

## Table des matières

<b>1. Introduction</b>	5
<b>2. Présentation de l'entreprise</b>	6
2.1. Les missions de l'entreprise	6
2.2. PSCHEEN et ses partenaires	6
2.3. Services de PSCHEEN	8
<b>3. Présentation du PROJET</b>	10
3.1. Le PROJET	10
3.2. Objectifs du PROJET	11
3.3. Méthodologie	11
<b>4. Analyse</b>	13
4.1. Analyse du système en place	13
4.1.1. Description du système de monitoring en place	13
4.1.2. Avant PROJET	15
4.2. Les outils	15
4.2.1. RG System	15
4.2.2. N8N	16
4.2.3. L'Écosystème Zyxel: Nebula, SecureReporter	16
4.3.4. WithSecure	17
4.4.5. CrashPlan	17
4.5.6. Microsoft 365	17
4.6.7. Synology	18
4.2. Configurations à implémenter	18
4.2.1. Pourquoi l'utilisation de N8N ?	18
4.2.2. Présentation du produit et de son utilisation	19
4.3. Les outils à mettre en place	21
4.3.1. Grafana	21
4.3.2. L'utilisation des API	21
<b>5. Réalisation</b>	23
5.1. Plan de réalisation	23
5.2. Réalisation RG System	23
5.2.1. Réalisation du workflow N8N	26
5.2.2. Affichage des données sur Grafana	27
5.3. Réalisation WithSecure	29
5.3.1. Réalisation du workflow N8N	30

5.3.2. Affichage des données sur Grafana .....	32
<b>5.4. Réalisation Microsoft 365 .....</b>	<b>33</b>
5.4.1. Réalisation du workflow N8N .....	34
5.4.2. Affichage des données sur Grafana .....	34
<b>5.5. Réalisation Synology C2 .....</b>	<b>35</b>
5.5.1. Réalisation du workflow N8N .....	35
<b>5.6. Réalisation Zyxel: Nebula, SecuReporter .....</b>	<b>36</b>
5.6.1. Réalisation du workflow SecuReporter .....	36
5.6.2. Configuration des types d'alertes sur l'interface SecuReporter .....	36
5.6.3. Réalisation du workflow N8N .....	37
5.6.4. Affichage des données sur Grafana .....	37
<b>5.7. Problèmes - Solutions .....</b>	<b>38</b>
<b>5.8. Résultat final .....</b>	<b>38</b>
<b>6. Conclusion.....</b>	<b>42</b>
<b>7. Bibliographie .....</b>	<b>44</b>

# 1. Introduction

De nos jours, le besoin de surveiller l'infrastructure informatique et les ressources réseau devient essentiel pour des entreprises en développement. Actuellement, toutes les entreprises sont équipées d'outils informatiques et de réseaux distants pour les plus importants.

Ce besoin est beaucoup plus important dans une entreprise qui fournit des services informatiques. Connaître l'état du matériel au sein de la société, mais également chez ses clients est primordial.

La performance optimale et la disponibilité continue de ces systèmes informatiques sont centrales pour les activités des clients; nécessitant une gestion efficace pour assurer une fiabilité sans faille. La dépendance d'une entreprise à la stabilité de son infrastructure est importante. Les dysfonctionnements, interruptions, et autres soucis techniques peuvent entraîner des pertes significatives et doivent donc être anticipés et prévenus lorsque ça arrive.

Dans ce rôle, l'administrateur système est responsable de la surveillance constante de l'infrastructure informatique des clients. Pour y parvenir, il utilise des outils avancés de gestion et de supervision qui permettent de suivre l'état de cette infrastructure en temps réel. Ces solutions logicielles offrent la possibilité d'être alerté automatiquement, via email ou SMS, dès l'apparition d'un incident. Cela permet d'intervenir rapidement pour résoudre les problèmes avant qu'ils ne deviennent perceptibles par les utilisateurs finaux.

La supervision de l'infrastructure informatique est donc un élément clé. Elle permet d'obtenir une vue d'ensemble sur le fonctionnement et les éventuels dysfonctionnements, tout en fournissant des données cruciales sur la performance globale du système.

Néanmoins, l'investissement nécessaire pour acquérir un système de gestion d'infrastructure informatique peut représenter un obstacle. Heureusement, des solutions *open source*<sup>1</sup>, à la fois performantes et économiques, existent. Lors de mon stage, j'ai eu l'opportunité d'implémenter et d'améliorer diverses infrastructures en utilisant les outils de supervision tels que N8N et RG System. Ces technologies offrent une adaptabilité et une efficacité répondant précisément aux besoins variés des infrastructures que j'ai eu à gérer.

---

<sup>1</sup> Conçu pour être accessible au public

## **2. Présentation de l'entreprise**

### **2.1. Les missions de l'entreprise**

PSCHEEN est une entreprise qui offre un service de gestion des systèmes informatiques pour ses entreprises clientes, extérieures au secteur de l'informatique. Leur prise en charge comprend tout, de l'acquisition et l'installation du matériel utilisé, à la maintenance et au support technique, en passant par la configuration des appareils. La société s'engage également à surveiller quotidiennement les processus de sauvegarde de données et un suivi de monitoring pour garantir leur bon déroulement et investiguer et résoudre tout incident qui pourrait survenir lors de ces opérations. Lorsque le domaine de la société n'est pas l'IT, PSCHEEN amène la solution à ces problèmes.

En sachant que ses clients ont des besoins uniques, PSCHEEN développe des solutions personnalisées qui s'adaptent à la taille et aux exigences spécifiques de chaque entreprise; offrant ainsi des conseils pertinents pour chaque situation. L'offre de PSCHEEN s'étend au-delà du matériel incluant la gestion de logiciels avec la fourniture de licences pour des programmes tels que SketchUp, Azure, Microsoft 365...

La société ne se limite pas à la fourniture et à la maintenance d'équipements informatiques tels que les ordinateurs et smartphones; elle prend également en charge la gestion du réseau des clients, proposant l'installation, la mise à jour, l'expansion et la réparation des infrastructures de réseau grâce à l'expertise de spécialistes en câblage.

Elle propose également un service d'outsourcing mettant à disposition des experts pour des remplacements, des missions de courte, moyenne ou longue durée ou pour renforcer des équipes.

Avec une expérience de plus de 20 ans dans le domaine, PSCHEEN se positionne comme un partenaire réactif et efficace, disposant d'une large présence géographique pour répondre rapidement aux besoins de ses clients. En effet, la société couvre actuellement les provinces de Liège et Namur, la région de Bruxelles et a également des clients au Luxembourg et dans le Nord de la France.

### **2.2. PSCHEEN et ses partenaires**

PSCHEEN est partenaire depuis de nombreuses années avec des sociétés de renommée mondiale telles que Microsoft, Iiyama (Écrans et autres outils physiques), Zyxel (Pare-feu), Lenovo (ordinateur, serveur et autres composants), SketchUp (Logiciel), Vectorworks (Logiciel), Synology (Serveur), With Secure (Logiciel)...

Ils travaillent ensemble pour trouver des solutions qui correspondent le mieux aux attentes des clients. Les partenaires établissent une relation de confiance permettant de leur trouver les meilleures solutions.

La société conserve son service de proximité et sa flexibilité qui font sa force depuis des années. C'est donc une réelle alliance entre les compétences d'une grande infrastructure et les services d'une entreprise à taille humaine.

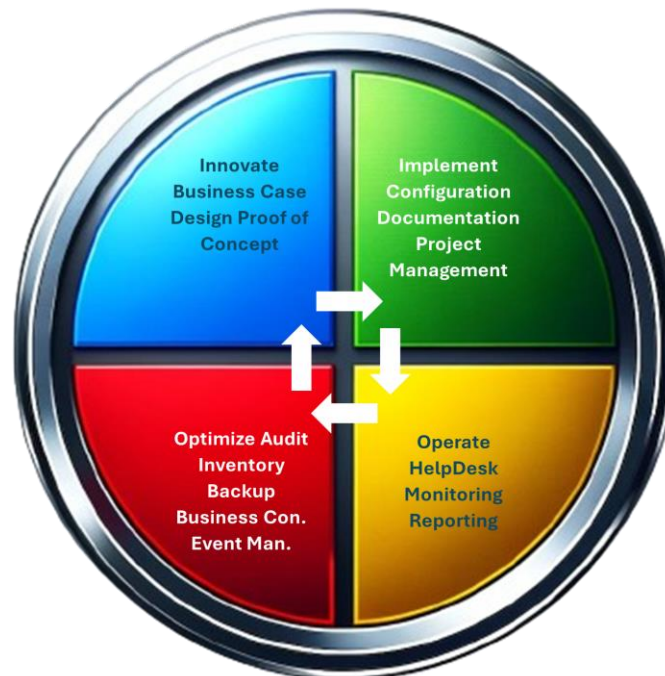
### Logos des produits utilisés par PSCHEEN



### Quelques références dans de nombreux domaines forgent l'image de la société



## 2.3. Services de PSICHEEN



*Figure 1: Services disponibles au sein de PSICHEEN*

PSICHEEN cherche continuellement des opportunités dans le domaine des Technologies de l'Information (Figure 1). Il anticipe les évolutions, conseille les clients sur les options et informe sur les innovations importantes du moment et du futur.

En bref, l'orientation dynamique et l'avenir sont au centre de PSICHEEN.

La principale activité est l'informatique. Avec ses quatre divisions, il fournit tout ce dont les clients ont besoin dans ce domaine, de l'architecture à la conception, la mise en œuvre et la gestion.

Il ajoute de la valeur grâce à :

- L'empathie envers les clients
- L'accompagnement des clients et si possible la proactivité
- La prise en charge maximale, selon les directives souhaitées

Il pense à l'avenir et offre ainsi ce qui est nécessaire maintenant et pour le futur.

L'expertise du groupe se retrouve dans les technologies suivantes :

- Routing et switching
- Wireless / Accès
- Gestion du réseau: mise en place, configuration, outil de monitoring et rapport
- Sécurité: Firewalls, contrôle d'accès et des structures hiérarchiques
- Stockage: préservation, protection et garantie de la haute disponibilité des données et du réseau

Les profils de clients de la société PSCHEEN sont:

- Des sociétés établies partout en Wallonie, à Bruxelles, dans le nord de la France et au Luxembourg
- Les bureaux d'architecture
- Tout type de PME qui requiert des besoins spécifiques en Informatique

Les certifications au sein de PSCHEEN:

- MS-900 : Pour des connaissances de base en cloud et pour améliorer la productivité et la collaboration entre les collaborateurs sur site, à distance et hybride
- AZ-900 : Pour les concepts cloud, l'architecture et les services Azure et la gestion et la gouvernance Azure
- Jamf PRO : Destiné aux professionnels informatiques qui souhaitent maîtriser la gestion et la sécurité des appareils Mac OS, iPad OS et iOS à l'aide de la plateforme Jamf Pro.

## 3. Présentation du PROJET

### 3.1. Le PROJET

PSCHEEN souhaite avoir une solution de monitoring fonctionnelle et pertinente qui est capable de surveiller divers types de données issues de multiples sources telles que les serveurs, pare-feu, antivirus, et routeurs. Il convient donc d'intégrer et de centraliser les différents logiciels utilisés au sein d'un système de monitoring unifié. Cette centralisation permettra non seulement d'optimiser la gestion de la sécurité, mais également de réduire significativement le temps nécessaire à la résolution des incidents.

Les données spécifiques seront soigneusement sélectionnées depuis les différentes solutions en place et centralisées via l'outil N8N. Cette approche permettra un suivi efficace à travers un dashboard ou une interface web simplifiée. Parmi les sources d'entrées d'information figurent RG System, Zyxel via la plateforme Nebula et SecuReporter, WithSecure, Crashplan, et Microsoft 365. La Figure 2 présente, en vert les sources de données, en rouge la centralisation et en mauve les données qui vont être observées dans nos dashboards ainsi que les tickets qui vont être générés. La partie "Traitement IA" est une partie à développer dans le futur et n'est pour le moment pas l'objectif visé.

Pour l'affichage et la gestion de ces données, j'ai proposé l'utilisation de Grafana, une solution que j'avais déjà expérimentée et testée durant mes études. Mon choix s'appuie sur sa capacité à fournir une visualisation claire et interactive des données, essentielle pour le monitoring efficace de notre infrastructure.

Ma contribution au projet va donc consister à implémenter et à configurer ce système de monitoring en tirant parti de mes compétences techniques et de mon expérience préalable avec Grafana. Mon rôle inclut également l'intégration fluide des différents services et produits sans perturber les systèmes existants. En optimisant l'utilisation des outils N8N et Grafana, je garantirai un système de surveillance robuste, personnalisable et facile à gérer, offrant ainsi une valeur ajoutée significative à notre gestion de la sécurité IT.



