INSTITUT INFORMATIQUE APPLIQUÉE

Document technique :

MISE EN PLACE D'UN SERVICE AUTOMATIQUE POUR DES RELANCES LOOKOUT

Besoin recensé :

Sécurité renforcée : Assurer une sécurité optimale pour les utilisateurs en garantissant une réponse rapide aux alertes Lookout, ce qui permet de minimiser les risques de compromission des données ou des systèmes.

Réactivité accrue : En relançant automatiquement les utilisateurs concernés par une alerte Lookout, vous assurez une réactivité rapide face aux menaces potentielles, ce qui peut réduire les délais de réponse et les dommages potentiels.

Réduction de la charge de travail : Automatiser le processus de relance des utilisateurs peut réduire la charge de travail manuelle pour les équipes de sécurité, ce qui leur permet de se concentrer sur des tâches plus stratégiques et complexes.

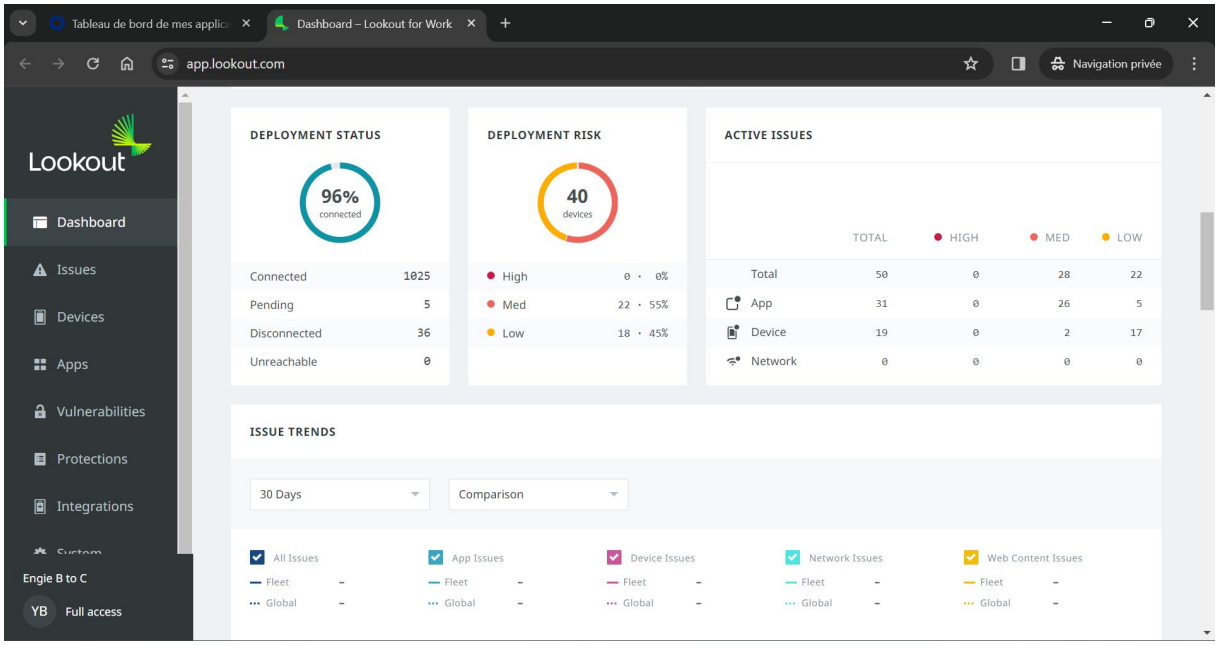
Amélioration de la conformité : En garantissant une réponse rapide et systématique aux alertes Lookout, vous pouvez mieux vous conformer aux normes de sécurité et aux réglementations en vigueur, ce qui est crucial dans de nombreux secteurs d'activité.

Minimisation des risques : En relançant automatiquement les utilisateurs concernés, vous augmentez les chances de résoudre rapidement les problèmes de sécurité potentiels, ce qui peut aider à minimiser les risques pour l'organisation dans son ensemble.

Meilleure utilisation des ressources : En automatisant la relance des utilisateurs, vous utilisez plus efficacement les ressources disponibles, en réduisant le besoin d'interventions humaines répétitives et en permettant aux équipes de se concentrer sur des tâches plus stratégiques.

Amélioration de la productivité : Une réponse rapide et efficace aux alertes Lookout peut contribuer à maintenir la productivité des utilisateurs en minimisant les interruptions causées par des problèmes de sécurité.

Présentation de Lookout :



Lookout for Work est un outil de sécurité pour les environnements de travail. Il fournit un aperçu complet de l'état de déploiement et des risques associés aux mobile professionnel (téléphone et tablette) au sein d'une organisation ENGIE, ainsi qu'un suivi des problèmes actifs.

État de déploiement : Cette section offre une vue d'ensemble de l'état de connexion des dispositifs au service. Elle indique combien de dispositifs sont actuellement connectés, en attente de connexion, déconnectés ou inatteignables.

