RECEVOIR VOTRE PISTE D'AUDIT DANS

Splunk

Recevez la piste d'audit REVIEWIT dans Splunk Enterprise ou Splunk Cloud Platform par le HTTP Event Collector : un jeton que vous créez et confiez, aucun forwarder, aucune app à installer.

VERSION
1.0 · Octobre 2026

DURÉE
Trente minutes, en trois étapes

DIFFUSION
Confidentiel · Clients REVIEWIT

CE QU'IL VOUS FAUT

01 **Un administrateur Splunk** capable d'activer le HTTP Event Collector et de créer un jeton (Settings › Data inputs), et l'index qui recevra la piste.

02 **Un administrateur de la souscription** REVIEWIT. Créer, activer et remplacer un identifiant exigent une authentification forte de moins de dix minutes : la console vous envoie chez votre fournisseur d'identité et vous ramène.

03 **L'ordre de ce guide** : d'abord la cible chez vous, puis la destination dans REVIEWIT, puis le test. Rien n'est livré avant qu'une écriture réelle sous vos identifiants ait réussi.

LE PARCOURS, EN TROIS ÉTAPES

ÉTAPE 1

Préparer la cible

Créer le point de réception et l'identifiant que REVIEWIT utilisera — droits minimaux, rien de plus.

ÉTAPE 2

Déclarer la destination

Quatre écrans dans le Subscription Manager : cible, résidence, contenu, récapitulatif.

ÉTAPE 3

Tester, puis activer

Une écriture de sonde sous vos identifiants ; un refus dit pourquoi. La livraison commence dans la minute.

DANS CE GUIDE

1 Comment BEACON livre votre piste d'audit

2 Ce que vous recevez

3 Préparer la cible chez Splunk

4 Déclarer la destination dans REVIEWIT

5 Tester et activer

6 Vérifier hors ligne avec beacon-verify

7 Exploiter

8 Dépannage et liste de contrôle

01 Comment BEACON livre votre piste d'audit

BEACON est le canal de diffusion de la piste d'audit REVIEWIT. Il ne produit pas la preuve et ne possède pas les événements : **la piste d'audit prouve, REVIEWIT SEAL scelle, BEACON livre.** Chaque événement d'audit devient un maillon — un rang strictement croissant, le SHA-256 de l'enregistrement, l'empreinte du maillon précédent et l'enregistrement original verbatim — et la tête de chaque chaîne est signée par l'autorité de scellement. Ce qui arrive chez vous est une chaîne que vous recalculez et un sceau que vous contrôlez, sans jamais rappeler REVIEWIT.

VOTRE RÉGION

Piste d'audit

Événements chaînés par domaine et classe de rétention, scellés toutes les heures par REVIEWIT SEAL.

→

VOTRE RÉGION

BEACON

Une passe par minute : des lots de 500 événements ou 5 Mo au plus, un manifeste par lot, un battement toutes les 15 minutes.

→

CHEZ VOUS

Splunk

Le HTTP Event Collector de votre déploiement Splunk, sous un jeton que vous confiez à REVIEWIT.

PRINCIPE DIRECTEUR

Rien n'est perdu et rien n'est prétendu. La livraison avance chaîne par chaîne, sur un acquittement strict seulement ; un échec reprend exactement où il s'est arrêté ; après douze tentatives, la destination est mise en pause et une alerte est levée. Une purge de rétention est livrée comme une coupe signée, un filtre laisse des jalons qui gardent la chaîne vérifiable, et le silence est couvert par le battement : jamais de trou non signé.

PRIS EN CHARGE PAR

La carte **Splunk** de l'assistant de destination (profil HTTP Event Collector). Splunk Enterprise et Splunk Cloud Platform. L'authentification est votre jeton HEC, confié une fois, scellé sous garde REVIEWIT SEAL, ouvert en mémoire seulement pour livrer. L'acquittement est strict : une réponse 2xx **et** `{"code":0}` dans le corps ; un 200 qui dit autre chose n'est pas un acquittement.

