Déploiement de mon premier Honeypot avec Cowrie et Splunk

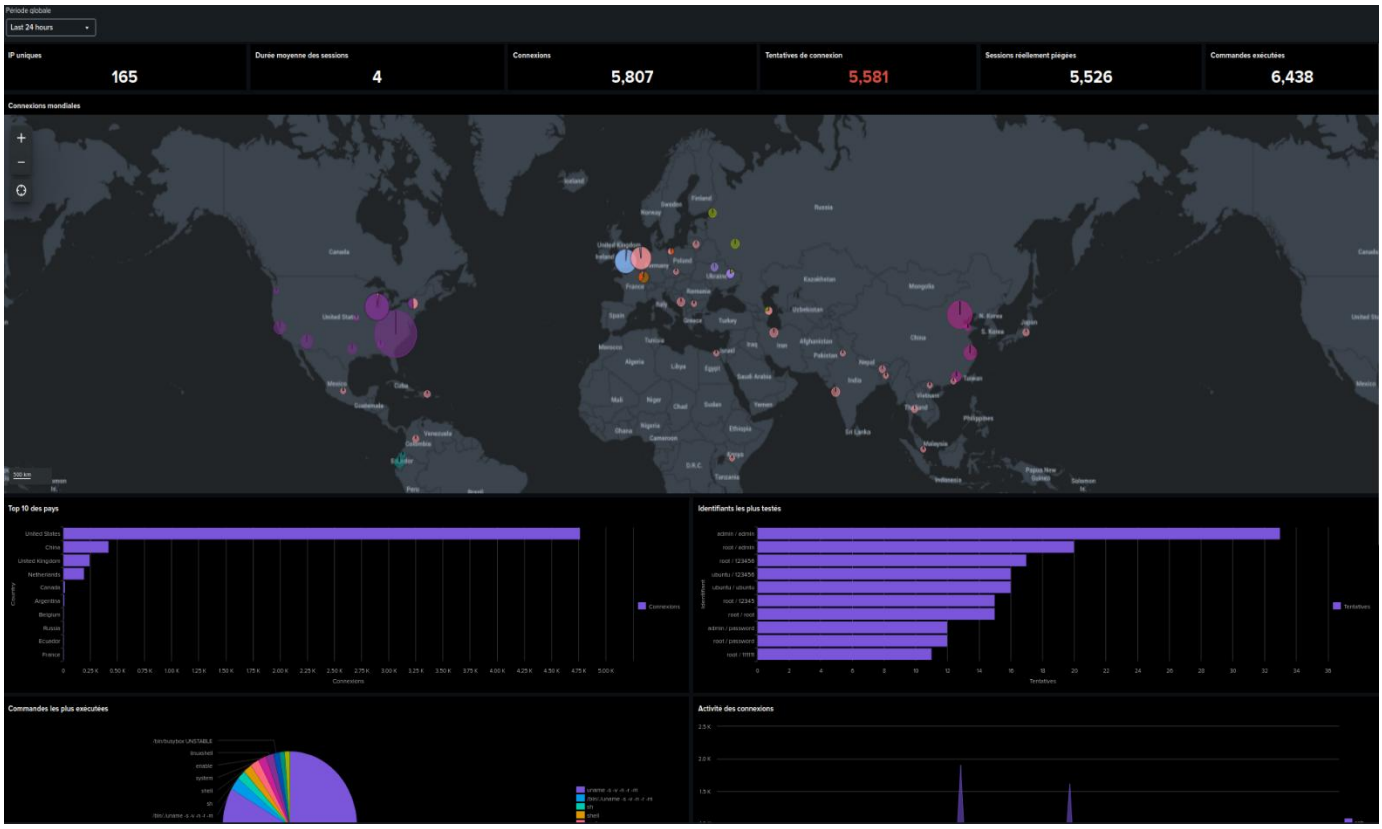
Collecte sécurisée de tentatives SSH et Telnet sur un VPS OVH

Mael Philibert

BTS SIO option SISR

Projet perso lié à l'administration système et cybersécurité

15 septembre 2026



Sommaire :

1) Contexte et objectifs :

Dans le cadre de mon apprentissage en autodidacte, j'ai souhaité mettre en place un honeypot accessible depuis Internet.

