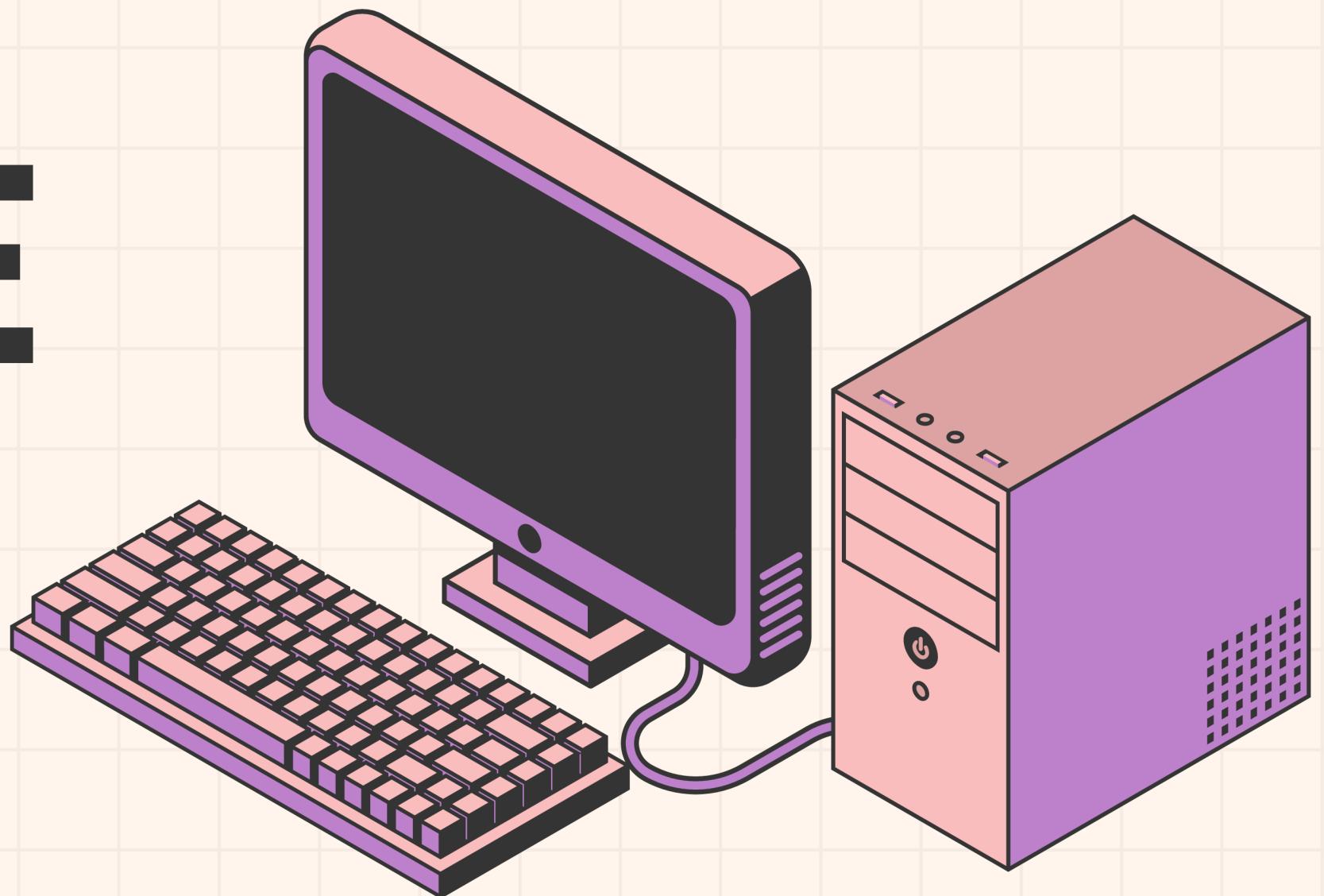
