Atelier veille - Fiche à remplir

Mode d'emploi

Vous avez 70 minutes pour mettre en place une veille réelle et la décrire dans cette fiche. Remplacez chaque texte entre crochets par votre réponse.

(Cadrage du temps au besoin)

Étape	Durée	À produire	Section à remplir
1	10 min	Choisir un contexte réel	Contexte
2	10 min	Formuler un axe de veille complet	Axe de veille
3	20 min	Trouver au moins 3 sources, dont une sur la sécurité	Fiches de source 1 à 3
4	15 min	Paramétrer l'outil de collecte	Outil de collecte
5	15 min	Finaliser les fiches et rédiger une note de veille	Note de veille

La restitution orale dure 2 minutes par personne ou par binôme.

Contexte

La veille doit porter sur un cas réel : projet d'alternance, application personnelle ou pile technique que vous utilisez.

Rubrique	Votre réponse
Nom et prénom	BOICHÉ Gauvain
Trinôme éventuel	Adam GABRIEL et Louis LEULIETTE
Projet ou application	Kubernetes
Pile technique	
Dépendances critiques	Docker
Contraintes	Service nuagique (AWS), pas local (kubectl)

Axe de veille

Un axe exploitable nomme un sujet précis, une décision à éclairer, un destinataire et une fréquence.

Élément	Votre réponse
Sujet	Fiabilité et Sécurité d'un déploiement Kubernetes uni-tenant multi-région
Question	Ma version Kubernetes est-elle sécurisée pour une application cliente ?
Destinataire	Equipe Dev(Sec)Ops
Fréquence	– Moniteur : quotidien – Amélioration continue : hebdomadaire – Astreinte : en cas d'incident soulevé
Langues et zone	– Français et Anglais – Europe (Paris, Amsterdam, Milan)
Ce qui est exclu	
Volume acceptable	Par DevOps : 10, 20 maximum (pour éviter la fatigue)

Axe formulé en une phrase : [sujet, pour décider de quoi, à destination de qui, à quelle fréquence]

Exemple : Vulnérabilités exploitées touchant nos dépendances Node.js, pour décider d'un correctif urgent, à destination de l'équipe backend, chaque matin.

Fiche de source 1 : Sécurité

Cette première source est obligatoirement consacrée à la sécurité, et de préférence primaire.

Rubrique	Votre réponse
Nom de la source	Equipe CVE officielle de Kubernetes
Adresse	https://kubernetes.io/docs/reference/issues-security/official-cve-feed/feed.xml Ou https://kubernetes.io/docs/reference/issues-security/official-cve-feed/index.json
Type	Editeur et Communautaire – Kubernetes a été créé par Google, récupéré depuis par la Cloud Native Computing Foundation et maintenue par un noyau dur de contributeurs « officiels » ainsi que par des contributeurs externes.
Primaire ou secondaire	Primaire
Axe de veille servi	Flux JSON dans n8n pour un flux dans Discord via un WebHook.
Mode de collecte	Flux RSS ou Flux JSON, compatible pour des scripts et des analyseurs statiques.
Types de contenus	Alertes de sécurité CVE dédiée et interne
Auteur	Le service CVE interne de Kubernetes
Date	Dans le contenu JSON : "date_published":"2026-09-14T16:42:26Z" Dans le contenu RSS : <pubDate>Mon, 14 Sep 2026 16:42:26 +0000</pubDate>
Preuve	Référence CVE classique et compatible avec la base CVE « traditionnelle » (https://app.opencve.io/cve/CVE-2026-76654) menant à un incident sur le dépôt Github (https://github.com/kubernetes/kubernetes/issues/142098)
Recoupement	La base OpenCVE confirme la même chose, mais OpenCVE récupère certainement l'info. On peut présager, quand même, que l'équipe CVE interne

Rubrique	Votre réponse
	est sur le coup. Peut-être aussi que les deux bases se renvoient les infos mutuellement.
Fiabilité de la source	A
Limite	Les ressources concernent uniquement Kubernetes et son écosystème précis, mais pas forcément ses dépendances (Docker) ou des problèmes transversaux (les hébergeurs, les répartiteurs de charge, etc)
Pourquoi elle est adaptée	CVE officielle d'un projet communautaire titanesque et essentiel.