L'objectif est de comprendre et de se rendre compte comment les robots recherchent des services **SSH** ou **Telnet** mal protégés, quels identifiants ils testent et quelles commandes ils exécutent après une authentification.

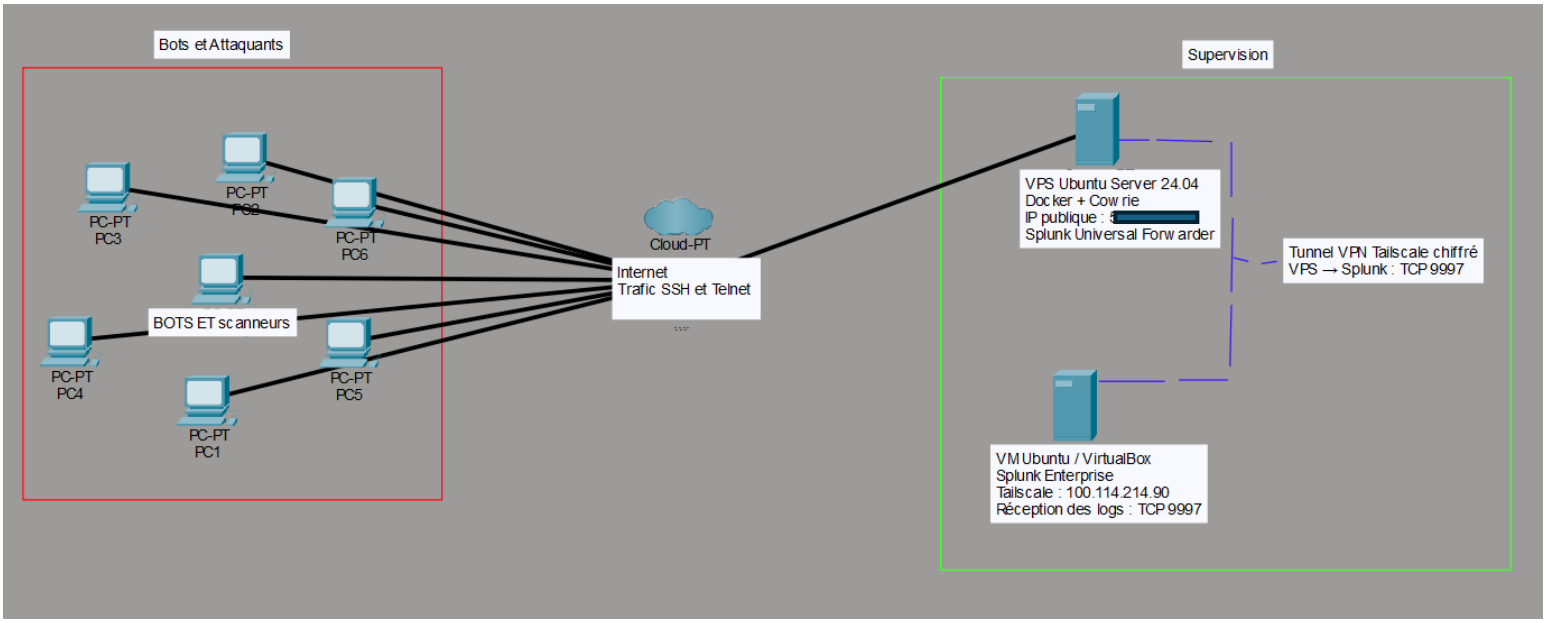
Le résultat principal est une chaîne complète de supervision : les événements produits sur le VPS sont centralisés dans Splunk Enterprise et présentés dans un tableau de bord que j'ai personnalisé et actualisé automatiquement.

Le projet reste défensif : Cowrie fournit un faux terminal, tandis que l'accès réel au VPS est séparé et protégé par une clé SSH sur un autre port.

Objectifs techniques

- Exposer un faux service SSH sur le port 22 et un faux service Telnet sur le port 23.
- Conserver l'administration réelle sur un port distinct et uniquement par clé SSH.
- Isoler Cowrie dans un conteneur Docker avec des ressources limitées.
- Acheminer les journaux vers une machine Splunk sans ouvrir Splunk directement sur Internet.
- Construire un tableau de bord lisible pour analyser l'activité en quasi-temps réel.

