PROJET SOC

2024

Rédigé par :
MESSAOUDI Ilyasse

Table des matières

Rappel du cadrage

Contexte

ESDOWN est une organisation pharmaceutique comportant une cinquantaine de personnes et intervient comme acteur national sur la fabrication et la vente de certains produits médicaux

Le site héberge l'infrastructure IT principal, la partie fabrication et la partie vente
A la suite de plusieurs cyber attaques perpétrées sur des acteurs du secteur pharmaceutique en Europe, la société ESDown a décidé de lancer plusieurs projets afin de sécuriser son infrastructure et surtout de monter une équipe SoC afin de détecter au mieux les potentielles intrusions et protéger les informations sensibles de l'organisation.

Afin d'identifier les vulnérabilités de son système d'informations, la société ESDown a effectué un pentest de son infrastructure et intégré les correctifs nécessaires à la sécurisation de ses systèmes.

A la suite de cela, la société ESDown a également effectué une analyse de risques avec la méthode EBIOS RM afin de mieux appréhender les différents projets liés à la sécurité de son SI.

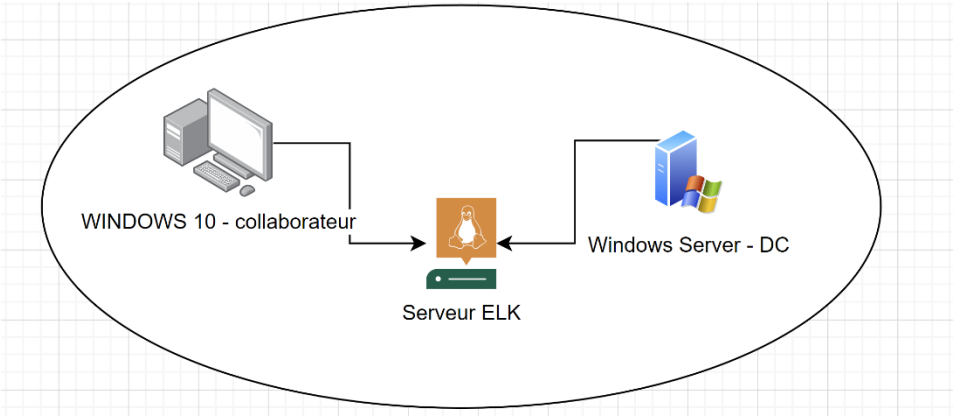
Je suis mandaté par l'organisation ESDOWN pour effectuer une étude afin de mettre en place un SoC sur le site principal.

Dans un contexte critique et sensible, la mise en place d'un SoC vise à garantir la conformité au RGPD et à assurer la certification HDS.

Identifications des actifs critiques

L'identification des actifs a été réalisée en se basant sur les biens supports utilisés par l'organisation ESDOWN.

Deux équipements essentiels ont été mis en avant : le WIN-DC, élément névralgique du SI, et un poste Windows 10 utilisé par un collaborateur. Ce dernier, n'étant pas sensibilisé aux risques cyber, pourrait être vulnérable à des attaques malveillantes, comme le phishing.



SCHEMA DE L'INFRASTRUCTURE CIBLE

Comme indiqué sur le schéma, le but est que le serveur ELK récupère l'ensemble des logs et assure un suivi complet des événements du WIN-DC ainsi que le poste client W10.

Rôles au sein du SOC

Type de SOC

De mon investigation jusqu'à la réflexion du contexte, une approche hybride semble être la meilleure solution.
Étant donné qu'ESDOWN se projetterait sur une infrastructure full-cloud et que leur routage est opérationnel et sécurisé par l'équipe réseau, faire appel à un prestataire externe pour son expertise complémentaire pourrait grandement renforcer la sécurité dans le cadre du SoC.

L'approche hybride constitue ainsi le meilleur compromis entre fiabilité et efficacité.
Bien que ESDown préfère un SoC interne, cette solution hybride offrirait une flexibilité accrue tout en garantissant une couverture optimale contre les menaces.

L'approche hybride permettrait également de bénéficier de prestataires en astreinte ou sur des HNO.

Ressources Humaines

Comme évoqué dans la précédente partie, je recommande la mise en place d'un SoC hybride, intégrant l'intervention de prestataires externes.

En ce qui concerne les ressources humaines internes, j'ai ciblé 3 types de postes à pourvoir.

Il est essentiel de recruter un analyste SoC de niveau 2, car l'administrateur actuellement en poste pourrait assumer les fonctions d'analyste S de niveau 1.
Cette configuration permettrait une bonne complémentarité des compétences et offrirait à l'administrateur la possibilité d'évoluer vers le niveau 2 à l'avenir, favorisant ainsi son développement professionnel.

Par la suite j'ai trouvé pertinent l'ajout d'un ingénieur observabilité dans l'équipe, pour créer de nouvelles métriques, développer des tableaux de bord, définir des alertes et générer des visualisations permettant un suivi approfondi des performances et des incidents.

