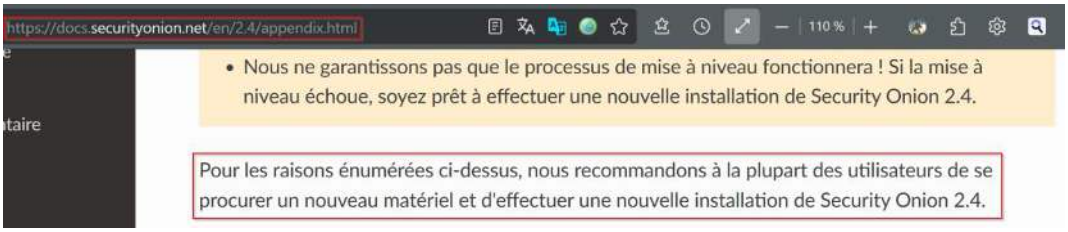


Illustration 52 : recommandation de procéder à une nouvelle installation pour la v2.4

b) Création de la machine virtuelle dans Proxmox

Nous avons créé et stocké la VM dans le stockage « local-ZFS » destiné à cet usage.

Ensuite nous avons attribué des ressources à la VM. Selon notre cas d'utilisation spécifique et le volume du trafic réseau à analyser nous avons décidé d'attribuer 8 cœurs de processeur, 20 Go de RAM et 200 Go de stockage (un minimum de 4 Go de RAM, 2 CPU et 200 Go de stockage est demandé).

Une configuration particulière devait être sélectionnée au niveau du type de processeur. Proxmox utilise par défaut un CPU de VM qui peut ne pas inclure toutes les fonctionnalités du CPU de l'hôte, donc nous avons sélectionné « host » pour avoir à disposition toutes ces fonctionnalités.

c) Assistant d'installation de Security Onion

Nous avons inséré l'ISO dans le lecteur virtuel de la VM et démarré cette dernière. L'installation s'est effectuée à partir de cette interface graphique minimale :

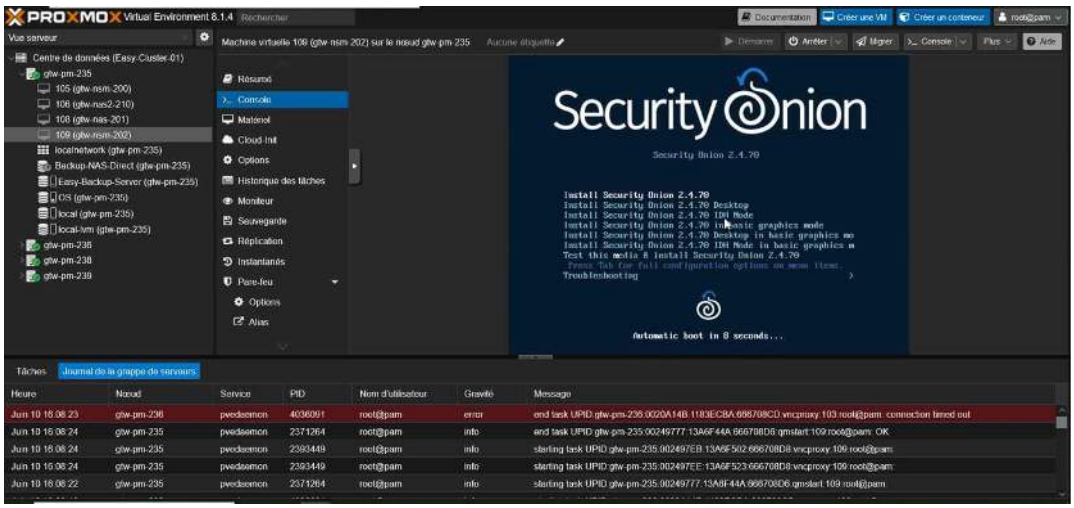


Illustration 53 : interface graphique d'installation de SO

Lors de cet assistant, nous avons pu configurer les interfaces réseau d'administration et de surveillance.

Cette configuration m'a permis de m'assurer que Security Onion était correctement intégré dans l'infrastructure réseau et qu'il fonctionnerait de manière optimale pour détecter et analyser les menaces.

2. Installation du honeypot OpenCanary

Nous avons décidé de nommer le honeypot avec un nom qui respecte la convention de nommage du Réseau EasyFormer (« gtw-nas-201 ») et qui est censé faire croire à un éventuel attaquant qu'il a affaire à un serveur très intéressant : un NAS…

Pour l'installation du honeypot (ou nœud IDH pour « Intrusion Detection Honeypot ») nous nous sommes aidés de la documentation[34] officielle.

a) Assistant d'installation du nœud IDH

L'ISO de Security Onion possède un assistant d'installation pour ajouter un nœud IDH à notre plateforme Security Onion.

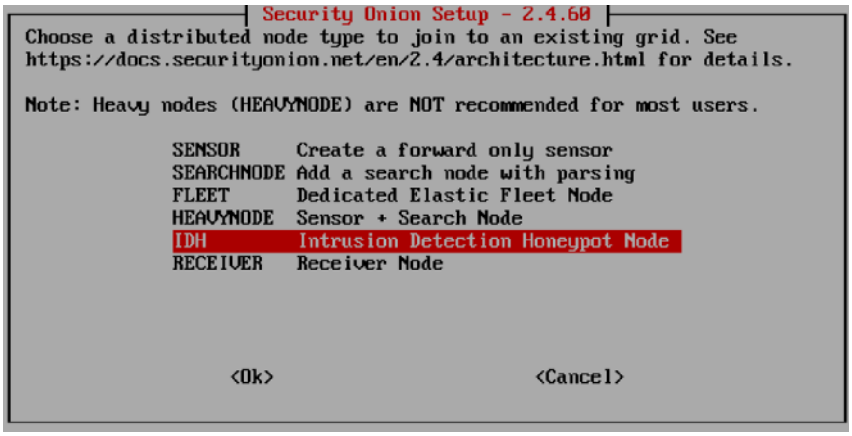


Illustration 54 : étape du choix du nœud IDH lors de l'assistant d'installation

Parmi les problèmes rencontrés dans ce projet, il y a le fait que même après plusieurs ré-installations, le nœud IDH ne fonctionnait pas. La raison était tout simplement un bug qui a été corrigé à la mise à jour suivante :

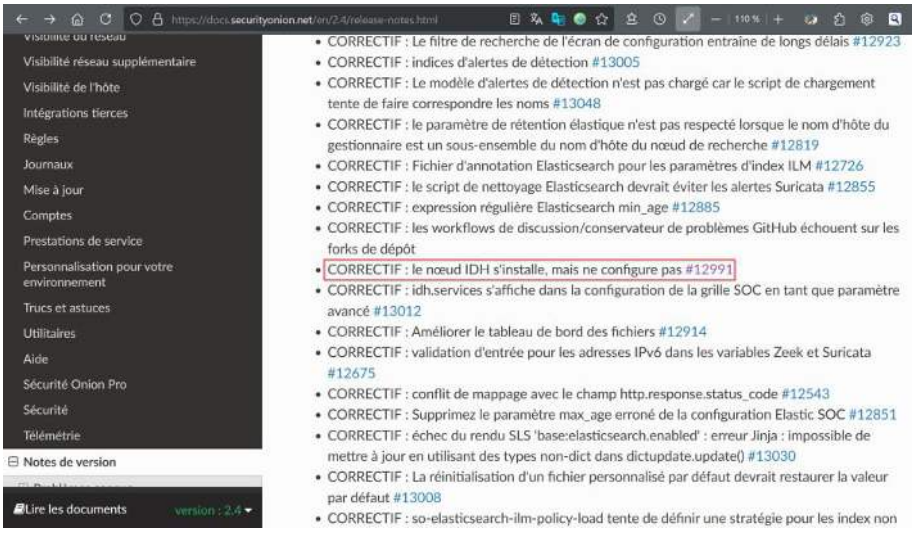


Illustration 55 : notes de version mentionnant un bug avec l'IDH désormais corrigé

[34] Section de la documentation de Security Onion traitant du honeypot : https://docs.securityonion.net/en/2.4/idh.html

L'assistant nous a permis finalement d'installer sur une nouvelle VM dans notre hyperviseur Proxmox un système sous Oracle Linux hébergeant un service OpenCanary tournant en réalité dans un container Docker.

