



Observatoire **astronomique**
de Strasbourg | ObAS



Sécurité à l'ObAS...



...l'Onion fait la force !

Une histoire racontée par Thomas et Christophe

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

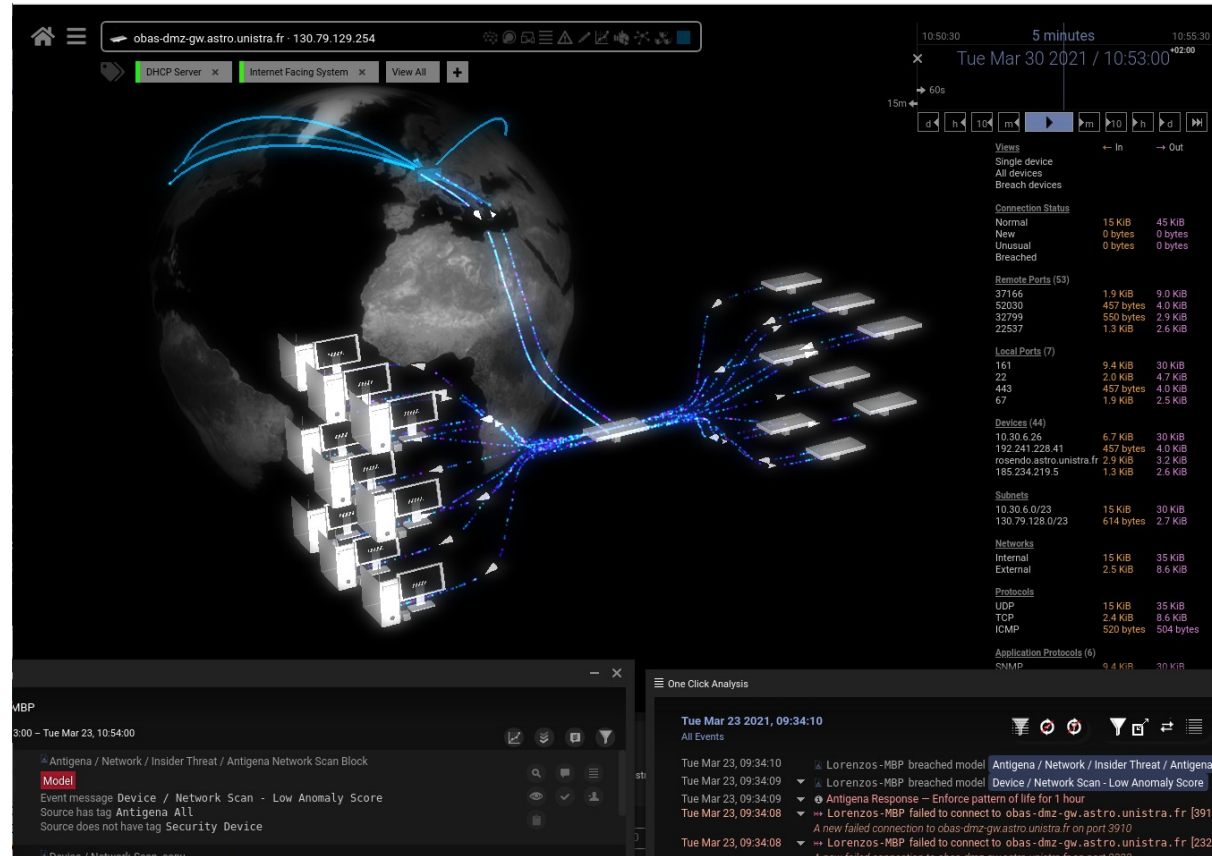
- 1) Évaluation des besoins
- 2) Veille technologique pour identifier les solutions du marché (NIDS et HIDS)
 - 1) DarkTrace
 - 2) Security Onion
 - 3) Crowdsec, Fail2ban, UFW, etc.
- 3) Évaluation des solutions
- 4) Déploiement de la solution retenue