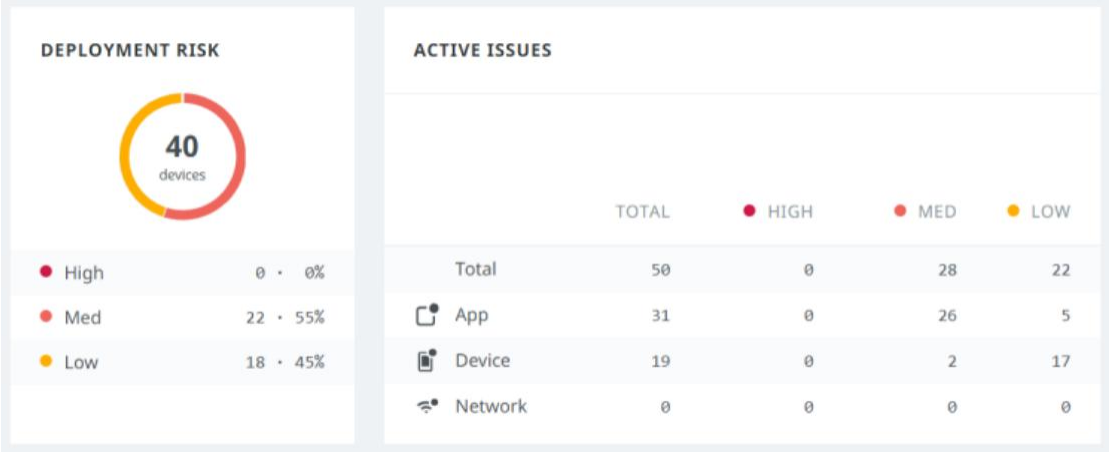
Risque de déploiement : Elle résume le niveau de risque associé aux dispositifs déployés, classés par niveau de risque élevé, moyen et faible.

Problèmes actifs : Cette partie détaille le nombre total de problèmes identifiés dans le système, divisés en catégories telles que les applications, les dispositifs et le réseau. Elle montre également la répartition des problèmes en fonction de leur gravité : élevée, moyenne ou faible.

Tendances des problèmes : Une analyse sur 30 jours des tendances des problèmes, permettant de comparer l'évolution dans le temps. Cette section peut également distinguer les problèmes liés aux applications, aux dispositifs, au réseau et au contenu Web, offrant une vue globale ou ciblée sur des aspects spécifiques.

L'interface fournit ainsi une vue globale sur l'état de sécurité et de connectivité des dispositifs au sein de l'organisation, permettant de prendre des mesures proactives pour résoudre les problèmes et réduire les risques.

Comment lancer l’automatisation des relances utilisateurs :

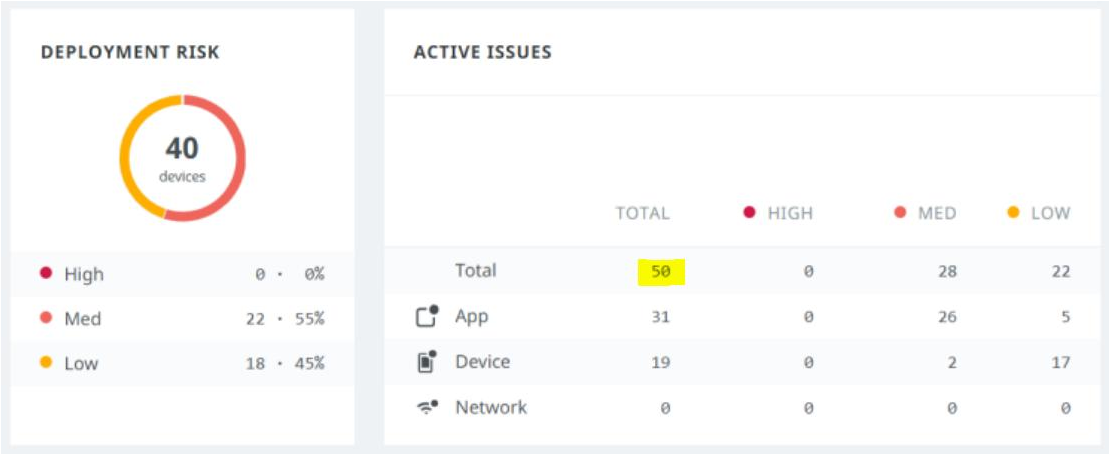


L'image montre deux sections clés d'un tableau de bord de surveillance de la sécurité des dispositifs : Risque de déploiement et Problèmes actifs.