Fiche de source 2

Choisissez une source d'une autre famille que la première.

Rubrique	Votre réponse
Nom de la source	CISA (America's Cyber Defense Agency)
Adresse	https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
Type	Institutionnelle – Source Cyber officielle du gouvernement du pays qui n'a pas de nom
Primaire ou secondaire	Secondaire
Axe de veille servi	Flux JSON exploitable par un outil tiers
Mode de collecte	Flux JSON ponctuel
Types de contenus	Alertes sur tous les outils connus par le CISA
Auteur	La cyberdéfense américaine, dans un but de... Comment savoir exactement. L'information y est contrôlée, assurément. Et les CVE qui sont jugées « wokes » doivent être supprimées j'imagine...
Date	Dans le flux : "dateAdded": "2026-10-04". Pas de mention de l'heure par contre.
Preuve	Références CVE
Recoupement	La base de données OpenCVE confirme les trois dernières « Citrix », « Zammad » et « Fortinet »
Fiabilité de la source	A- (les infos publiées sont fiables, mais ce sont les non-publiées qui sont inquiétantes).
Limite	Je ne vois rien d'oublié, sauf sciemment.
Pourquoi elle est adaptée	Base de CVE connues.

Fiche de source 3

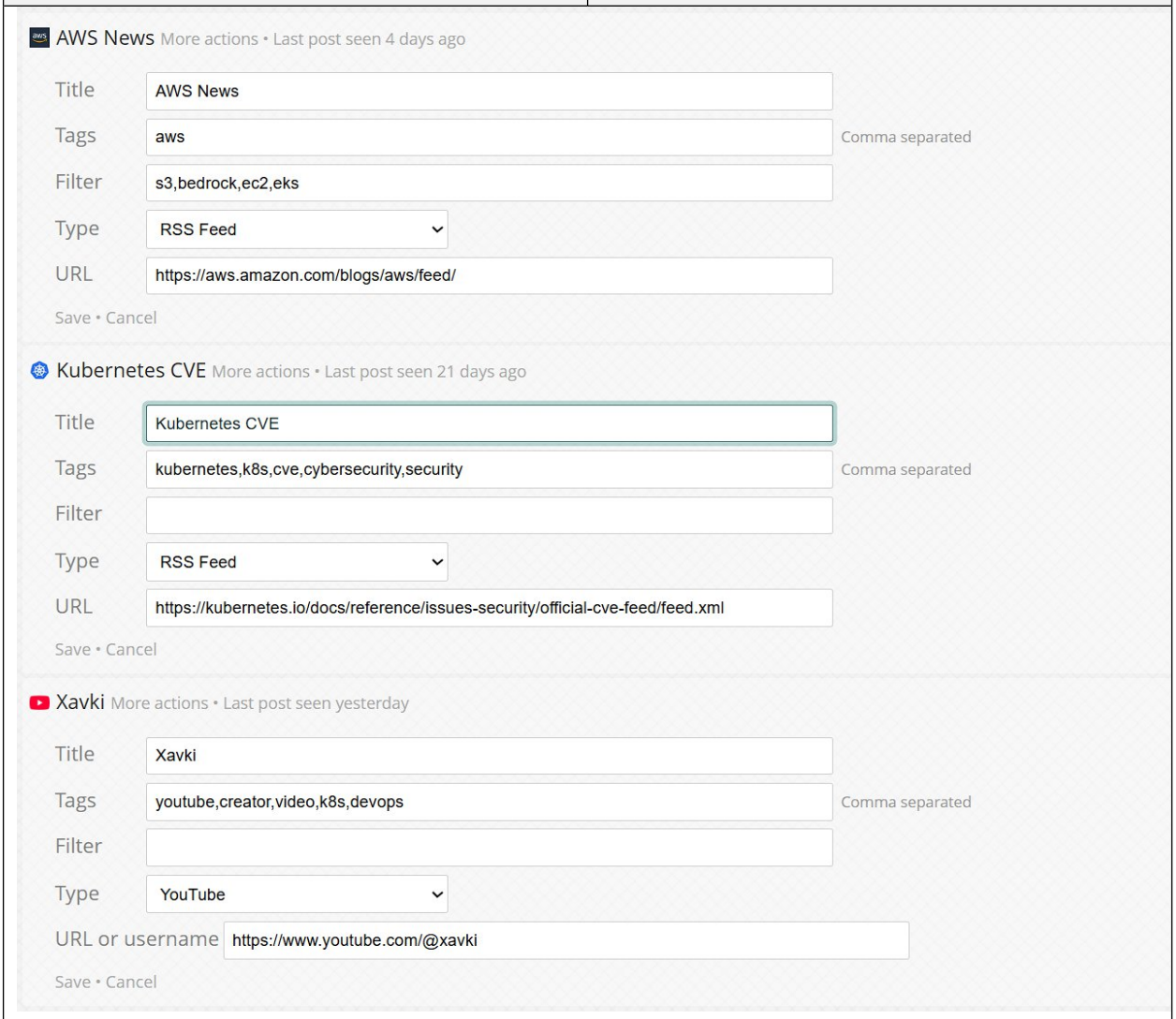
Ajoutez d'autres fiches en copiant ce tableau si vous retenez plus de trois sources.