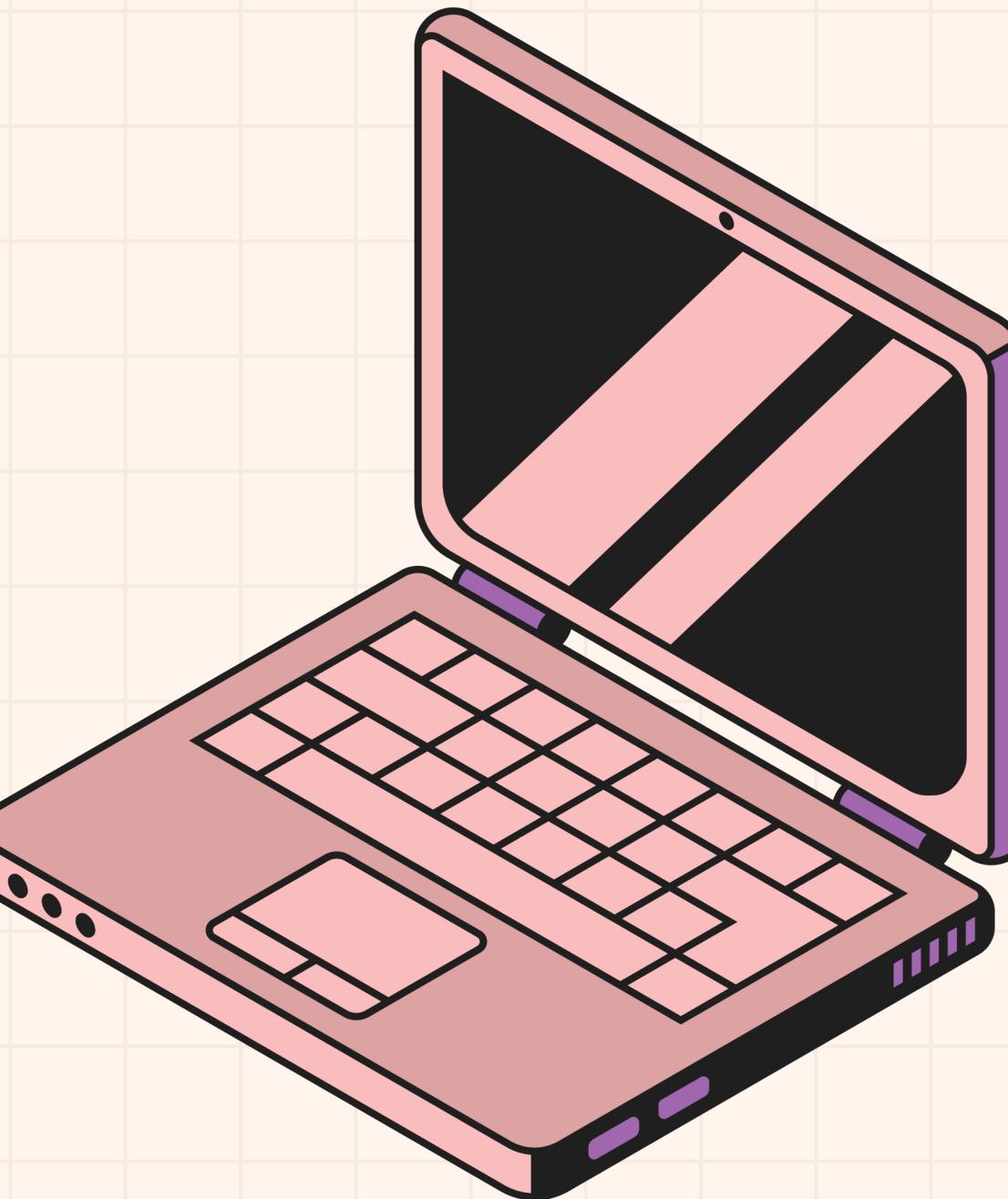


