jres RENNES 2024

Observatoire astronomique de Strasbourg | ObAS

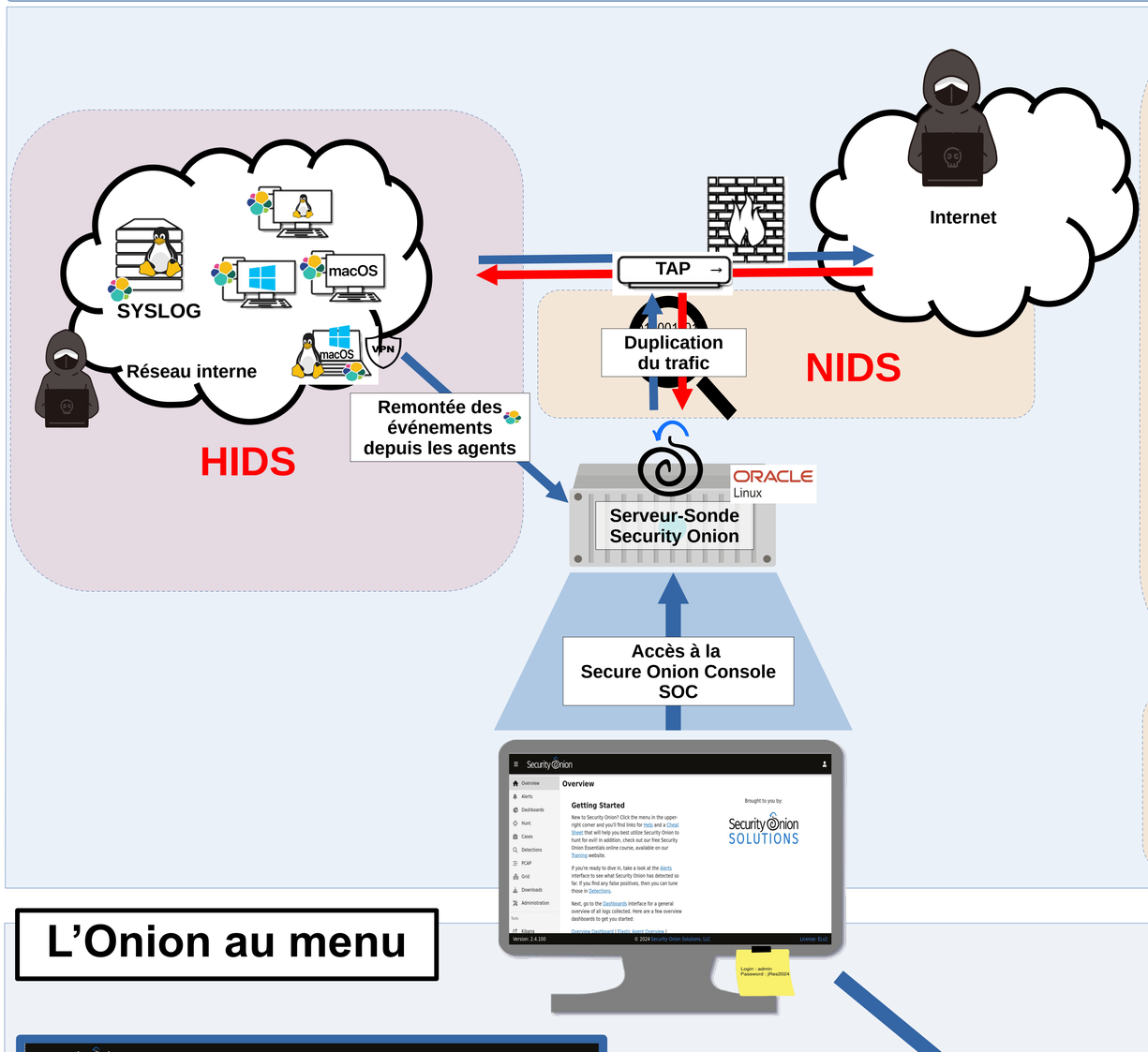
Thomas Keller, Christophe Saillard

Sécurité dans les labos, l'Onion fait la force

Security Onion

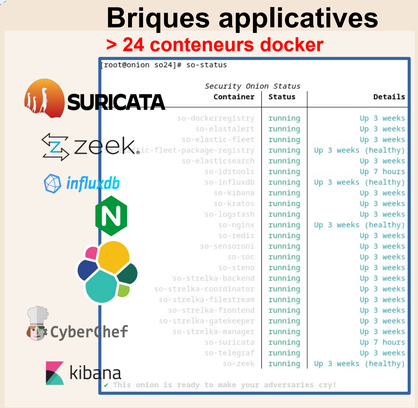
« Made by defenders for defenders »

Une distribution Linux qui intègre un large éventail de logiciels libres de sécurité permettant une **surveillance des flux réseau** jusqu'aux logs des **équipements terminaux**. La solution offre des fonctionnalités de **SIEM**, **NIDS**, **HIDS** et bien plus encore...



Briques applicatives

> 24 conteneurs docker



Matériel

> DELL R730XD + MD1200
> CPU XEON E5 (6C/12T)
> RAM 64G
> HD 96 TB

> Entre 10 et 12 jours de rétention du trafic

Count	Type
53 622	suricata
3 884	yara
1 644	sigma

59150 règles de détection disponibles

	Count	event.severity_label