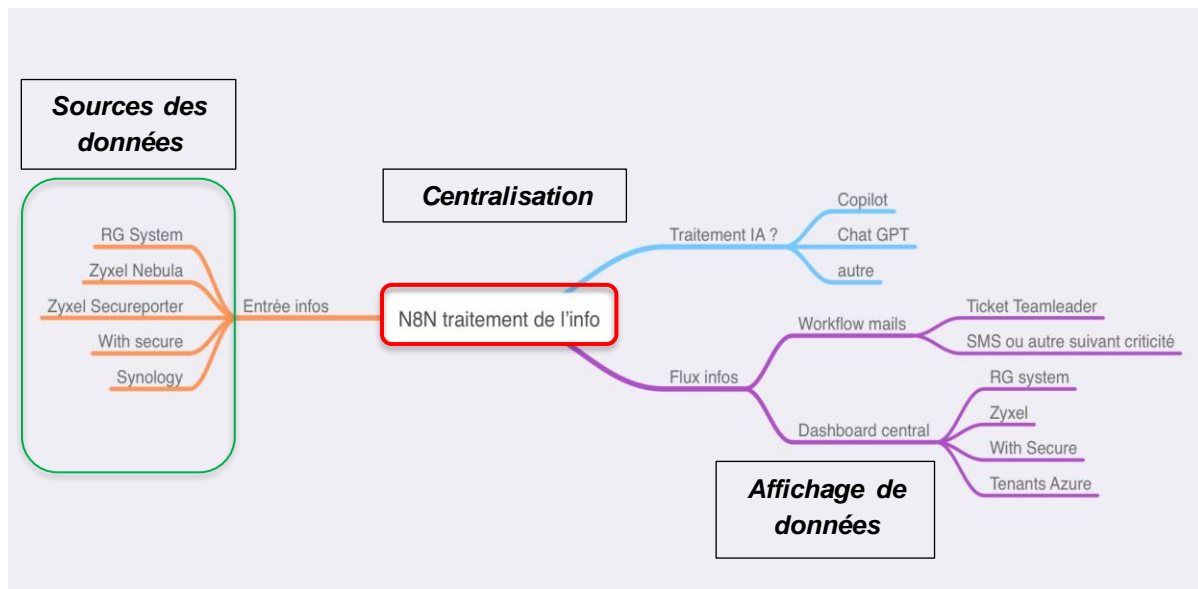


Figure 2: Diagramme représentant l'objectif du PROJET

## 3.2. Objectifs du PROJET

PSCHEEN travaille avec plusieurs marques comme RG System, WithSecure, Synology, Zyxel, et Microsoft. Il existe différentes plateformes de monitoring sur l'interface de ces solutions. L'objectif principal du stage est de concevoir et de mettre en œuvre une plateforme de monitoring centralisée qui intègre les diverses sources de données actuellement dispersées sur différentes interfaces web. Cette solution vise à optimiser le suivi des incidents chez les clients, à réduire le temps de réponse des employés, et à offrir une vue globale sur les différents outils utilisés, améliorant ainsi l'efficacité opérationnelle et la sécurité.

En intégrant toutes les sources de données dans une plateforme unique, le personnel de PSCHEEN pourra surveiller et gérer les incidents de manière plus efficace, réduisant ainsi les temps de réponse et d'intervention. L'optimisation des processus de monitoring et la diminution du recours aux interfaces multiples permettront à l'entreprise de réaliser des économies significatives en termes de ressources humaines et matérielles. De plus, une plateforme de monitoring centralisée permettra une détection plus rapide des incidents de sécurité, renforçant la capacité de PSCHEEN à protéger les données de ses clients contre les menaces potentielles.

## 3.3. Méthodologie

Dans cette section, je récapitulerai les découvertes et réalisations faites tout au long du projet. J'examinerai en détail les principaux résultats obtenus, mettant en lumière les solutions innovantes et les avancées significatives dans le domaine de la surveillance et de la gestion de l'infrastructure informatique.

Un autre aspect crucial est l'analyse de l'évolution personnelle. J'évaluerai l'impact du PROJET sur mon développement personnel en identifiant les compétences acquises, les défis surmontés et les leçons apprises, notamment en termes de créativité, de flexibilité et de résolution de problèmes.

J'étudierai également les défis rencontrés tout au long du projet. Cela inclut l'examen des obstacles survenus lors de la mise en œuvre du système de surveillance, l'analyse des solutions adoptées pour les surmonter et l'identification des opportunités d'amélioration pour l'avenir.

Une part importante du PROJET sera consacrée à l'évaluation des contributions et aux perspectives futures. J'évaluerai l'impact du projet sur l'entreprise et proposerai des recommandations pour l'extension et l'amélioration continue du système de surveillance, en mettant l'accent sur l'intégration de nouvelles sources de données et le développement de fonctionnalités avancées.

J'explorerai aussi les aspects du métier d'administrateur système. Cela implique d'examiner les expériences acquises dans le cadre des tâches de maintenance et de support technique en identifiant les compétences développées et en évaluant leur pertinence dans un contexte professionnel.

Un point central sera de souligner l'importance du système de surveillance centralisé dans la gestion efficace des infrastructures informatiques d'une entreprise. Je mettrai en lumière les avantages obtenus par PSCHEEN grâce à la solution proposée.

Je réfléchirai également sur l'acquisition et le développement de compétences techniques tout au long du projet en identifiant les domaines où j'ai réalisé des progrès.

Enfin, je proposerai des recommandations stratégiques pour l'amélioration continue du système de surveillance, en tenant compte des enseignements tirés de l'expérience et des perspectives d'évolution dans le domaine de la cybersécurité.

## 4. Analyse

### 4.1. Analyse du système en place

#### 4.1.1. Description du système de monitoring en place

Comme déjà présenté, PSCHEEN assure la gestion des parcs informatiques de ses clients, leur configuration et l'installation des machines nécessaires en fonction des besoins. En plus de ces tâches, pour les clients sous un contrat "premium", PSCHEEN s'occupe du monitoring des NAS<sup>2</sup> (Synology ou Qnaps) chez ses clients. Les NAS sont configurés afin de réaliser les sauvegardes nécessaires de manière quotidienne. Lorsque cette tâche est effectuée, un mail avec le statut du NAS est envoyé vers une boîte mail backup dédié à cette tâche. Un fichier Excel (Figure 3) est créé avec le statut de la sauvegarde à partir des mails traités par l'outil N8N via des workflows (Figure 4). Cet outil envoie également un ticket sur la plateforme Teamleader (Figure 5), pour qu'en cas d'erreur de sauvegarde, les techniciens puissent la corriger manuellement.

Backup_status	receivedDateTime	subject
ERREUR	2022-07-12T01:00:22Z	ALERTE PSHSRVNAS01 Network backup - La tâche BU_Ext a échoué sur PSHSRVNAS01
OK	2022-07-12T03:16:57Z	PSHSRVNAS05 172.16.10.12 La tâche Synology C2 cloud backup - Synology C2 a été effectuée avec succès sur pshsrvnas05
OK	2022-07-12T01:38:31Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-11T01:37:08Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-10T01:37:18Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-09T01:38:07Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-08T01:43:44Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-06T01:37:10Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-05T01:37:11Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès
OK	2022-07-04T01:45:26Z	ALERTE PSHSRVNAS01 Active Backup for Microsoft 365 - La tâche de sauvegarde [Pscheen.com] sur [PSHSRVNAS01] a été effectuée avec succès

Figure 3: Journal des sauvegardes NAS

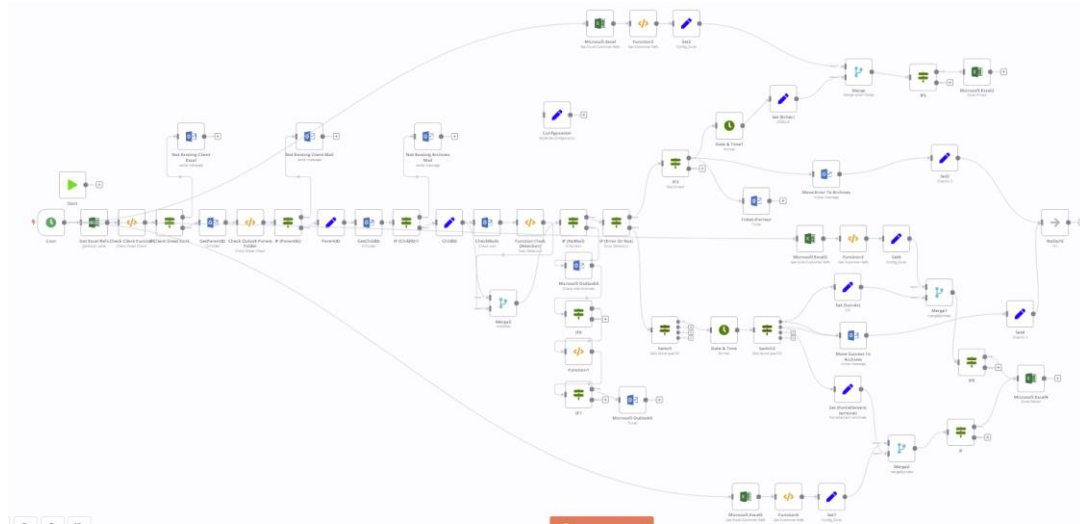


Figure 4: Workflow, tâches automatisées via N8N

<sup>2</sup> Un serveur de stockage en réseau

Tickets								
Q Rechercher...		Sélectionner un segment						
Identifi... ↓	Statut	Client	Sujet	Date de création	Entreprise	Boîte de réception	Temps consacré	Responsabilité
17228042	Nouveau	SPRL Atelier D'architecture ...	FW: AAdd	26/03/2024 - 08:57		helpdesk@pscheen....		
17227943	Nouveau	Timothy Graffart	TR: Test de transfert de mail	26/03/2024 - 08:46	PSCHEEN	helpdesk@pscheen....		
17226236	Nouveau	SPRL Studio L Architects	Fwd: Nouveau collaborateur	25/03/2024 - 18:43		helpdesk@pscheen....		Jordan ALLIANCE
17224793	Nouveau	Claude Neuberg	Problème de synchronisation de mon...	25/03/2024 - 15:38	ATRIUM ARCHITECTES	helpdesk@pscheen....		Profiles PSCHÉEN
17224086	Nouveau	AP Gustin SPRL	Création compte 365	25/03/2024 - 14:34		helpdesk@pscheen....		Philippe DUCHESNE
17165257	Nouveau	Alain Ernotte	"Nous récupérons les informations au...	14/03/2024 - 14:14	Alias Consult SRL	helpdesk@pscheen....		Timothy GRAFFART

Figure 5: Système de ticketing Teamleader

Les autres appareils comme les ordinateurs et les serveurs des clients sont monitorés grâce à l'outil RG System qui a sa propre interface de ticketing (Figure 6). Des agents RG System <sup>3</sup>sont installés sur la plupart des appareils; configurant la récupération des informations de type OS, version, IP, disk, valeur SNMP (serveur) etc. Ils peuvent les afficher à tout moment, créer des tickets en cas d'erreur sur les appareils ou alors créer une topologie des appareils connectés sur le réseau.

Criticité	Numéro de ticket	Statut	Action	Acquitté	Nœud	Agent	Date	Titre
	TIVSMDXCBSW3			<input type="checkbox"/>	WKS	PC-JULIE	26/03/2024 10:20	Défaillance matérielle : Statut Smart - WDC WD5000AAKX-07U6A...
	TIVSKHHZCDC0			<input type="checkbox"/>	Serveurs	malagneex02	26/03/2024 06:11	Trafic réseau trop faible - 30 minutes - 200 kbit/s
	TIVSJTMBSKN4			<input type="checkbox"/>	Serveurs	Malagneex01	26/03/2024 04:45	Trafic réseau trop faible - 30 minutes - 200 kbit/s
	TIVSJ7DPQ9KW			<input type="checkbox"/>	Serveurs	PRBSRVNAS02	26/03/2024 03:24	Valeur Snmp - Raid Free size (octets) - 15 minutes

Figure 6: Système de ticketing RG System

WithSecure<sup>4</sup>est utilisé comme un *EndPoint Protection*<sup>5</sup>, chez les clients et aussi en interne. Il est possible d'accéder aux informations sur le statut du firewall, de l'antivirus ou alors d'autres informations sur les mises à jour. WithSecure génère des alertes (Figure 6) qui sont envoyées par mail aux administrateurs lorsqu'il détecte des incidents de sécurité.

Pour terminer, PSCHÉEN utilise Nebula, qui est la plateforme de Zyxel, pour gérer la configuration (faite en amont en atelier) pour ses installations de hardware<sup>6</sup>, que ce soit pour des points d'accès ou des pare-feu. Ensuite, il les installe chez les clients. Pour le moment, il n'existe pas de suivi ni de notification pour cette partie, au sein de l'entreprise.

<sup>3</sup> <https://www.rgsystem.fr/>

<sup>4</sup> <https://www.withsecure.com/fr/home>

<sup>5</sup> Une extrémité d'un canal de communication.

<sup>6</sup> Élément matériel d'un système informatique.

Heure	Gravité	Source	Entreprise	Cible	Description	Reconnu	Menu
07/23/22							
il y a 6 heures 27 mars 2024, 07:01:23	Action requise	Analyse planifiée ou déclenchée localement/à distance Analyse manuelle	Chorale l'Arche de Noah	DESKTOP-10RQ557	« riskware » a été détecté dans « mailpv.exe » et aucune action n'a été effectuée	Aucun(e)	...
il y a 6 heures 27 mars 2024, 06:37:23	Attention	Navigation basée sur la réputation Protection de la navigation	Chorale l'Arche de Noah	DESKTOP-10RQ557	La page Web « hoxxps://gounlimited.to » a été bloquée en raison d'une réputation jugée suspecte.		Confirmer Afficher tous les événements ciblés Afficher des événements similaires
il y a 14 heures 26 mars 2024, 22:43:03	Action requise	Analyse planifiée ou déclenchée localement/à distance Analyse manuelle	MATAGNE HODY	MATAGNEWKS02	« riskware » a été détecté dans « IObit Driver Booster 8.0.2.189.exe » et aucune action n'a été effectuée		Mettre en quarantaine le fichier infecté Exclure le fichier par SHA1

Figure 7: WithSecure Interface des événements de sécurité

### 4.1.2. Avant PROJET

Le système en place réalisait les tâches demandées, mais sans permettre une vision globale. Les employés devaient consulter chaque logiciel et aller chercher dans chaque fichier de sauvegarde les alertes et les résultats des différentes tâches. De plus, pour chaque client, il existait un fichier et une interface différents; il était donc assez compliqué de trouver les informations pertinentes et les alertes précisant où intervenir en cas d'urgence.

Les systèmes de monitoring qui avaient une absence de suivi de sauvegarde ou d'incident pouvaient engendrer la perte des données, empêcher le bon fonctionnement du parc informatique et mener jusqu'à la perte d'un client. Nous ne pouvions jamais surveiller à cent pour cent le système et il restait toujours un léger pourcentage de perte acceptable pour les parcs sous contrôle de PSCHEEN. Il ne fallait cependant jamais négliger l'importance d'un bon système de monitoring en place, qui fonctionnait de façon efficace en facilitant les tâches et en diminuant au maximum l'intervention humaine.

## 4.2. Les outils

Patrick Scheen a progressivement intégré diverses solutions technologiques chez PSCHEEN afin de répondre à une variété de besoins opérationnels, y compris le monitoring sans, toutefois s'y limiter uniquement. Avant mon intégration en tant que stagiaire, une sélection de ces outils avait été mise en place pour faciliter la gestion des infrastructures informatiques et la sécurité des systèmes. Voyons maintenant en détail les solutions mises en œuvre.

