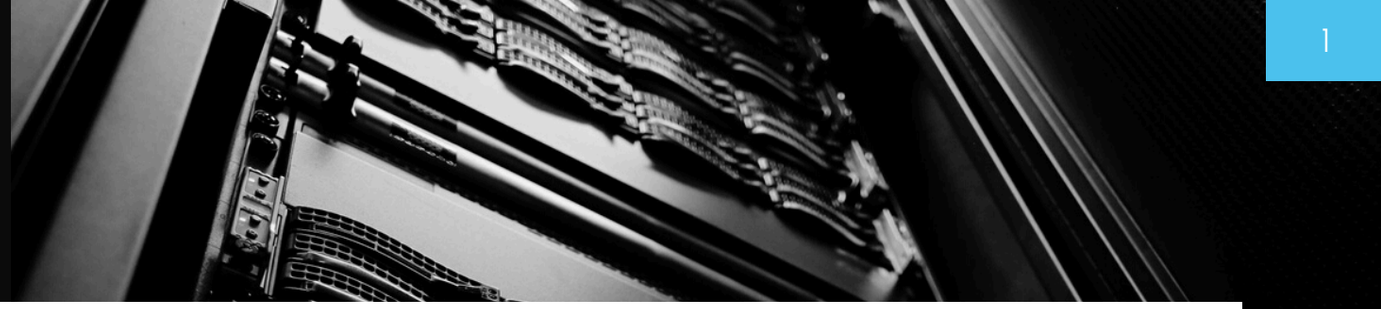
Endiguard.VAC (VAC algo, - XDR) et routage BGP décisionnel

INTRODUCTION



- BGP ? VAC ? XDR (Extended Detection and Reponse) ?
- EDR (Endpoint) c'est bien, un XDR c'est mieux 😉 (+ sources)
- Trois systèmes en 1, VAC, routage BGP décisionnel, XDR
- Fonctionnent technologiquement ensemble
- Tout paquet entrant / sortant du DC passe par ces systèmes

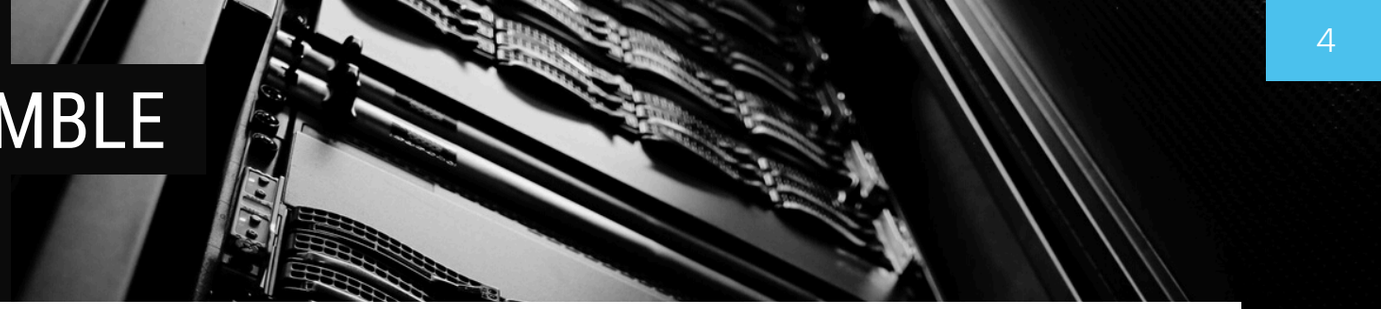
ÉTAT DES LIEUX, SUR LA PARTIE COUCHES BASSES OSI (VAC / BGP)

- De plus en plus d'attaques DoS et DDoS
- De plus en plus d'attaques par amplification (ex. UDP/DNS)
- Des organisations criminelles de location de botnet
- Trop d'hébergeurs laissent les serveurs comme vecteurs
- De plus en plus de machines connectées
- Les risques liés aux protocoles : syn spoof/flood, injection RST, UDP flood, fragmentation (Treadrop), Slowloris HTTP, etc.

ÉTAT DES LIEUX, SUR LA PARTIE COUCHES HAUTES OSI (XDR)

- Beaucoup de CMS, pas forcements maitrisés en sécurité
- Grand nombre d'attaques par injection, RCE, phishing
- Des organisations criminelles de location de rootkits
- Développeurs, agences (web) assez éloignées en sécurité
- Des menaces de plus en plus nombreuses et complexes
- Accès ouvert aux 0day, positif, mais il faut être réactif !
- Un manque de maîtrise de certains utilisateurs (updates...)

ÉTAT DES LIEUX, SUR L'ENSEMBLE



- Les systèmes existants, orientés avant tout sur la B.P
- L'approche par le coût
- Le problème des éditeurs externes dans le SI (certifications)
- Le manque de maîtrise sur une architecture primordiale
- Une grande partie des solutions GAFAM, peu souverain
- Manque éventuel de réactivité (attaques, maj des éditeurs)
- Le millefeuille, faisant que le client final a un TTR trop long !