A. LES CONFIGURATIONS

1. Autorisation de la communication entre le nœud IDH et le manager

Après avoir installé notre nœud IDH, il a fallu autoriser la connexion entre le nœud IDH et le « manager », c'est-à-dire le serveur hébergeant Security Onion. Cela consiste à mettre en place des règles de *firewalling*. Pour cela nous avons suivi la documentation qui propose de le faire en ligne de commande avec :

```
sudo so-firewall-minion --role=IDH  --IP=x.x.x.x
```

Ou via l'interface graphique :

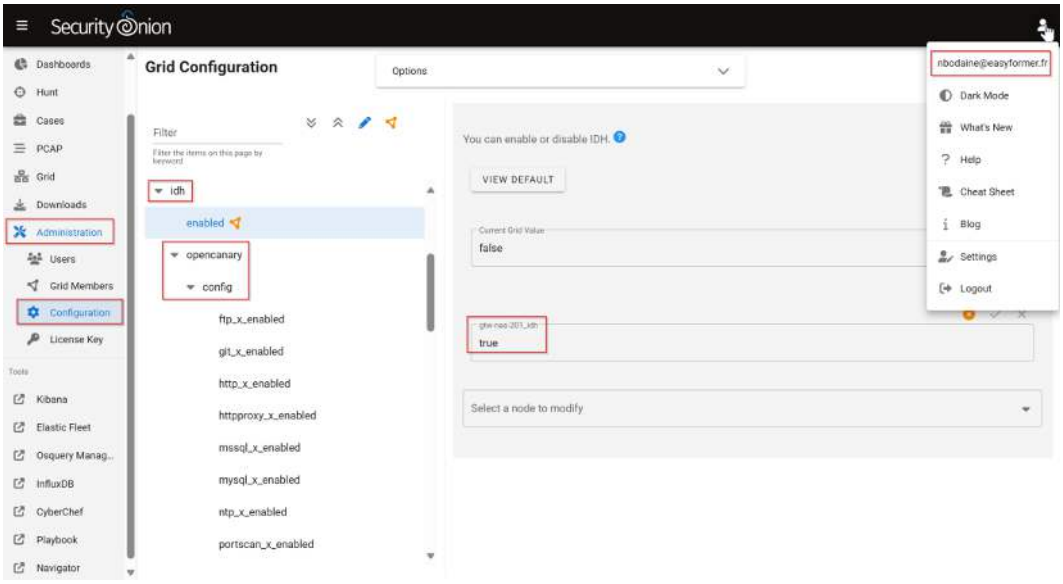


Illustration 56 : menu de configuration du firewall local dans la SOC

Après avoir effectué cette configuration, nous avons bien retrouvé notre nœud IDH dans la section « Grid » de l'interface web de Security Onion :

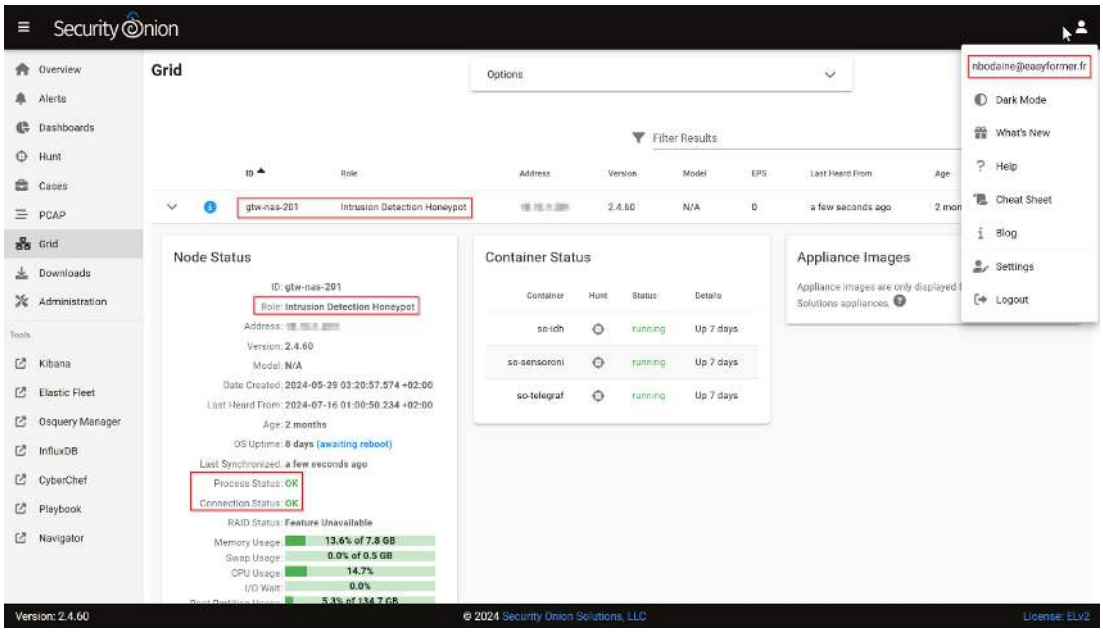


Illustration 57 : statut de connexion « OK » pour le nœud IDH

Son statut de connexion « OK » signifie qu'il arrive bien à communiquer avec le *manager*.

2. Configuration des services leurres d'OpenCanary

Nous avons ensuite configuré les services leurres qui tourneront sur le nœud IDH. Etant donné que dans le Réseau EasyFormer des NAS de la marque Synology sont présents, il nous est paru pertinent de simuler un NAS de type Synology à la manière d'un « skin ». Voici la page web de connexion au véritable NAS Synology du Réseau EasyFormer :

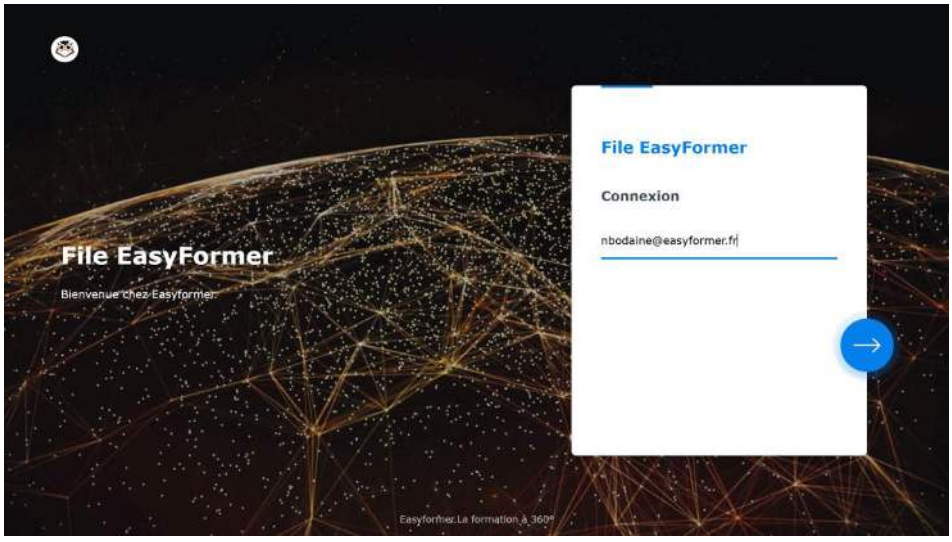


Illustration 58 : page de connexion au véritable NAS Synology d'EasyFormer

Pour la configuration des services leurres d'OpenCanary il suffit de modifier le fichier de configuration « /etc/opencanary/opencanary.conf ». Il est possible de simuler de nombreux services

dont SSH, Telnet, SMB et bien d'autres. Pour cela, nous nous sommes aidés de la documentation[35] officielle d'OpenCanary.

Voici maintenant la page web de connexion du faux NAS Synology simulé par OpenCanary :

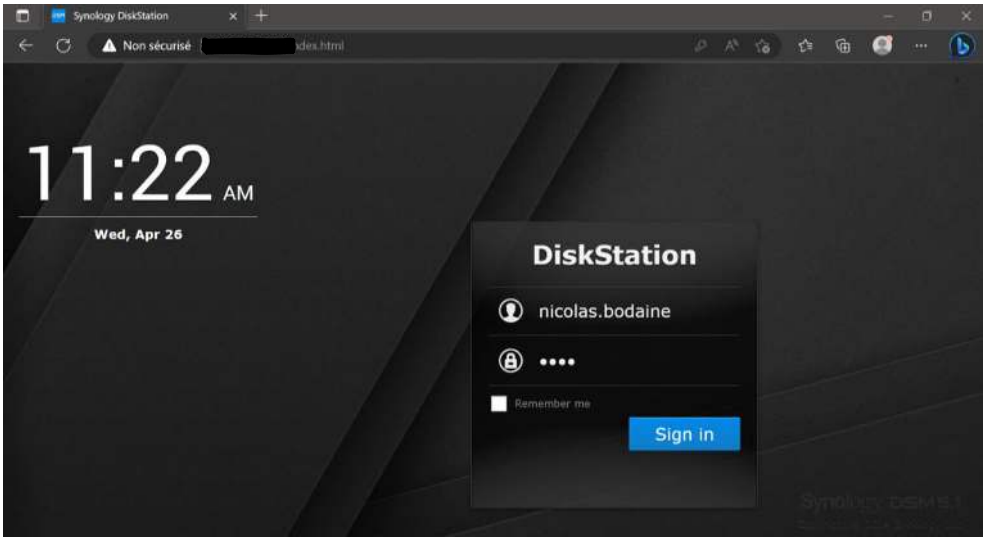


Illustration 59 : page de connexion au service Synology simulé par OpenCanary

Nous pouvons remarquer la présence de « Synology DiskStation » dans l'onglet de navigateur et « Synology DSM » en bas à droite de la page de connexion.