Enfin pour finaliser l'équipe, un responsable SoC aura un rôle clé en tant que coordinateur, avec une expertise en gestion des incidents de sécurité et une solide connaissance des meilleures pratiques en cybersécurité.

Avec les acteurs internes, voici la proposition d'une matrice RACI.
Cette matrice définit les responsabilités de chaque rôle pour diverses tâches et processus dans un SoC.

Matrice **RACI** - Les 4 responsabilités

R = Réalisateur	A = Approbateur	C = Consultant	I = Informé
Qui ? *Personne qui réalise la tâche et est responsable de son achèvement*	Qui ? *Personne qui approuve l'achèvement d'une tâche*	Qui ? *Personne qui conseille, intervient avant une décision*	Qui ? *Personne qui doit être informé après une décision ou une action*
Mission *Réaliser à bien la tâche qui lui a été attribuée*	Mission *Veiller à la bonne réalisation d'une tâche et à sa validation finale*	Mission *Contribuer à l'efficience d'une tâche via ses conseils et opinions*	Mission *Être tenu à jour de la bonne avancée du projet*
Particularité *Une tâche peut être répartie sur plusieurs responsables*	Particularité *Une autorité unique par tâche*	Particularité *Plusieurs personnes peuvent être consultées (souvent des profils experts)*	Particularité *La personne informée n'intervient pas activement dans la réalistion de la tâche*

source : https://systemproject.fr/matrice-raci/

R Réalisateur
A Approbateur

MATRICE RACI
ESDOWN - SOC

Consultant C
Informé I

Responsabilités / Tâches	Analyste SOC - niv1	Analyste SOC - niv2	Ingénieur Observabilité	Responsable SOC
Surveillance en temps réel	R	A	C	I
Réponse initiale aux incidents	R	A	I	I
Développement de métriques et visualisations	I	C	R	A
Traitement des incidents avancés	I	R	C	A
Optimisation des outils de sécurité	A	I	R	I
Reporting/Communication	I	C	C	R

Définition du plan de détection

Étude des Cyber Kill chains des sources de menace.

Dans la note de cadrage, l'étude de risques met en évidence que les groupes APT dénommés **"Codoso"** et **"Ember Bears"** représentent les menaces les plus importantes actuellement.

Dans cette section, nous allons analyser ces deux groupes, examiner les techniques qu'ils utilisent, et identifier les méthodes de détection permettant de contrecarrer leurs offensives.

Analyse de Codoso – APT19

Dans un premier temps, **Codoso** ou bien encore APT19, est un groupe basé en Chine qui a ciblé divers secteurs, notamment la défense, la finance, l'énergie, l'industrie pharmaceutique, et bien d'autres.

Étant donné qu'ESDOWN opère dans le secteur pharmaceutique, il est évident que cette organisation constitue une cible potentielle.

Domaine	ID	Utilisation	Moyen de détection
Entreprise	T1071.001	APT19 utilise HTTP pour les communications C2 et pour une variante de malware HTTP.	Surveillance du trafic HTTP
Entreprise	T1547.001	Une variante de malware HTTP d'APT19 établit une persistance en modifiant le registre.	Surveillance des clés de registre
Entreprise	T1059	APT19 télécharge et lance du code à l'intérieur d'un fichier SCT.	Analyse des fichiers SCT et surveillance des commandes exécutées.
Entreprise	T1059.001	APT19 utilise des commandes PowerShell pour exécuter des payloads	Surveillance des commandes PowerShell et détection d'exécution inhabituelle.
Entreprise	T1543.003	Malware APT19 sur le port22	Surveillance port 22
	T1132.001	APT19 utilise Base64 pour encoder les communications vers le serveur C2.	Surveillance du trafic HTTP
Entreprise	T1140	Le malware HTTP APT19 déchiffre les chaînes en utilisant des clés XOR à un octet.	Surveillance du trafic HTTP
Entreprise	T1564.003	APT19 utilise des paramètres -w hidden pour masquer les fenêtres PowerShell.	Surveillance des commandes PowerShell
Entreprise	T1574.002	APT19 lance un malware HTTP qui utilise un DLL malveillant chargé par un exécutable légitime.	Surveillance ID 4622 windows

Domaine	ID	Utilisation	Moyen de détection
Entreprise	T1112	APT19 modifie plusieurs clés de registre avec une variante de malware sur le port 22.	Surveillance port 22
Entreprise	T1027.010	APT19 utilise Base64 pour obfusquer les commandes exécutées.	Surveillance réseau de présence de base64
Entreprise	T1588.002	APT19 utilise des outils publics comme Empire.	Surveillance des commandes PowerShell
Entreprise	T1566.001	APT19 envoie des emails de spearphishing avec des pièces jointes malveillantes.	Analyse des pièces jointes des emails pour détecter les menaces.
Entreprise	T1218.010	APT19 utilise Regsvr32 pour contourner les techniques de contrôle des applications.	Surveillance des exécutions de Regsvr32 pour détecter les utilisations suspectes.
Entreprise	T1218.011	APT19 configure sa charge utile pour s'injecter dans rundll32.exe.	Analyse des processus rundll32.exe pour détecter les injections suspectes.
Entreprise	T1082	APT19 collecte des informations sur l'architecture système comme le nom d'hôte et les informations sur le CPU par son malware sur le port 22.	Surveillance port 22
Entreprise	T1016	APT19 collecte l'adresse MAC et l'adresse IP de la machine victime par son malware sur le port 22.	Surveillance port 22
Entreprise	T1204.002	APT19 incite les utilisateurs à lancer des pièces jointes malveillantes via spearphishing.	Analyse des pièces jointes des emails pour détecter les fichiers malveillants.