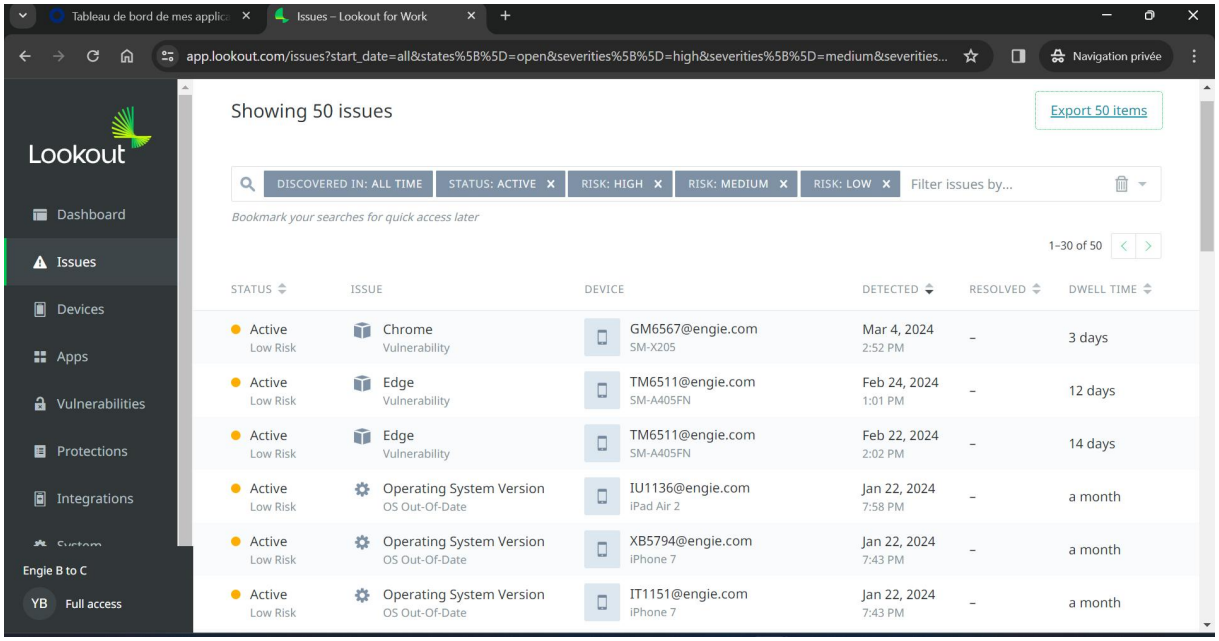
Risque de déploiement : Indique que sur 40 dispositifs évalués, 22 sont classés à risque moyen (55%) et 18 à faible risque (45%). Il est important de noter qu'aucun dispositif n'est à haut risque, ce qui est une indication positive, mais il reste essentiel d'adresser les risques moyens et faibles pour maintenir la sécurité.

Problèmes actifs : Sur un total de 50 problèmes identifiés, 28 sont de gravité moyenne et 22 de faible gravité, ce qui souligne l'absence de problèmes hautement critiques. Les problèmes sont majoritairement liés aux applications (31), suivi par les problèmes de dispositifs (19). Aucun problème réseau n'est signalé, ce qui suggère que les principaux défis se situent au niveau des applications et des dispositifs eux-mêmes.

Cette vue d'ensemble fournit une base pour l'analyse des risques et la prise de décisions en matière de gestion de la sécurité, permettant de cibler les interventions là où elles sont le plus nécessaires.



Pour approfondir l'analyse et la gestion des alertes, je vais procéder à un export des alertes spécifiques en sélectionnant le nombres «50» mis en évidence. Cette action me permettra d'accéder à des informations détaillées sur chaque alerte, facilitant ainsi leur examen approfondi et leur traitement éventuel.



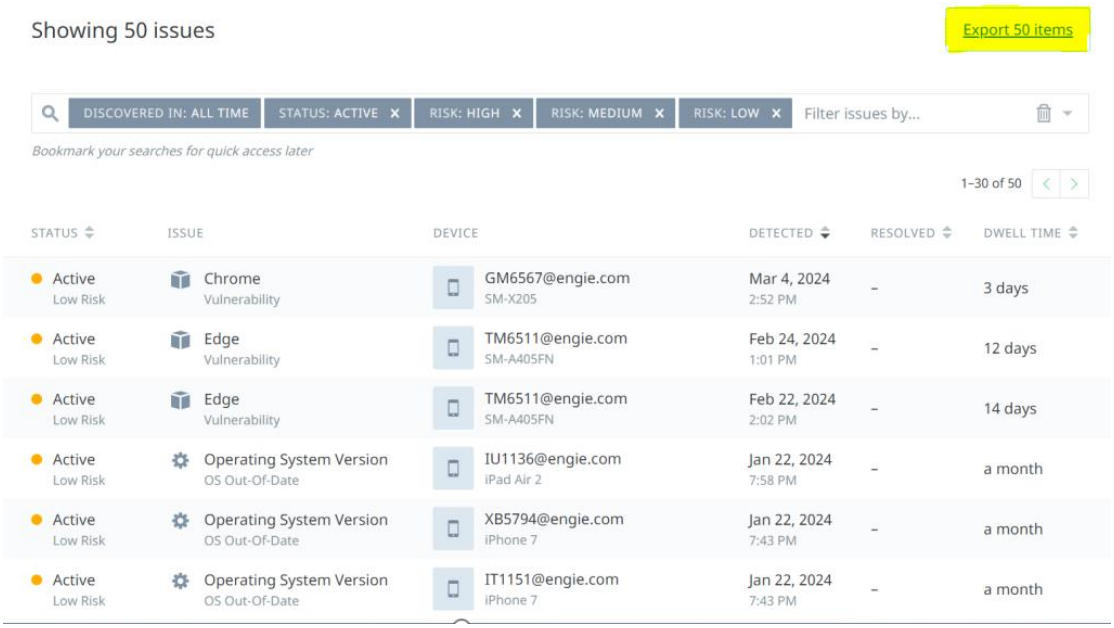
Voici une description des trois types d'alertes visibles :

