Sécurité à l'ObAS...

...l'Onion fait la force !

Une histoire racontée par Thomas et Christophe

21/03/2022

Cette histoire se passe à l'ObAS

- Mais au fait , c'est quoi l'ObAS ?
  - UMR7550 Observatoire astronomique de Strasbourg
  - 100 personnes (en vrai, il y a du monde)
  - 2 grandes équipes de recherche
  - 1 ERC
  - Centre de Données de Strasbourg (Infrastructure de Recherche CNRS)
  - Un planétarium, mais bientôt plus

  - Et surtout un jardin avec des moutons et des écureuils

Oups, on a oublié ça

- 1 salle serveur (8 racks) + 2 racks au DC
- ~ 40 Serveurs physiques (Ubuntu, Centos, Debian)
- ~ 70 VM
- ~ 200 postes (Linux, MacOS, Windows)
- ~ 40 commutateurs
- 2 informaticiens beaux et sympas (+1 gars en CDD super compétent)

Contexte du projet de sécurisation

- **Incident de sécurité interne courant 2018**
  - On a rien vu, réseau interne zone de confiance
- Prise de conscience : **le danger peut aussi venir de l'intérieur !**
- Se protéger uniquement de l'extérieur ne suffit plus
- Plus jamais ça...

- **Étude de la sécurisation dans le cadre d'un contrat d'apprentissage de licence pro** de oct. 2020 à sep. 2021

Cahier des charges

- Détection des scans et BF SSH
- Détection des accès aux fichiers sensibles
- Détection des comportements anormaux sur le réseaux
- Sécurisation des postes de travail et serveurs

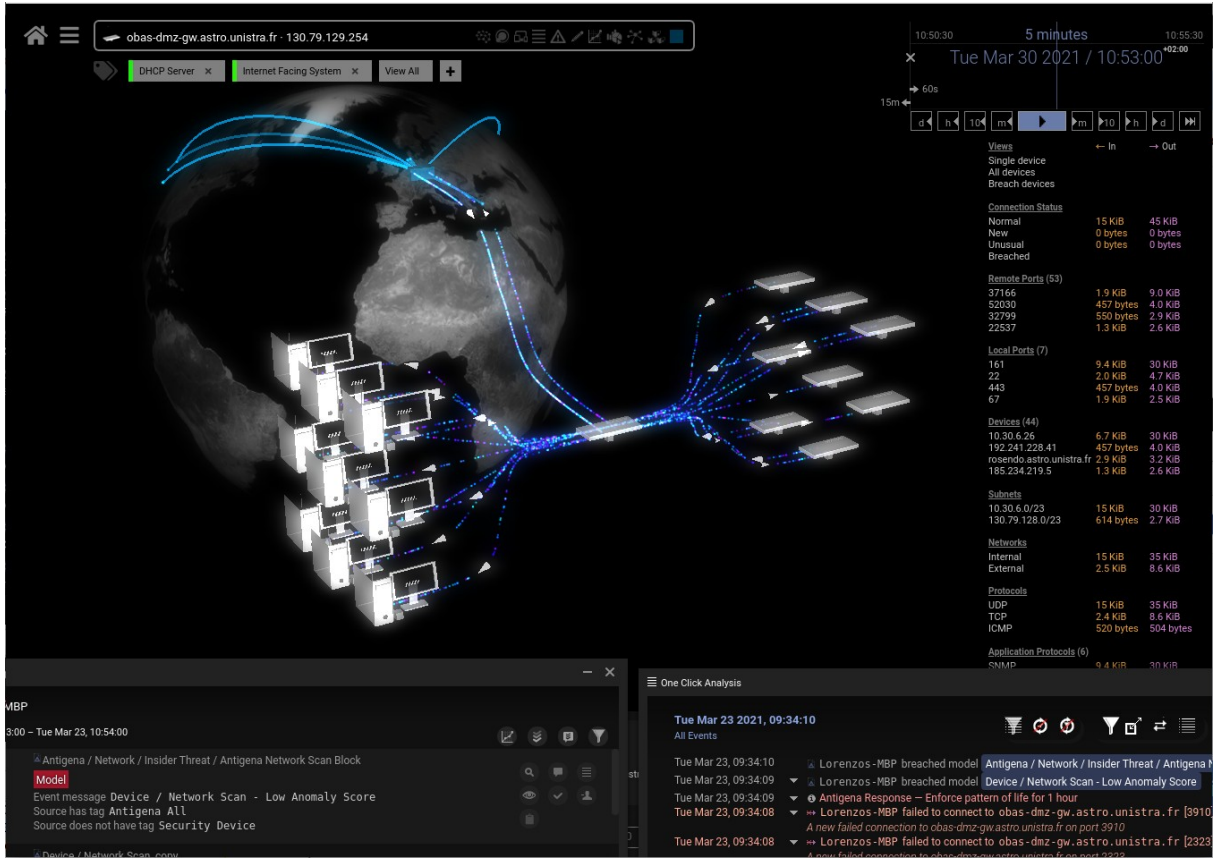
Déroulement du projet

1) Évaluation des besoins
2) Veille technologique pour identifier les solutions du marché (NIDS et HIDS)
    1) DarkTrace
    2) Security Onion
    3) Crowdsec, Fail2ban, UFW, etc.
3) Évaluation des solutions
4) Déploiement de la solution retenue