Rubrique	Votre réponse
Nom de la source	AWS News
Adresse	https://aws.amazon.com/blogs/aws/feed/
Type	Editeur (fournisseur nuagique)
Primaire ou secondaire	Dans le contexte k8s : Secondaire
Axe de veille servi	Flux RSS
Mode de collecte	Flux RSS
Types de contenus	Alertes, Nouveautés, Articles de blog
Auteur	Employés AWS, soit rédacteurs généralistes (mais spécialisés AWS quand même), soit experts Cyber (alertes sur des CVE), soit Chefs de Produit (nouveaux déploiements)
Date	Dates et heure en clair : <pubDate>Wed, 30 Sep 2026 22:10:00 +0000</pubDate>
Preuve	Il n'y a pas de « preuve » en soit, mais les articles sont rédigés par des internes qui ont travaillé sur les produits
Recoupement	Certainement d'autres blogs d'enthousiastes, des Redditeurs ou autres consommateurs des produits pour en parler
Fiabilité de la source	A
Limite	Trop d'information, dur de recouper efficacement si on ne cherche qu'une info précise (EKS, pour k8s) sans outil tiers (LLM ou algorithme monolithique)
Pourquoi elle est adaptée	Les fournisseurs se doivent d'assurer un maximum de sécurité et de compatibilité de leurs services avec les produits (EKS pour k8s) et disposent d'une vue maximisée sur les éventuelles failles logicielles avec leur nombre de clients.