Vulnérabilité de Chrome : Signale une faiblesse dans le navigateur Google Chrome qui pourrait être exploitée pour compromettre la sécurité de l'appareil ou des données de l'utilisateur. La vulnérabilité peut résulter de diverses causes, comme des mises à jour logicielles non appliquées ou des failles de sécurité découvertes récemment.

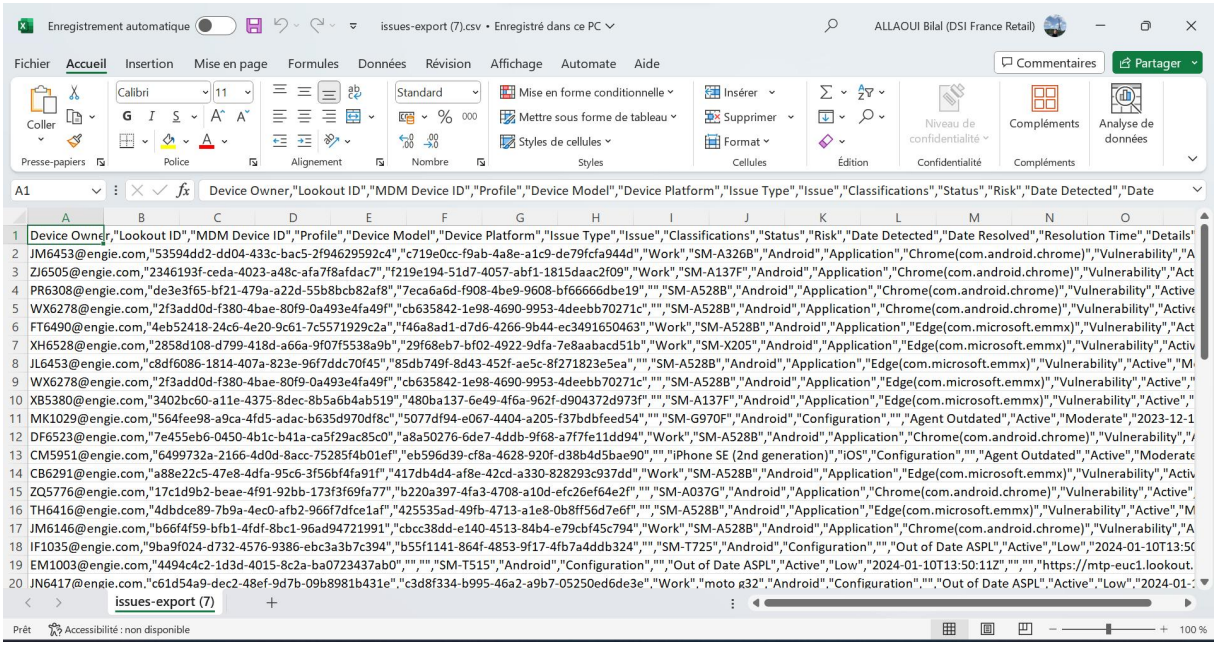
Vulnérabilité de Edge : Identique à l'alerte de Chrome mais concerne le navigateur Microsoft Edge. Ces vulnérabilités mettent en lumière des points faibles susceptibles d'être exploités pour effectuer des attaques malveillantes ou voler des informations.

Version du système d'exploitation obsolète : Indique que le système d'exploitation de l'appareil est dépassé et nécessite une mise à jour pour corriger des failles de sécurité et améliorer les performances. L'utilisation d'un OS obsolète augmente le risque d'exposition à des vulnérabilités et des attaques malveillantes car il ne bénéficie plus des dernières corrections de sécurité.