COMPAGNIE DES ALPES



INTRODUCTION

Dans cette introduction, je vais vous présenter les différentes missions que j'ai réalisées au cours de cette semaine de stage. Ensuite, je partagerai mon ressenti sur la vie en entreprise.



MON PROJET



Power BI

Power BI est un outil de Business Intelligence permettant de collecter, analyser et visualiser des données sous forme de tableaux de bord interactifs. Il se connecte à diverses sources (bases de données, fichiers, API) pour transformer les données brutes en informations exploitables. Grâce à ses visualisations dynamiques, il aide à la prise de décision en mettant en évidence les tendances et anomalies.

X

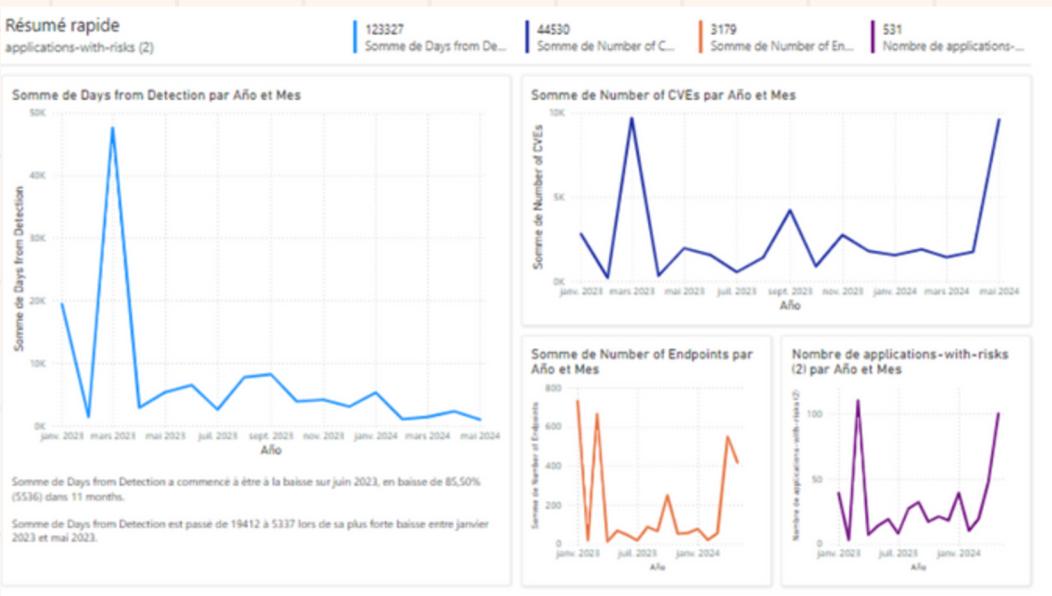


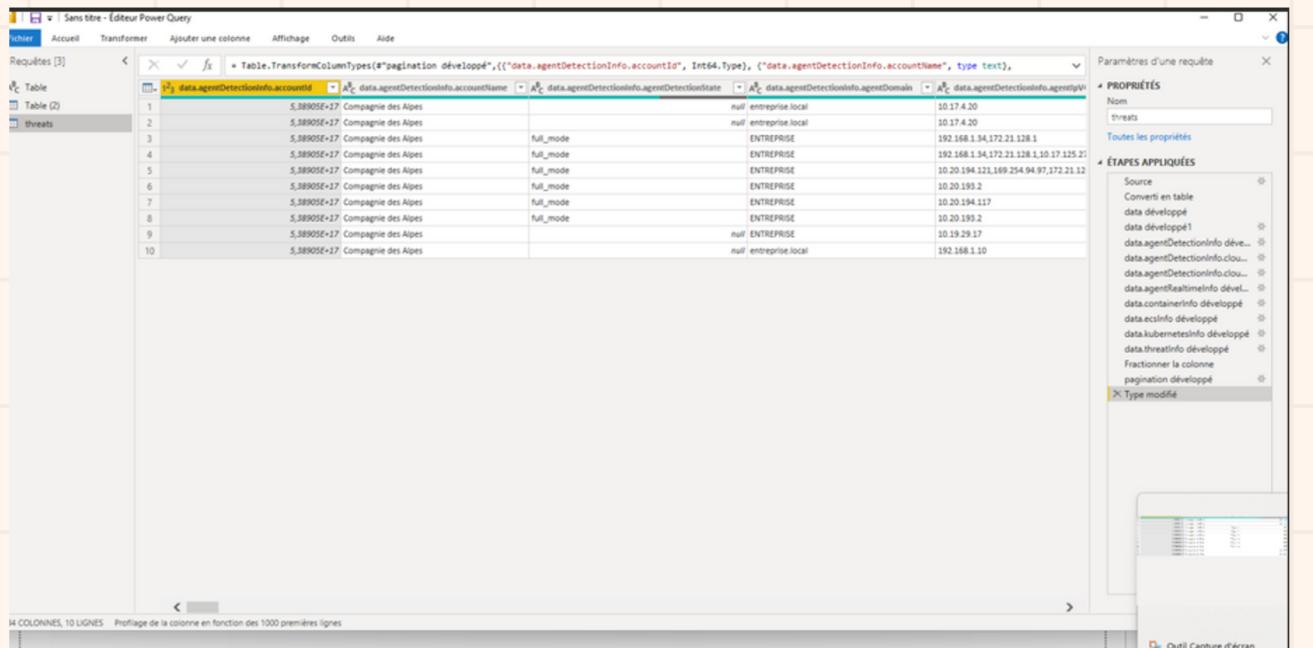
SentinelOne™

SentinelOne est une solution de cybersécurité basée sur l'intelligence artificielle, conçue pour détecter, prévenir et répondre aux menaces en temps réel. Il analyse les comportements suspects sur les endpoints (postes de travail, serveurs) pour bloquer les attaques avant qu'elles ne causent des dommages. Grâce à l'automatisation et à l'IA, il offre une protection proactive contre les ransomwares, malwares et autres cybermenaces.