### 4.2.1. RG System

RG System est notre solution phare dans le domaine de la supervision et de la gestion informatique. Avec sa plateforme tout-en-un, elle répond efficacement aux besoins des entreprises en matière de surveillance, de sécurité et de support à distance.

Grâce à son architecture entièrement web, RG System offre une gestion à distance des ressources informatiques, sans contraintes géographiques. Certifiée ISO 27001, cette solution assure une gestion sécurisée des données, conforme aux standards internationaux de sécurité.

Sa capacité à offrir un monitoring complet des infrastructures IT et à paramétrer des alertes personnalisables est un atout majeur pour anticiper les problèmes et assurer une continuité de service.

L'API<sup>7</sup> ouverte de RG System permet son intégration avec des outils d'automatisation comme N8N. Cette synergie facilite le développement de workflows personnalisés, réduisant ainsi la charge de travail manuel et améliorant l'efficacité des processus de surveillance.

#### 4.2.2. N8N

N8N est un puissant outil d'automatisation de workflows, offrant une distribution fair-code, accessible et personnalisable. Grâce à son architecture basée sur les nœuds, il permet de connecter divers outils et services au sein d'un même workflow.

Sa capacité à s'intégrer avec plus de 200 services et applications différents rend possible l'automatisation de tâches complexes, contribuant ainsi à une plus grande efficacité opérationnelle.

La simplicité d'utilisation de N8N, avec des options de démarrage flexibles et une version cloud, en fait un choix idéal pour les utilisateurs de tous niveaux techniques.

Dans nos projets, N8N joue un rôle crucial dans l'automatisation des processus en récupérant des données via des API depuis diverses plateformes. Cette capacité à orchestrer et à automatiser les interactions entre différents environnements permet d'améliorer la précision et la réactivité des systèmes de surveillance et de gestion IT.

#### 4.2.3. L'Écosystème Zyxel: Nebula, SecureReporter

Zyxel se présente comme un fournisseur de solutions réseau, avec une gamme étendue de produits conçus pour établir et sécuriser les connexions internet des entreprises. Cette société développe des dispositifs et des logiciels qui visent à améliorer la performance du réseau tout en le gardant sécurisé contre les menaces extérieures. Les solutions Zyxel s'adressent aux besoins variés des petites et moyennes entreprises ainsi qu'aux grandes organisations, en proposant des équipements réseau, des solutions de sécurité et de la connectivité cloud.

Le Nebula Control Center (NCC) est une plateforme de gestion réseau basée sur le cloud qui permet aux administrateurs de configurer, surveiller, et gérer leurs dispositifs réseau de manière centralisée. Cette solution s'oriente vers la facilitation du déploiement et de la maintenance du réseau grâce à des fonctionnalités telles que la configuration automatique et la gestion à distance. Le NCC se distingue par son interface intuitive et par sa capacité à offrir une vue d'ensemble claire des réseaux d'entreprise, facilitant ainsi la prise de décisions et l'optimisation des ressources.

SecuReporter est une plateforme d'analyse et de reporting qui se concentre sur la sécurité du réseau. Elle fournit aux administrateurs des informations détaillées sur les activités réseau, les menaces détectées et les vulnérabilités potentielles. En analysant le trafic réseau, SecuReporter aide les entreprises à identifier et à réagir rapidement aux incidents de sécurité; offrant ainsi une couche supplémentaire de protection. Les rapports générés par la plateforme permettent une évaluation précise de la posture de sécurité du réseau et facilitent la conformité aux normes réglementaires.

---

<sup>7</sup> Interface de programmation d'application

#### 4.3.4. WithSecure

WithSecure fournit une série de solutions de cybersécurité ciblant les besoins divers des entreprises dans le numérique. Ce logiciel offre un service de Monitoring, donnant accès à une surveillance de sécurité continue, visant à rendre la sécurité de haut niveau plus accessible. PSCHEEN utilise leur produit "Elements Endpoint Protection and Response" (EDR) qui est conçu pour renforcer la détection des menaces et la protection des données. Il existe d'autres produits comme le service "Managed Detection and Response" (MDR), qui agit comme une extension de l'équipe de sécurité interne, améliorant les capacités à prévenir et répondre aux attaques.

Avec une orientation vers la préparation et la réponse aux incidents, WithSecure aide les entreprises à se prémunir contre les cyberattaques grâce à des solutions avancées.

Les mises à jour régulières des solutions logicielles de WithSecure garantissent aux clients de bénéficier des protections les plus récentes contre les menaces. En offrant une gamme de services allant de la protection des points d'extrémité à la réponse aux incidents et la gestion des menaces de ransomware, WithSecure vise à fournir une couverture complète pour naviguer en toute sécurité.

WithSecure propose également des ressources pour prévenir et récupérer des attaques de ransomware. Cette société participe activement à des conférences et événements sur la cybersécurité. Avec PSCHEEN, j'ai eu l'occasion de participer à un de leurs événements appelé "Cyber Tour".

#### 4.4.5. CrashPlan

Crashplan est un outil de sauvegarde flexible permettant à l'entreprise de faire des sauvegardes sur des serveurs NAS, sur des plateformes cloud ou vers d'autres espaces de stockage peu communs et privés. Il se distingue par sa facilité d'utilisation, sa sécurité renforcée et sa capacité à fonctionner en arrière-plan de manière transparente pour l'utilisateur.

Pour les entreprises, les avantages sont:

- Une sauvegarde continue des données
- Des politiques de sauvegarde personnalisée et adaptée aux besoins
- L'adaptation aux sauvegardes de volumes de données variées
- La possibilité d'ajuster les paramètres de sauvegarde comme la fréquence et le type de données sauvegardées permettant à PSCHEEN d'offrir un service adapté aux besoins de ces clients.

Le service offre aussi une protection en chiffrant les données avant l'envoi sur le cloud ou sur d'autres espaces de stockage, tout en soutenant leur conformité réglementaire.

#### 4.5.6. Microsoft 365

Du point de vue de Microsoft 365, le monitoring et la récupération des alertes sont des tâches indispensables. Microsoft propose de nombreux services et applications essentiels pour les entreprises. PSCHEEN, en tant que partenaire, utilise au maximum

ces ressources pour la messagerie, le stockage “Sharepoint”<sup>8</sup> et pour des applications de collaboration. Les alertes venant du tenant Microsoft 365 peuvent signaler des événements tels que des tentatives de phishing, des fuites de données, des violations de politique de sécurité et des systèmes compromis.

Suivre les messages générés par 365 apporte une réactivité immédiate aux incidents de sécurité. Cela permet d'intervenir rapidement en cas de problème et de limiter les dégâts chez les clients.

Il est important que les bonnes personnes soient informées et prêtes à agir. La présence d'une configuration pour un système d'alerting et de monitoring joue un rôle crucial.

#### 4.6.7. Synology

Du point de vue de la sauvegarde et de la récupération des données, Synology C2 Backup offre des fonctionnalités essentielles pour les entreprises, notamment pour PSCHEEN en tant que partenaire. Synology propose une gamme de solutions de stockage et de sauvegarde qui sont largement utilisées pour garantir la sécurité des données et assurer la continuité des activités.

En exploitant pleinement les ressources offertes par Synology C2 Backup, PSCHEEN peut sécuriser efficacement les données de ses clients, notamment en ce qui concerne la sauvegarde des données critiques, la protection contre la perte de données et la reprise après sinistre.

## 4.2. Configurations à implémenter

### 4.2.1. Pourquoi l'utilisation de N8N ?

Lorsqu'on parle d'outil d'automatisation, il existe quelques solutions très connues et puissantes (Zapier, N8N, Jira, Integrity etc.) L'avantage de N8N est que cette solution est totalement opensource et gratuite sans abonnement ou autre. Il est possible de l'installer localement pour éviter de voir exposées les données internes sur internet. Il existe aussi un cloud où nous pouvons gérer nos workflows<sup>9</sup>. Le choix de cet outil était déjà fait avant mon arrivée chez PSCHEEN, car ils l'utilisent aussi pour gérer les backups des serveurs clients. La version était très ancienne (1.0.0 par rapport à la version récente qui est 1.29). J'ai créé un docker-compose<sup>10</sup> avec la dernière version de l'outil, mais implémenté mes solutions dans la précédente, car je ne pouvais pas mettre le système de monitoring hors ligne durant mon utilisation.

J'ai réalisé des recherches pour des solutions équivalentes à N8N de mon côté, afin de mieux comprendre comment l'automatisation se fait via ces outils. J'ai analysé les solutions comme Zapier, Jira, Integrity. J'ai remarqué que, ce qui fait la puissance de N8N est le fait de pouvoir créer des scripts dans différents langages de programmation comme JavaScript et Python. Un autre avantage est le fait de pouvoir héberger l'outil dans un docker en interne, ce qui évite d'exposer les données en ligne. N8N a déjà des nœuds adaptés pour communiquer avec plusieurs applications disponibles qui

---

<sup>8</sup> Un composant Office 365 pour gérer et organiser le contenu (fichiers, images, vidéos etc.), le partager et y accéder en ligne.

<sup>9</sup> Processus par lequel un travail est accompli.

<sup>10</sup> Outil destiné à définir et exécuter des applications Docker à plusieurs conteneurs.



facilitent sa configuration pour les utilisateurs. J'ai donc trouvé que c'était un bon choix pour réaliser le système de monitoring centralisé via l'utilisation de N8N.

#### 4.2.2. Présentation du produit et de son utilisation

Dans la colonne de gauche de la Figure 8 nous allons observer les éléments suivants:

- **Workflows:** C'est la partie la plus utilisée de cet outil. Les workflows vont servir à automatiser les tâches de façon intelligente.
- **Templates:** C'est l'espace dédié aux utilisateurs de la communauté qui partagent librement leurs workflows utiles pour aider et apporter des idées aux autres utilisateurs.
- **Credentials:** Utilisé souvent pour enregistrer les crédeniels. Vu que le but est d'automatiser les tâches répétitives, les crédeniels vont devoir être insérés à plusieurs reprises et, une fois enregistrés, N8N va pouvoir se connecter aux différentes ressources possibles en utilisant ces données.
- **Variables:** Cet espace nous sert à créer des variables globales qu'on peut aller chercher et utiliser dans plusieurs workflows.
- **All executions:** C'est un historique des dernières exécutions des workflows réalisées.

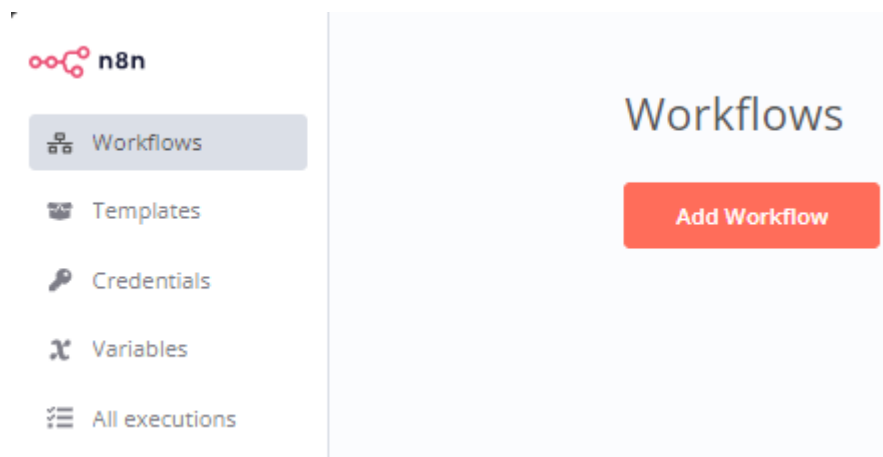


Figure 8: Interface N8N

Voici un exemple de Workflow (Figure 9) pour mieux comprendre sa fonctionnalité. Les différents carrés sont appelés des nœuds. Ces nœuds vont communiquer avec différentes ressources, traiter les données, exécuter du code JS ou Python de façon automatisée afin de pouvoir manipuler et envoyer les données vers la destination souhaitée.

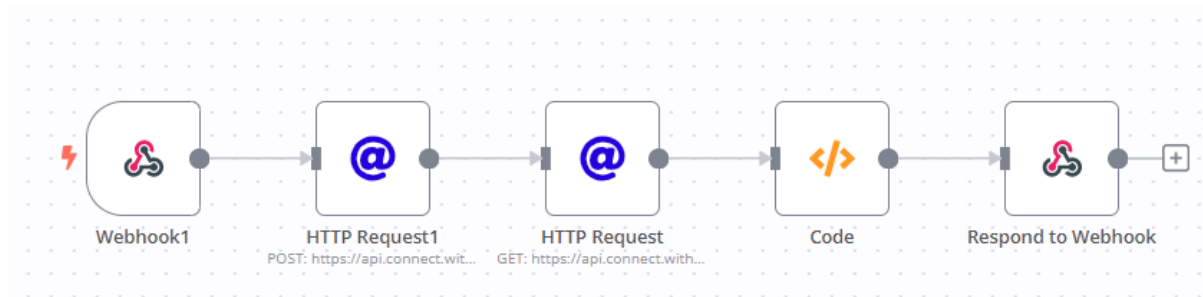


Figure 9: Exemple de workflow

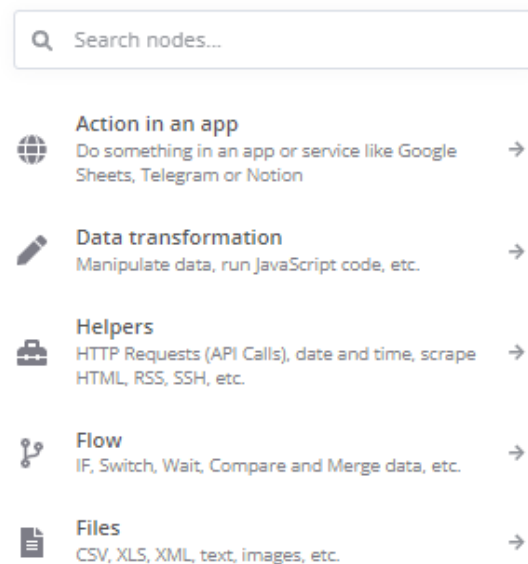


Figure 10: Panel pour les ajouts de nœud

Voici les différentes options possibles:

- **Action in an app:** Nous avons différents nœuds préconfigurés pour des applications spécifiques et souvent utilisées par les utilisateurs. Exemple: Dropbox, Github, Linkedn, différentes bases de données.
- **Data transformation:** Souvent utilisé pour la transformation de données pour créer des tableaux, transformer en fichier JSON<sup>11</sup>, manipuler les dates et heures, utiliser des scripts Java et Python.
- **Helpers:** Pour les applications qui ne fournissent pas de nœud préconfiguré, il existe des helpers pour pouvoir récupérer les données via les API<sup>12</sup> avec des requêtes HTTP Request<sup>13</sup>.
- **Flows:** Les flows sont utilisés pour comparer des données et faire une sélection de celles-ci parmi d'autres pour les transmettre et faire continuer le workflow.