Voici un tableau récapitulatif des techniques utilisées par le groupe APT19 ainsi que des mesures de détections possibles.

Analyse de Ember Bears

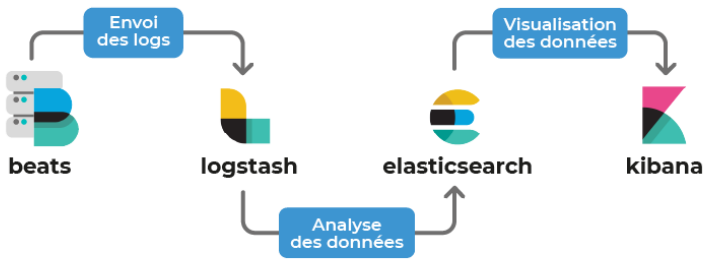
Dans cette seconde sous-partie, je mettrai en lumière les différentes attaques du groupe Ember Bears, un groupe de cyberespionnage parrainé par l'État russe et actif depuis au moins mars 2021.

Domaine	ID	Utilisation	Moyen de détection
Entreprise	T1059.001	Ember Bears a utilisé PowerShell pour télécharger et exécuter du code malveillant.	Surveillance des commandes Powershell
Entreprise	T1059.003	Ember Bears a utilisé cmd.exe et Windows Script Host (wscript) pour exécuter du code malveillant.	Surveillance des commandes Powershell et cmd
Entreprise	T1059.007	Ember Bears a utilisé JavaScript pour exécuter du code malveillant sur la machine d'une victime	Analyse des scripts JS
Entreprise	T1203	Ember Bears a exploité la vulnérabilité CVE-2017-11882 de Microsoft Office.	Mise a jour du client
Entreprise	T1562.001	Ember Bears a exécuté un script batch pour désactiver Windows Defender sur un hôte compromis	Surveillance des commandes Powershell et cmd
Entreprise	T1105	Ember Bears a utilisé des outils pour télécharger du code malveillant	Surveillance réseau
Entreprise	T1112	Ember Bears a utilisé un script batch open source pour modifier les clés de registre de Windows Defender	Surveillance des commandes Powershell et cmd et surveillance des clés de registre
Entreprise	T1027	Ember Bears a masqué les logiciels malveillants pour éviter d'être détecté	Ember Bears a masqué les logiciels malveillants pour éviter d'être détecté. [3]
Entreprise	T1027.001	Ember Bears a ajouté des espaces supplémentaires entre les caractères du code JavaScript pour augmenter la taille globale du fichier	Surveillance des scripts JS, si fichier avec du yara scan
Entreprise	T1027.002	Ember Bears a intégré des logiciels malveillants pour éviter d'être détecté	Surveillance système
Entreprise	T1588.002	Ember Bears a obtenu et utilisé des scripts open source de GitHub	Surveillance réseau et scan yara sur les fichiers
Entreprise	T1588.003	Ember Bears a volé des certificats légitimes pour signer des payloads malveillantes	Surveillance système
Entreprise	T1566.001	Ember Bears a envoyé des e-mails de spearphishing contenant des pièces jointes malveillantes sous forme de fichiers PDF, de documents Word, de fichiers JavaScript et d'exécutables de fichiers du panneau de configuration (CPL)	Surveillance réseau et scan yara sur les fichiers
Entreprise	T1566.002	Ember Bears a envoyé des e-mails de spearphishing contenant des liens malveillants	Surveillance réseau et scan yara sur les fichiers
Entreprise	T1553.002	Ember Bears a utilisé des certificats volés à Electrum Technologies GmbH pour signer des payloads	Surveillance système
Entreprise	T1218.002	Ember Bears a utilisé des fichiers du panneau de contrôle (CPL), envoyés par courrier électronique, pour l'exécution	Scan yara sur les fichiers
Entreprise	T1204.001	Ember Bears a tenté d'inciter les utilisateurs à cliquer sur un lien malveillant dans un e-mail de spearphishing	Surveillance système + réseau
Entreprise	T1204.002	Ember Bears a tenté d'attirer ses victimes pour qu'elles exécutent des fichiers malveillants	Surveillance réseau
Entreprise	T1102	Ember Bears a utilisé le réseau de diffusion de contenu (CDN) de Discord pour diffuser des logiciels malveillants et des scripts malveillants à un hôte compromis	Surveillance réseau et scan yara sur les fichiers
Entreprise	T1027.010	Ember Bears a obfusqué les scripts malveillants pour éviter d'être détecté	scan yara + si hash malveillant le bloquer