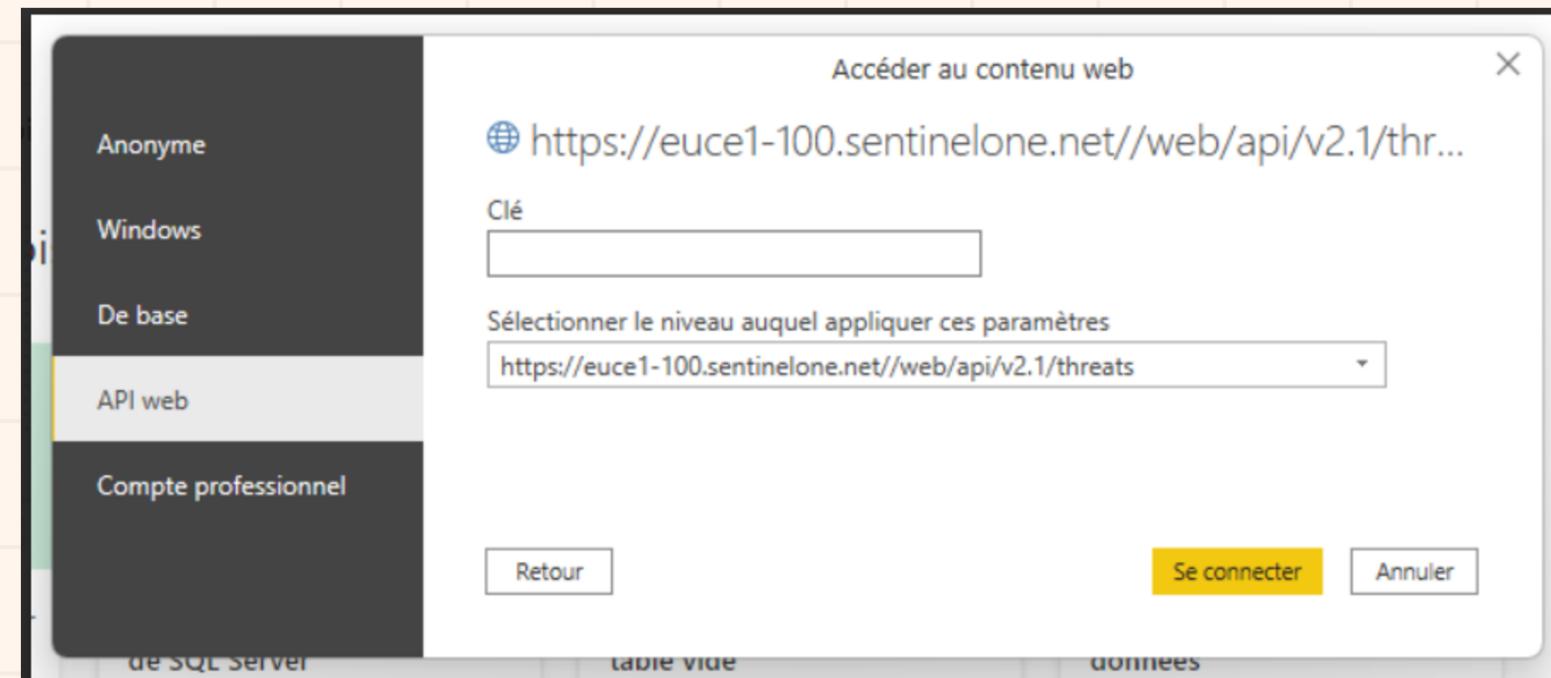
LE BUT DE MON PROJET

Ma mission lors de ce premier stage était de connecter Power BI à SentinelOne afin de permettre l'affichage d'informations cruciales, comme les tentatives d'attaques ou toute donnée utile à l'équipe cybersécurité. L'objectif était de générer des tableaux de bord interactifs mettant en évidence les vulnérabilités et autres indicateurs clés. Pour cela, j'ai dû trouver une solution permettant d'établir cette connexion. J'ai principalement utilisé ChatGPT et une documentation existante, mais celle-ci était assez ancienne et ne correspondait pas aux nouvelles versions du logiciel, ce qui a compliqué la mise en place du projet.





The screenshot shows the Power Query Editor interface. On the left, there's a navigation pane with 'Requêtes [3]' and a table named 'threats'. The main area displays a table with 10 rows of data. The columns are: 'accountName' (containing 'Compagnie des Alpes'), 'agentDetectionInfo.accountDomain' (containing 'null entreprise local', 'full_mode', 'ENTREPRISE', etc.), 'agentIpAddress' (containing '10.17.4.20', '192.168.1.34', etc.), and 'agentPort' (containing '10.17.4.20', '192.168.1.34', etc.). A tooltip for 'agentIpAddress' lists several IP addresses. On the right, there are 'PROPRIÉTÉS' and 'ÉTAPES APPLIQUÉES' panes.



The screenshot shows a 'Accéder au contenu web' dialog box. It features a sidebar with authentication options: 'Anonyme', 'Windows', 'De base' (selected), 'API web', and 'Compte professionnel'. Below the sidebar, there's a 'Clé' input field containing the URL 'https://euce1-100.sentinelone.net/web/api/v2.1/threats'. At the bottom, there are 'Retour', 'Se connecter' (highlighted in yellow), and 'Annuler' buttons.