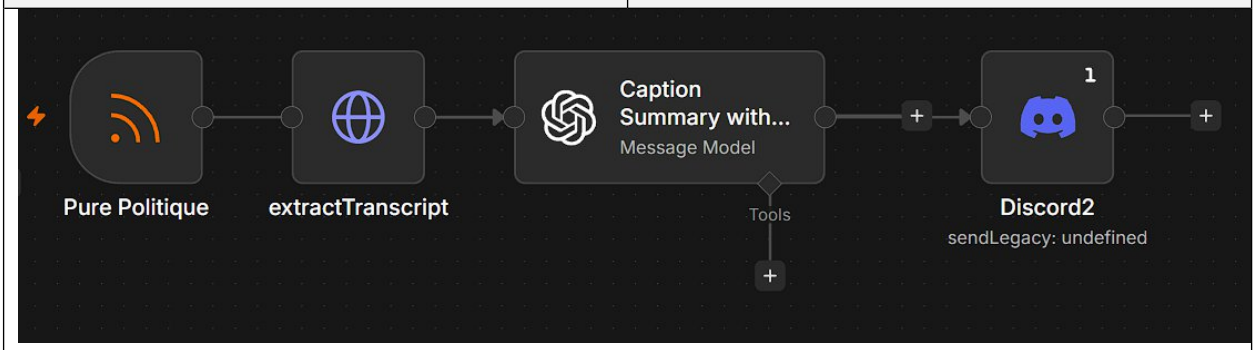
Outil de collecte

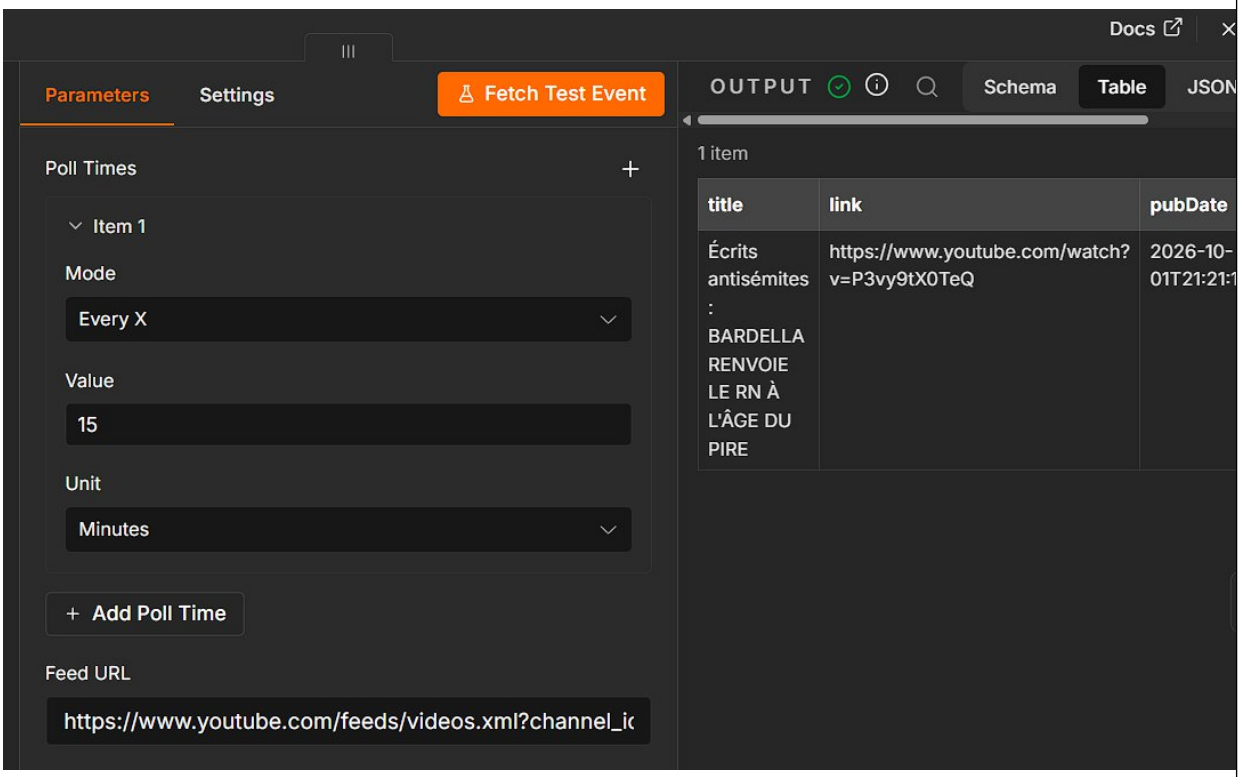
L'outil doit être réellement paramétré : une capture d'écran ou une démonstration en fait foi.