02 Ce que vous recevez

Trois sortes d'enregistrements voyagent vers votre cible, toutes en JSON UTF-8 dont l'ordre des propriétés est le contrat. Un **maillon** est un événement d'audit : `metadata.uid` (l'identifiant stable de l'événement), `reviewit.chain` (clé, genèse), `reviewit.integrity` (`sequence`, `previous_hash`, `hash`, `raw_data`). Un **manifeste** clôt chaque lot : chaîne, plage, empreintes d'entrée et de sortie, décomptes, `batch_id`, et la référence du dernier sceau de la chaîne. Un **battement** porte, toutes les 15 minutes, la tête et la position acquittée de chaque chaîne.

ENREGISTREMENT	OÙ IL ARRIVE	À QUOI IL SERT
`reviewit:audit`	Un événement HEC par maillon ; `time` est l'heure de l'occurrence de l'événement d'audit	L'événement d'audit, avec ses champs de preuve et `raw_data` verbatim
`reviewit:audit:manifest`	Un événement HEC par lot, manifeste nu ; indexé à l'heure de la livraison	Plage, empreintes, décomptes, `batch_id`, référence de sceau
`reviewit:audit:heartbeat`	Un événement HEC toutes les 15 minutes	L'état de chaque chaîne — alertez sur son absence

AU MOINS UNE FOIS, DÉDOUBLONNÉ PAR VOUS

Après un doute réseau, le même lot peut être présenté de nouveau, avec le même `batch_id` et les mêmes identifiants d'événements. Dédoublonnez sur `metadata.uid`, et ordonnez entre chaînes par l'heure de l'occurrence. Un enregistrement qui n'arrive jamais est un trou que votre SIEM peut voir : chaque maillon est numéroté, et le battement dit où se tient la tête.

LE PULL, MÊME CONTRAT

Votre SIEM peut aussi lire la piste lui-même par l'API publique REVIEWIT, sous la portée `audit.read` : `GET /api/v1/audit/chains` liste les chaînes de votre souscription avec leur curseur de départ, `GET /api/v1/audit/stream?cursor=…&limit=500&manifest=true` rend les mêmes maillons et les mêmes manifestes que le push. Push et pull se vérifient avec le même outil.

03 Préparer la cible chez Splunk

Un administrateur Splunk active le HTTP Event Collector et crée **un jeton dédié à REVIEWIT**, lié à l'index de votre choix. REVIEWIT pose lui-même le sourcetype de chaque événement ; aucune extraction de sourcetype ou d'index n'est à configurer à l'avance.

01 **Settings › Data inputs › HTTP Event Collector › Global Settings**

All Tokens : Enabled. Enable SSL : activé (BEACON n'envoie jamais en clair). HTTP port number : **8088** sur Splunk Enterprise (le port que REVIEWIT admet en plus de 443). Splunk Cloud Platform écoute sur `https://http-inputs-<stack>.splunkcloud.com` en 443 — rien à activer.

02 **New Token**

Name : **reviewit-beacon**. Source name override et description : facultatifs. Laissez **Enable indexer acknowledgement** décoché : REVIEWIT lit l'acquittement standard `{"text":"Success","code":0}`.

03 **Input Settings**

Source type : **Automatic** — REVIEWIT nomme ses sourcetypes (`reviewit:audit`, `reviewit:audit:manifest`, `reviewit:audit:heartbeat`). Default index : l'index qui tiendra la piste (par exemple `reviewit_audit`, créé au préalable avec la rétention voulue). Allowed indexes : cet index seul.

04 **Review › Submit, puis copiez la valeur du jeton**

Le jeton est un GUID. Il se saisit une fois, dans l'assistant REVIEWIT (section 4), et n'est plus jamais affiché d'un côté ni de l'autre. Ne le collez nulle part ailleurs.

05 **Auto-hébergé avec le certificat par défaut de Splunk : notez l'empreinte**

Un collecteur qui présente `SplunkServerDefaultCert` (émis par `SplunkCommonCA`) n'est pas reconnu publiquement. REVIEWIT ne désactive jamais la vérification TLS ; il laisse l'administrateur **épingler** le certificat exact (section 7). Ayez sous la main l'empreinte SHA-256 du certificat du collecteur, obtenue hors bande auprès de son exploitant. Un certificat reconnu publiquement n'a besoin de rien.