2) Architecture tu projet



Zone	Composants	Rôle
VPS OVH	Ubuntu 24.04, Docker, Cowrie, Forwarder	Recevoir et journaliser les tentatives
Réseau privé	Tailscale	Transporter les journaux vers le poste local
Machine locale	VirtualBox, Ubuntu Desktop, Splunk Enterprise	Indexer, rechercher et visualiser les données

3) Déploiement et sécurisation

Cowrie a été déployé sur un VPS Ubuntu à l'aide de Docker Compose. Les ports publics 22 et 23 redirigent respectivement vers les services SSH et Telnet du honeypot.

L'administration réelle a été déplacée sur le port 22222 afin de ne pas entrer en conflit avec Cowrie.

22 TCP = SSH Cowrie = exposition à internet / Faux environnement

23 TCP = Telnet Cowrie = exposition à internet / Faux environnement

22222 TCP = Vrai SSH = Internet limité / Clé SSH, pare feu de base UFW

9997 TCP = Réception Splunk = Tailscale uniquement / .

Local Host : 8000 TCP = Interface Splunk = exposition internet / .

4) Collecte et centralisation des logs JSON dans Splunk

Splunk Enterprise a été installé dans une machine virtuelle Ubuntu Desktop disposant de 6 Go de mémoire vive.

Un Universal Forwarder installé sur le VPS surveille le fichier cowrie.json.

Il transmet les nouveaux événements vers Splunk sur le port 9997 (configuré manuellement dans Splunk).

Les deux machines communiquent grâce à Tailscale (voir schéma), ce qui évite d'exposer le récepteur Splunk sur l'adresse publique.

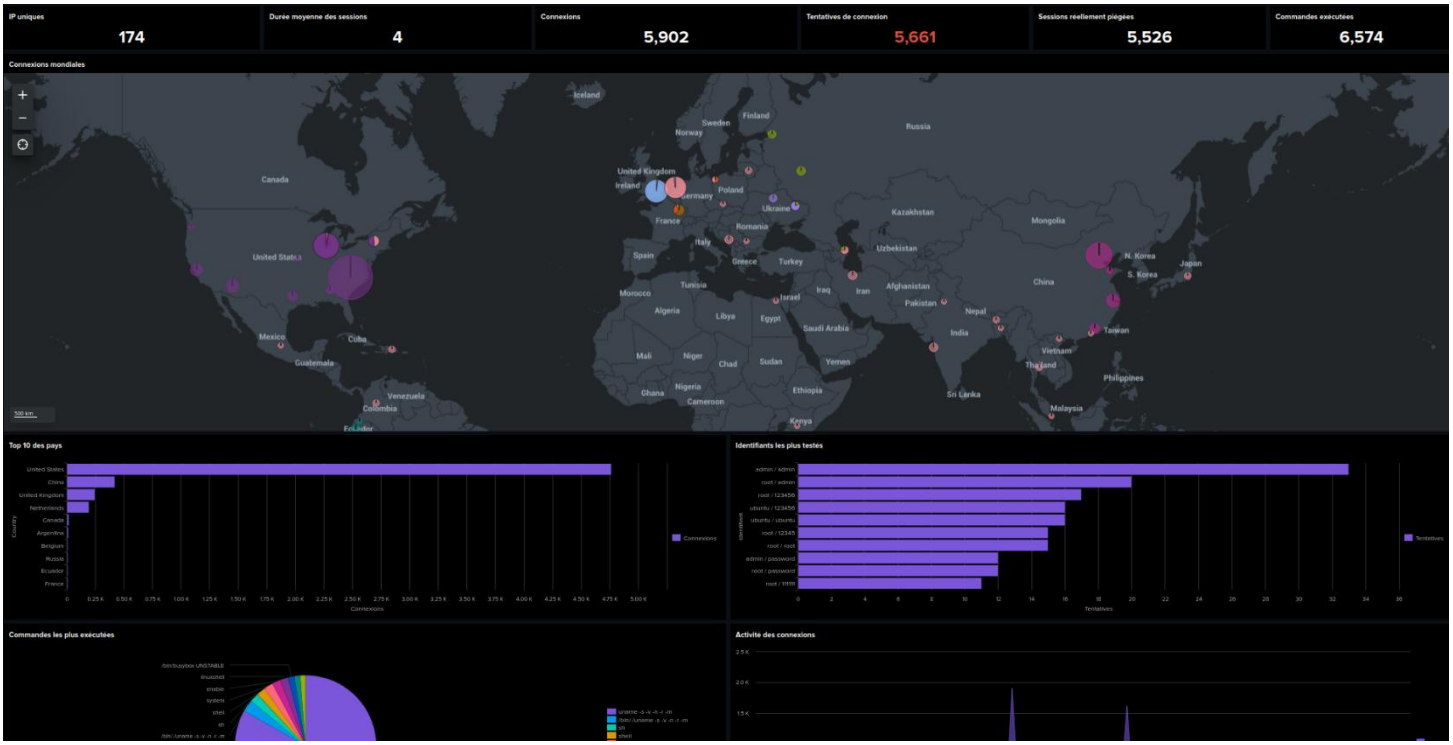
Configuration logique du Forwarder :

```
[monitor:///var/lib/docker/volumes/cowrie_cowrie-var/_data/log/cowrie/cowrie.json]
index = cowrie     sourcetype = _json     disabled = false
[tcpout:splunk_vm]     server = adresse_tailscale_de_la_vm:9997     useACK = true
```