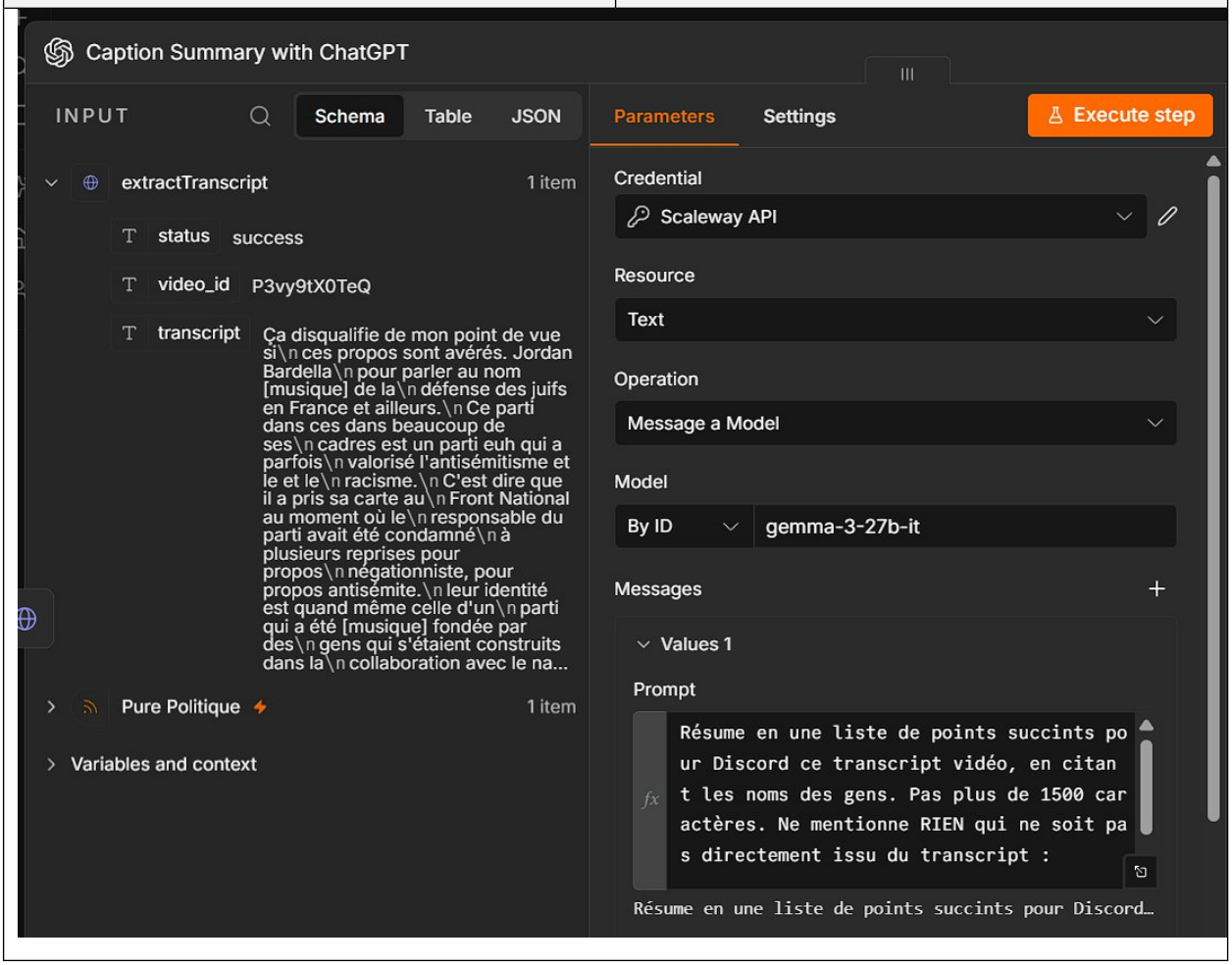
Rubrique	Votre réponse
Outil choisi	selfoss
Licence	GPL-3
Hébergement	Auto-hébergé
Raison du choix	1 – Disponible sur mon serveur auto-hébergé 2 – Gratuit 3 – Léger 4 – Compatible SSO sur mon serveur (LDAP)
Flux ou abonnements ajoutés	