DarkTrace vs SecurityOnion

DarkTrace

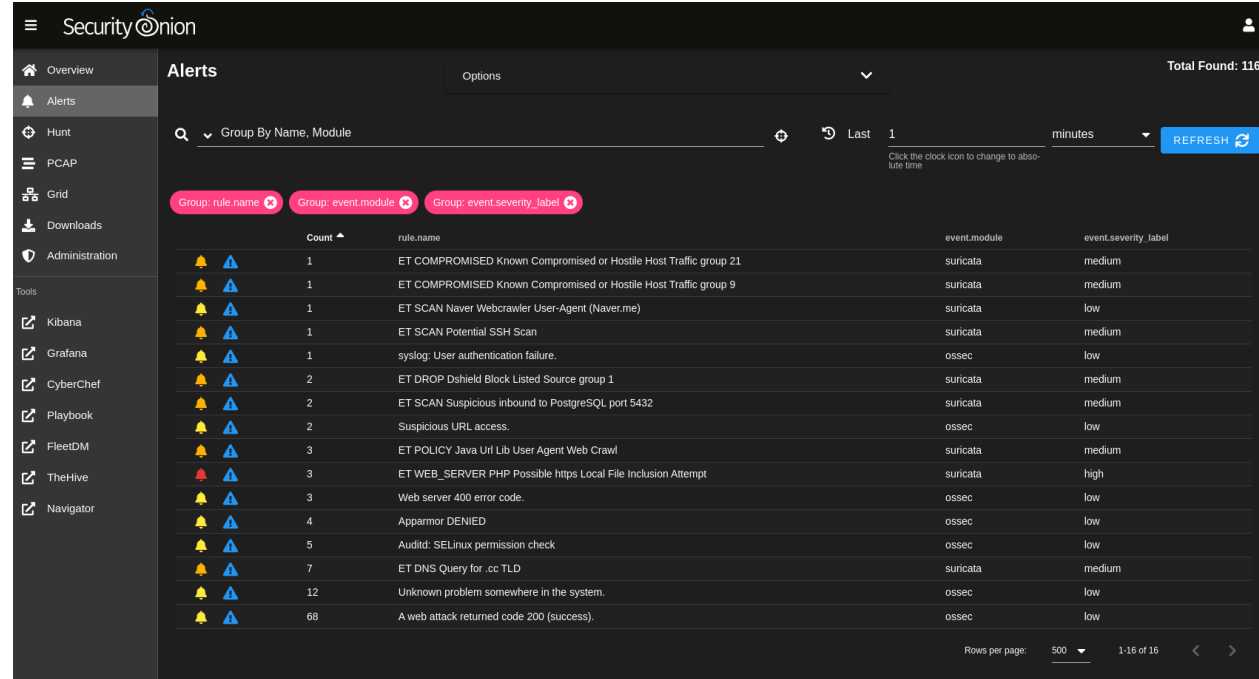
- Solution commerciale
- IA
- POV de plusieurs mois
- Interface vraiment bien
- Pas d'agent pour linux
- Tarif vraiment trop élevé
- Appliance en location
- NIDS uniquement



DarkTrace vs SecurityOnion

SecurityOnion

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



The screenshot displays the SecurityOnion Alerts interface. The left sidebar contains navigation options: Overview, Alerts, Hunt, PCAP, Grid, Downloads, Administration, and Tools (Kibana, Grafana, CyberChef, Playbook, FleetDM, TheHive, Navigator). The main area shows a list of alerts with the following columns: Count, rule.name, event.module, and event.severity_label. The alerts are sorted by Count in descending order.

Count	rule.name	event.module	event.severity_label
1	ET COMPROMISED Known Compromised or Hostile Host Traffic group 21	suricata	medium
1	ET COMPROMISED Known Compromised or Hostile Host Traffic group 9	suricata	medium
1	ET SCAN Naver Webcrawler User-Agent (Naver.me)	suricata	low
1	ET SCAN Potential SSH Scan	suricata	medium
1	syslog: User authentication failure.	ossec	low
2	ET DROP Dshield Block Listed Source group 1	suricata	medium
2	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
2	Suspicious URL access.	ossec	low
2	ET POLICY Java Url Lib User Agent Web Crawl	suricata	medium
3	ET WEB_SERVER PHP Possible https Local File Inclusion Attempt	suricata	high
3	Web server 400 error code.	ossec	low
4	Apparmor DENIED	ossec	low
5	Auditd: SELinux permission check	ossec	low
7	ET DNS Query for .cc TLD	suricata	medium
12	Unknown problem somewhere in the system.	ossec	low
68	A web attack returned code 200 (success).	ossec	low