⚠	83 309	medium
⚠	15 070	low
⚠	2 321	high

100700 alertes sur 24h (05/11/2024)

Au delà du NIDS et du HIDS, à quoi peut nous servir l'Onion ? Quelques exemples...
> À déceler des erreurs de configurations dans les règles de filtrage
> À lever des doutes lors des signalements d'incidents par le CERT
> À vérifier si des utilisateurs ont interagi avec des liens dans des campagnes de phishing depuis notre réseau ou si des équipements communiquent avec des IOCs.

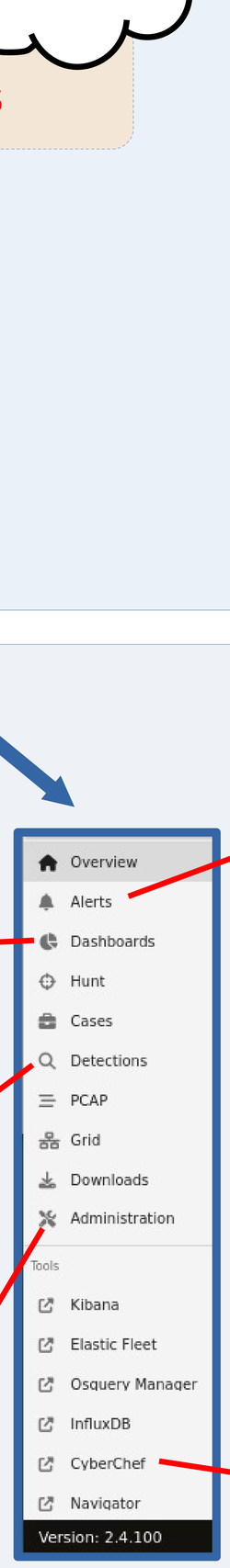
L'Onion au menu

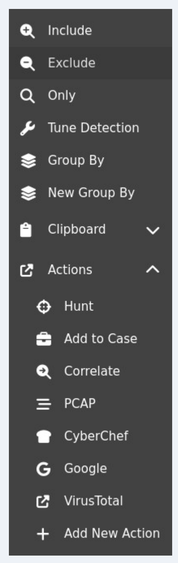
Ciblage de données précises à l'aide de requêtes OQL (*Onion Query Language*) basées sur la syntaxe de ElasticSearch

Par exemple : zones géographiques, IP sources et ports de destinations

Création/suppression activation/désactivation et personnalisation des règles de détection