<sup>11</sup> JavaScript Object Notation est un format d'échange de données en texte lisible.

<sup>12</sup> Interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

<sup>13</sup> Protocole qui permet de récupérer des ressources telles que des documents HTML

- Files: Lit les PDF, fichiers, calendriers et tout autre type de fichier et extrait les informations. Il peut aussi écrire dans ces fichiers pour stocker les données.

## 4.3. Les outils à mettre en place

### 4.3.1. Grafana

Grafana est une plateforme open source de surveillance et d'analyse de données. Ce logiciel est souvent utilisé pour visualiser et analyser une quantité importante de données en temps réel ou depuis des sources de données. Il est particulièrement reconnu pour sa puissance en monitoring des infrastructures informatiques. Il possède des tableaux de bord (dashboard) dynamiques qui peuvent être personnalisés et adaptés en fonction des besoins de ses utilisateurs. D'autres logiciels alternatifs sont Zabbix, Solarwinds, Splunk etc.

Il y a plusieurs avantages qui m'ont poussé à faire ce choix d'outil pour l'affichage de notre dashboard, comme la personnalisation et la centralisation de différentes sources de données, le filtrage de données facilitant l'utilisation de l'outil pour ses utilisateurs, des alertes intégrées, des plugins<sup>14</sup> disponibles (surtout en format JSON) et une documentation solide et une communauté active. Grafana peut être configuré pour récupérer les données venant de N8N, les traiter et les afficher. L'autre choix d'affichage, proposé par mon maître de stage, était de réaliser une interface web. Il décidera finalement de confier cette tâche plus tard, à un développeur. Ces avantages font de Grafana un outil intéressant pour notre système de monitoring.

Il faut préciser que pour pouvoir réaliser le dashboard sur Grafana, on fait tourner l'outil qui est hébergé en local dans un docker-compose<sup>15</sup> qui est installé sur une machine Ubuntu<sup>16</sup> hébergée sur un serveur ESXi<sup>17</sup>. J'ai déployé la machine et installé l'outil en local pour pouvoir profiter de notre serveur que nous avons déjà en place ici dans les bureaux et pour ne pas exposer des informations sur internet dans des clouds<sup>18</sup> ou bases de données.

### 4.3.2. L'utilisation des API

Les utilisateurs envoient des requêtes vers un serveur en indiquant une action souhaitée (récupération et/ou modification des données, opération spécifique...). En retour, le serveur répond à la demande et réalise la tâche nécessaire. Les informations retournées par l'utilisation des API sont souvent en format JSON ou XML. Par contre, la communication se fait par des protocoles HTTP, REST, SOAP etc. Dans notre cas, nous allons souvent utiliser les requêtes HTTP.

Pour le monitoring des backups, PSCHÉEN utilisait des scripts afin de récupérer les différents logs et alertes via les boîtes mail. Cependant, pour améliorer la surveillance, j'ai mis l'accent sur l'utilisation des API et la maximisation de l'automatisation grâce à celles-ci. Si, pour une raison ou une autre, les API ne sont pas disponibles ou coûtent

---

<sup>14</sup> Logiciel conçu pour être greffé à un autre logiciel à travers une interface prévue à cet effet.

<sup>15</sup> Outil destiné à définir et exécuter des applications Docker.

<sup>16</sup> Système d'exploitation.

<sup>17</sup> Serveur qui héberge des machines virtuelles.

<sup>18</sup> Espace de stockage distant.

trop cher pour la société, je continuerai alors à générer des alertes par mail et à les traiter de cette façon-là.

L'utilisation des API a été proposée par mon maître de stage Patrick SCHEEN, car plusieurs solutions utilisées nous proposent des interactions via les API.

Les API sont des moyens de communication très puissants avec les applications, car elles peuvent:

- Permettre une intégration facile avec d'autres systèmes ;
- Offrir une grande flexibilité dans la configuration ;
- Rendre accessible des données en temps réel ;
- Standardiser les interactions entre différents systèmes.

L'utilisation des API maximise les capacités de notre outil N8N. Cette technologie offre à notre équipe la capacité de créer des systèmes de surveillance robustes qui peuvent s'adapter à nos besoins.

## 5. Réalisation

### 5.1. Plan de réalisation

Pour commencer mon PROJET, j'ai élaboré un plan en me basant sur la Figure 2, détaillant les différentes étapes à suivre pour chaque workflow. Les étapes du plan sont les suivantes :

1. Recherche de la documentation API ;
2. Création des token d'authentification<sup>19</sup> ;
3. Test des clés API ;
4. Réalisation du workflow sur N8N ;
5. Affichage des données sur Grafana.

En suivant le plan, pour chaque source précédemment sélectionnée (Figure 1), j'obtiens un workflow automatisé sur N8N et un dashboard sur Grafana. N8N exécute les workflows lorsqu'ils sont déclenchés par un appel de Grafana ou périodiquement en fonction de nos besoins. Au total, 18 workflows ont été réalisés. Je vais donc présenter, dans ce chapitre, les workflows essentiels pour chaque source.

Les workflows essentiels incluent ceux qui couvrent les principales fonctionnalités du système de monitoring, que ce soit par l'utilisation des API ou par le tri et la récupération des alertes via les boîtes mail. Ils ont été choisis, car ils représentent les aspects cruciaux du monitoring, garantissant une surveillance efficace et réactive. Ces workflows sont cruciaux, car ils permettent une gestion optimale des alertes et une intégration fluide avec nos outils existants.

L'ordre de présentation des workflows est basé sur leur fréquence d'utilisation et leur importance dans notre infrastructure ainsi que celle de nos clients. En commençant par les workflows les plus utilisés et les plus critiques, nous assurons que les aspects les plus vitaux du système de monitoring sont bien couverts et compris.

### 5.2. Réalisation RG System

RG System, comme déjà expliqué ([4.2.1](#)), est l'outil qui a la plus grande importance dans notre infrastructure. La tâche qu'elle traite est de servir d'inventaire et récolter les données SNMP<sup>20</sup>.

RG System fonctionne de la façon suivante. Des agents RG sont installés et configurés dans chaque workstation<sup>21</sup> et serveur. Ces agents sont configurés pour récupérer des informations sur le trafic réseau, l'espace disque ou une défaillance matérielle. Lorsque les agents détectent ce genre d'événements, ils génèrent un ticket (Figure 11) qui peut être consulté sur l'interface de ticketing RG System comme présenté ci-après.

---

<sup>19</sup> Une forme d'authentification qui permet à un utilisateur d'accéder à un service en ligne, une application ou un site web sans qu'il n'ait à ressaisir ses identifiants.

<sup>20</sup> Simple Network Management Protocol est un protocole destiné au transfert d'informations de gestion sur des réseaux.

<sup>21</sup> Poste de travail




 <b>MRFSRVNAS</b>	09/04/2024 13:02	Valeur Snmp - Raid Free size (octets) - 15 minutes
 <b>TCLESXI01</b>	09/04/2024 13:00	Trafic réseau trop faible - 30 minutes - 200 kbit/s
 <b>MATAGNESRVTS01</b>	09/04/2024 12:57	Mémoire pleine - 1 heure - 95%

Figure 11: Exemple de tickets générés par RG System

L'objectif principal de notre workflow va être de récupérer ces tickets pour pouvoir les suivre et réagir en temps réel depuis notre système de monitoring.

Pour cela, j'ai commencé par consulter la documentation de RG System. Celle-ci était assez claire et il existait plusieurs API intéressantes comme lister les tickets d'un agent ou d'un appareil réseau. Cependant, ce qui m'intéressait était de récupérer l'ensemble des tickets pour l'organisation, car PSCHEEN traite le suivi de multiclients avec chacun sa propre infrastructure.

J'ai alors décidé de contacter le support de RG System pour avoir des renseignements des API qui pouvaient être utiles. Celui-ci m'a redirigé vers un autre lien où était expliquée l'utilisation des API. J'y ai trouvé la requête dont j'avais besoin, mais j'ai d'abord dû en tester plusieurs pour comprendre quels types et quelles quantités de données sont retournées. J'ai appris à maîtriser de mieux en mieux l'utilisation des API en testant les différentes possibilités avec RG System.

Avant de lancer une requête HTTP et avoir une réponse, il faut générer un token d'authentification (Figure 12). Cela est aussi fait via une API et fonctionne de la façon suivante :

GET

/api/auth Try to authenticate the user and if successful expose the user summary

The authentication token required for authenticated api call will be provided in this summary

Parameters

Name	Description
<b>userName</b> * required string (query)	The user login name <input type="text" value="matthieu.huleux@rg-systemes.com"/>
<b>password</b> * required string (query)	The user password <input type="password"/>
<b>apiKey</b> * required string (query)	The key referring to an api client allowed by api owner to process requests <input type="text" value="81b10f214ec"/>

Execute

Clear

Figure 12: Exemple de récupération de la clé API

Il faut:

1. D'abord contacter le support et demander une clé d'accès pour générer le token d'authentification.
2. Ensuite, utiliser l'API api/auth disponible dans la documentation.

3. Remplir les champs par l'utilisateur, le mot de passe et la clé d'accès récupérée par le support (Figure 12).
4. Une fois les tokens créés, on peut les utiliser via le doc API de RG.

Remarque: Le compte qui recevra cette clé d'API devra obligatoirement être Gestionnaire de compte dans le dashboard RG System.

Cette commande me retourne un token que je vais pouvoir utiliser pour lancer les requêtes HTTP et récupérer les informations dont j'ai besoin.

La prochaine API qui va m'être utile est structurée de cette manière:

<https://api.rg-supervision.com/api/{{token}}/ticket/list/{node}>

L'API nous demande de remplir les champs entre les accolades. Dans la partie token (orange), j'insère le token récupéré depuis l'API d'authentification. Le node (rouge) est le nœud pour lequel je veux récupérer la liste des tickets. Je dois insérer l'ID de l'organisation PSCHEN, car c'est le nœud "parent" qui va me servir à récupérer tous les tickets de nos clients.

Avant d'utiliser cette requête HTTP dans N8N, je teste d'abord simplement en la copiant dans mon navigateur web et en exécutant la recherche dont voici le résultat (un seul ticket retourné parmi la liste):

```
"result": {
  "code": 200,
  "text": "OK",
  "apiCode": 0,
  "message": "Success"
},
"data": {
  "tickets": {
    "fe194080-f66d-11ee-be2f-ff4a246e82f4": {
      "creationDate": "2024-04-09T12:37:57+00:00",
      "status": "new",
      "isAcquitted": false,
      "isMuted": false,
      "title": "Valeur Snmp - Raid Free Size (Octets) - 15 minutes",
      "criticality": "critical",
      "displayId": "TIVWY9ABACG0",
      "originalId": "TIVWY9ABACG0",
      "customId": null,
      "comment": null,
      "raiseCount": 1,
      "nodeId": 141497,
      "nodeName": "Serveurs",
      "isRecovered": false,
      "isClosed": false,
      "isOpen": false,
      "isOpened": false,
      "deletedAttachment": false,
      "id": "fe194080-f66d-11ee-be2f-ff4a246e82f4",
      "detectionContext": 2,
      "source": 35926302,
      "agentId": "PP01-A6-H0",
      "agentName": "PSH\\PSHSRVNAS05",
      "agentType": "E"
    }
  }
}
```

Figure 13: Données retournées par le serveur

Sur la figure 13, j'observe que les données ont été retournées en JSON. Parmi ces données, je regarde quelles sont les informations qui peuvent être intéressantes pour un cas de monitoring.

Voici la liste des éléments qui peuvent être récupérés et leur pertinence:

1. creationDate: La date de la création de tickets est très importante pour le suivi des tickets.

2. isAcquitted: Représente le statut d'acquisition. J'ai sélectionné cet élément pour pouvoir filtrer lors de l'automatisation sur N8N. Les tickets déjà parcourus auront le statut "Acquitté" et ne seront plus visibles dans notre dashboard.
3. title: La description de la génération du ticket. C'est ici que nous avons l'information sur l'erreur et donc le traitement débute en tenant compte de cette zone.
4. Criticality: Information sur le niveau de criticité.
5. Id: Est simplement l'ID du ticket pour le retrouver facilement sur l'interface de RG System si on a besoin de plus d'information.
6. nodeName: Indique si l'appareil est un workstation ou un serveur.
7. agentName: Indique le nom de l'appareil sur le réseau pour l'identifier et intervenir facilement.

Ces éléments réunis nous donnent suffisamment d'informations pour traiter les données reçues.

### 5.2.1. Réalisation du workflow N8N

Voici la version finale de mon workflow (Figure 14). Les différentes parties sont:

- Le webhook (en rouge) et la réponse au webhook qui sont deux nœuds travaillant en parallèle pour traiter les informations. Une fois que Grafana va exécuter le workflow en faisant appel au lien se trouvant dans le nœud webhook, le workflow va continuer jusqu'à atteindre "Respond to Webhook" qui va être la réponse (les données) que notre workflow va retourner à Grafana pour qu'il puisse les afficher.
- Requête HTTP (en vert) qui interroge le serveur RG System pour récupérer les informations qu'on a vues dans la capture d'écran précédente
- Nœud code (en orange), c'est-à-dire le code informatique que j'ai écrit pour manipuler les données. Durant la création des workflows, cette partie a pris énormément de temps à réaliser, car je n'avais jamais programmé en langage JavaScript et j'ai souvent été obligé de manipuler les données reçues.