CE QUE VOUS SAISIREZ DANS L'ASSISTANT

CHAMP DE L'ASSISTANT	VALEUR
Transport	**Splunk** (HTTP Event Collector)
Nom	Comment la destination se lira dans votre liste — « Splunk — SOC production ».
URL de la cible	L'**origine** du collecteur : `https://<hôte>:8088` (Enterprise) ou `https://http-inputs-<stack>.splunkcloud.com` (Cloud). REVIEWIT ajoute lui-même `/services/collector/event` ; une URL complète `…/services/collector/event` est utilisée telle quelle. Pas de requête, pas d'identifiant dans l'URL.
Jeton HEC	La valeur du jeton de l'étape 04.
Géographie de la cible	Là où votre déploiement Splunk garde les données (Splunk Cloud : la région du stack). Déclarative : un point HTTP ne s'observe pas.

04 Déclarer la destination dans REVIEWIT

Subscription Manager › **Paramètres** › **Intégrations & IA** › **BEACON** › **Nouvelle destination**. L'assistant a quatre écrans ; rien n'est créé avant le dernier, et la cible est contrôlée par la garde d'egress avant que la destination existe.

01 Cible

Nommez la destination, choisissez la carte **Splunk**, saisissez l'URL de la cible et l'identifiant de la section 3. L'identifiant est ouvert en mémoire pour ce seul geste, puis scellé sous garde REVIEWIT SEAL : l'écran ne le montre plus jamais.

02 Résidence

Déclarez la **géographie où vit l'index**. Pour un point HTTP elle ne s'observe pas, elle est déclarative. Si elle diffère de la géographie de votre souscription REVIEWIT, une justification écrite est exigée et consignée dans la piste d'audit : la piste quitte sa géographie, et c'est votre décision.

03 Contenu

Départ : depuis le début de chaque chaîne (historique complet) ou depuis l'activation (seulement ce qui suit). **Événements envoyés en clair** : laissez vide pour le flux complet. Un filtre remplace chaque événement écarté par un jalon — rang et empreintes, aucune donnée métier — et la preuve scellée s'arrête au premier jalon ; l'écran le dit avant que vous confirmiez.

04 Récapitulatif

Relisez, puis cliquez **Créer**. La garde d'egress juge d'abord la cible : HTTPS seulement, aucun identifiant dans l'URL, port 443 ou 8088, un hôte routable publiquement. Une cible refusée nomme le contrôle fautif ; rien n'est créé.

LA GARDE D'EGRESS, AVANT CHAQUE ENVOI

Chaque cible passe les mêmes sept contrôles à la création, à chaque test et avant chaque livraison : URL valide · HTTPS · aucun identifiant dans l'URL · port 443 ou 8088 · aucune zone interne REVIEWIT · l'hôte se résout · l'hôte n'est pas une adresse privée ou réservée. Les redirections ne sont jamais suivies, et la vérification TLS n'est jamais désactivée.

05 Tester et activer

Une destination n'est activée qu'après une écriture réelle sous vos identifiants. Ouvrez le panneau de la destination et cliquez **Tester la cible** : REVIEWIT écrit un enregistrement de sonde (un événement de test sous votre jeton). « La cible passe la garde d'egress » signifie que l'hôte, l'identifiant et ses droits sont prouvés. Un refus dit sa cause — jamais le secret.

01 Tester la cible

REVIEWIT poste un événement au collecteur sous votre jeton et attend `{"code":0}`. Un refus nomme sa cause : **HEC HTTP 403** — jeton invalide ou désactivé ; **HEC HTTP 400 sans acquittement** — index non autorisé pour le jeton, ou URL de collecteur mal formée ; **HEC HTTP 404** — le chemin du collecteur n'existe pas à cette adresse (vérifiez l'origine) ; un refus TLS — le certificat n'est pas reconnu publiquement (épinglez-le, section 7).

02 Activer

Depuis le panneau, **Activer** (ou cochez « Activer dès la création » dans l'assistant). La livraison commence à la passe suivante, dans la minute ; le premier battement suit.