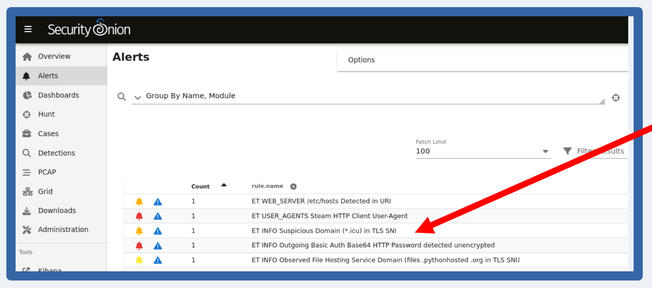
Administration de toutes les briques logicielles depuis un point unique



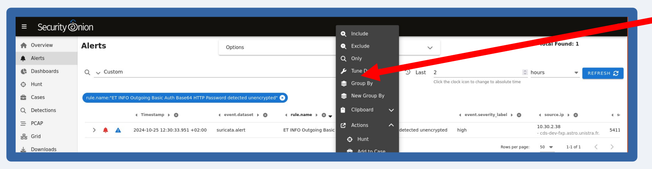


Menu contextuel

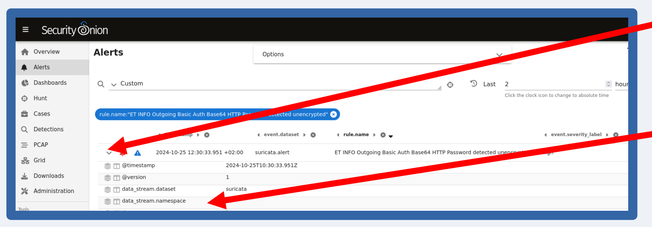
Exemple de traitement d'une alerte



1. Une alerte critique (mot de passe en clair) est repérée depuis la page des alertes.

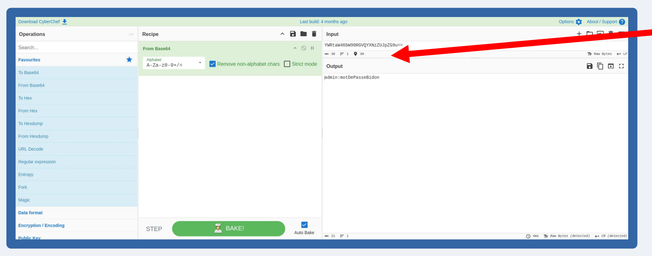


2. L'alerte est sélectionnée.



3. En cliquant sur le chevron on accède à l'intégralité des données de l'alerte.

4. Le mot de passe encodé en base 64 est accessible dans le champs *network.data.decoded*.



5. L'outil *CyberChef* nous permet de décoder la chaîne de caractères.

Une solution aux petits onions...

Une solution clé en main et facile à administrer

...SO intègre une collection d'outils sous un même environnement et évite de devoir déployer et d'administrer une multitude de serveurs dédiés.

Projet open source, gratuit et très dynamique

...une offre « pro » existe qui donne accès à plus de fonctionnalités, au support…

Pas besoin de matériel spécifique

...vous pouvez l'installer **sur un seul serveur** physique, une VM, tout dépend de vos besoins et de votre infra réseau. Il existe aussi des appliances...

Très bien documentée

...de nombreuses ressources (doc et vidéos) sont disponibles sur le web.

...qui fait parfois pleurer

Un projet très voire trop actif

...mises à jour très voire trop fréquentes, des changements parfois radicaux sur certaines fonctionnalités (exemple : suppression du support de *Wazuh* au profit d'*Elastic Agent)*

Un projet de moins en moins « open » ?

...fonctionnalités réservées à la version « pro », appliances…

« Le temps ne respecte pas ce qui se fait sans lui »

...malgré une belle ergonomie, il faut se bloquer du temps pour bien l'utiliser...