Si je tente une connexion, celle-ci n'aboutit évidemment pas et le message suivant s'affiche :

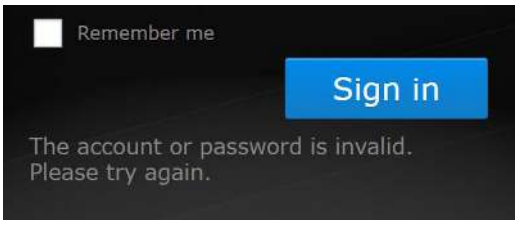


Illustration 60 : message mentionnant une tentative de connexion au honeypot échouée

Rien n'indique que je suis en train d'essayer de me connecter à un honeypot. L'illusion est parfaite !

[35] Page de documentation d'OpenCanary :
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration

3. Création des utilisateurs de Security Onion

Nous avons créé des utilisateurs supplémentaires dans Security Onion tout en nous assurant de créer des comptes nominatifs afin de pouvoir attribuer chaque action effectuée à un individu spécifique si des besoins d'investigation se faisaient ressentir.

Il est possible d'utiliser la ligne de commande ou l'interface web d'administration pour cela :

```
[                                    ~]$ sudo so-user-add nbodaine@easyformer.fr
Enter new password:
Syncing users and roles between SOC and Elastic...
Elastic state will be re-applied to affected minions. This may take several minutes...
Successfully added new user to SOC
```

Illustration 61 : ajout d'un utilisateur en ligne de commande

Vous pouvez constater ci-dessous l'apparition de mon nom d'utilisateur dans l'interface web. Nous avons ensuite attribué à chaque utilisateur les permissions appropriées depuis ce même menu :

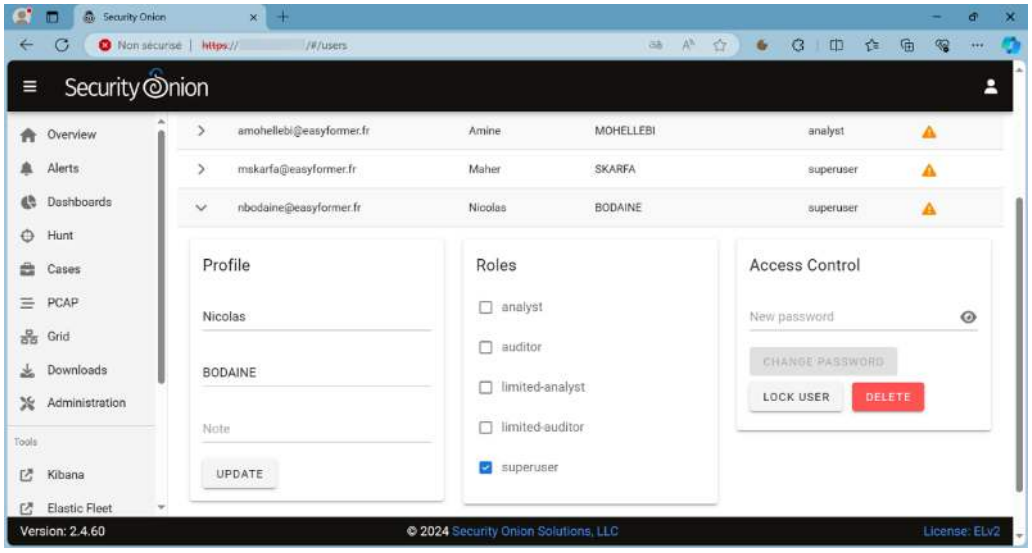


Illustration 62 : interface web d'administration des utilisateurs

Par la suite je me suis connecté avec mon utilisateur pour continuer la configuration de SO afin que ce soit celui-ci qui apparaisse dans les logs plutôt qu'un utilisateur « admin » générique et impersonnel.

4. Importation de règles Sigma de détection d'intrusion

Les règles Sigma sont des modèles de détection de journaux conçus pour être indépendants des plateformes, permettant de **décrire des cas d'utilisation de détection de menaces de manière agnostique par rapport à la technologie**.

Autrement dit : les règles Sigma servent à **standardiser les détections quel que soit l'outil SIEM utilisé**. L'objectif principal est de fournir une forme structurée dans laquelle les chercheurs ou les

analystes peuvent décrire leurs méthodes de détection une fois développées et les rendre partageables avec d'autres.

Ces règles permettent aux équipes de sécurité de transformer les descriptions en requêtes spécifiques à la plateforme de journalisation utilisée, facilitant ainsi la détection des activités suspectes.

De nombreuses règles Sigma sont disponibles en open source sur Internet. Nous pouvons par exemple retrouver sur le dépôt Github de SigmaHQ[36] des jeux de règles spécialement conçues pour détecter des tentatives de connexion à un honeypot de détection d'intrusion OpenCanary :

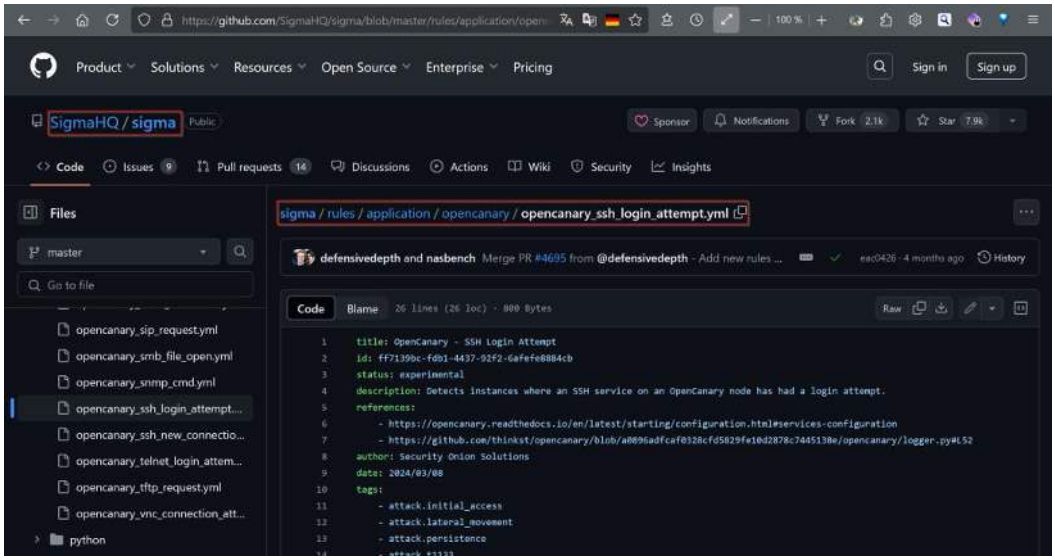


Illustration 63 : repository Github de SigmaHQ contenant de nombreuses règles Sigma

Nous avons donc intégré des règles Sigma dans notre plateforme Security Onion, qui visent à identifier les tentatives de connexion sur notre nœud OpenCanary qui utilisent des protocoles surveillés (par exemple des connexions SSH, des requêtes HTTP POST, etc.).

[36] Lien vers le *repository* : https://github.com/SigmaHQ/sigma/tree/master/rules

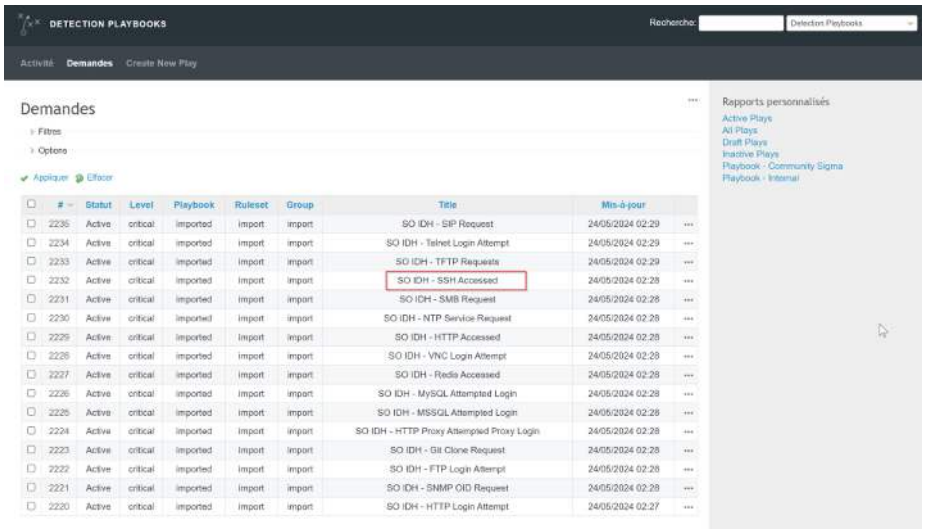


Illustration 64 : liste des règles Sigma dans Security Onion pour la surveillance de l'IDH OpenCanary