5) Tableau de bord et premiers résultats

Le tableau de bord Cowrie Live a été créé dans Dashboard Studio et personnalisé pour une meilleure expérience. Les recherches sont actualisées plus ou moins toutes les minutes et utilisent une période globale de 24 heures.

Les vues principales regroupent les indicateurs, la carte mondiale, les pays d'origine, les identifiants testés, les commandes et l'activité temporelle. Voici les résultats après 16 HEURES d'attente :



Indicateur	Valeur observée	Interprétation
Adresses IP uniques	174	Sources distinctes observées
Connexions	5 902	Ouvertures de sessions SSH ou Telnet
Tentatives d'authentification	5 661	Couples utilisateur et mot de passe testés
Sessions authentifiées dans Cowrie	5 526	Accès au faux terminal, pas au vrai VPS
Commandes exécutées	6 574	Actions saisies dans les sessions simulées
Durée moyenne	4 secondes	Sessions automatisées généralement très courtes

On observe aussi différents identifiants essayer, notamment un top 3 avec :

Admin / admin

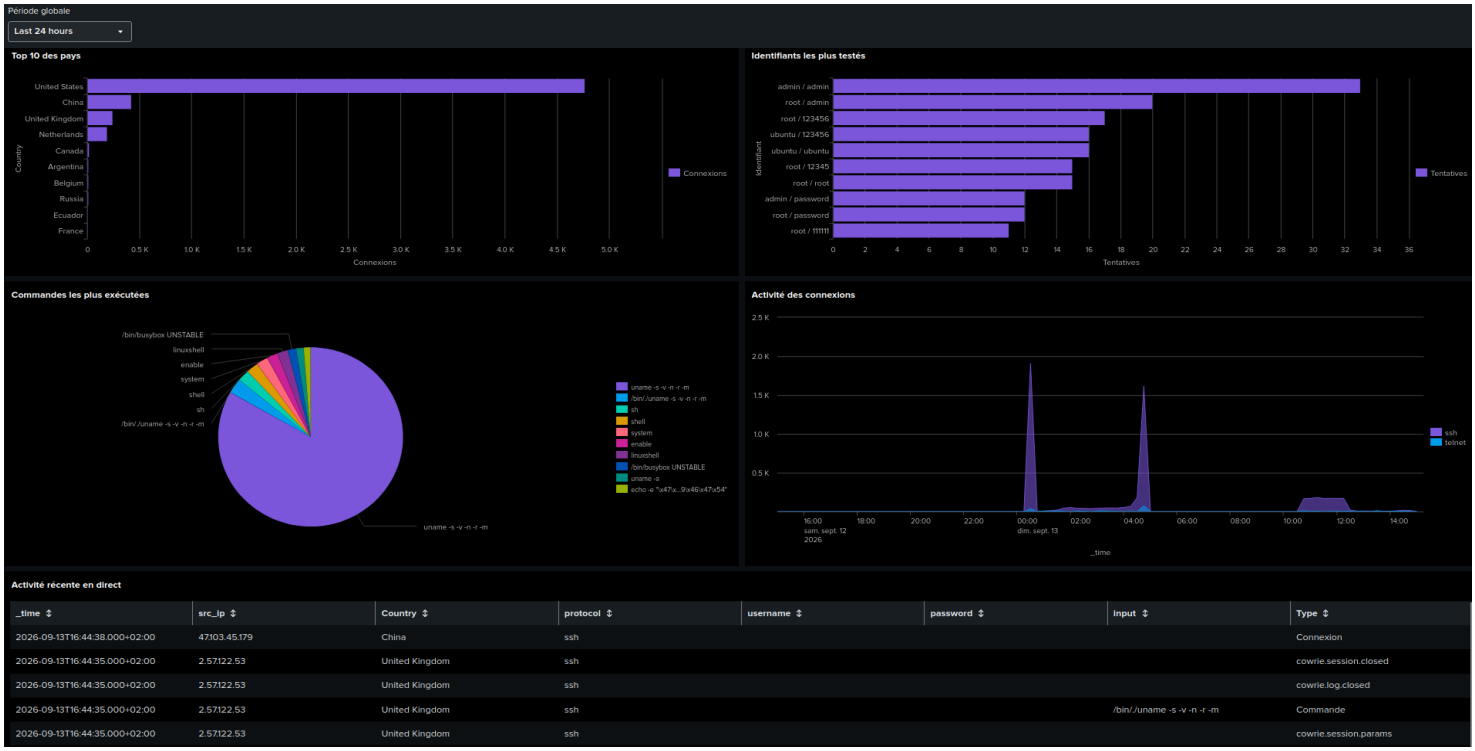
Root / admin

Root / 123456

6) Analyse technique :

La commande la plus fréquente est uname -s -v -n -r -m. Elle sert à récupérer des informations sur le noyau, le nom de la machine et l'architecture.

Son utilisation répétée confirme qu'une grande partie de l'activité provient de scripts automatisés qui cherchent à identifier rapidement le système distant.



_time	src_ip	Country	protocol	username	password	Input	Type
2026-09-13T16:44:38.000+02:00	47.103.45.179	China	ssh				Connexion