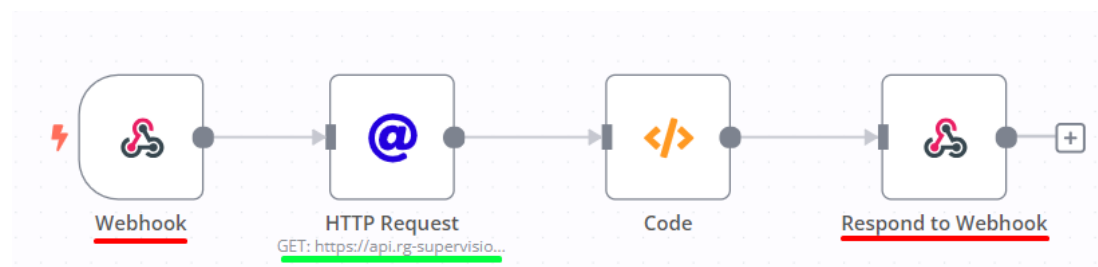


Figure 14: Workflow réalisé pour RG System

La figure de ce nœud représente de l'intérieur (Figure 15):

Dans cette figure, la partie soulignée en rouge représente le filtrage que j'effectue sur le statut d'acquisition et sur le niveau de criticité du ticket.



La partie orange regroupe et isole les données de notre liste précédente pour envoyer uniquement cette partie vers Grafana.

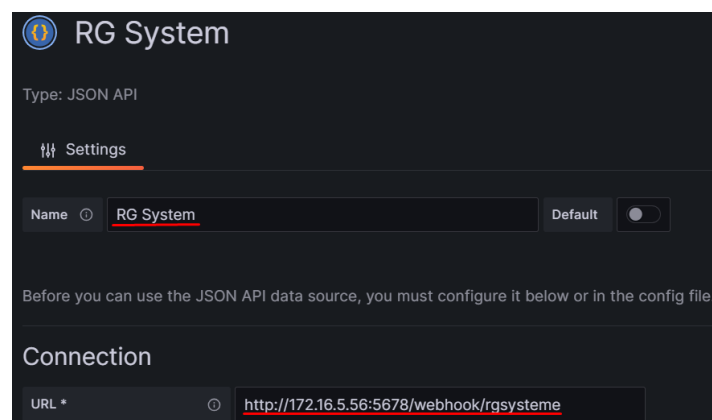
```
JavaScript
1 // Filtre et extrait des informations spécifiques de chaque ticket
2 const tickets = items[0].json["data"]["tickets"];
3 const filteredAndFormattedTickets = Object.values(tickets).filter(ticket =>
4   ticket.isAcquitted === false && ticket.criticality === "critical"
5 ).map(ticket => {
6   return {
7     displayId: ticket.displayId ?? null,
8     agentName: ticket.agentName ?? null,
9     nodeName: ticket.nodeName ?? null,
10    title: ticket.title ?? null,
11    criticality: ticket.criticality ?? null,
12    isAcquitted: ticket.isAcquitted ?? null,
13    creationDate: ticket.creationDate ?? null
14   };
15 });
16
17 // Enveloppe le résultat dans un objet avec une clé "devices"
18 const output = {
19   devices: filteredAndFormattedTickets
20 };
21
22 return {json: output};
23
```

Figure 15: Nœud code de N8N

### 5.2.2. Affichage des données sur Grafana

Pour réaliser la visualisation sur Grafana, il faut tout d'abord créer une source de données pour qu'il sache où aller chercher les informations. Mais avant cela, vu que nous utilisons N8N qui fournit les données en JSON, nous avons installé un plugin qui reconnaît ce type de données entrantes.

Ensuite, nous allons créer une source de données (Figure 16). Je ne vais pas expliquer chaque élément dans cette configuration, mais uniquement les plus importants qui sont le nom de la base de données et l'URL qui nous sert à connecter celle-ci et notre application.



The screenshot shows the Grafana configuration page for a data source named "RG System". The "Settings" tab is active. Under "Name", the value "RG System" is entered. Below this, a message states: "Before you can use the JSON API data source, you must configure it below or in the config file." Under the "Connection" section, the "URL" field is populated with "http://172.16.5.56:5678/webhook/rssysteme".

Figure 16: Configuration de la source de données Grafana

L'IP sur l'image est celle du docker, c'est-à-dire de l'environnement où notre outil N8N est hébergé. Cette IP est utilisée pour plusieurs outils, c'est pourquoi nous utilisons le numéro de port 5678 qui identifie "l'adresse" de N8N.

Une fois notre source de données et l'outil connectés, nous pouvons passer à la configuration de la visualisation (Figure 17). En appuyant sur le bouton "créer une visualisation" et en sélectionnant la source de données connectée précédemment (RG System), nous sommes prêts pour l'arrivée des données.

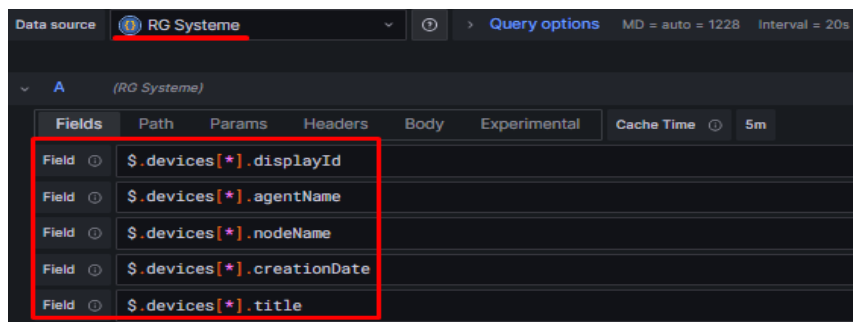


Figure 17: Configuration d'affichage des données

Nous voulons afficher les données en un tableau. Ces champs représentés sur l'image nous permettent de choisir quelle donnée afficher sur quelle colonne.

D'après notre configuration, notre tableau va afficher en ordre les données sur:

- L'ID des tickets
- Le nom de l'agent
- Le type d'appareil
- La date de création du ticket
- La description

L'écriture "\$." représente une syntaxe de Grafana pour récupérer les données. Le mot "devices" fait référence à un dictionnaire et "[\*]" est utilisé pour récupérer chaque élément qui se trouve dans celui-ci. Le contenu du dictionnaire correspond aux informations que l'on retrouve sur nos tickets RG System.

Suite à notre configuration, nous nous retrouvons avec un premier dashboard finalisé:

RG SYSTEM				
Ticket ID	Agent	SRV/WKS	Date	Description
TIVWVOG44AGX	PSH\PSHSRVNAS05	Serveurs	2024-04-09 09:01:08	Valeur Snmp - Raid Free Size (Octets) - 15 minutes
TIVWTIZA65QA	PRBSRVNAS02	Serveurs	2024-04-09 04:20:05	Valeur Snmp - Raid Free size (octets) - 15 minutes
TIVWT9K900HT	PSH\PSHSRVNAS01	Serveurs	2024-04-09 03:45:55	Valeur Snmp - 1st Raid free size (Octets) - 30 minutes
TIVWT9K900HS	PSH\PSHSRVNAS01	Serveurs	2024-04-09 03:45:55	Valeur Snmp - Disk 4 status (1 is OK) - 15 minutes
TIVWQREGV3B9	MRFSRVNAS	Serveurs	2024-04-08 22:18:49	Valeur Snmp - Raid Free size (octets) - 15 minutes
TIVVHJG5DNK2	ETAUSRVNAS01	SERVEURS	2024-04-04 19:52:39	Valeur Snmp - 1st Raid free size (Octets) - 30 minutes

Figure 18: Visualisation du dashboard RG System sur Grafana

Dans ce dashboard (Figure 18), nous allons observer en ordre:

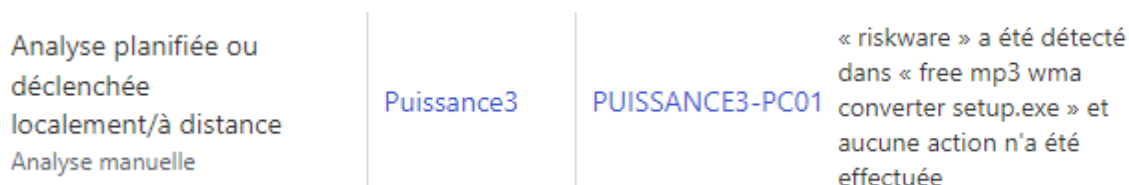
1. Le titre suivi d'une icône qui, lorsqu'on clique dessus, va nous diriger vers notre application RG System, dans un nouvel onglet, pour facilement gérer d'autres paramètres.
2. Les titres (explications) des différentes colonnes de façon claire. L'icône représente le filtrage que nous avons activé pour faciliter le suivi des tickets.
3. Nos données ont été filtrées une première fois sur le niveau de criticité. Les tickets affichés sont d'office des tickets importants et devront être consultés en premier.

## 5.3. Réalisation WithSecure

Withsecure est l'outil qui nous sert de "endpoint protection". Il est installé dans les appareils surveillés. Il requiert une licence pour pouvoir être utilisé. La tâche la plus importante qu'il accomplit est la surveillance et la prise de mesure en cas de danger.

Withsecure possède une base de données des liens, des exécutables et des fichiers malveillants et, lorsque ces derniers sont détectés sur un appareil, il va les mettre en quarantaine ou les supprimer.

Lorsque les agents détectent ce genre d'événements de sécurité, ils génèrent une alerte (Figure 19) qui peut être consultée sur l'interface d'événement Withsecure comme présenté ci-après:



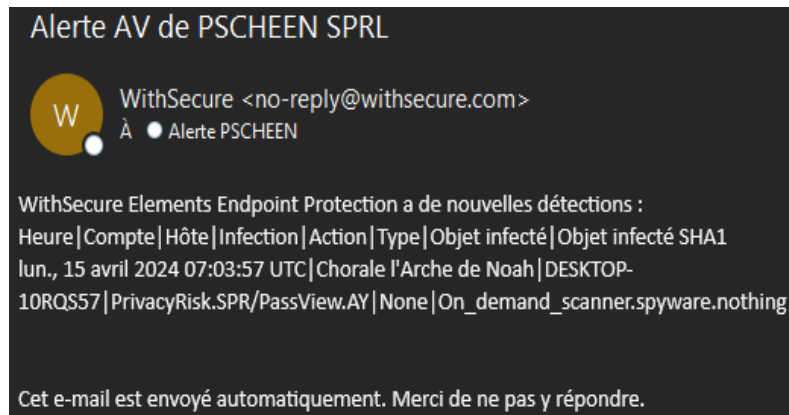
L'objectif principal de nos workflows est d'afficher 3 dashboards.

1. Le premier va être d'obtenir les alertes des workstations et des serveurs depuis l'interface ci-dessus pour pouvoir les suivre et réagir en temps réel depuis notre système de monitoring.
2. Le deuxième sera de récupérer la liste des mises à jour faites automatiquement sur les différentes machines à l'aide d'un rapport envoyé chaque semaine. On relève également le nombre d'incidents traités directement par l'outil Withsecure.
3. La troisième étape consiste à analyser, sous forme de graphiques, le nombre d'incidents qui surviennent le plus souvent.

Après avoir parcouru les API disponibles, j'ai découvert que, malheureusement, les API de monitoring qui sont intéressantes étaient sous licence et payantes. Alors j'ai cherché une autre solution. J'ai remarqué que Withsecure nous permet de générer des alertes par courrier électronique ainsi que des rapports hebdomadaires. J'ai alors décidé de récupérer les informations via ces courriers et de les traiter sur notre outil N8N.

Pour pouvoir réaliser cette étape, je me suis rendu sur l'interface web Withsecure et ai activé les envois d'alerte et de rapport par mail sur notre adresse mail d'alerting.

Ensuite, mes alertes ont commencé à apparaître sur la boîte mail `alerte@pscheen.com` dédiée à cette tâche. La figure 20 présente l'alerte qui est reçue par mail.



*Figure 20: Configuration des alertes d'infections*

### 5.3.1. Réalisation du workflow N8N

La gestion des workflows de récupération de données à partir d'emails ou d'autres sources non-API peut devenir complexe. La figure 21 détaille un workflow N8N bien documenté. Il est essentiel que chaque workflow créé soit accompagné d'une documentation détaillée et enrichie de commentaires. Ceci permettra aux futurs utilisateurs de comprendre et d'améliorer le workflow si nécessaire.

Le workflow étant unidirectionnel, il est assez simple de comprendre sa fonctionnalité.

Voici une explication brève de ce workflow:

1. Grafana envoie une demande pour recevoir les informations que N8N traite.
2. N8N parcourt la boîte mail alerte, récupère le contenu des messages se trouvant dans le sous-dossier Withsecure.
3. N8N va ensuite filtrer en prenant uniquement les messages non lus et mettre leur statut en "lu".
4. N8N traite les informations récupérées de la boîte mail pour uniquement traiter les données intéressantes via un script Java Script.
5. Les données sont transformées en format JSON et envoyées à Grafana pour l'affichage.
6. Un deuxième flux crée des tickets d'alerte pour le service après-vente sur Teamleader.

Pour les dashboards de Withsecure, nous avons 3 workflows comme la figure 21. La différence entre les workflows est souvent le tri sur le type d'appareil (pour savoir s'il s'agit d'un serveur ou d'un ordinateur), sur les clients et sur le contenu du mail envoyé par Withsecure.