En cliquant sur une règle il est possible d'afficher un certain nombre d'informations la concernant notamment son auteur, des URL de référence et son code écrit en langage Yaml :

```yaml
title: SO IDH - SSH Accessed
id: b7a09f0a-88ca-4fe0-bc8a-92106133e231
status: experimental
description: Detects when the SSH service on a SO IDH node has had a new connection
  (logtype 4000) or login attempt (logtype 4002).
author: Security Onion Solutions
license: MIT
references:
- https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
- https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
logsource:
  product: opencanary
detection:
  selection:
    logtype:
    - 4000
    - 4001
    - 4002
  custom_filter:
    source.ip:
    - x.x.x.x
  condition: selection
falsepositives:
- None
fields:
- source.ip
level: critical
```

Illustration 65 : code Yaml d'une règle Sigma de détection de connexion SSH sur un nœud IDH OpenCanary

C'est ainsi que les règles Sigma visibles dans l'interface « Playbook » recherchent certains journaux émis par OpenCanary, ce qui permet de détecter les tentatives d'accès non autorisées, qu'elles proviennent d'une interface web manuelle ou d'outils automatisés.

En cas de présence d'un log surveillé, cela génère une alerte qui peut être consultée dans l'interface « Alertes ».

5. Déploiement des agents Elastic pour la collecte des journaux des points de terminaison

Les **Agents Elastic** sont **des composants légers installés sur des machines pour collecter et envoyer divers types de données à Elasticsearch ou Logstash**.

Nous avons donc configuré la collecte des journaux à partir des points de terminaison du réseau à l'aide des agents Elastic. Cela peut se faire sur des systèmes Linux, Windows et macOS mais aussi sur certains pare-feu FreeBSD comme pfSense et OPNsense.

Au préalable il faut configurer le pare-feu de la plateforme Security Onion pour qu'elle accepte les connexions, il y a pour cela un lien de raccourci rapide cliquable dans la section « Administration » :

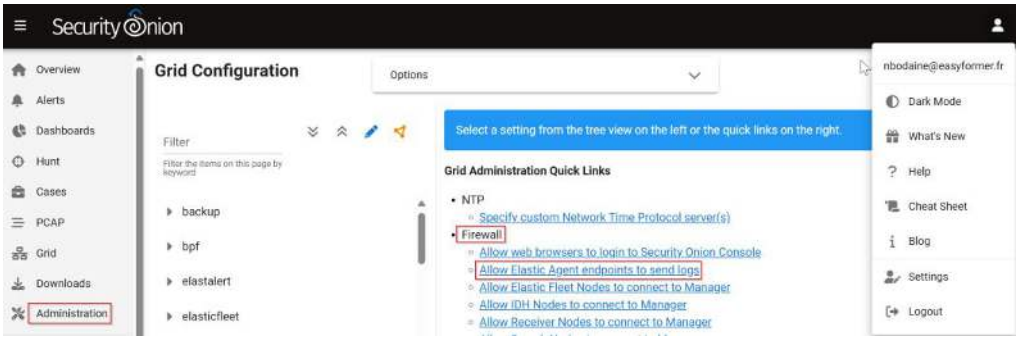


Illustration 66 : lien de raccourci vers la page de configuration des règles de firewall pour les agents Elastic

Il suffit ensuite de spécifier les adresses IP autorisées à communiquer avec le *manager* SO :

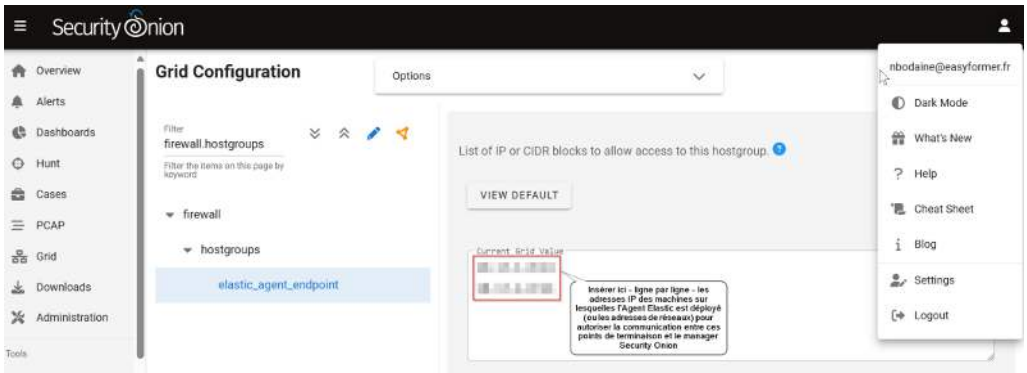


Illustration 67 : page de configuration des règles de firewall pour les agents Elastic

Nous avons ensuite téléchargé les agents Elastic depuis la section « Downloads » de la console Security Onion (SOC). Ces agents sont préconfigurés et spécifiques à notre installation de SO. Pour qu'ils fonctionnent le nom d'hôte du serveur SO doit pouvoir être résolu. Nous avons donc configuré notre DNS afin que SO soit joignable par son nom d'hôte.

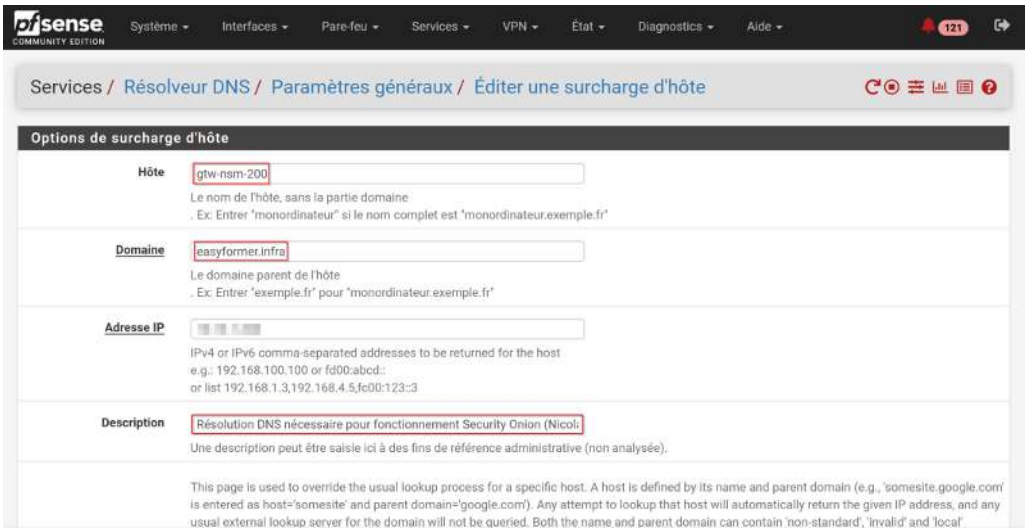


Illustration 68 : page de configuration du résolveur DNS sur pfSense

Les agents communiquent avec le *manager* (= le serveur SO) sur les ports TCP 8220, 8443 et 5055. Il a donc fallu autoriser également ces communications via notre firewall pfSense :

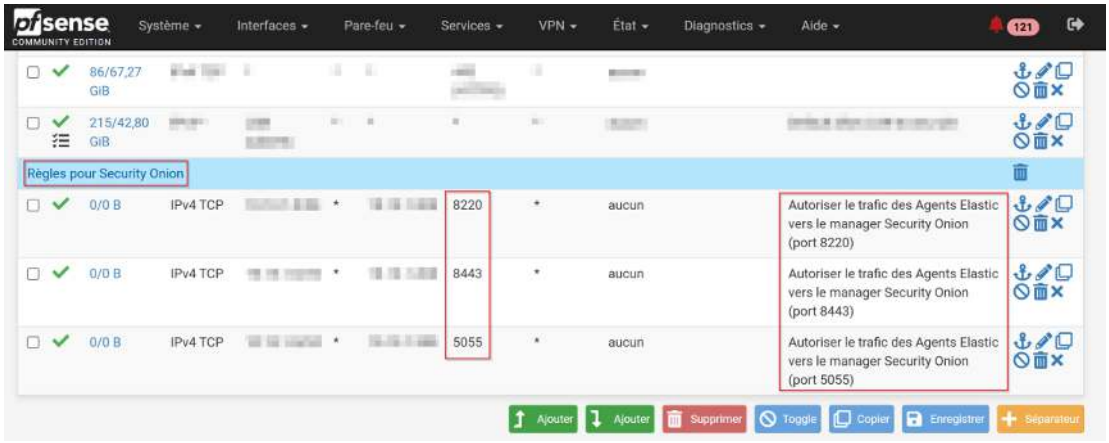


Illustration 69 : configuration des règles de firewall sur pfSense pour les agents Elastic

a) Ingestion des journaux d'un serveur Windows

Ensuite, il a fallu installer les agents sur les points de terminaison. Pour un système Windows c'est une méthode classique avec un fichier .exe à exécuter en tant qu'administrateur et qui lance un script d'installation :