Mise en place d’un dashboard

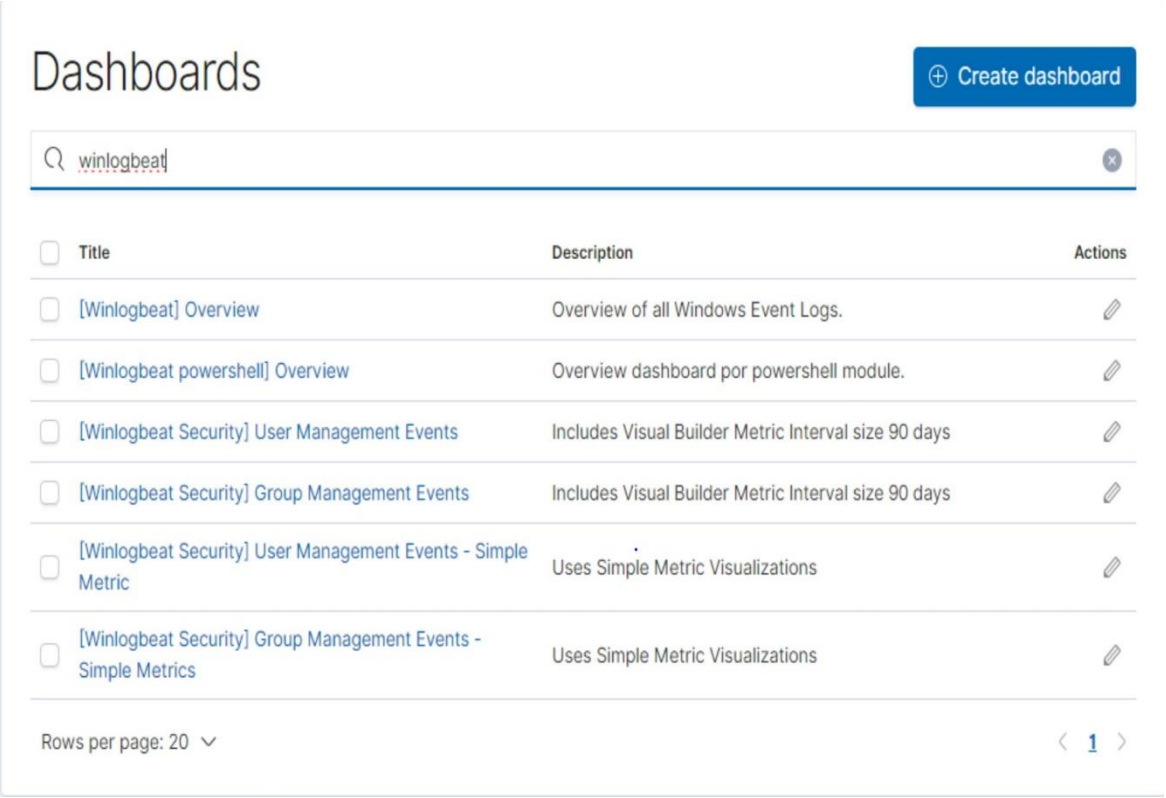
J'ai choisi, comme indiqué dans l'introduction, la suite ELK pour le SoC. Cette solution regroupe les fonctionnalités essentielles pour l’ingestion et la centralisation des logs.

La suite ELK se compose de Logstash, qui collecte et transforme les logs avant de les envoyer à Elasticsearch, le moteur de recherche qui stocke et indexe les données.
Et enfin Kibana étant l’interface pour visualiser les données et créer des tableaux de bord.



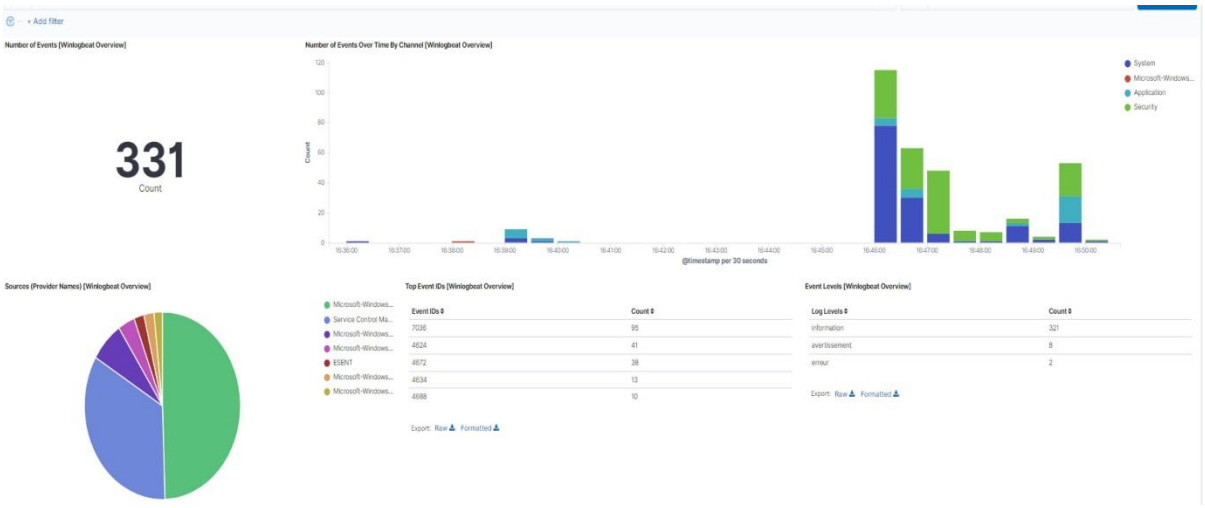
Étant donné que la proposition du SoC repose sur deux machines Windows, Windows serveur et Windows10, la collecte des logs sera effectuée à l'aide de Winlogbeat.