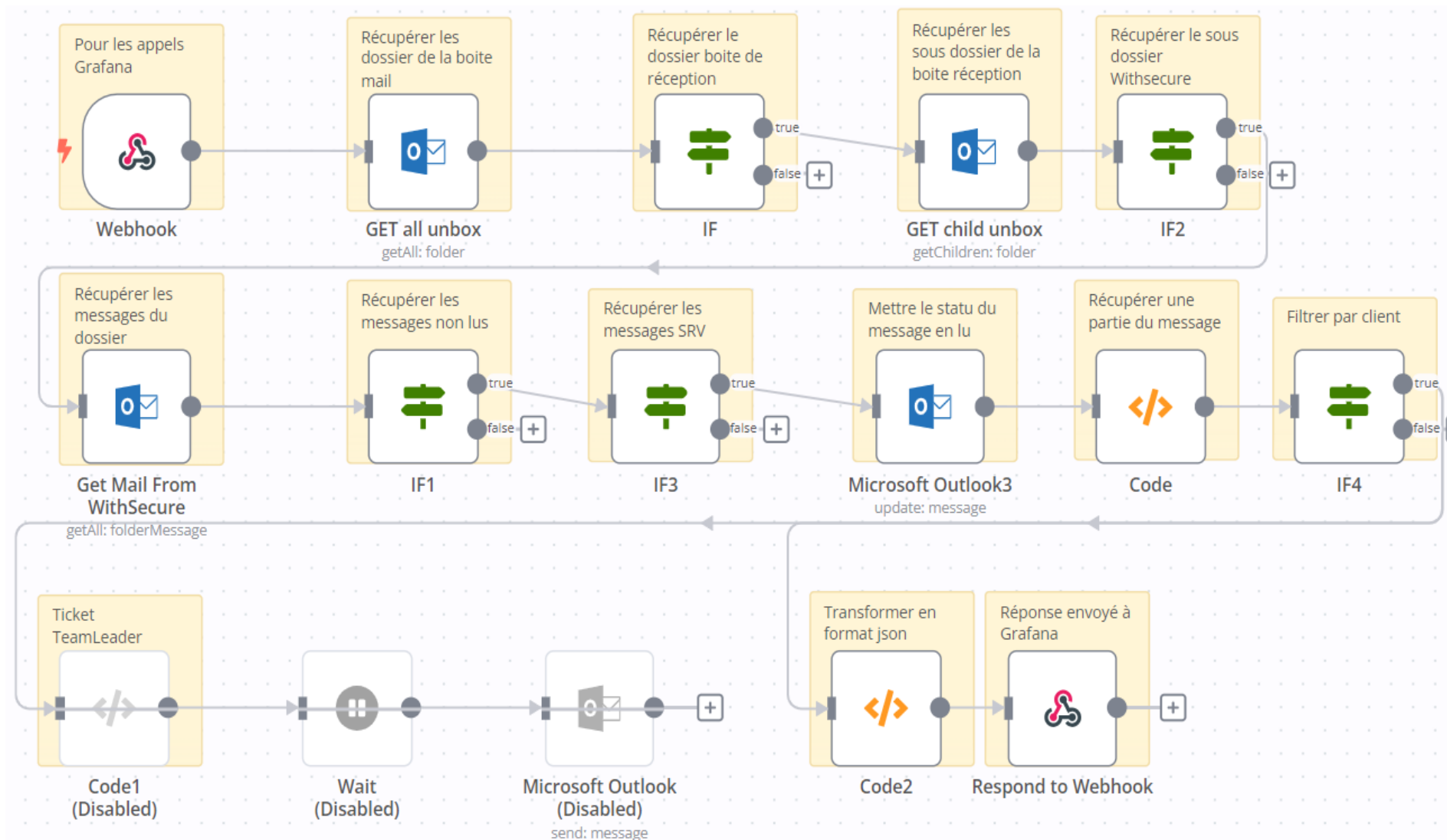
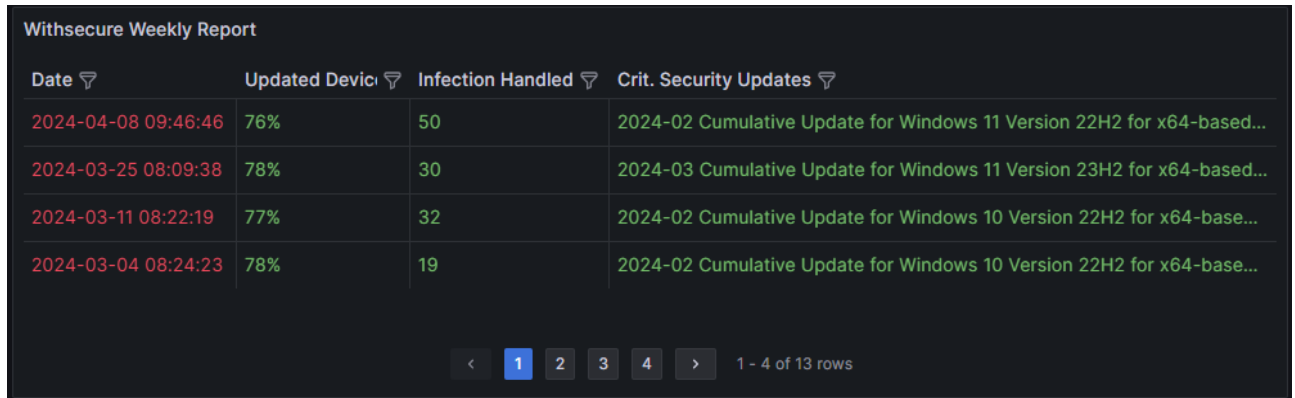


Figure 21: Workflow N8N du dashboard Withsecure serveur

### 5.3.2. Affichage des données sur Grafana

Pour notre EndPointWithsecure, nous avons réalisé 3 dashboards. Le troisième étant très semblable au second, je n'en expliquerai que 2 (Figures 22 et 23).

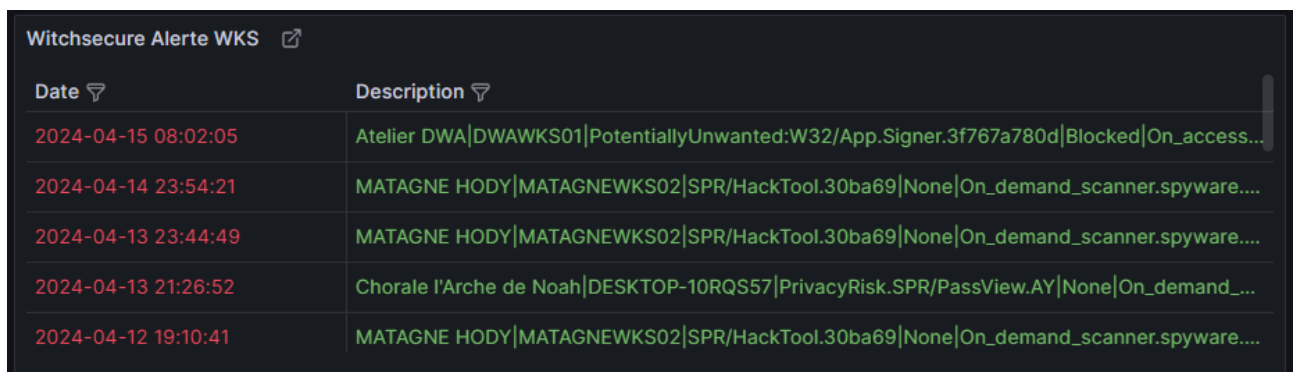


Date	Updated Device	Infection Handled	Crit. Security Updates
2024-04-08 09:46:46	76%	50	2024-02 Cumulative Update for Windows 11 Version 22H2 for x64-based...
2024-03-25 08:09:38	78%	30	2024-03 Cumulative Update for Windows 11 Version 23H2 for x64-based...
2024-03-11 08:22:19	77%	32	2024-02 Cumulative Update for Windows 10 Version 22H2 for x64-base...
2024-03-04 08:24:23	78%	19	2024-02 Cumulative Update for Windows 10 Version 22H2 for x64-base...

Figure 22: Dashboard des rapports hebdomadaires

Voici une explication des colonnes qui diffèrent par rapport aux autres affichages :

- Updated Device: Nous donne, en pourcentage, le taux de machines mises à jour.
- Infection Handled: Représente l'information sur le nombre d'événements pris en charge par Withsecure (quarantaine et suppression).



Date	Description
2024-04-15 08:02:05	Atelier DWA DWAWS01 PotentiallyUnwanted:W32/App.Signer.3f767a780d Blocked On_access...
2024-04-14 23:54:21	MATAGNE HODY MATAGNEWKS02 SPR/HackTool.30ba69 None On_demand_scanner.spyware....
2024-04-13 23:44:49	MATAGNE HODY MATAGNEWKS02 SPR/HackTool.30ba69 None On_demand_scanner.spyware....
2024-04-13 21:26:52	Chorale l'Arche de Noah DESKTOP-10RQS57 PrivacyRisk.SPR/PassView.AY None On_demand_...
2024-04-12 19:10:41	MATAGNE HODY MATAGNEWKS02 SPR/HackTool.30ba69 None On_demand_scanner.spyware....

Figure 23: Dashboard des alertes ordinateurs clients

## 5.4. Réalisation Microsoft 365

Microsoft 365 et Azure sont des outils essentiels pour PSCHÉEN et ses clients. Ils sont souvent utilisés pour des applications de partage, de sharepoint et de stockage. Microsoft a déjà un dashboard très avancé sur sa plateforme 365 et Azure monitor, mais il va être intéressant de récupérer les alertes instantanément (Figures 24 et 25), car ces outils peuvent avoir des accès très importants sur les espaces de stockage et sur les comptes ainsi que les machines virtuelles Azure.

Nous voulons donc intégrer dans notre système de monitoring les alertes concernant les appareils et les comptes MS 365. Pour ce faire, nous avons activé les alertes de notification MS 365 pour les points de terminaison defender et dirigé les mails vers la boîte mail d'alerting.

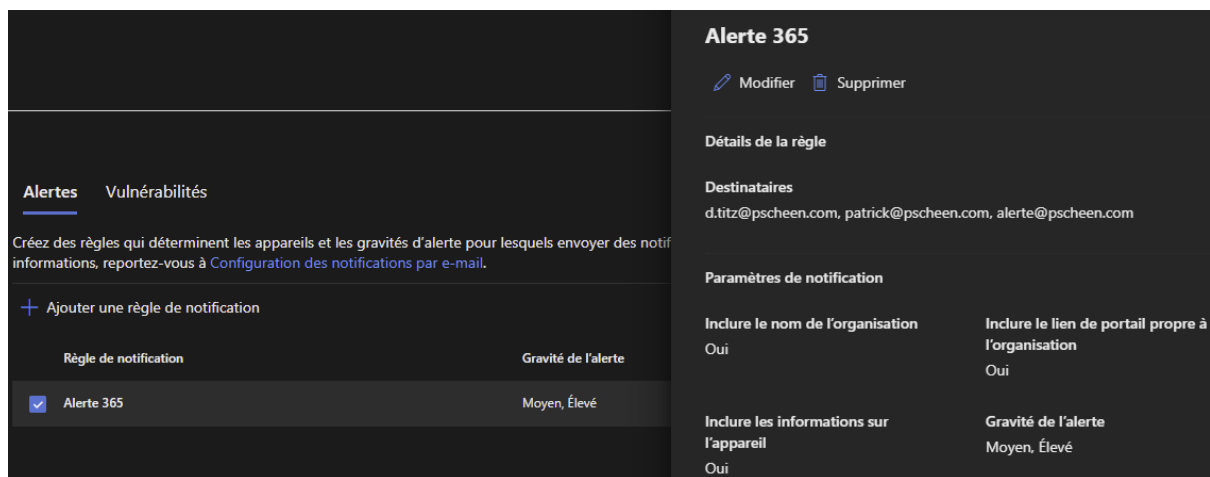


Figure 24: Configuration de Microsoft defender pour les alertes

Nous attendons une alerte reçue par mail pour analyser quels types de données sont envoyées avec cette alerte.



Figure 25: Premier mail d'alerte MS 365

### 5.4.1. Réalisation du workflow N8N

Le workflow N8N est intéressant, car c'est un workflow qui va envoyer les informations sur le dashboard et aussi générer des tickets Teamleader et faciliter les techniciens à suivre et intervenir plus rapidement (Figure 26).

La première partie qui récupère le mail de la boîte est semblable. La seule différence c'est que dans notre boîte mail, alerte@pscheen.com, nous avons des sous-dossiers dédiés aux différents outils. Le sous-dossier sera donc celui de MS 365. Une fois le mail récupéré, nous utilisons un code JavaScript pour soustraire la partie importante de la capture que nous avons affichée plus haut. En fonction de nos besoins, on a décidé de récupérer la date de l'événement et le sujet du mail pour afficher dans notre dashboard Grafana. Le sujet développe suffisamment l'incident et nous donne donc déjà une idée d'où aller voir. C'est pourquoi nous avons trouvé cette information pertinente.

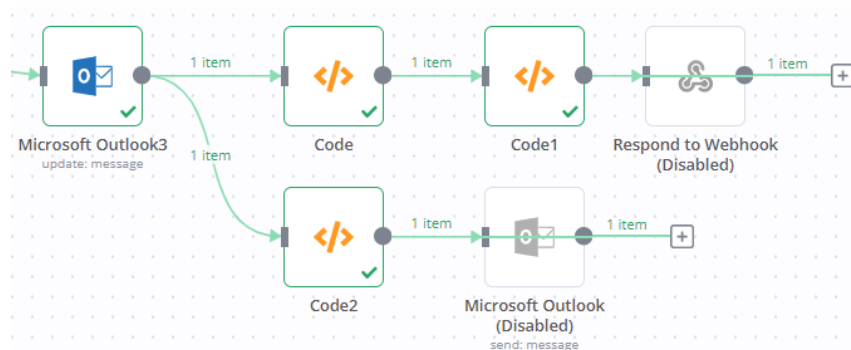


Figure 26: Envoi des données sur Grafana et Teamleader après la manipulation

### 5.4.2. Affichage des données sur Grafana

Les données sont organisées et triées sur Grafana pour arriver vers l'affichage sur la figure 27.

Date	Description
2024-04-05 10:49:52	Medium severity alert: A suspicious file was observed on pshwks08

Figure 27: Dashboard Grafana pour le tenant Microsoft

Pour cette partie, comme nos données vont également être visibles sur Teamleader, il est intéressant de présenter un rendu sur cette plateforme qui est dédiée aux techniciens (Figure 28).

Statut	Client	Sujet	Date de création	Entreprise	Boîte de récepti...
Clôturé	Alerte PSCHÉEN	Medium severity alert: A suspici...	09/04/2024 - 09:...		helpdesk@psche...