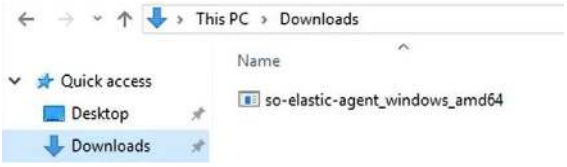


Illustration 70 : exécutable de l'agent Elastic pour les systèmes Windows

Ensuite il est possible de configurer les politiques des agents en lançant Elastic Fleet depuis la SOC :

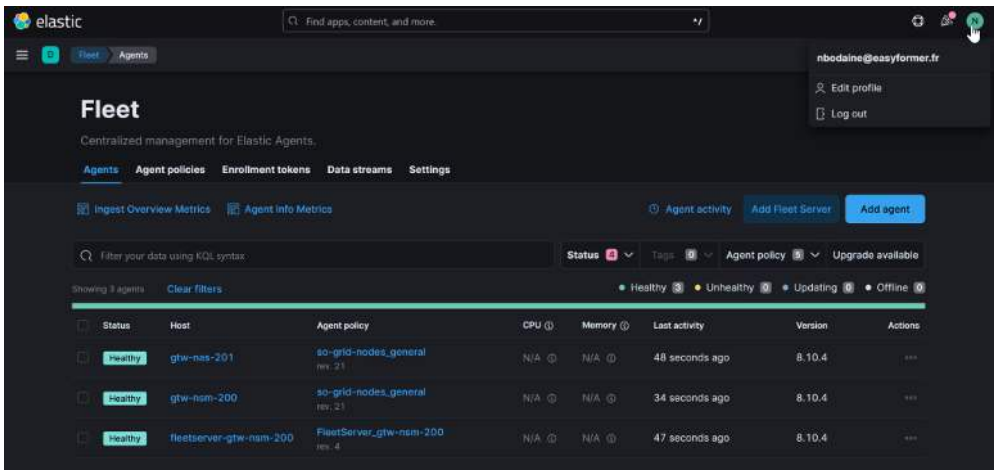


Illustration 71 : interface web d'Elastic Fleet

Elastic Fleet est **une interface web qui contrôle la configuration des agents Elastic déployés dans notre environnement**.

Chaque Agent Elastic se voit attribuer une politique d'agent. Ces « *Agent policies* » sont essentiellement **des listes d'intégrations ou de directives indiquant les journaux à ingérer et ce qu'il faut en faire**.

Après avoir cliqué sur « Agent policies », nous avons pu, par exemple, consulter et modifier la politique de journalisation nommée « endpoints-initial » qui est attribuée à tous les points de terminaison comme, par exemple, un serveur Windows ou un ordinateur portable macOS.

Cette politique est composée de plusieurs types d'intégrations. Je vais par exemple vous parler de l'intégration « elastic-defend-endpoints » :

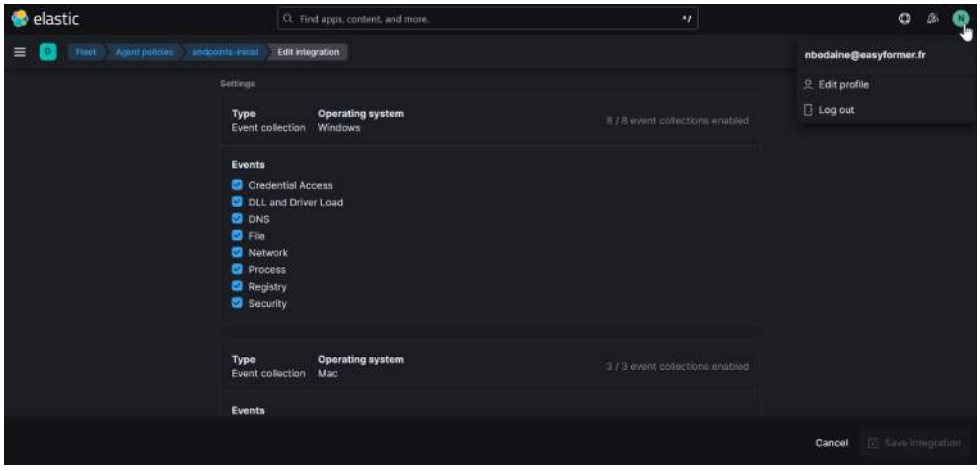


Illustration 72 : page de configuration de l'intégration « elastic-defend-endpoints »

C'est une configuration qui permet que l'agent Elastic pour Windows récolte automatiquement les journaux d'évènement du réseau, des processus système, du DNS, du registre, les informations d'identification, etc. L'agent peut aussi faire d'autres choses avec un abonnement Elastic Platinum comme la protection contre les ransomware par exemple.

Avec l'intégration « osquery-endpoint », il est également possible d'effectuer des requêtes Osquery (de style base de données) en direct sur les agents Elastic pour savoir par exemple quelles machines de notre environnement ont un jeu de clé de registre particulier ou si elles ont téléchargé un fichier qui correspond à une valeur de hashage particulière.

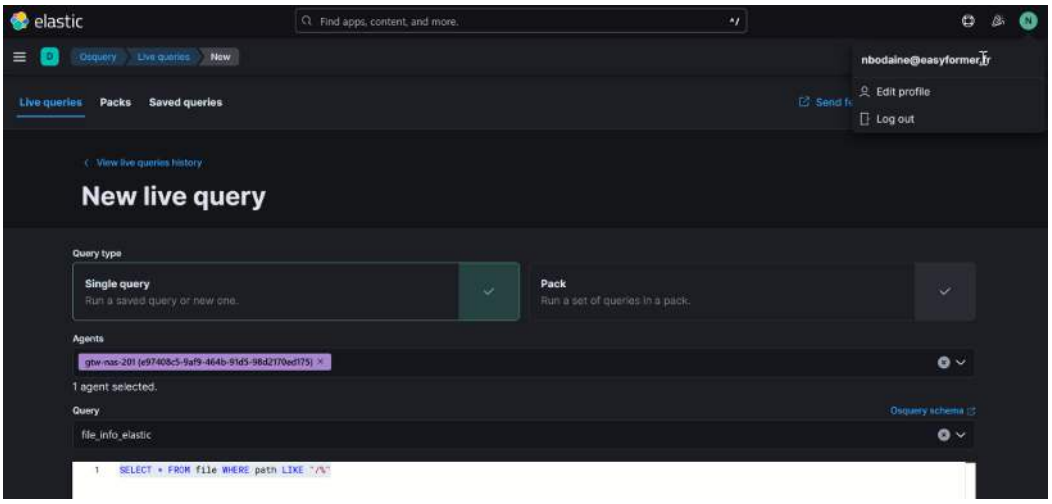


Illustration 73 : page web pour lancer des requêtes Osquery sur les agents Elastic

Il est également possible de dupliquer une politique pour la modifier et l'appliquer à des machines particulières.

b) Ingestion des journaux du pare-feu pfSense

Nous avons également utilisé une intégration Elastic servant à analyser les journaux de notre pare-feu pfSense, incluant les journaux DHCP, OpenVPN, etc.

La première chose à faire est d'activer l'intégration Elastic pour pfSense afin que l'agent installé sur notre serveur Security Onion puisse écouter le trafic entrant de notre pare-feu pfSense.