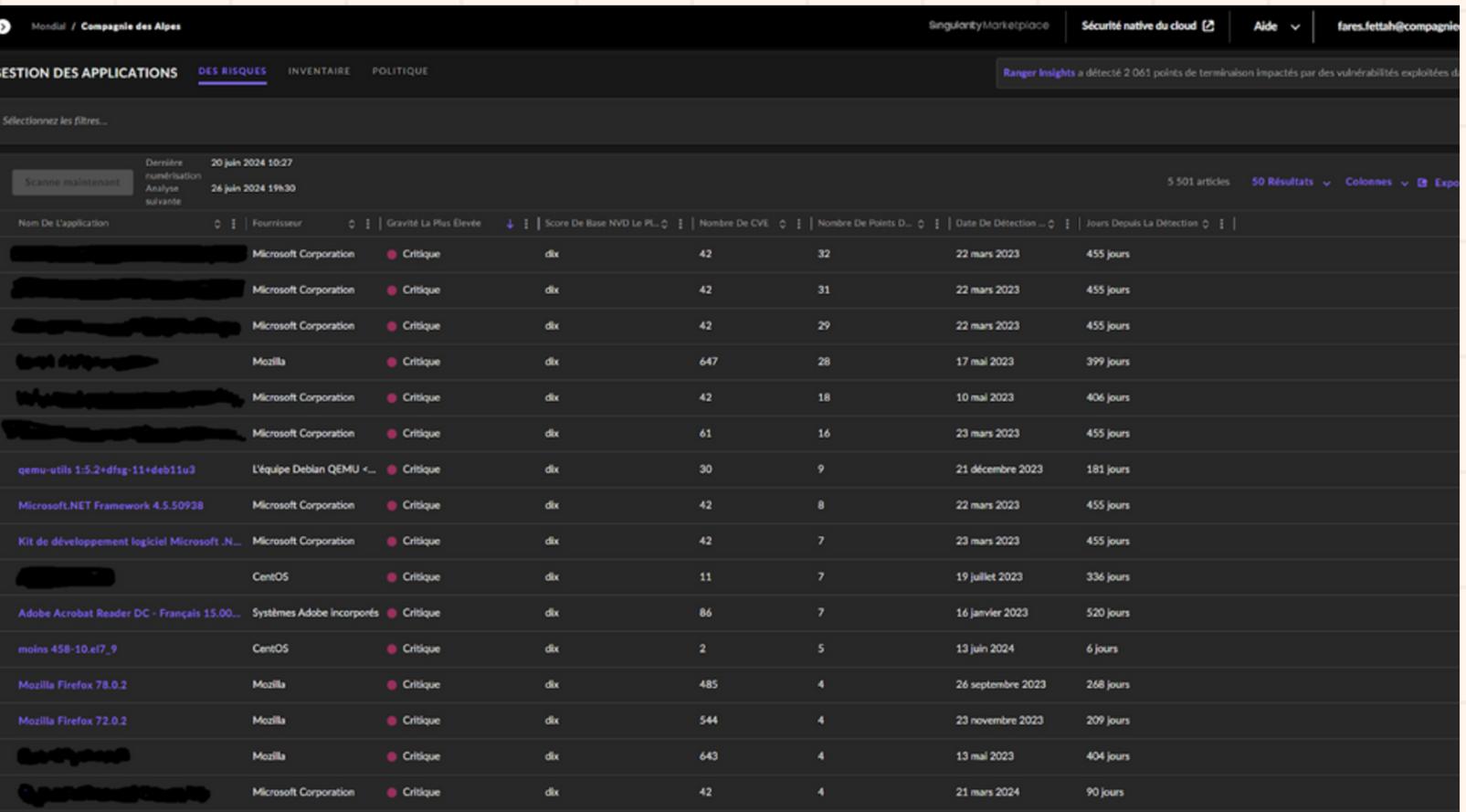
Dans cette partie, j'ai pu récupérer différentes informations essentielles, ce qui m'a permis d'afficher les données demandées de manière claire et structurée. Grâce à cette intégration, j'ai pu générer des tableaux de bord interactifs et des diagrammes mettant en évidence les informations cruciales requises par l'équipe. Cela a facilité la visualisation des vulnérabilités et des événements de sécurité en temps réel.

40

Dans cette deuxième partie, j'ai dû explorer différentes méthodes pour établir la connexion. Au début, j'étais assez perdu, car je disposais de peu d'informations. Cependant, cette mission m'a appris à être plus autonome, à rechercher efficacement des solutions et à mieux comprendre le fonctionnement des outils. Finalement, j'ai sollicité un administrateur afin d'obtenir la clé d'API de SentinelOne, ce qui m'a permis d'établir la connexion et d'afficher les données demandées dans Power BI.