Winlogbeat offre nativement des tableaux de bord complets prêts à l'emploi.



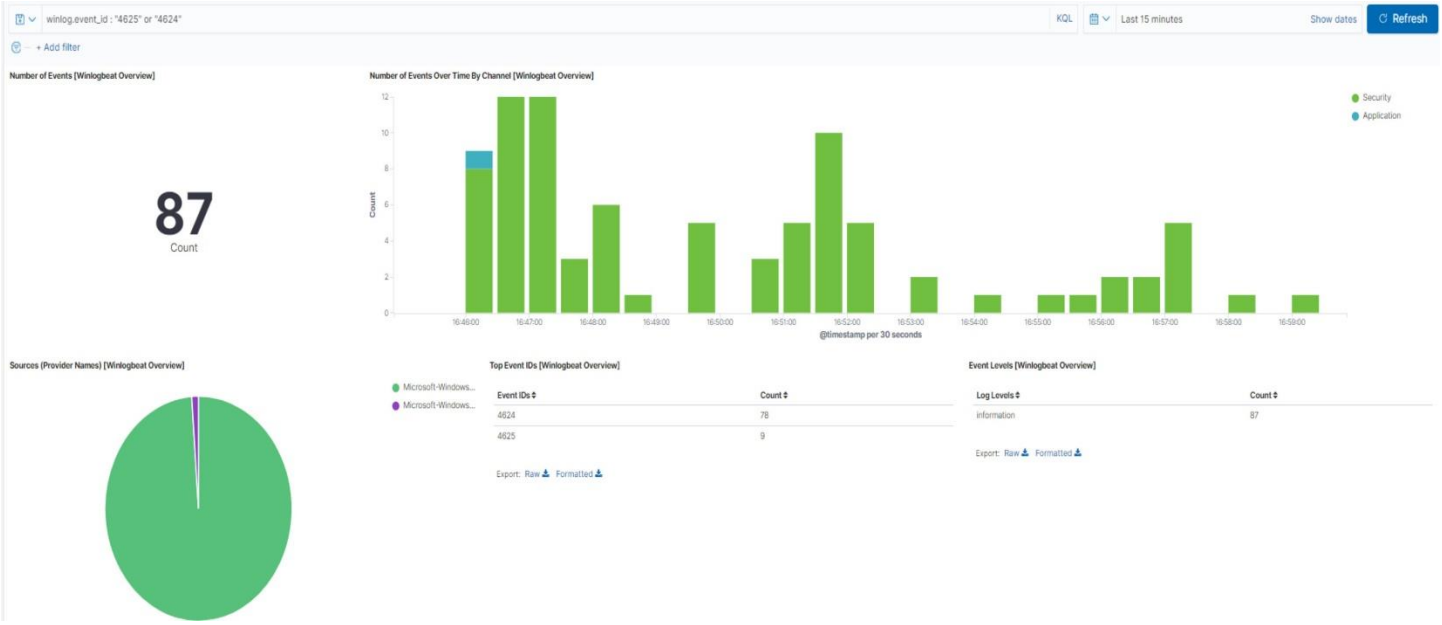
Template Winlogbeat

Ce premier modèle propose un ensemble complet d'événements Windows avec leur ID et le nombre d'occurrences sur une période définie.