DarkTrace vs SecurityOnion

DarkTrace

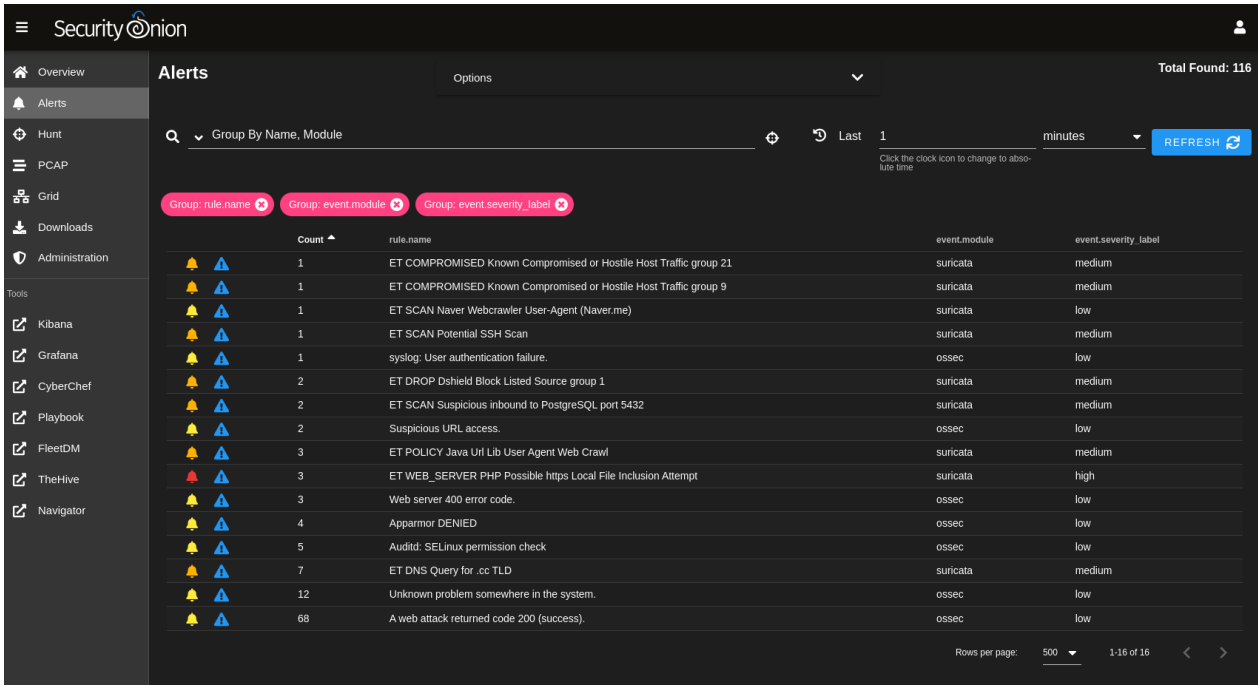
- Solution commerciale
- IA
- POV de plusieurs mois
- Interface vraiment bien
- Pas d'agent pour linux
- Tarif vraiment trop élevé
- Appliance en location
- NIDS uniquement



DarkTrace vs SecurityOnion

SecurityOnion

- Solution libre
- HIDS +NIDS
- Interface sobre
- Tarif vraiment cool
- Coche toutes les cases



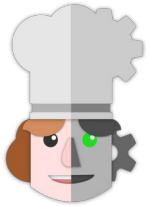
Security Onion

- Création en 2008
- Suite cohérente de nombreux logiciels de sécurité libres
- Actuellement Sur DOCKER (avant sous Ubuntu)
- La société SecurityOnionSolutions (2014) fourni des prestations de support, formation et vend des appliances
- https://securityonionsolutions.com