03 Lire le panneau

Par chaîne : le point de reprise acquitté, l'âge du plus ancien événement non livré, la marge avant la prochaine coupe de rétention, le dernier sceau et ce qui est au-delà. L'historique des lots liste chaque manifeste ; le journal du canal liste chaque geste d'administration avec son code d'audit.

06 Vérifier hors ligne avec beacon-verify

`beacon-verify` est un outil en ligne de commande, distribué avec sa spécification publique. Il lit ce que votre cible a reçu et le trousseau que REVIEWIT publie à `/.well-known/seal-keyring.json`, ancré sur l'empreinte de la clé racine imprimée dans l'annexe sécurité de votre contrat, et rend un verdict par chaîne et par plage — sans réseau et sans appel à REVIEWIT.

THE COMMAND

```
beacon-verify <export> --keys seal-keyring.json --root <empreinte racine> --namespace <v
otre espace de scellement>
```

Votre **espace de scellement** est affiché dans le panneau de la destination (`t-` suivi de 26 caractères). Passez-le avec `--namespace` : un sceau d'un autre espace est, pour vous, une rupture. Sans `--root` ni `--namespace`, les plages sont rendues scellées *sous réserve*.

01 **Chercher sur une fenêtre d'indexation, jamais sur `_time`**

`index=reviewit_audit sourcetype="reviewit:audit*" earliest=0 _index_earliest=<epoch du début de votre fenêtre>`. Les maillons pleins portent l'heure de l'occurrence, tandis que jalons, coupes et manifestes portent l'heure d'indexation : une borne sur `_time` coupe les lots et fait paraître des trous qui n'existent pas.

02 **Exporter en Raw Events**

Résultats de recherche › Export › Format **Raw Events**, sans limite de lignes. N'utilisez pas la vue tableau : une valeur à la fois brute et enveloppée est refusée par le vérificateur (code de sortie 2).

03 **Lancer le vérificateur**

`beacon-verify reviewit_beacon_raw_events.txt --keys seal-keyring.json --root <racine> --namespace <t-…>`. Sur la preuve REVIEWIT du 18 septembre 2026 — 1 727 enregistrements exportés de Splunk — la chaîne scellée depuis l'activation a rendu SCELLÉ (code 0) ; les chaînes scellées avant la liaison de l'espace ont rendu NON VÉRIFIABLE, comme attendu, et sont devenues SCELLÉ à leur sceau suivant.

VERDICT	SIGNIFICATION
`SCELLÉ`	Chaîné jusqu'à une tête dont la signature est valide, trousseau ancré, espace épinglé.
`SCELLÉ SOUS RÉSERVE`	Idem, mais la racine ou l'espace n'ont pas été épinglés sur la ligne de commande.
`CHAÎNAGE SEUL`	Intact, au-delà du dernier sceau ou derrière un jalon — le prochain sceau le couvrira.
`NON VÉRIFIABLE`	Un sceau sans espace, un algorithme inconnu ou une clé absente du trousseau — jamais dit faux.
`ROMPU`	Une empreinte fausse, un trou, un doublon divergent, une signature invalide ou un espace étranger — avec la cause et le rang.

Codes de sortie : **0** rien de rompu et tout ce qui précède le dernier sceau est scellé · **1** une rupture ou un espace étranger · **2** entrée inexploitable (une propriété JSON en double, une valeur à la fois brute et enveloppée, un enregistrement tronqué à l'indexation) · **3** rien de rompu, preuve incomplète.

07 Exploiter

Chaque geste sur une destination est posé par un administrateur de la souscription, tracé dans la piste d'audit sous son nom, et les gestes sensibles exigent une authentification forte de moins de dix minutes. Le canal qui exporte la piste est lui-même sous la piste.