2026-09-13T16:44:35.000+02:00	2.57.122.53	United Kingdom	ssh				cowrie.session.closed
2026-09-13T16:44:35.000+02:00	2.57.122.53	United Kingdom	ssh				cowrie.log.closed
2026-09-13T16:44:35.000+02:00	2.57.122.53	United Kingdom	ssh			/bin/./uname -s -v -n -r -m	Commande
2026-09-13T16:44:35.000+02:00	2.57.122.53	United Kingdom	ssh				cowrie.session.params

Les bots testent ces valeurs car des équipements ou serveurs mal configurés utilisent encore parfois des comptes par défaut. Dans Cowrie, ces essais sont enregistrés sans fournir l'accès au système réel.

On observe également le classement des pays enregistrant le plus grand nombre de tentatives de connexion, a commencer par les États-Unis, suivis de la Chine, du Royaume-Uni et des Pays-Bas.

Conclusion.

Ce projet m'a permis de mettre en place une chaîne de supervision complète, depuis l'exposition contrôlée d'un honeypot jusqu'à la centralisation et à l'analyse graphique des événements dans Splunk.

L'architecture mise en place sépare clairement le faux service destiné à attirer les bots de l'accès réel d'administration. Elle constitue une base exploitable pour poursuivre mon apprentissage de Splunk, de Linux et de la sécurité des systèmes.

Cette expérimentation montre également qu'une machine exposée sur Internet peut rapidement être ciblée par des tentatives de connexion automatisées.

Il est donc essentiel de sécuriser correctement les serveurs, les équipements réseau et, plus généralement, tout système accessible **depuis Internet.**

Mael Philibert