Security Onion

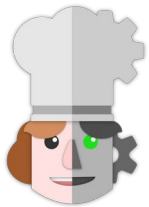
- Création en 2008
- Suite cohérente de nombreux logiciels de sécurité libres
- Actuellement Sur DOCKER (avant sous Ubuntu)
- La société SecurityOnionSolutions (2014) fourni des prestations de support, formation et vend des appliances
- <https://securityonionsolutions.com>



Dans l'Onion tout est bon



SURICATA



CyberChef

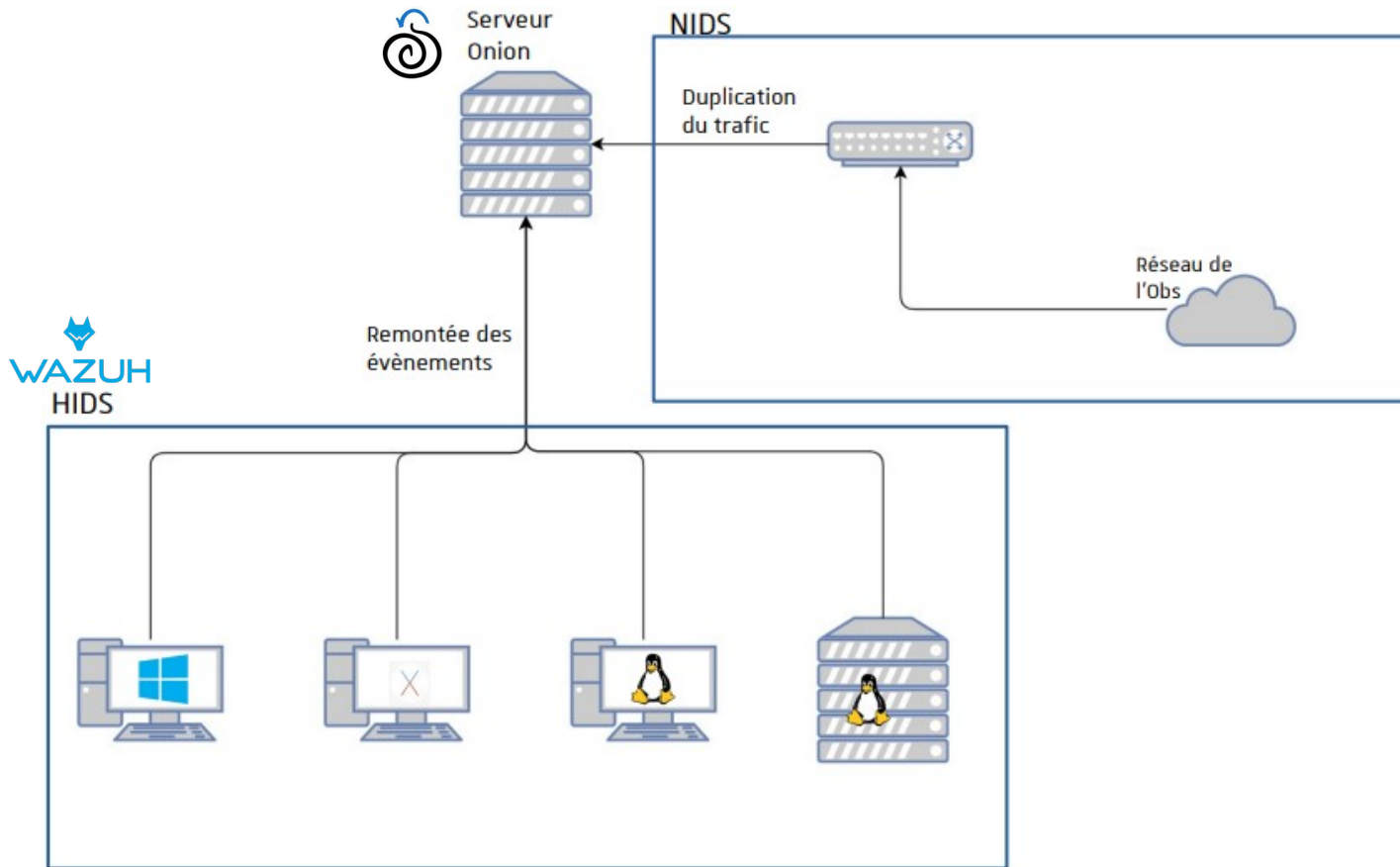


WAZUH



TheHive

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 ?**