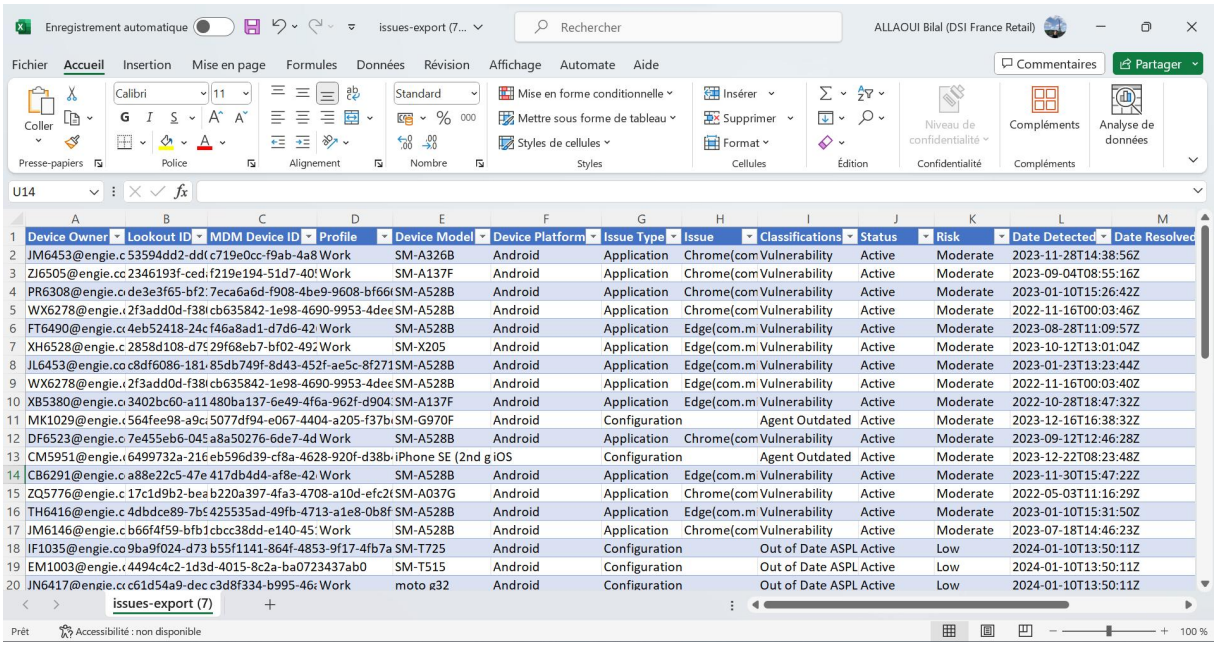
Export des alertes :



Je vais exporter des alertes spécifiques en cliquant sur le bouton "Export 50 items" mis en évidence. Cette démarche me permettra d'obtenir des informations détaillées sur chaque alerte, simplifiant ainsi leur analyse approfondie et leur éventuel traitement

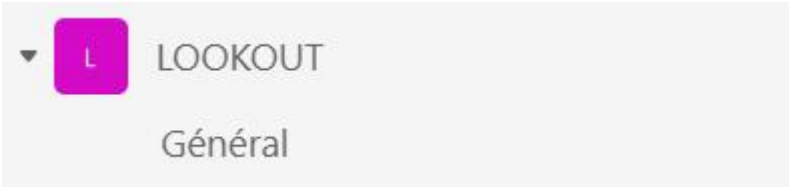


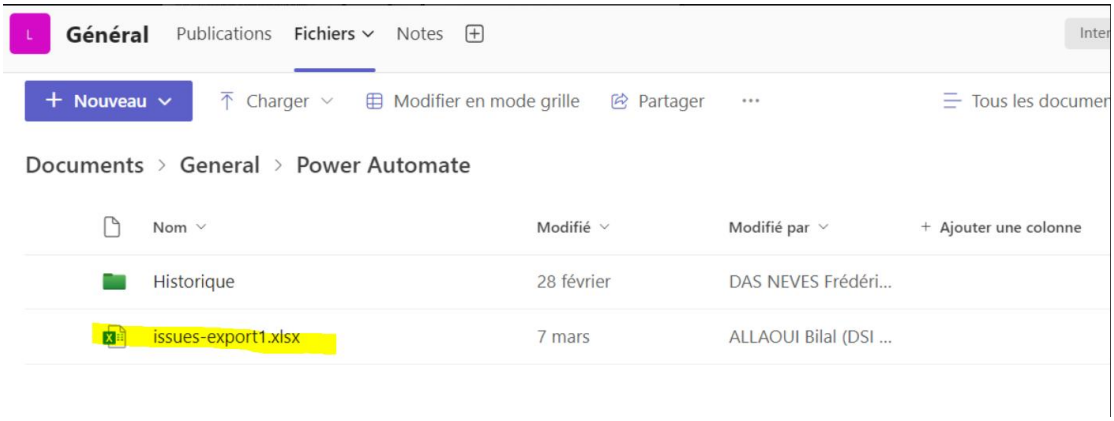
Voici les alertes enregistrées sous forme de données brutes ; je vais maintenant les formater pour une meilleure lisibilité.