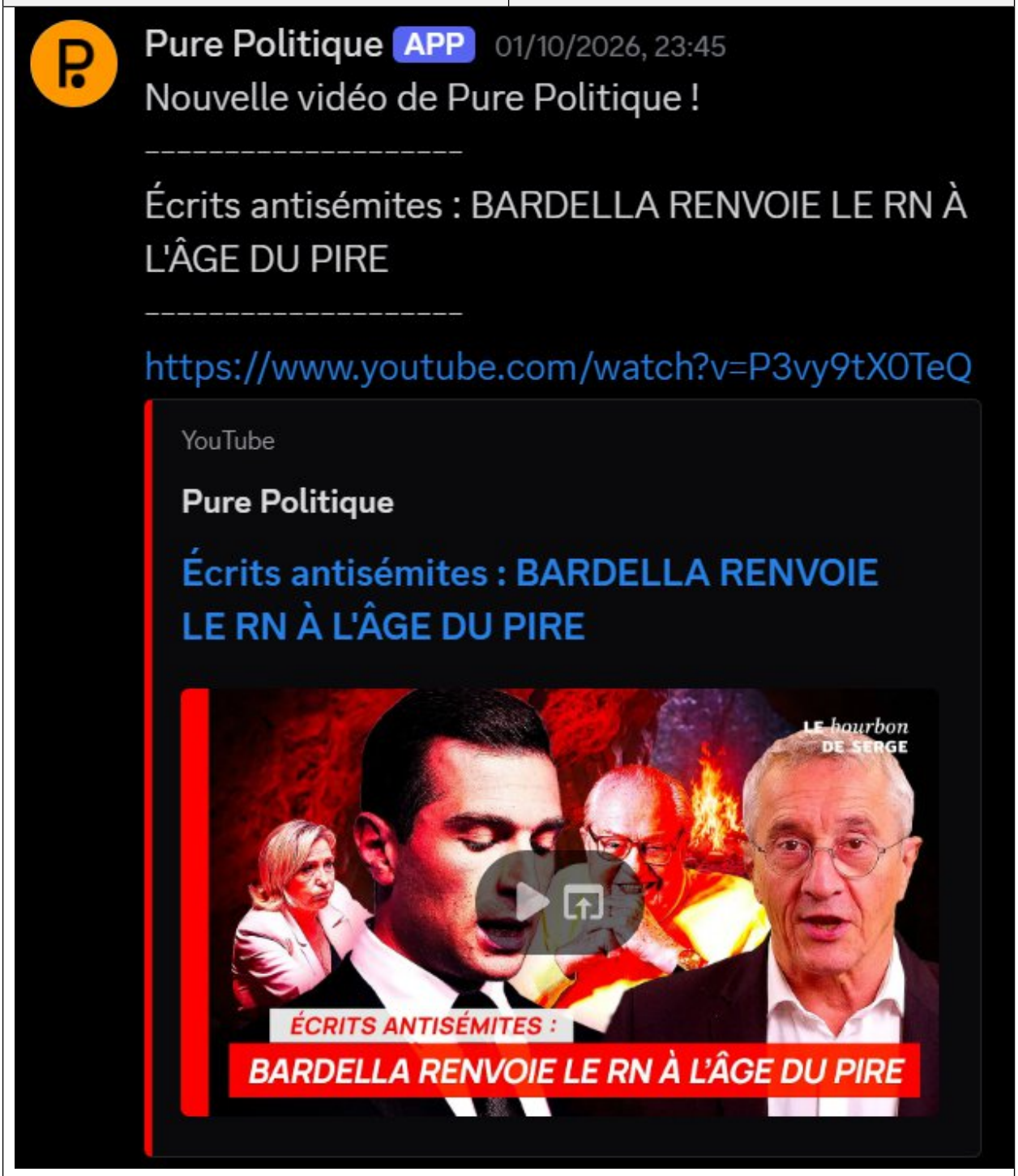
Rubrique	Votre réponse
	
Filtres et étiquettes	Aws, k8s, cve, cybersecurity, youtube, devops (et d'autres secondaires)
Alerte configurée	Pour l'instant aucune ; une solution pro-active serait un flux RSS contrôlée dans n8n, avec un Webhook Discord (pour du perso) ou Slack (pour du pro) avec soit un bulletin instantanée (peut mener à une fatigue) soit un bulletin général de fin de journée (posté 30m avant la fin de journée pour permettre de finir la journée sur de la veille). Pour l'exemple, un flux n8n qui poste du contenu politique selon une vidéo de la chaîne « Pure Politique » :