Ajouter l'intégration pfSense à la politique « so-grid-nodes-general » signifie que les agents Elastic fonctionnant sur notre nœud Security Onion seront en mesure d'accepter le trafic envoyé via Syslog depuis un pare-feu pfSense. Pour cela, nous avons cliqué sur cette politique, puis sur « Add Integration » :

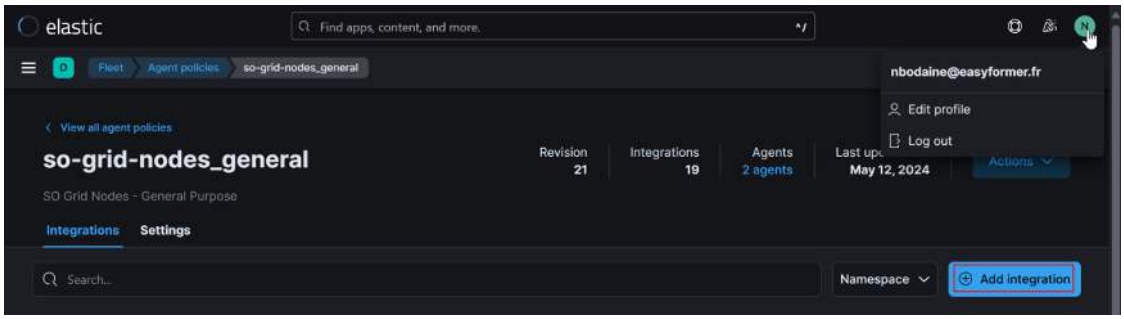


Illustration 74 : page de configuration de la politique « so-grid-nodes-general »

Nous avons cherché « pfsense » dans la barre de recherche pour trouver l'intégration pfSense, puis nous avons cliqué dessus pour continuer :

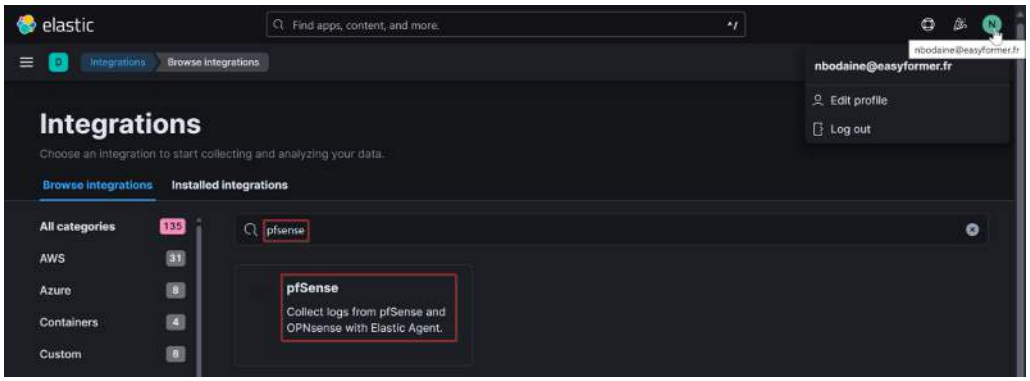


Illustration 75 : page de choix de l'intégration pfSense

Une page d'information s'affiche. Nous avons cliqué sur « Add pfSense » :

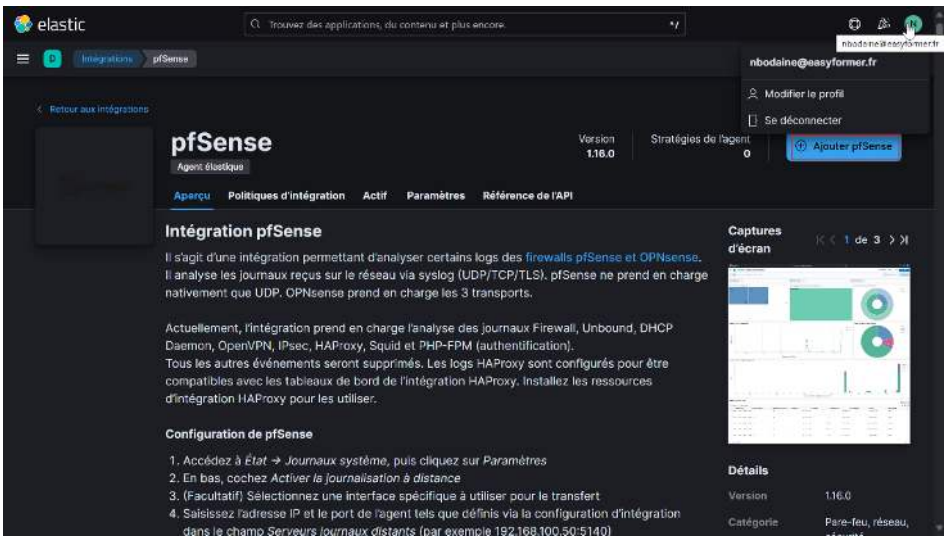


Illustration 76 : page d'information de l'intégration pfSense

Ensuite nous avons spécifié que notre nœud SO écoutera le port UDP 9001 sur toutes ses interfaces :

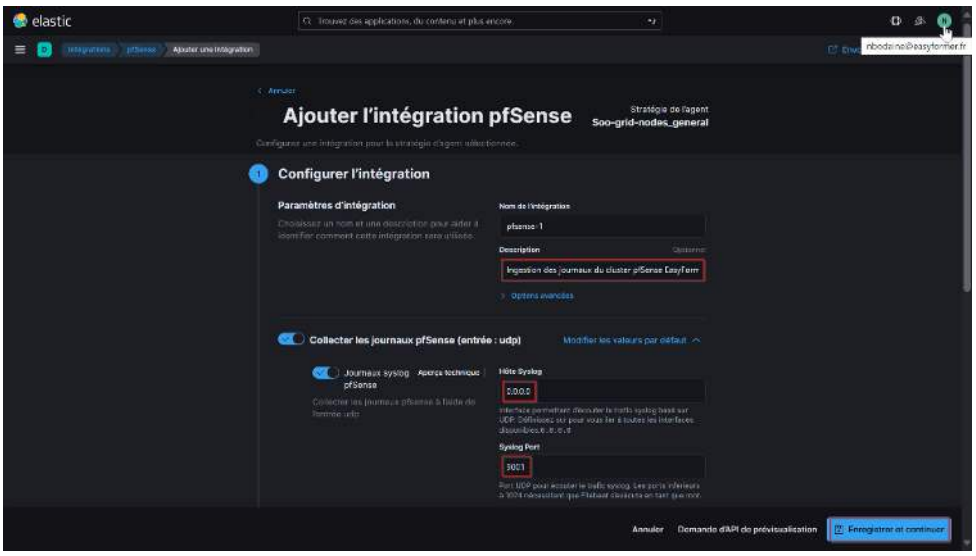


Illustration 77 : configuration de l'intégration pfSense

Ensuite, nous avons mis à jour la configuration du pare-feu local de notre serveur Security Onion pour accepter ce trafic. Nous avons mis l'adresse IP interne de l'interface virtuelle (VIP) du cluster pfSense qui enverra les journaux :

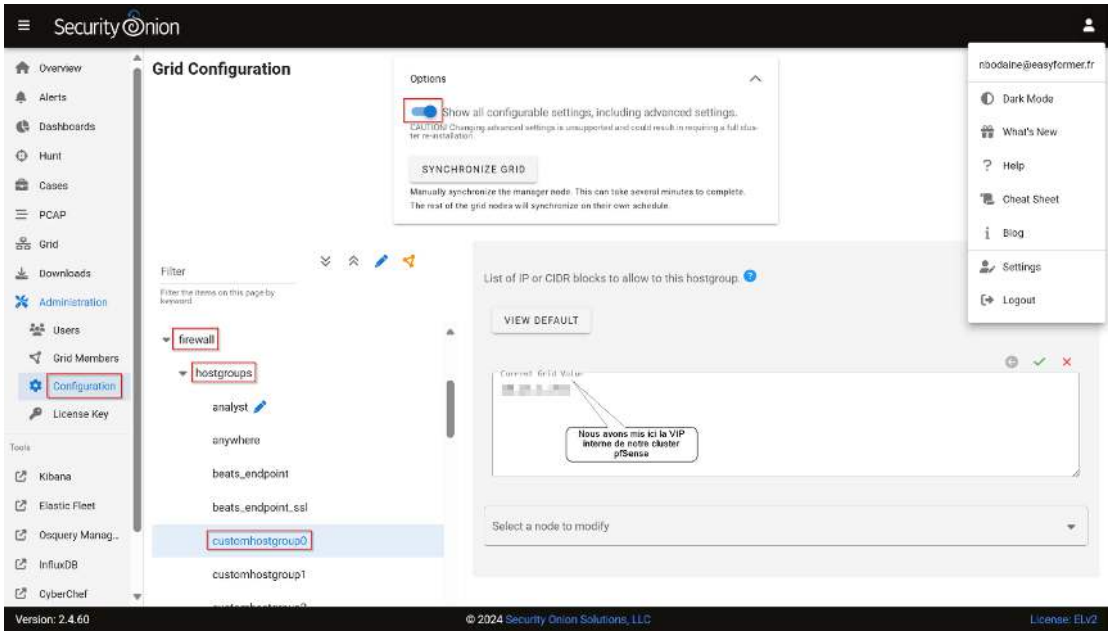


Illustration 78 : configuration du pare-feu local de SO pour la réception des logs du pfSense envoyés depuis l'une de ses VIP

Pour le « customportgroup0 », nous avons renseigné le port UDP 9001 :

