Crowdsec

Celui qui nous intéresse aujourd'hui répond au nom de CrowdSec et arbore une belle licence MIT toute propre et toute libre. Massivement collaboratif, CrowdSec est appelé à gagner en efficacité au fure et à mesure que sa communauté d'utilisateurs grandira.

crowdsec
Image not found or type unknown

Cet article vous présente un test de l'installation et des principales fonctionnalités de CrowdSec, il y a bien cet article qui était pas mal, mais il teste une version déjà bien ancienne (13 révisions depuis).

On compare CrowdSec à un fail2ban copieusement dépoussiéré, mais ne vous y trompez pas, on ne parle pas ici d'un dépoussiérage mais d'une approche radicalement nouvelle de concevoir vos parefeux, ce pour l'ensemble de vos services, VM, ou containers exposés sur le Net. Pour faire simple, CrowdSec va analyser vos journaux de connexion à la recherche des ip aggressives et confier à des bouncers le soin de les bloquer. CrowdSec se base autant sur la détection du comportement d'une IP que sur sa réputation.

CrowdSec se définit comme un EDR (Endpoint Detection and Response), ce qui lui confère un super pouvoir face aux poussiéreux antivirus et au désormais sénile Fail2Ban : la faculté de pouvoir corréler les analyses. Et dans notre cas précis, le fonctionnement collaboratif et crowdsourcé de ces analyses renforce leur acuité. Sur le papier, on a donc tout bon au niveau de la réponse à apporter aux nouveaux types de menaces parfois complexes à détecter.

L'assistant d'installation qui nous accompagne durant le procesus de configuration va détecter vos services et vous proposer des scénarios adaptés à votre environnement.

Le concept de réputation des adresses ip permet à CrowdSec d'établir des listes de blocage, sur la base d'un fonctionnement collaboratif (crowdsourcing). Si une IP attaque des machines monitorées par CrowdSec, cette IP vient alimenter en temps réel une liste de blocage mutualisée, réactualisée quotidiennement. Lorsque CrowdSec repère une adresse IP au comportement agressif, le scénario déclenché et l'horodatage sont envoyés à l'API REST pour être vérifiés et intégrés si besoin dans la liste de blocage. C'est donc automatique, ça fait forcément gagner du temps, et ça permet de détecter des choses bien plus fines qu'une analyse de logs au papier calque :)

Sous le capot, on retrouve du GoLang (donc un support IPV6 by design) et des scenarios YAML. Prometheus, Metabase et Docker viennent complèter notre stack.

C'est parti pour une installation avec la découverte de cet assistant

Le git se trouve ici

On commence par récupérer la dernière version de CrowdSec :

```
$ curl -s https://api.github.com/repos/crowdsecurity/crowdsec/releases/latest | grep browser_download_url| cut -d '"' -f 4  | wget -i
```

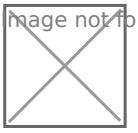
on décompresse l'archive et on lance le wizard qui va nous guider pour configurer correctement CrowdSec

```
$ tar xvzf crowdsec-release.tgz
$ cd crowdsec-v1.0.13/
$ sudo ./wizard.sh -i
```

CrowdSec détecte vos services, puis vous propose ensuite une liste de collections adaptées à votre environnement, notez que j'ai recontré des difficultés à ce stade à cause d'un petit bug graphique m'empêchant de voir ce qui est sélectionné ou pas, rien de méchant et ce devrait être vite corrigé. En outre la détection préalable des services entraine un choix par défaut, donc en validant à l'aveuglette le choix par défaut, ça tombe en marche ;)

Précisons que le concept de collection est de fournir à un service de quoi se défendre : c'est à dire un parser de logs adapté au service ainsi qu'un scenario de détection des attaques sur ce service.

Un peu plus loin CrowdSec nous invite à nous munir d'un bouncer qui sera en charge des blocages, CrowdSec se contentant de l'analyse des journaux de connexions. Une petite visite du hub CrowdSec vous permettra de trouver les bouncers qui correspondent à votre environnement :

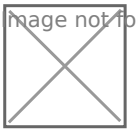


En fonction de vos services à protéger, vous installerez donc les bouncers qui vont bien avec la commande

```
$ sudo cscli bouncers add nom-du-bouncer
```

Enfin, une fois l'installation achevée, le processus se lance, et vous propose de vous familiariser avec cscli, l'utilitaire qui va vous permettre de piloter notre CrowdSec... et je vous vois venir, vous aimeriez bien un truc un peu plus sexy et graphique que de la cli pure.

On y retrouve par exemples nos listes communautaires d'IP à la fréquence énervée d'updates et absolument tout dont a besoin, sauf pour le dircom...



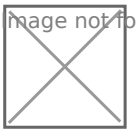
C'est justement grâce à cscli que nous allons pouvoir déployer un joli dashboard avec Prometheus, Metabase et Docker. Le test a été réalisé sur ParrotSec par pur masochisme, mais si vous êtes sur une Debian like, pour installer docker il vous faudra taper la commande suivante (un "apt-get install docker" ne fonctionnera pas) :

```
$ sudo apt-get install -y docker.io
```

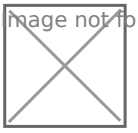
Une fois docker installé, on peut lancer le setup du dashboard avec cscli :

```
$ sudo cscli dashboard setup
```

Cette commande va nous créer un container Metabase, avec un identifiant et un password autogénéré. Nous allons donc pouvoir nous rendre sur notre dashboard à l'url http://127.0.0.1:3000 (notez que seules les connexions depuis les IP locales sont acceptées... follow the white rabbit to whitelist).



Et vous voilà un maillon de la securité proactive sauce CrowdSec. Vous l'aurez compris, plus nous serons nombreux à l'utiliser, plus CrowdSec gagnera en acuité.



Nous avons pu échanger un peu avec l'équipe qui a su répondre à nos interrogations, notamment concernant le business model. La confidentialité de vos données est une préoccupation réelle et CrowdSec n'a aucune vue dessus, son business model s'oriente sur cette base de données de réputation d'IP, par définition très volatile. C'est donc également très respectueux du RGPD et le succès de CrowdSec nous semble assuré, tant pas les compétences de l'équipe que par la manière dont ce projet a été pensé. Un succès que beaucoup semblent sentir, puisque la team CrowdSec a récemment levé 5 millions de dollars (https://crowdsec.net/2021/05/05/fundraiser-announcement/), et la cadence de développement laisse augurer beaucoup de dynamisme et de nouveautés (on attend avec impatience les collections et bouncers - en particulier Apache !).

Revision #1
Created 3 October 2021 21:28:38 by garfi
Updated 3 October 2021 21:28:47 by garfi