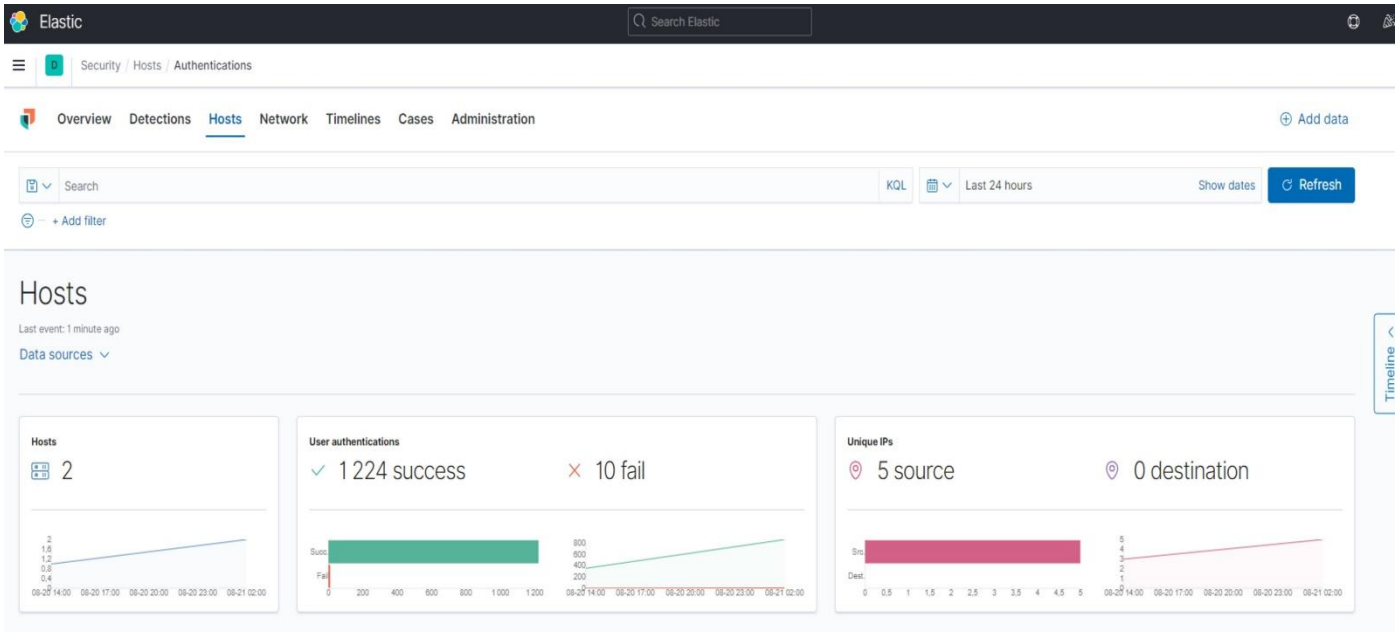
Cet affichage en temps réel des logs permettra aux analystes de repérer d’un coup d'œil sur l’ensemble des postes, les différentes alertes potentielles et d'adopter une réaction proactive face aux éventuelles menaces.

Ce deuxième tableau de bord regroupe les différents ID liés à l'authentification Windows. Il permet de détecter une machine compromise et d'être alerté en cas d'attaque par force brute ou d'élévation de privilèges, qu'elle soit verticale ou horizontale.



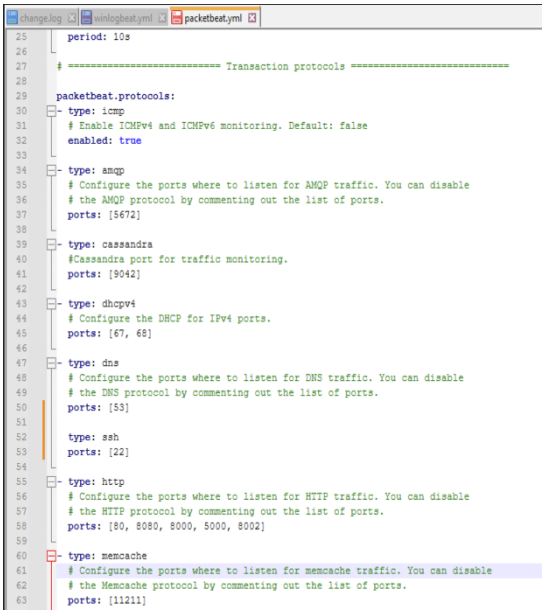
Pour l'exemple, nous avons deux ID soit 4624, connexion réussie ou 4625, connexion échouée.
On peut très bien paramétrer des affichages de comptes bloquées sur a des tentatives de brute-force.

Pour un affichage plus complet avec des graphiques dans la section Security, nous pouvons visualiser toutes les informations disponibles qui complètent la partie précédente.