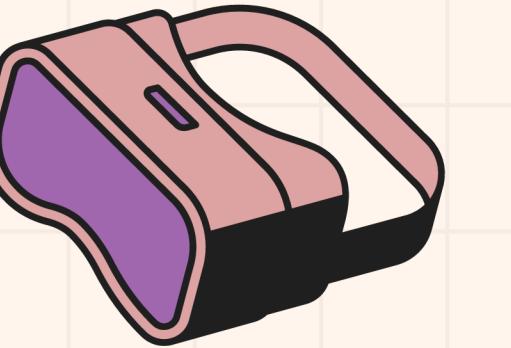
SENTINELONE

A project is a series of planned tasks with a clear objective, often involving multiple steps. It can be carried out by individuals or teams and is designed to achieve specific outcomes within a set timeframe.



The screenshot shows a dashboard titled "GESTION DES APPLICATIONS" with a sub-tab "DES RISQUES" selected. The interface includes a header with "Mondial / Compagnie des Alpes" and navigation links for "SingularityMarketplace", " Sécurité native du cloud", "Aide", and "fares.fettah@compagnie". A message at the top right states "Ranger Insights a détecté 2 061 points de terminaison impactés par des vulnérabilités exploitées dans les dernières 24 heures". The main content is a table listing vulnerabilities, with columns including "Nom De L'application", "Fournisseur", "Gravité La Plus élevée", "Score De Base NVD Le Plus Bas", "Nombre De CVE", "Nombre De Points Détectés", "Date De Détection", and "Jours Depuis La Détection". The table lists items such as Microsoft Corporation products like Edge, Internet Explorer, and Microsoft Edge, Mozilla Firefox, and various Linux distributions like CentOS and Ubuntu.

Nom De L'application	Fournisseur	Gravité La Plus élevée	Score De Base NVD Le Plus Bas	Nombre De CVE	Nombre De Points Détectés	Date De Détection	Jours Depuis La Détection
[REDACTED]	Microsoft Corporation	Critique	dix	42	32	22 mars 2023	455 jours
[REDACTED]	Microsoft Corporation	Critique	dix	42	31	22 mars 2023	455 jours
[REDACTED]	Microsoft Corporation	Critique	dix	42	29	22 mars 2023	455 jours
[REDACTED]	Mozilla	Critique	dix	647	28	17 mai 2023	399 jours
[REDACTED]	Microsoft Corporation	Critique	dix	42	18	10 mai 2023	406 jours
[REDACTED]	Microsoft Corporation	Critique	dix	61	16	23 mars 2023	455 jours
qemu-utils 1:5.2+dfsg-11+deb11u3	L'équipe Debian QEMU <...>	Critique	dix	30	9	21 décembre 2023	181 jours
Microsoft.NET Framework 4.5.50938	Microsoft Corporation	Critique	dix	42	8	22 mars 2023	455 jours
Kit de développement logiciel Microsoft .NET Framework 4.8.0.3922	Microsoft Corporation	Critique	dix	42	7	23 mars 2023	455 jours
[REDACTED]	CentOS	Critique	dix	11	7	19 juillet 2023	336 jours
Adobe Acrobat Reader DC - Français 15.00.11220.100.20230926	Systèmes Adobe incorporés	Critique	dix	86	7	16 janvier 2023	520 jours
moins 458-10.x17_9	CentOS	Critique	dix	2	5	13 juin 2024	6 jours
Mozilla Firefox 78.0.2	Mozilla	Critique	dix	485	4	26 septembre 2023	268 jours
Mozilla Firefox 72.0.2	Mozilla	Critique	dix	544	4	23 novembre 2023	209 jours
[REDACTED]	Mozilla	Critique	dix	643	4	13 mai 2023	404 jours
[REDACTED]	Microsoft Corporation	Critique	dix	42	4	21 mars 2024	90 jours



MERCI