Rubrique	Votre réponse





Rubrique	Votre réponse
	

Rubrique	Votre réponse
	
Export possible	– Export des sources en XML – Pas d'export visible des contenus en format contrôlé

- ☒ Les trois sources arrivent dans l'outil
- ☒ Au moins un filtre ou une étiquette fonctionne
- ☐ Une alerte a été testée

Note de veille

Rédigez une note à partir d'une information réelle trouvée aujourd'hui dans l'une de vos sources.

Ligne	Votre réponse
Le fait	Un utilisateur avec des droits d'écriture sur des objets spécifiques peut créer un conteneur omniscient, auto-géré et non cloisonné.
La source	Nathan HERZ (natherz97) 14 septembre 2026 à 18 :42 UTC+2 https://github.com/kubernetes/kubernetes/issues/142097
Crédibilité de l'information	Je dirais 2 ; le fait que son incident ait été pris en compte et fixé par une MR indique qu'il a soulevé un vrai problème, MAIS, la seule interaction qu'il a eut est avec visiblement un BOT du service Kubernetes. Aucun autre humain en vue dans l'incident.
L'impact pour nous	Aucun utilisateur avec des accès en écriture sur le StateController n'a été déployé dans notre base de code, que des comptes de services IAM avec des permissions sur des noms d'espace. A vérifier malgré tout, peut-être qu'un accès au StateController se fait par défaut.
L'action proposée	Mettre à jour au moins à la version 1.34 de k8s pour avoir le fix mentionné dans l'incident.

Restitution orale

Vous disposez de 2 minutes : préparez une phrase par ligne.

Point	Votre phrase
Mon axe de veille	Mon axe de veille pour l'exercice est un agrégateur RSS classique auto-hébergé, comme quand j'étais étudiant en IT. Une solution pérenne pour moi serait d'utiliser n8n maintenant, avec des webhooks pour poster dans Discord.
Mes trois sources et pourquoi elles sont adaptées	1. L'équipe CVE officielle de Kubernetes, parce que... Voilà quoi. Pas besoin d'en dire plus 2. Le CISA, la CyberDéfense Américaine, qui recense toutes les CVE connus de ses services. Fiable en tant que grosse institution. Il faut juste que les CVE ne soient pas wokes ou féminines ou communistes et ça passe 3. AWS News, qui donne de tout lié à l'écosystème AWS, y compris EKS, qui s'occupe de déployer les grappes k8s, fiable vu qu'ils ont des stats sur l'usage, les failles et les défaillances des services avec force journaux
Ce que la source sécurité m'a appris aujourd'hui	Deux nouvelles CVE, mais en soit rien que je n'ai déjà su déterminer auparavant. A la rigueur j'ai appris que des fois, il existe des équipes CVE internes aux produits, quand je pensais que c'était VRAIMENT extérieur
Ce que je garde demain	Rien, les flux RSS c'est un peu dépassé en soit. Assurer une veille efficace ans un monde d'infobésité demande d'utiliser des outils plus fins et des filtres dynamiques
Ce que j'abandonne	Tout espoir.

Avant de rendre la fiche :

- ☒ L'axe comporte sujet, question, destinataire et fréquence
- ☒ Trois fiches de source au minimum sont complètes
- ☒ Au moins une source est consacrée à la sécurité

- ☒ L'outil de collecte fonctionne
- ☒ La note de veille cite sa source et propose une action
- ☐ Plus aucun texte entre crochets ne subsiste (*je ne comprends pas... Ça veut dire quoi ? J'utilise des crochets et des parenthèses pour tout un tas de raisons [notamment des parenthèses dans les parenthèses comme usage typographique classique]*)