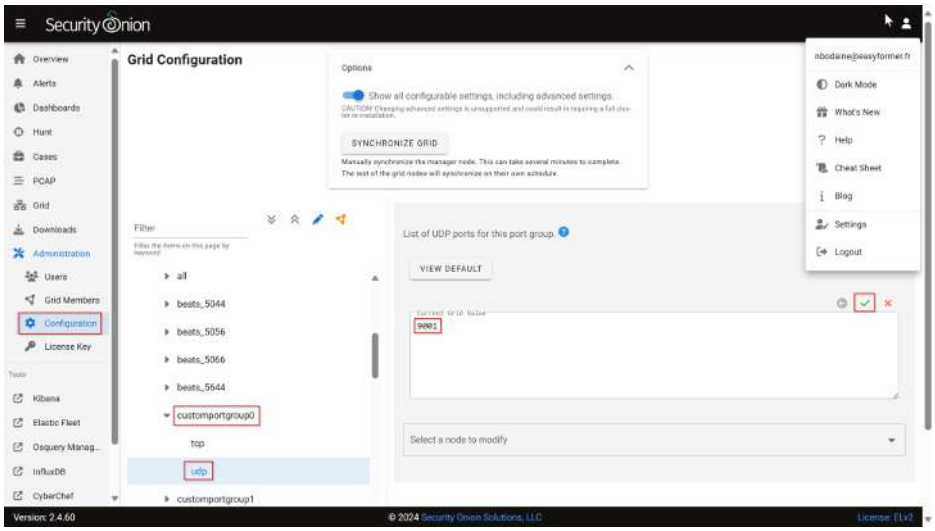


Illustration 79 : configuration du pare-feu local de SO pour la réception sur son port 9001 des logs du pfSense

Enfin, sous « role », nous avons indiqué quel type de nœud doit accepter ce trafic. Dans notre cas, nous voulions l'envoyer à notre unique nœud « standalone », ensuite nous avons développé « chain », « INPUT », « hostgroups », « customhostgroup0 », « portgroups » et avons spécifié d'accepter le trafic de « customportgroup0 ».

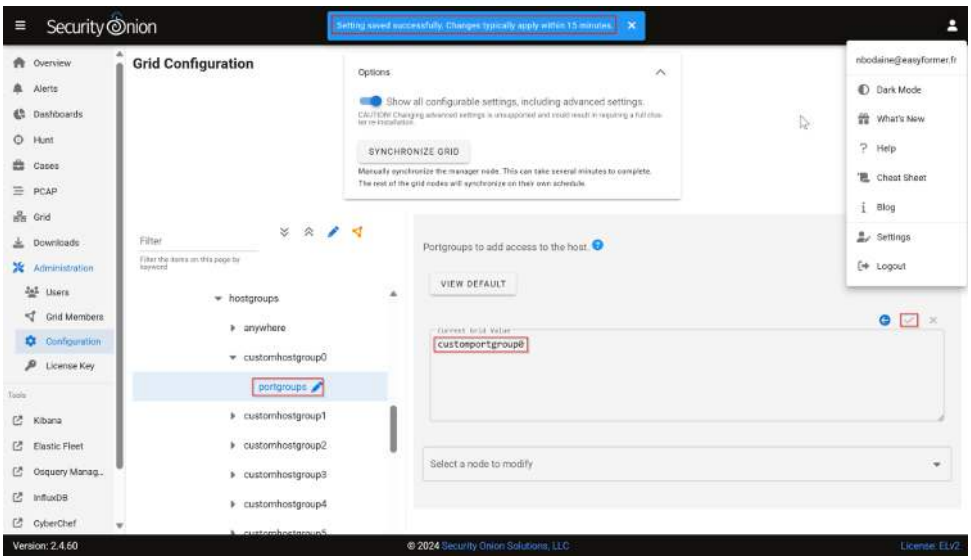


Illustration 80 : configuration du portgroup custom

En cliquant sur « *Synchronize Grid* », nous avons mis à jour cette modification de configuration.

Nous sommes allés ensuite sur l'interface web d'administration de pfSense, sous « *Status*/Etat » puis « *System Logs*/Journaux système » puis « *Settings*/Paramètres » puis tout en bas de la page il a fallu cocher « *Enable Remote Logging*/ Activer la journalisation distante » pour activer l'envoi de messages de journal à un serveur Syslog distant. Nous avons autorisé d'envoyer depuis l'adresse du pfSense qui

a été spécifiée précédemment dans la configuration de « customhostgroup0 ». Nous avons choisi IPv4 comme protocole IP, nous avons entré l'adresse IP de réception de notre nœud Security Onion et le port 9001, puis nous avons sélectionné tous les types de journaux et cliqué sur « *Save* » pour mettre à jour la configuration :

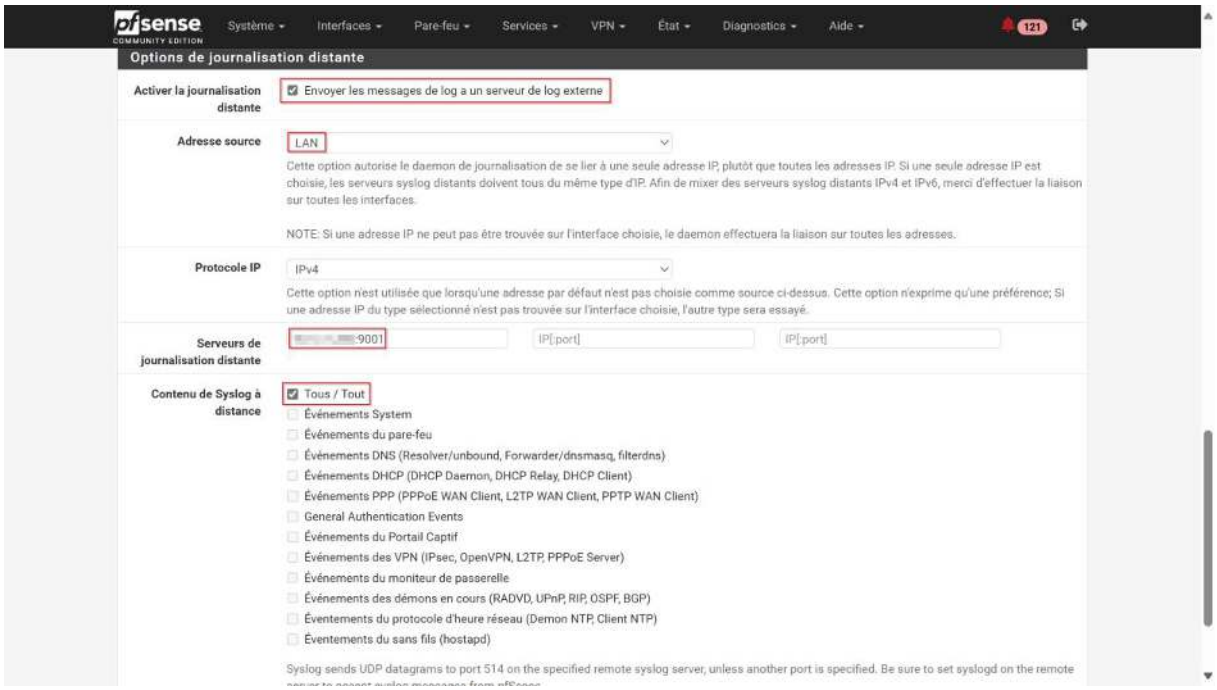


Illustration 81 : activation de l'envoi des logs depuis pfSense vers un serveur Syslog

Il a suffi ensuite d'enregistrer et d'appliquer ce nouveau paramétrage dans pfSense.

6. Mise à jour de Security Onion vers la version 2.4.70

Lors de la sortie de Security Onion version 2.4.70 nous avons effectué la mise à jour depuis la version 2.4.60 en utilisant la commande « soup » (pour **S**ecurity **O**nion **UP**dater ») :

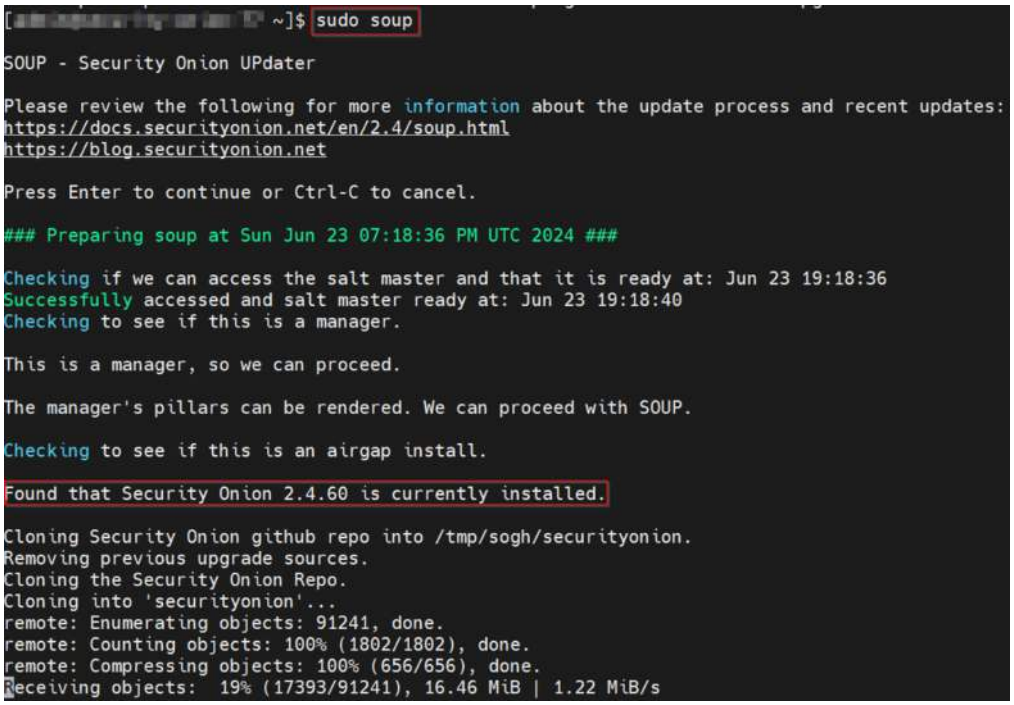


Illustration 82 : lancement de la commande « soup » pour la mise à jour de SO depuis la version 2.4.60