Figure 28: Système de ticketing Teamleader



## 5.5. Réalisation Synology C2

Il est très important que les personnes concernées au sein de PSCHEEN soient informées en temps réel des alertes émises par Synology C2 Backup afin de garantir une réponse rapide et appropriée aux incidents de sécurité et aux situations critiques. La mise en place d'une configuration solide pour le système d'alerte et de surveillance est donc essentielle pour maintenir la sécurité des données et assurer la satisfaction des clients. C'est pourquoi nous avons décidé d'insérer un dashboard Synology C2 qui surveille l'espace de stockage sur le cloud C2. La plateforme de Synology (Figure 29) pour les partenaires va nous soutenir pour le suivi et pour réagir en cas de besoin.

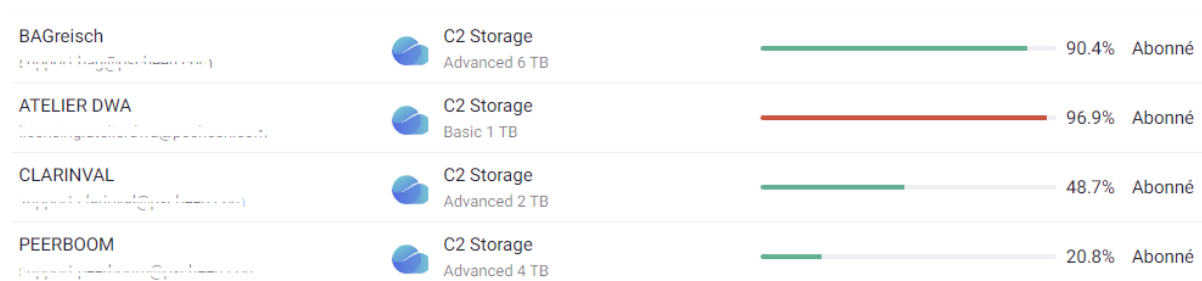


Figure 29: Une vue globale de comment l'espace stockage en cloud est surveillé sur l'interface

Nous utilisons les alertes générées par cette interface pour les stocker dans une boîte mail. Ensuite, nous filtrons les mails pour récupérer ceux dédiés au stockage. Ils sont alors envoyés sur l'outil d'automatisation N8N pour être traités via différents nœuds et code Javascript. Lorsque l'espace de stockage est saturé, un ticket sur Teamleader est généré pour notre sales manager qui peut à son tour contacter les clients et leur proposer des licences ou des abonnements afin d'augmenter leur espace de stockage disponible et éviter une perte de données en cas d'incident.

### 5.5.1. Réalisation du workflow N8N

Lorsqu'un client atteint un pourcentage élevé de son espace de stockage cloud, le client et le pourcentage sont affichés dans le dashboard (Figure 30).

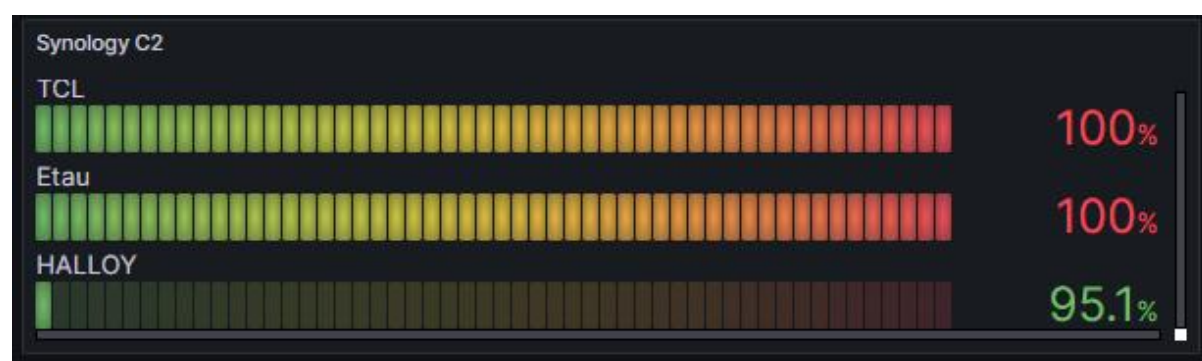


Figure 30: Dashboard des clients ayant plus ou presque plus d'espace sur C2

## 5.6. Réalisation Zyxel: Nebula, SecuReporter

Les licences Zyxel que nous avons commandées pour pouvoir utiliser les API ont pris du temps à arriver; c'est pourquoi nous avons commencé à développer la partie Secu Reporter. Les licences étaient nécessaires pour pouvoir utiliser les API et faciliter l'automatisation de tâches, et pour récupérer les données plus pertinentes que la version basique.

### 5.6.1. Réalisation du workflow SecuReporter

Nous allons voir en détail le workflow lié aux alertes des appareils que nos clients utilisent.

PSCHEEN ne gère pas les firewalls depuis la plateforme Nebula. C'est un choix qui a été fait par les administrateurs, car ils avaient l'impression d'avoir beaucoup moins de paramètres possibles sur Nebula due à l'usage facile de la plateforme. Il est donc intéressant d'analyser chaque alerte venant d'un pare-feu. Pour faciliter le traitement des alertes, nous avons décidé de les fusionner dans un seul dashboard et les filtrer sur nos clients pour avoir uniquement les alertes des clients qui ont un abonnement de surveillance chez PSCHEEN.

### 5.6.2. Configuration des types d'alertes sur l'interface SecuReporter

Voici les raisons pour lesquelles notre plateforme va générer des alertes:

- "Nombre d'attaques de gravité maximale dépasse 1 fois en 5 minutes"
- "Nombre d'attaques dépasse 10 fois en 5 minutes"
- "Nombre d'attaques de logiciels malveillants/virus dépasse 10 fois en 5 minutes"
- "Nombre de hits de Malware/IPS (plus haute gravité)/ADP (anomalie de protocole) dépasse 10 en 1 minute"
- "Nombre de fichiers malveillants détruits dépasse 10 fois en 5 minutes"
- "Nombre de fichiers suspects détruits dépasse 10 fois en 5 minutes"
- "Nombre de connexions à des sites Web de menaces dépasse 5 fois en 60 minutes"
- "Nombre d'adresses IP internes attaquées par une adresse IP de menace externe dépasse 50 fois en 10 minutes"
- "Nombre de connexions à des adresses IP de menace dépasse 1 fois en 60 minutes"
- "Nombre de connexions à des domaines DNS de menace/bloc dépasse 5 fois en 60 minutes"
- "Le même logiciel malveillant/virus est détecté plus de 2 fois en 15 minutes"
- "Nombre de scans/floods d'anomalies de trafic détectés dépasse 1 fois en 5 minutes"
- "Nombre de décodeurs d'anomalies de protocole TCP/UDP/ICMP/IP dépasse 1 fois en 5 minutes"

Une fois les alertes activées, nous commençons à recevoir les notifications (Figure 31) sur notre dossier SecuReporter dans la boîte mail [alerte@pscheen.com](mailto:alerte@pscheen.com).

<b>SecuReporter</b> <b>Alert - ERU ATP200</b> This email notification was 13:50	<b>SecuReporter</b> <b>Alert - DOICESCO GW01</b> This email notification was 12:20
<b>SecuReporter</b> <b>Alert - TCL GW01</b> This email notification was 13:40	<b>SecuReporter</b> <b>Alert - GESINTER GW01</b> This email notification was 12:10

Figure 31: Exemples d'alertes reçues par mail

### 5.6.3. Réalisation du workflow N8N

Ce workflow va prendre en charge les alertes des appareils réseau, souvent les firewalls, mais aussi les switches.

Les alertes ont déjà été configurées sur la plateforme SecuReporter, pour que quand elles sont générées, le nom du client et de l'appareil soient insérés dans le sujet du mail.

Notre workflow va parcourir la boîte mail en utilisant les ID des dossiers, lire le contenu du dossier, et retourner l'ensemble des mails d'alertes reçus par SecuReporter.

Ce workflow nous a généré énormément d'alertes en 1 jour. Monsieur Scheen m'a alors demandé de cibler plus précisément les incidents de haut niveau. Nous avons alors décidé par la suite de changer les paramètres depuis l'interface de SecuReporter. Par exemple, pour la règle "Nombre de decodeurs d'anomalies de protocole TCP/UDP/ICMP/IP dépasse 1 fois en 5 minutes", nous sommes passés de 1 à 3 fois.

### 5.6.4. Affichage des données sur Grafana

Lorsque l'envoi des données est complété, nous avons créé une source d'entrée dans Grafana. Nous avons décidé d'afficher dans les mails reçus la date, le sujet (qui contient le nom du client et l'appareil) et le contenu du mail filtré et simplifié grâce à l'utilisation d'expressions régulières (Regex<sup>22</sup>) pour obtenir le résultat sur la figure 32.

SecuReporter		
Date 🚩	Device 🚩	Description 🚩
2024-04-19 09:20:23	Alert - TCL GW01	Connect to threat/block DNS domain count is over 5 tim...
2024-04-19 09:00:13	Alert - BIEC ATP100	Connect to threat/block DNS domain count is over 5 tim...
2024-04-19 08:40:08	Alert - ERU ATP200	Number of traffic anomaly scans/floods detected is ove...
2024-04-19 08:30:12	Alert - TCL GW01	Number of protocol anomaly TCP/UDP/ICMP/IP decoder...

Figure 32: Dashboard Grafana des alertes appareils clients

<sup>22</sup> Un pattern que nous souhaitons rechercher et localiser dans du texte (Expression régulière).

## 5.7. Problèmes - Solutions

Dans le cadre de ce PROJET, plusieurs obstacles sont apparus, nécessitant des solutions adaptatives et créatives pour atteindre les objectifs fixés par PSCHEEN.

Parmi les défis rencontrés, l'apprentissage et la maîtrise d'outils nouveaux ont été des étapes cruciales. L'intégration de l'outil d'automatisation N8N a demandé une connaissance profonde dans le langage JavaScript et une compréhension précise de chaque nœud. Toutefois, grâce à une démarche déterminée et une exploration méthodique, ces obstacles ont été surmontés.

Une autre problématique majeure était la fusion, au sein de N8N, des diverses sources de données, provenant de plateformes variées telles que MS365, WithSecure, Zyxel, etc. Chaque plateforme ayant ses propres protocoles d'envoi d'informations, j'ai dû développer une approche personnalisée pour leur intégration. Par exemple, j'ai dû créer des scripts spécifiques pour harmoniser les formats de données et assurer leur compatibilité au sein de N8N. Grâce à l'apprentissage de l'utilisation de N8N et des API, cette difficulté a été progressivement surmontée, ce qui a permis une consolidation efficace des données provenant de multiples sources.

L'apprentissage et la manipulation d'API ont également représenté un défi, nécessitant un investissement en temps et en énergie. La procédure pour obtenir des clés API autorisées, combinée à la recherche et à la compréhension des documentations techniques, ont constitué des étapes essentielles, mais compliquées. Il y a des temps d'attente de 1 à 2 semaines pour que les supports nous fournissent nos clés. Malgré ces obstacles, ma détermination à les surmonter a été récompensée par une meilleure compréhension des mécanismes sous-jacents et une utilisation plus efficace des API pour répondre aux besoins spécifiques de surveillance et de reporting de PSCHEEN.

En somme, chaque difficulté rencontrée au cours de ce projet a été abordée avec une approche méthodique et une volonté constante d'apporter des solutions adaptatives et innovantes.

## 5.8. Résultat final

Dans cette section (Figure 33), nous examinons divers tableaux de bord utilisés pour la surveillance et la gestion de la sécurité informatique au sein de PSCHEEN. Chaque tableau de bord offre une perspective unique sur les aspects critiques de la sécurité des systèmes, allant des incidents de sécurité et des alertes de performance aux états des sauvegardes et aux mises à jour des dispositifs.

### **SecuReporter**

Le tableau de bord SecuReporter fournit des informations importantes sur les événements de sécurité récents. Il affiche les dates des incidents, les dispositifs impliqués et des descriptions détaillées des alertes. Par exemple, on peut y voir des alertes pour des dispositifs déconnectés pendant plus de 15 minutes, des connexions fréquentes à des domaines DNS suspects, et des anomalies dans les décodeurs de protocoles comme TCP/UDP/ICMP. Ces informations permettent aux administrateurs de réagir rapidement aux problèmes de sécurité.

### **Withsecure Weekly Report**

Ce tableau de bord résume les mises à jour de la semaine précédente en termes de sécurité. Il indique les dates, le pourcentage de dispositifs mis à jour, le nombre d'infections traitées, et les détails des actualisations critiques de sécurité appliquées. Par exemple, on y trouve des mises à jour cumulatives pour Windows 10, essentielles pour maintenir la sécurité du système d'information. Ce rapport hebdomadaire aide à assurer que tous les dispositifs sont à jour et protégés contre les menaces.

### **Withsecure Alerte WKS**

Le tableau de bord Withsecure Alerte WKS est dédié aux alertes de sécurité détectées sur les postes de travail. Il affiche les dates des alertes ainsi que des descriptions détaillées, telles que la détection de logiciels potentiellement indésirables (PUA) comme le W32/App.Signer. Ces informations incluent également les chemins d'accès aux fichiers infectés, permettant une réponse rapide et ciblée pour éliminer les menaces.

### **Nebula Top devices by usage**

Ce tableau de bord présente un diagramme illustrant la consommation de données des principaux dispositifs du réseau. Les dispositifs sont identifiés par des codes tels que PSHSW02 et AP01, avec des valeurs spécifiques de données utilisées en gigaoctets (Go). Par exemple, PSHSW02 affiche une consommation de 96,9 Go, ce qui en fait le plus gros utilisateur de bande passante. Cette visualisation aide à identifier les dispositifs ayant une forte utilisation et à surveiller les performances du réseau.

### **RG SYSTEM**

Le tableau de bord RG SYSTEM affiche des événements importants concernant la surveillance des serveurs et des postes de travail. Il liste les dates des événements, les identifiants de tickets, les agents impliqués, et les descriptions des problèmes tels que la surveillance de l'espace libre sur les disques RAID. Par exemple, on peut voir des alertes pour des tailles libres RAID SNMP surveillées sur des intervalles de 15 à 30 minutes, permettant de maintenir la santé des systèmes de stockage.