Dans l’Onion tout est bon

zeek

SURICATA

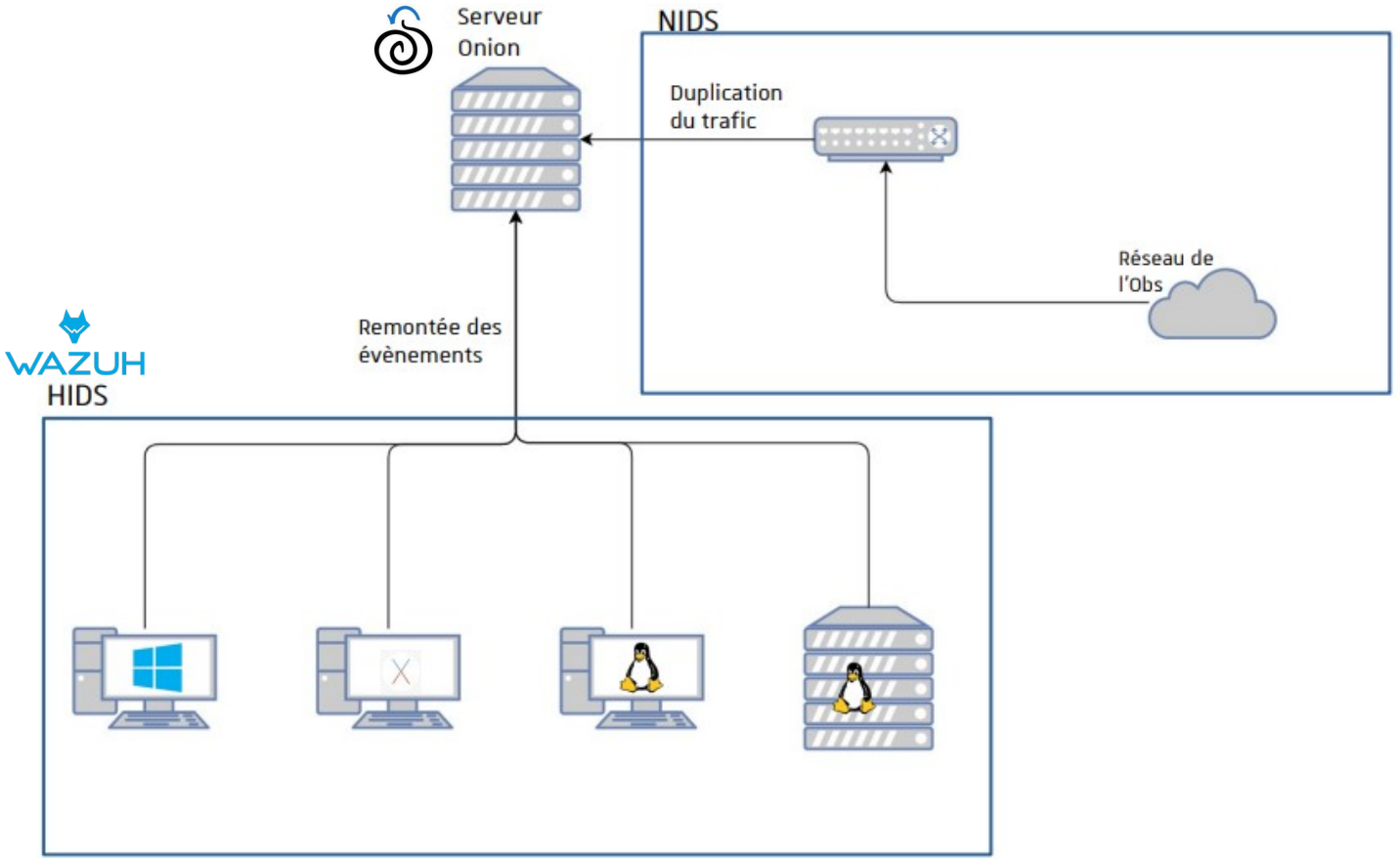


CyberChef

TheHive

WAZUH

Il est où ton Onion ?



L’Onion fait pleurer

- Juste pour lui trouver des défauts
  - Alertes très nombreuses
  - Temps de triage long, plus que prévu (15 min/jour)
  - Demande quand même des compétences et du temps
  - On laisse passer des trucs

L’Onion fait pleurer mais de rire

- Couvre tous nos besoins HIDS NIDS
- Administration facile (soup) et personnalisation des règles
- Projet très actif (~1 m-à-j par mois), il faut suivre :-)
- Une seule interface Security Onion Console (SOC)
- Alertes vraiment vraiment intéressantes
- On pourrait y passer la journée, c’est trop cool

Tu veux le voir mon Onion ?

Actuellement déployé sur un serveur DELL

- 730xd 24C / 64 Go / 50T

Démo

Conclusion

- On est loin d’une utilisation dans les règles de l’art
- Comme le badminton , même en étant nul c’est bien
- Encore des trucs à comprendre :
  - Drop de paquets
  - Paramétrage fin
  - Amélioration des notifications mail
- C’est quand la prochaine formation sécu ?

...à suivre


Merci d'être resté jusqu'ici.
Des questions ? On en remet une couche ?