Le script s'est exécuté et la mise à jour a pu se terminer sans problème particulier :

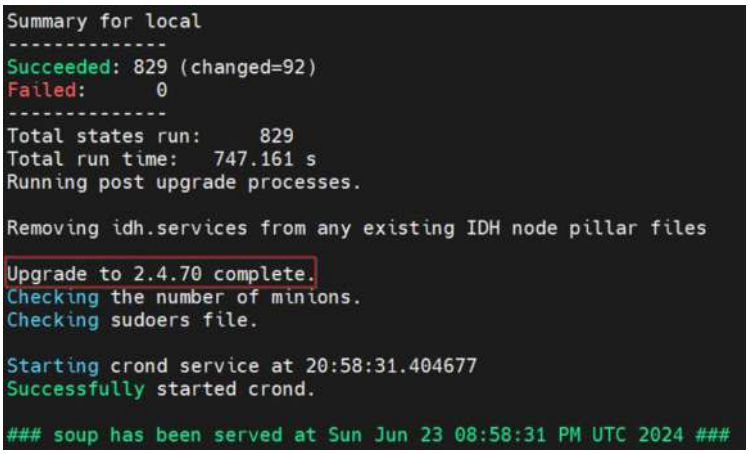


Illustration 83 : fin de la sortie du terminal mentionnant le succès de la mise à jour vers la version 2.4.70

X. GLOSSAIRE

Dans ce glossaire je référence des termes techniques, des anglicismes ou des acronymes dont je fais suivre la signification et/ou une définition.

AFB, Analyse Fonctionnelle des Besoins : Processus de définition des besoins et des exigences fonctionnelles pour un projet ou un système.

AIS, Administrateur d'Infrastructures Sécurisées : Titre professionnel RNCP.

ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information : Service français et autorité nationale en matière de sécurité des systèmes d'information. Elle propose les règles de protection des systèmes d'information de l'État, assure la veille, détection, alerte et réaction aux attaques informatiques.

Brainstorming : Technique de réunion où les participants génèrent des idées et des solutions de manière libre et créative.

CDC, Cahier des Charges : Document détaillant les spécifications et les exigences d'un projet.

CIC, Canadian Institute for Cybersecurity : Institut canadien pour la cybersécurité.

Cloud computing : Accès à des services informatiques via Internet à partir d'un fournisseur.

CVE, Common Vulnerabilities and Exposures : Base de données répertoriant les vulnérabilités connues dans les logiciels et systèmes.

DDoS, Distributed Denial of Service : Attaque visant à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer.

DLP, Data Loss Prevention : Technologie visant à détecter et prévenir les fuites de données sensibles.

EDR, Endpoint Detection and Response : Solution de sécurité permettant de détecter et répondre aux menaces sur les points de terminaison.

Pare-feu de nouvelle génération : Pare-feu offrant des fonctionnalités avancées de filtrage et de sécurité.

FOSS, Free and Open Source Software : Logiciel libre et open source.

Gartner Inc. : Entreprise américaine de conseil et de recherche dans le domaine de la technologie et des techniques avancées.

IDH, Intrusion Detection Honeypot : Système de détection des intrusions simulant un service leurre pour détecter les attaquants et analyser leurs méthodes.

IDS, Intrusion Detection System : Système de détection des intrusions.

IPS, Intrusion Prevention System : Système de prévention des intrusions.

Logiciel libre : Logiciel dont l'utilisation, l'étude, la modification et la duplication sont permises, techniquement et juridiquement.

Magic Quadrant (MQ) : Série de rapports d'études de marché publiés par Gartner, démontrant les tendances du marché.

MOA, Maîtrise d'OuvrAge : Entité responsable de la définition des besoins et des objectifs d'un projet.

MOE, Maîtrise d'Œuvre : Entité responsable de la réalisation technique d'un projet.

NIST, National Institute of Standards and Technology : Organisme américain de normalisation et de recherche technologique.

NSM, Network Security Monitoring : Surveillance des événements de sécurité sur le réseau.

On-premises : Utilisation du serveur et de l'environnement informatique de l'entreprise sur site.

Open source : Logiciels dont la licence permet la libre redistribution, l'accès au code source et la création de travaux dérivés.

PFE, Projet de Fin d'Etudes : Projet réalisé par les étudiants en fin de cursus universitaire.

PoC, Proof of Concept : Démonstration de faisabilité d'un concept ou d'une idée.

Port Knocking : Technique de sécurité où l'accès à un service réseau est accordé après une séquence spécifique de tentatives de connexion.

Ransomware : Logiciel malveillant qui empêche l'accès aux données et propose leur récupération contre le paiement d'une rançon.

Security Onion (SO) : Plateforme open source de surveillance et de défense du réseau.

Security Onion Console (SOC) : Interface web de gestion et de surveillance de Security Onion.

SOC, Centre d'Opérations de Sécurité : Infrastructure dédiée à la surveillance et à la gestion de la sécurité des systèmes d'information.

SOAR, Security Orchestration, Automation and Response : Plateforme intégrée pour la gestion des incidents de sécurité de manière automatisée.

SPA, Single Packet Authorization : Méthode de sécurité de type « port knocking » utilisant un seul paquet réseau chiffré pour authentifier et autoriser l'accès à un service.

Tarpit : Technique de sécurité ralentissant les attaquants en maintenant les connexions réseau ouvertes de manière intentionnelle.

URL Knocking : Technique de sécurité où l'accès à un service est accordé après avoir accédé à une série d'URL spécifiques.

XDR, Extended Detection and Response : Solution de sécurité intégrée fournissant une visibilité et une réponse améliorée aux menaces.

Zero Trust Security Model : Modèle de sécurité où aucun utilisateur ou dispositif n'est automatiquement de confiance, nécessitant une vérification stricte pour chaque accès.

XI. WEBOGRAPHIE

Glossaire ANSSI : https://cyber.gouv.fr/glossaire

Gérez un projet digital avec une méthodologie en cascade : https://openclassrooms.com/fr/courses/4296701-gerez-un-projet-digital-avec-une-methodologie-en-cascade/

Page Wikipédia de Clifford Stoll : https://en.m.wikipedia.org/wiki/Clifford_Stoll

Rencontrez le savant fou qui a écrit le livre sur la façon de chasser les pirates informatiques : https://www.wired.com/story/meet-the-mad-scientist-who-wrote-the-book-on-how-to-hunt-hackers/

Honeypot : un pot-pourri...juridique : http://actes.sstic.org/SSTIC04/Droit_et_honeypots/SSTIC04-article-Barel-Droit_et_honeypots.pdf

Projet de pots de miel distribués : https://honeytarg.cert.br/honeypots/

T-Pot : Le Honeypot OpenSource le plus complet du marché : https://www.geeek.org/t-pot-honeypot-opensource-docker/amp

Technologie de tromperie utilisant des pots de miel open source : https://kahsay-kalayu.medium.com/deception-technology-using-open-source-honeypots-e78b4c66a4ac

Défense active et contre-mesures offensives : https://www.enisa.europa.eu/topics/incident-response/glossary/information-operations-2013-active-defence-and-offensive-countermeasures?v2=1 :

Documentation Security Onion pour l'IDH OpenCanary : https://docs.securityonion.net/en/2.4/idh.html

Configuration des services leurres sur OpenCanary : https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration

5 minutes d'introduction aux règles Sigma : https://www.linkedin.com/pulse/5-minute-intro-Sigma-rules-thomas-knowles

Documentation Security Onion pour Playbook : https://docs.securityonion.net/en/2.4/playbook.html#playbook

Requêtes DSL dans Elastic : https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html

Configuration de ElastAlert : https://docs.securityonion.net/en/2.4/elastalert.html#elastalert

Comment transmettre des cartes réseau PCIe avec Proxmox VE sur Intel et AMD : https://www.servethehome.com/how-to-pass-through-pcie-nics-with-proxmox-ve-on-intel-and-amd/

سبحانك اللهم وبحمدك، أشهد أن لا إله إلا أنت، أستغفرك وأتوب إليك