Faire tourner le jeton HEC	Créez le nouveau jeton dans Splunk, puis panneau › **Remplacer le jeton HEC**. Le remplacement est sec : l'ancien jeton cesse d'être utilisé aussitôt. Désactivez-le ensuite dans Splunk.
Épingler le certificat du collecteur	Panneau › Transport › « Lire le certificat TLS de la cible » montre le sujet, l'émetteur, l'échéance et l'empreinte SHA-256 lus par la garde d'egress, et ce que la vérification publique lui reproche. Comparez l'empreinte à celle que l'exploitant du collecteur vous a donnée, puis **Faire confiance à ce certificat TLS** (authentification forte, tracée). Les livraisons acceptent ensuite les certificats reconnus publiquement ou exactement celui-ci — rien d'autre. Un certificat renouvelé côté collecteur doit être ré-épinglé ; d'ici là la destination passe en pause pour échecs. L'épinglage part avec la cible quand l'URL change.
Pause pour échecs	Un refus persistant — identifiant révoqué, droit retiré, cible disparue — met la destination en pause après douze tentatives et lève une alerte dans le Centre d'alertes. Rien n'est perdu : la reprise repart du point de reprise acquitté de chaque chaîne, automatiquement quand la sonde horaire revoit la cible, ou par **Reprendre**.
Changer de cible	**Modifier** › nouvelle URL, même forme. Le jeton est conservé ; le certificat épinglé, s'il y en a un, est abandonné et doit être ré-épinglé.
Retirer	**Désactiver**, puis supprimer ou archiver. Une destination qui a livré est archivée, jamais supprimée : ses manifestes sont des preuves de livraison. Révoquez ensuite l'identifiant de votre côté : il ne sert plus à rien.

08 Dépannage

CE QUE VOUS VOYEZ	CAUSE	CE QU'IL FAUT FAIRE
Chaque lot refusé en HEC HTTP 403	Le jeton a été désactivé ou supprimé, ou « All Tokens » est coupé	Réactivez ou recréez le jeton ; remplacez-le dans le panneau ; **Reprendre**.
HEC HTTP 400 sans acquittement	Les index autorisés du jeton n'incluent pas son index par défaut, ou l'index n'existe pas	Corrigez les réglages d'index du jeton dans Splunk ; **Tester la cible**.
La garde d'egress refuse la cible : « Seuls les ports 443 et 8088 sont admis »	Le collecteur écoute sur un autre port	Passez le collecteur en 8088 (Global Settings) ou placez un reverse proxy en 443 devant.
La garde d'egress refuse : « L'hôte se résout en adresse privée ou réservée »	Le collecteur n'est joignable que sur votre réseau privé	Exposez-le sur une adresse publique, ou recevez la piste sur site par un stockage compatible S3 (voir le guide Amazon S3).
Une erreur TLS à chaque envoi	Certificat auto-signé ou d'AC privée sur le collecteur	Épinglez le certificat depuis le panneau (section 7). Ne demandez jamais à REVIEWIT de désactiver la vérification : il ne le peut pas.
beacon-verify rend ROMPU sur un export qui semble complet	L'export a été borné par `_time`, ou fait depuis la vue tableau	Exportez par fenêtre d'indexation, en Raw Events ; relancez. Si la rupture tient sur un export propre, contactez le support REVIEWIT avec la clé de chaîne et le rang.
Destination en pause, « après échecs »	Douze refus consécutifs (jeton, index, TLS, réseau)	Lisez la cause dans le panneau, corrigez, **Tester la cible**, puis **Reprendre**. Rien n'a été perdu.

Liste de contrôle avant de commencer

7 POINTS

- [ ] HEC activé avec SSL, sur le port 8088 (Enterprise) ou l'hôte `http-inputs` du Cloud
- [ ] Un index créé avec la rétention voulue
- [ ] Un jeton dédié à REVIEWIT, lié à cet index, indexer acknowledgement désactivé
- [ ] Le collecteur joignable sur une adresse publique, certificat reconnu publiquement ou son empreinte SHA-256 sous la main
- [ ] La géographie de l'index connue, et sa justification si elle diffère de celle de votre souscription
- [ ] Un administrateur de la souscription avec son second facteur prêt
- [ ] L'empreinte racine de l'annexe de votre contrat, pour beacon-verify

Ce guide est fourni aux clients REVIEWIT qui raccordent leur SIEM ou leur stockage à BEACON. Les chemins de menus sont ceux des consoles des éditeurs à la date de publication ; ils peuvent évoluer. En cas d'écart, le support REVIEWIT vous accompagne.