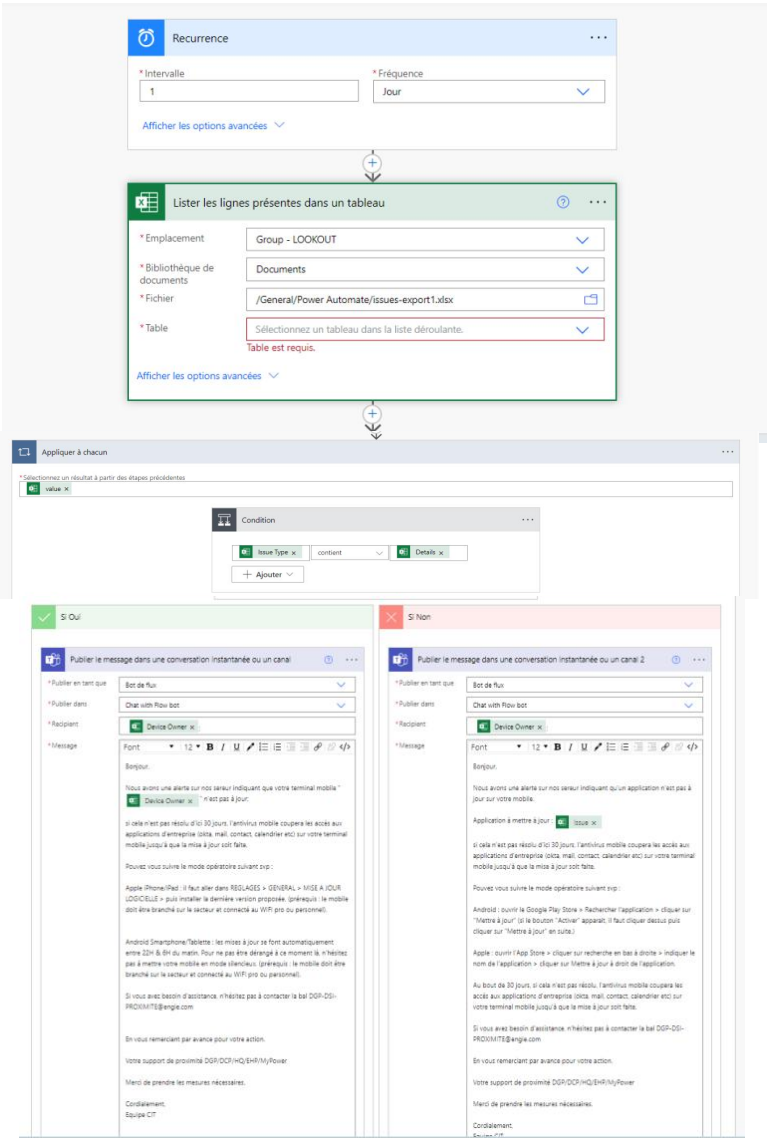
Device Owner	Lookout ID	MDM Device ID	Profile	Device Model	Device Platform	Issue Type	Issue	Classifications	Status	Risk	Date Detected	Date Resolved
JM6453@engie.c	53594dd2-dd(	c719e0cc-f9ab-4a8	Work	SM-A326B	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2023-11-28T14:38:56Z	
ZJ6505@engie.cc	2346193f-ced	f219e194-51d7-40!	Work	SM-A137F	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2023-09-04T08:55:16Z	
PR6308@engie.c	de3e3f65-bf2:	7eca6a6d-f908-4be9	9608-bf66(	SM-A528B	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2023-01-10T15:26:42Z	
WX6278@engie.(	2f3add0d-f38	cb635842-1e98-4690	9953-4dee	SM-A528B	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2022-11-16T00:03:46Z	
FT6490@engie.cc	4eb52418-24c	f46a8ad1-d7d6-42	Work	SM-A528B	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2023-08-28T11:09:57Z	
XH6528@engie.c	2858d108-d7	29f68eb7-bf02-492	Work	SM-X205	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2023-10-12T13:01:04Z	
JL6453@engie.co	c8df6086-181	85db749f-8d43-452f	ae5c-8f271	SM-A528B	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2023-01-23T13:23:44Z	
WX6278@engie.(	2f3add0d-f38	cb635842-1e98-4690	9953-4dee	SM-A528B	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2022-11-16T00:03:40Z	
XB5380@engie.c	3402bc60-a11	480ba137-6e49-4f6a	962f-d904	SM-A137F	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2022-10-28T18:47:32Z	
MK1029@engie.(	564fee98-a9c	5077df94-e067-4404	a205-f37b	SM-G970F	Android	Configuration		Agent Outdated	Active	Moderate	2023-12-16T16:38:32Z	
DF6523@engie.c	7e455eb6-045	a8a50276-6de7-4d	Work	SM-A528B	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2023-09-12T12:46:28Z	
CM5951@engie.(	6499732a-216	eb596d39-cf8a-4628	920f-d38b	iPhone SE (2nd g	iOS	Configuration		Agent Outdated	Active	Moderate	2023-12-22T08:23:48Z	
CB6291@engie.c	a88e22c5-47e	417db4d4-af8e-42	Work	SM-A528B	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2023-11-30T15:47:22Z	
ZQ5776@engie.c	17c1d9b2-bea	b220a397-4fa3-4708	a10d-efc2(	SM-A037G	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2022-05-03T11:16:29Z	
TH6416@engie.c	4dbdce89-7b5	425535ad-49fb-4713	a1e8-0b8f	SM-A528B	Android	Application	Edge(com.m	Vulnerability	Active	Moderate	2023-01-10T15:31:50Z	
JM6146@engie.c	b66f4f59-bfb1	cbcc38dd-e140-45:	Work	SM-A528B	Android	Application	Chrome(com	Vulnerability	Active	Moderate	2023-07-18T14:46:23Z	
IF1035@engie.co	9ba9f024-d73	b55f1141-864f-4853	9f17-4fb7a	SM-T725	Android	Configuration		Out of Date ASPL	Active	Low	2024-01-10T13:50:11Z	
EM1003@engie.(	4494c4c2-1d3d-4015	8c2a-ba0723437ab0		SM-T515	Android	Configuration		Out of Date ASPL	Active	Low	2024-01-10T13:50:11Z	
JN6417@engie.cc	c61d54a9-dec	c3d8f334-b995-46:	Work	moto g32	Android	Configuration		Out of Date ASPL	Active	Low	2024-01-10T13:50:11Z	