Template Packetbeat

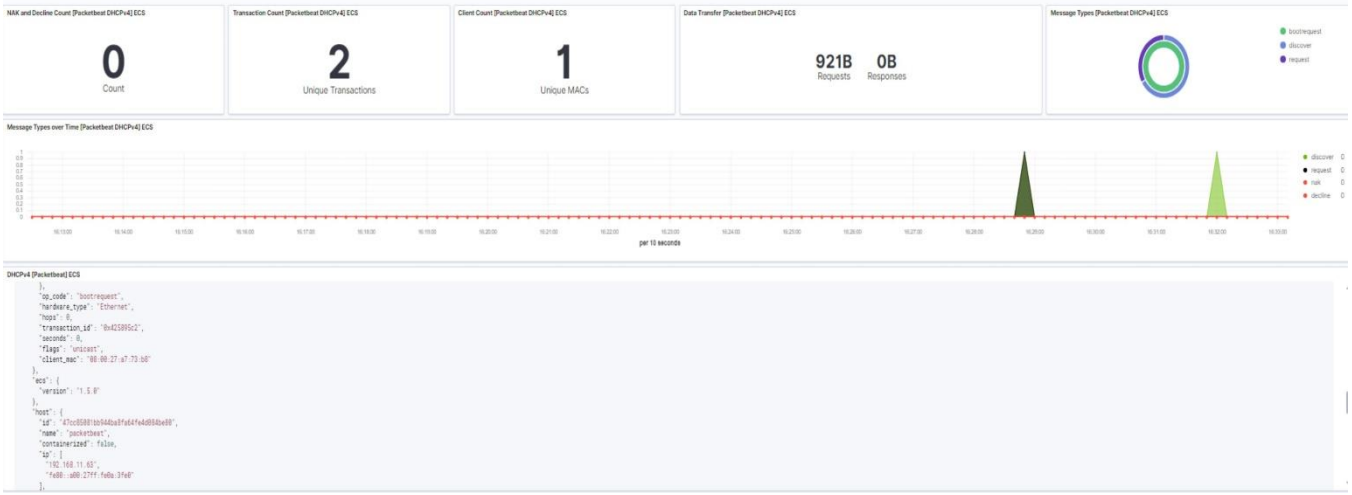
Pour améliorer l'analyse des logs sur notre système ELK, j'ai intégré une nouvelle métrique qui permettra une analyse plus approfondie du réseau.
Cette métrique offre la possibilité d'ajouter des services avec leurs ports.



Grâce à Packetbeat, nous pouvons suivre précisément le trafic réseau de l'ensemble des machines, ce qui permet de définir des limites ou des conditions spécifiques.

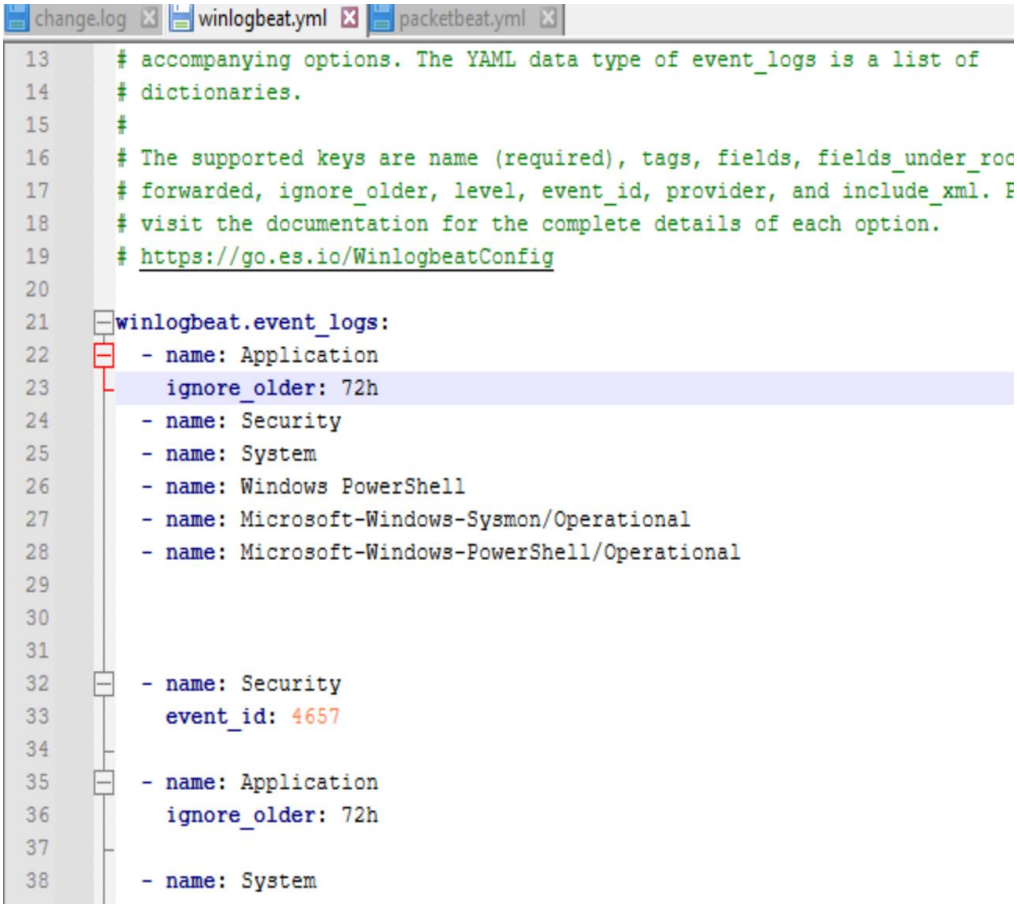
Dans cette section Overview, il est également possible de visualiser les transactions HTTP. Par exemple, ce qui permet aux analystes de mener des investigations en cas de détection de payloads ou de C2.