### **CrashPlan**

CrashPlan fournit des informations sur l'état de sauvegarde des dispositifs de différentes organisations. Ce tableau de bord montre les dispositifs surveillés, leur état d'alerte, le pourcentage de santé ou de performance, et les adresses IP associées. Par exemple, le dispositif PSHEEN01 a un statut OK avec 99,9% de performance, indiquant une bonne santé du système. Ces données sont essentielles pour assurer la continuité des sauvegardes et la récupération des données en cas de besoin.

### **MS365 Alerte**

Le tableau de bord MS365 Alerte présente les alertes de sécurité détectées dans l'environnement Microsoft 365. Il affiche les dates des alertes et des descriptions telles que l'observation de fichiers suspects. Par exemple, une alerte de gravité moyenne a été signalée pour un fichier suspect sur le dispositif pshwks08. Ce tableau de bord aide à surveiller et à gérer les menaces potentielles dans l'environnement cloud de Microsoft.

### **Synology C2**

Le tableau de bord Synology C2 montre le statut des dispositifs de stockage avec des noms de clients spécifiques comme TCL, Etau, et HALLOY. Il affiche les espaces de stockages dans le cloud en pourcentage, où 100% indique que l'espace est complet. Ce tableau de bord est essentiel pour la gestion et la surveillance de l'infrastructure de stockage.

### **Firmware Status**

Ce tableau de bord donne une vue d'ensemble des versions de firmware des dispositifs du réseau. Il liste les dispositifs, leurs versions actuelles de firmware, et leur statut de mise à jour. Par exemple, les dispositifs PSHSM01 à PSHSM04 sont tous à jour avec la version V4.98 (ABNH\_0). Assurer que le firmware est à jour est crucial pour la sécurité et la performance des dispositifs.

### **Nebula Alert**

Le tableau de bord Nebula Alert affiche les alertes concernant les interruptions de service des dispositifs. Il montre les dates des alertes, les dispositifs concernés, et des descriptions telles que des points d'accès ou des commutateurs étant hors ligne pendant plus de 5 minutes. Par exemple, l'alerte du 2024-04-15 indique que le point d'accès AP03 a été hors ligne pendant plus de 5 minutes. Ce tableau de bord aide à identifier et à résoudre rapidement les problèmes de connectivité réseau.

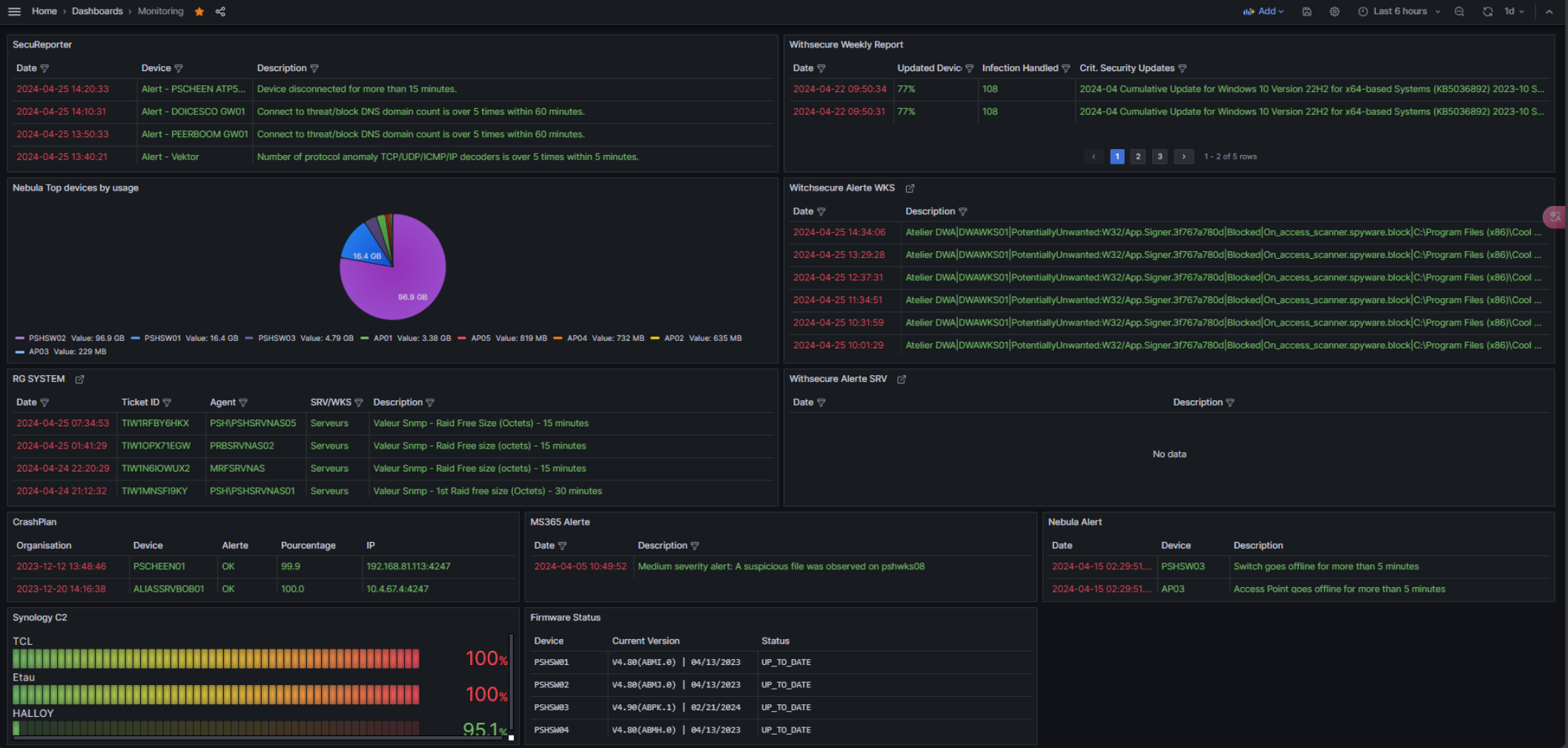


Figure 33: Dashboard final du système de monitoring chez PSCHÉEN

## 6. Conclusion

La conclusion d'un projet est une étape cruciale qui permet de récapituler les principales découvertes et réalisations, ainsi que de mettre en lumière les contributions et les perspectives futures. Dans cette conclusion, je vais approfondir davantage mes réflexions, en mettant en avant mon évolution personnelle, les défis rencontrés, les améliorations apportées et les retours reçus tout au long de ce projet de fin d'études.

Avant de débiter ce projet, plusieurs interrogations ont émergé quant à la meilleure approche à adopter pour répondre aux besoins spécifiques de l'entreprise. J'ai dû réfléchir à la manière de fusionner efficacement les différentes sources de données, à la meilleure façon de présenter ces données sur les tableaux de bord Grafana, et à la manière d'automatiser les processus pour garantir une surveillance en temps réel de l'infrastructure informatique de l'entreprise.

Ces questions ont été autant de défis à relever, mais aussi d'opportunités d'apprentissage et d'évolution personnelle. J'ai dû faire preuve de créativité et de flexibilité pour trouver des solutions adaptées, en naviguant à travers des domaines techniques variés tels que la programmation, l'intégration de systèmes et la gestion de données.

Nous avons débuté ce projet en analysant les besoins spécifiques de PSCHEEN en matière de surveillance et de reporting, mettant en évidence les lacunes dans l'infrastructure existante et les défis auxquels ils étaient confrontés. En réponse à ces besoins, nous avons proposé une approche basée sur l'utilisation d'outils d'automatisation tels que N8N, combinée à l'intégration de sources de données variées telles que RG System, WithSecure, Microsoft 365, Synology C2, Nebula et SecuReporter.

L'implémentation de ce système de surveillance a été réalisée de manière méthodique, en suivant un plan de réalisation détaillé pour chaque outil et source de données. Nous avons commencé par la recherche et la compréhension des API disponibles, la création des tokens d'authentification nécessaires, puis la mise en place des workflows N8N pour automatiser la récupération et le traitement des données. En parallèle, nous avons configuré Grafana pour l'affichage des données sous forme de tableaux de bord personnalisés, offrant ainsi une vue d'ensemble concise de l'état de l'infrastructure informatique de l'entreprise.

Au fil du projet, des améliorations significatives ont été apportées pour répondre aux besoins du maître de stage. Par exemple, nous avons affiné l'affichage des tableaux de bord Grafana en filtrant les données par client; ce qui a permis une visualisation plus claire et plus précise des alertes et des incidents. De plus, nous avons optimisé les processus d'automatisation pour assurer une surveillance continue et proactive de l'infrastructure informatique de l'entreprise.

Chaque étape de ce processus a été accompagnée de son lot de défis, allant de l'apprentissage et de la maîtrise de nouveaux outils et langages de programmation, à l'intégration de sources de données hétérogènes et aux délais d'obtention des clés API. Cependant, grâce à une approche déterminée et une volonté constante de surmonter les obstacles, nous avons réussi à relever ces défis et à proposer une solution complète et fonctionnelle à PSCHEEN.



Pour l'avenir, des perspectives d'amélioration et d'extension de ce système de surveillance sont envisageables. Il serait notamment possible d'explorer de nouvelles sources de données et d'intégrer des fonctionnalités supplémentaires, telles que la détection d'anomalies et la prévision des incidents. De plus, des efforts continus seront nécessaires pour maintenir et mettre à jour ce système, afin de garantir sa fiabilité et sa pertinence à long terme.

En dehors du sujet principal, j'ai également eu l'occasion d'explorer d'autres aspects du métier d'administrateur système, en participant à des tâches de maintenance et de support technique. Cela inclut la réalisation de configurations de VPN pour les clients, la migration des serveurs Windows vers de nouvelles versions et la gestion des backups NAS qui rencontrent des problèmes. Ces expériences m'ont permis d'acquérir une compréhension plus approfondie du fonctionnement des systèmes informatiques en entreprise, ainsi que des compétences pratiques dans la résolution de problèmes et la gestion des incidents.

Mon parcours professionnel au sein de ce projet m'a permis de mener à bien des tâches variées, allant de l'apprentissage de nouveaux outils à la résolution de problèmes techniques complexes. En tant qu'étudiant, j'ai dû relever le défi de m'adapter à un environnement professionnel exigeant, tout en faisant preuve d'autonomie et de détermination pour atteindre les objectifs fixés par PSCHEEN. Le déploiement a été réalisé avec succès au sein de l'entreprise.

Le retour reçu de la part de mon maître de stage, et du reste de l'équipe, a été très positif, avec une reconnaissance exprimée quant à la qualité du travail accompli et à l'impact positif sur l'activité de l'entreprise. Cette validation a été gratifiante et a renforcé ma confiance en mes compétences ainsi qu'en ma capacité à contribuer de manière significative à des projets professionnels.

En conclusion, ce travail de fin d'études a mis en lumière l'importance vitale d'un système de surveillance centralisé dans la gestion efficace des infrastructures informatiques d'une entreprise. En fusionnant des outils d'automatisation sophistiqués et en exploitant pleinement les API disponibles, nous avons pu concevoir pour PSCHEEN un système de monitoring robuste et adaptable. Celui-ci lui offre la capacité de surveiller en temps réel l'état de son infrastructure et de réagir promptement aux incidents.

Cette expérience a été une aventure enrichissante à de multiples égards. Elle m'a offert l'opportunité de cultiver mes compétences techniques, de surmonter des défis complexes, et surtout, de contribuer de manière tangible à l'amélioration des processus informatiques au sein d'une entreprise. Je quitte ce projet empreint d'un profond sentiment de satisfaction et de gratitude, nourri par la certitude renouvelée de mon potentiel et de ma capacité à évoluer dans le domaine de la cybersécurité.

## 7. Bibliographie

- Build, Collaborate & Integrate APIs | SwaggerHub. (s. d.). [https://app.swaggerhub.com/apis/ZyNETNCC/zyxel-nebula\\_open\\_api/0.1.24](https://app.swaggerhub.com/apis/ZyNETNCC/zyxel-nebula_open_api/0.1.24)
- ChatGPT. (s. d.). <https://chat.openai.com/>
- Dib, F. (s. d.). regex101 : build, test, and debug regex. Regex101. <https://regex101.com/>
- Grafana documentation | Grafana documentation. (s. d.). Grafana Labs. <https://grafana.com/docs/grafana/latest/>
- JavaScript Documentation Standards – Coding Standards Handbook | Developer.WordPress.org. (2019, 25 avril). WordPress Developer Resources. <https://developer.wordpress.org/coding-standards/inline-documentation-standards/javascript/>
- JavaScript tutorial. (s. d.). <https://www.w3schools.com/js/default.asp>
- Newest questions. (s. d.). Stack Overflow. <https://stackoverflow.com/questions/>
- Nginx Proxy Manager. (s. d.). <https://nginxproxymanager.com/guide/>
- O365devx. (2022, 3 octobre). Welcome to Office 365 Management APIs. Microsoft Learn. <https://learn.microsoft.com/en-us/office/office-365-management-api/>
- Perplexity. (s. d.). <https://www.perplexity.ai/>
- RegExp.Prototype.test() - JavaScript | MDN. (2023, 25 septembre). MDN Web Docs. [https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\\_Objects/RegExp/test](https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/RegExp/test)
- RG Supervision API Documentation. (s. d.). <https://api.rg-supervision.com/api/doc/>
- Sitemap. (s. d.). CyberTechTalk Wiki. <https://wiki.andriejsazanowicz.com/sitemap>
- Synology Inc. (s. d.). Programme de partenariat. <https://c2.synology.com/fr-fr/partner>
- Wazuh. (s. d.-a). Wazuh documentation. <https://documentation.wazuh.com/current/index.html>
- Welcome | 2.19 | Portainer Documentation. (s. d.). <https://docs.portainer.io/>
- Welcome | n8n Docs. (s. d.). <https://docs.n8n.io/>
- WithSecureTM Connect. (s. d.). <https://connect.withsecure.com/api-reference/elements#overview>
- YouTube. (s. d.). <https://www.youtube.com/>
- Zyxel SecuReporter. (s. d.-a). SecuReporter. <https://secureporter.cloudcnm.zyxel.com/?next=/new-srpt/alert>
- Zyxel\_Carter. (2022, 21 janvier). Zyxel Nebula OpenAPI. Zyxel Community. <https://community.zyxel.com/en/discussion/12536/zyxel-nebula-openapi>