Voici une présentation plus nette des données pour une lisibilité améliorée. Ce fichier est sauvegardée sous le nom «issues-export1.xlsx» dans TEAMS, dans l'équipe «LOOKOUT».





Mise en place d’un flux Power Automate :



Ce flux automatisé est conçu pour être exécuté quotidiennement. Sa première action consiste à lister toutes les lignes d'un tableau spécifique situé dans un fichier Excel stocké sur un groupe SharePoint. Ce tableau contient des informations sur des alertes de sécurité générées par Lookout pour le travail, un outil de cybersécurité mobile.

Ensuite, pour chaque alerte listée, le flux exécute une condition qui vérifie le type d'alerte (contenu du champ "Issue Type"). Si l'alerte concerne une application non mise à jour ou un système d'exploitation obsolète, le flux procède à une étape conditionnelle supplémentaire.

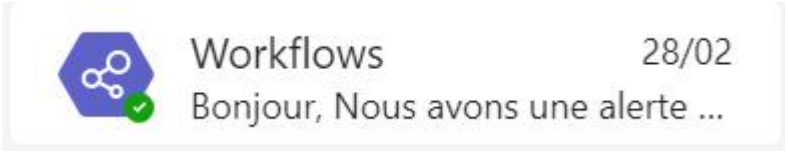
Dans cette étape conditionnelle, si l'alerte est confirmée comme concernant un appareil spécifique, le flux envoie un message personnalisé au propriétaire de l'appareil via Microsoft

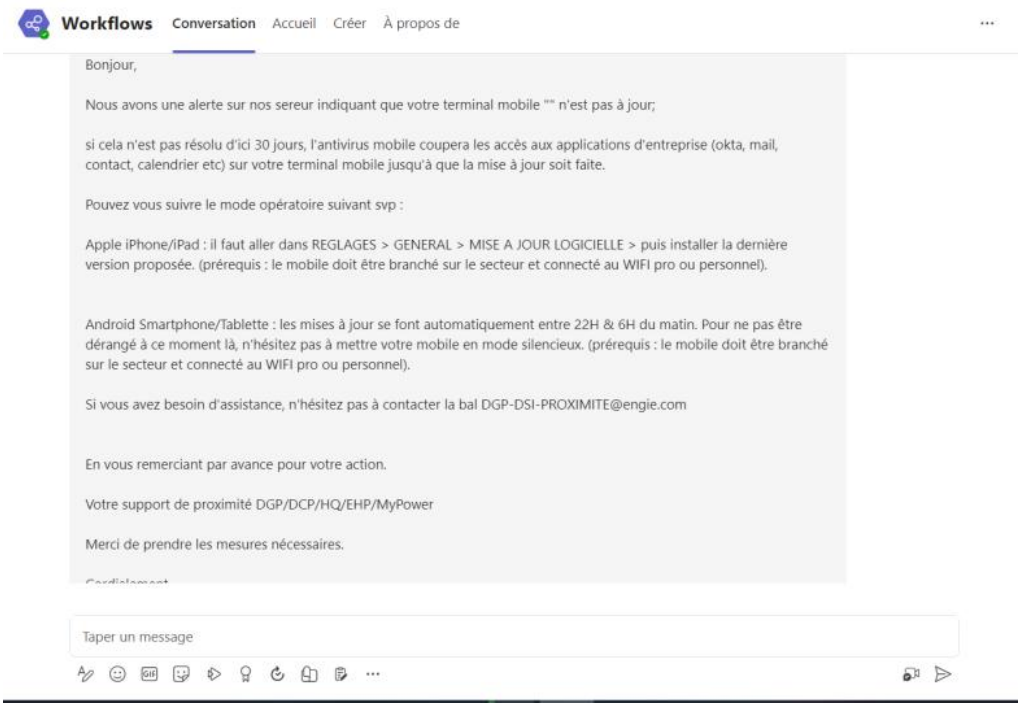
Teams. Ce message l'informe de la nécessité de mettre à jour son application ou son système d'exploitation pour résoudre le problème de sécurité identifié. Le message contient des instructions spécifiques sur la manière de procéder à la mise à jour, adaptées à l'appareil iOS ou Android concerné.