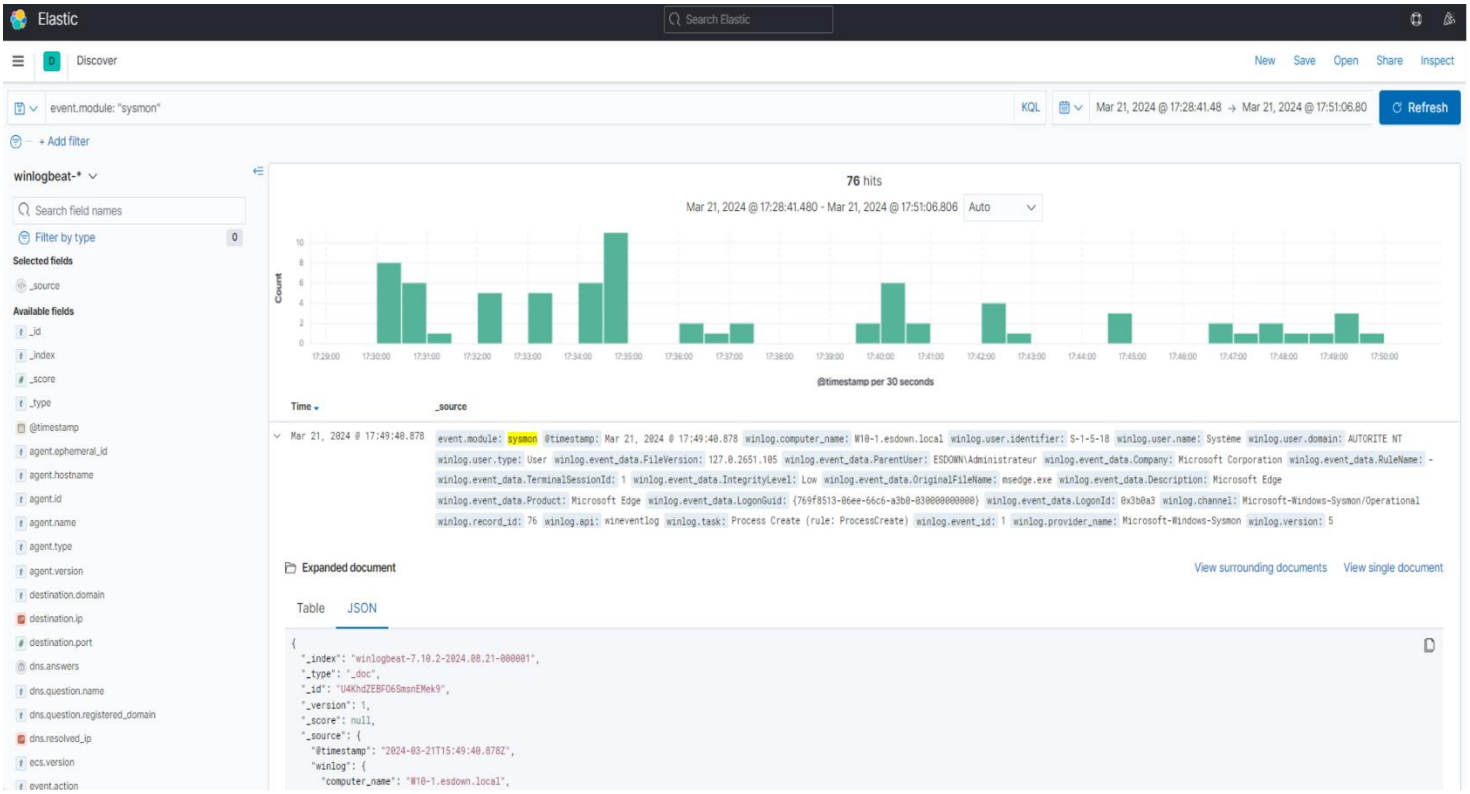
Nous pouvons également suivre les transactions et négociations DHCP et DNS, ce qui permet de détecter d'éventuelles attaques intrusives, comme celles menées par une équipe redteam, au sein d'ESDOWN.



Template avec Sysmon

Pour optimiser au mieux notre collecte de logs, il a fallu intégrer Sysmon, qui est un outil qui permet une meilleure journalisation des évènements de sécurité système sous Windows.





Dans cet extrait, l'ID Sysmon 1 indique la création d'un processus. Il fournit le nom de l'utilisateur, la machine concernée, le nom du service ainsi que le chemin du répertoire où le processus a été créé.

Dans cet exemple, ces informations permettent à l'analyste de détecter brièvement différentes attaques, telles que le masquerading ou le process hollowing.

Conclusion

Nous voyons que la proposition du SoC via la stack ELK, est crucial pour garantir la pérennité de la sécurité et de l'intégrité de l'entreprise ESDOWN.
Les dashboards proposés permettent d'identifier, en temps réels, les attaques en cours, de comprendre leur nature et d'y répondre de manière appropriée.

Grâce à l'analyse réseau avec Packetbeat, aux logs générés par Winlogbeat et à l'intégration de Sysmon, nous obtenons une complémentarité.

De ce fait, grâce à ces intégrations, nous pouvons visualiser des chemins d'attaque tels que ceux observés précédemment avec APT19 ou même avec Ember Bear.