En résumé, ce flux automatisé joue un rôle crucial dans la gestion des alertes de sécurité liées à des applications non mises à jour ou à des systèmes d'exploitation obsolètes. En informant directement les utilisateurs concernés via Microsoft Teams, il contribue à accélérer le processus de correction des vulnérabilités et à maintenir le niveau de sécurité des appareils mobiles au sein de l'organisation.

Message sur TEAMS :

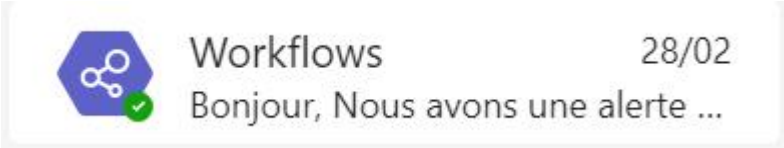
Voici le processus par lequel les utilisateurs reçoivent les notifications du flux :





Ce que je souhaite mettre en place :

Dans un premier temps je souhaiterais changer le logo et la nomination du flux sur TEAMS



Je voudrais modifier le logo et le nom du flux sur TEAMS.
Le nom: Equipe CIT DGP
Avec ce logo :

Dans un deuxième temps, Pour renforcer l'autonomie de ce projet, j'ai l'intention de développer un script Python qui automatisera les processus effectués manuellement jusqu'à présent, notamment l'exportation des données depuis Lookout et leur intégration dans Teams.


C: > Users > Bilal > Downloads > auto lookout (1).py > ...

```python
import requests
import asyncio
import ssl

# Paramètres de l'API Lookout
API_KEY_LOOKOUT = 'eyJraWQiOiIxODoxNjo3NzoyMjo2Mzo0YjpmZjoyMzoxOTpmMTpjZjozYTpjYjphZTozODo0NDo5NjpmYTozNDpjMDpjMTo5Zj
ALERT_ENDPOINT = 'https://api.lookout.com/alerts'

# Paramètres de l'API Microsoft Graph
TOKEN_MICROSOFT_GRAPH = 'VOTRE_TOKEN_MICROSOFT_GRAPH'
TEAMS_API_URL = 'https://graph.microsoft.com/v1.0/teams'

# Ignorer les erreurs de certificat SSL si nécessaire
ssl._create_default_https_context = ssl._create_unverified_context

# Fonction pour trouver un utilisateur à l'aide de son GAIA sur Teams
async def trouver_utilisateur_par_gaia_sur_teams(gaia):
    # Mettez ici votre code pour rechercher l'utilisateur sur Teams en utilisant son GAIA
    print(f"Recherche de l'utilisateur avec le GAIA sur Teams : {gaia}")

    # Remplacez cette ligne par votre propre logique pour trouver l'utilisateur sur Teams
    # et retournez les informations pertinentes si trouvé
```

Ce script Python automatisé effectue plusieurs tâches clés liées à la gestion d'alertes et à la communication sur Microsoft Teams. Voici un résumé de son fonctionnement :

Paramètres Initiaux : Le script utilise des clés API pour se connecter à l'API Lookout et à l'API Microsoft Graph. Il configure également le contexte SSL pour ignorer les erreurs de certificat, si nécessaire.

Trouver un Utilisateur sur Teams : À l'aide de la fonction trouver_utilisateur_par_gaia_sur_teams, le script cherche un utilisateur spécifique sur Microsoft Teams en utilisant son identifiant GAIA. Cette recherche simule la récupération des détails de l'utilisateur comme son nom, email, et l'équipe à laquelle il appartient, basé sur l'identifiant GAIA fourni.

Envoyer une Relance : La fonction envoyer_relance est conçue pour envoyer un message personnalisé à un utilisateur sur Teams, adapté selon le type d'alerte (haute, moyenne ou basse). Le message est envoyé via l'API Microsoft Graph, et la réponse est vérifiée pour confirmer l'envoi réussi.

Gérer les Alertes : La fonction principale gerer_alertes interroge l'API Lookout pour recevoir les alertes actives. Pour chaque alerte récupérée, elle détermine le type d'alerte et utilise le GAIA pour trouver l'utilisateur correspondant sur Teams. Une fois l'utilisateur trouvé, elle lance une tâche asynchrone pour envoyer une relance appropriée basée sur le type d'alerte.

Exécution Asynchrone : Le script utilise asyncio pour gérer les tâches asynchrones, permettant ainsi d'effectuer des requêtes HTTP et d'envoyer des messages sur Teams de manière efficace et non bloquante.

Exécution du Script : Enfin, le script lance la fonction main qui démarre le processus de gestion des alertes en appelant gerer_alertes.

En résumé, ce script sert à automatiser la surveillance des alertes de sécurité via Lookout, recherche des utilisateurs spécifiques sur Teams selon leurs identifiants GAIA, et envoie des notifications personnalisées sur Teams pour informer ou demander des actions en fonction de la gravité des alertes détectées.

Suite à plusieurs réunions avec diverses équipes d'Engie, je suis en attente de leur feedback pour finaliser le développement du script. Une fois cette étape complétée, nous procéderons à sa phase de test avant son déploiement effectif.