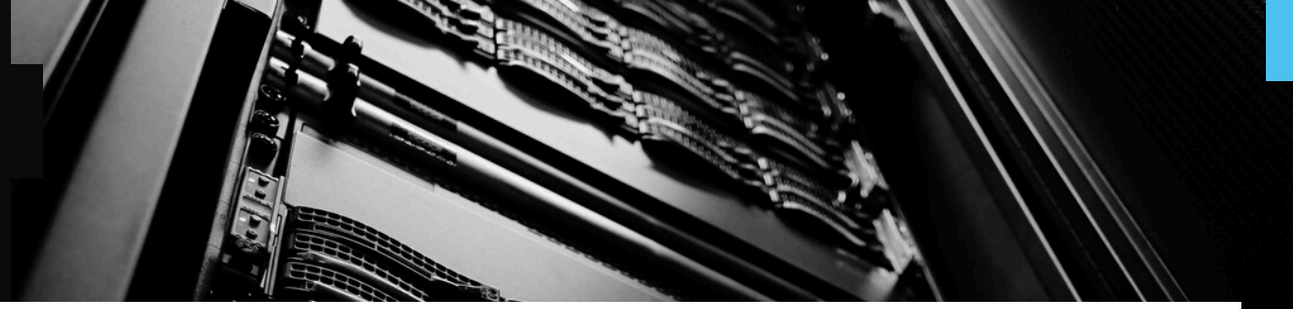
PREMIÈRE PARTIE : LE VAC ALGORITHMIQUE

- Notre technologie :
    - Ensemble de contre-mesures spécifiques (stats pays)
    - Détection algorithmique d'attaques par randomisation
    - Capteurs logiques et contre-mesures ciblées (XDR)
    - Sondes locales et distantes (honeypots)
- Critérisation des attaques et prise de décisions
- Redondance et évolutions (scalabilité sur le calcul, etc.)

DEUXIÈME PARTIE : ROUTAGE BGP DÉCISIONNEL

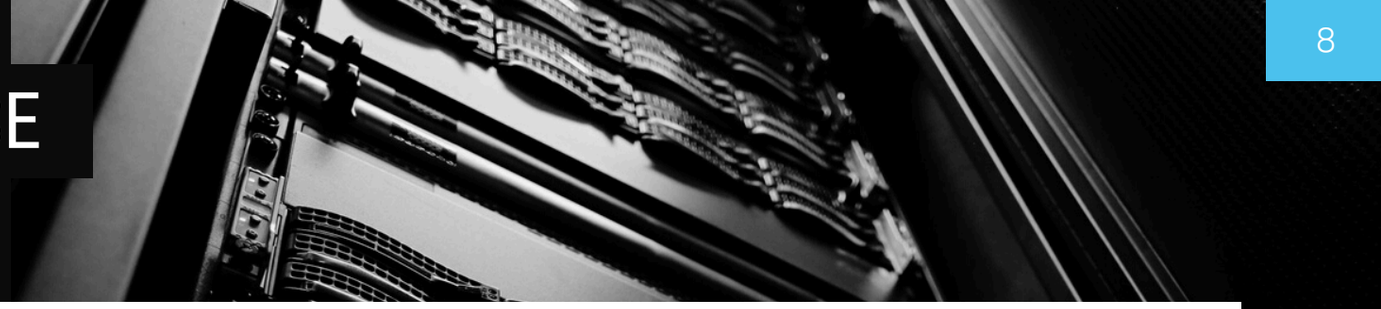
- Principe de routes, confiance et redondance
- La technologie BGP, une bonne base, mais ancienne
- Détection du BGP hijacking, BGP spoofing (fausses routes)
- BGP Leaks (bad neighbor…)
- Erreurs RPKI (erreur humaine sur la légitimité)
- Nos améliorations et son interaction avec le VAG algo (BGP blackhole, etc.)

TROISIÈME PARTIE : LE XDR



- Intervient sur les couches diverses (HTTPs, sessions, IPSec)
- Remontées vers un cluster central depuis les serveurs d'app
- Détection d'anomalies par volume de données
- Détection d'anomalies liées à des CMS courants (WP, Presta.)
- Inspection des trames SSL/TLS, IPSec (pas des données !)
- Inspection DPI des headers TCP/UDP, HTTP, etc. (URG/HOST)
- Détection de brute force, remontées des charges (load, etc.)

L'ENSEMBLE SUR LA RÉPONSE



- Corrélation multi couches, combinant les données
- Réponses automatisées sur la menace, réactivité
- Modèle d'apprentissage afin d'affiner détection/réponse
- Diminution de l'impact (réduire les faux positifs)
- Utilisation d'algo de modélisation (hypercube, patterns)
- Visibilité sur la menace et la réponse (logs, mails, graphs)
- Amélioration sur la conformité (PCI-DSS, post-mortem)

LE FUTUR...

- Qualification visa CSPN de l'ANSSI en cours...
- Déploiement chez nos partenaires hébergeurs
- Réduction de certaines latences (<5 ms, contre 5-20 ms)
- Amélioration du « machine learning », algo de régression
- Amélioration des interfaces pour les tiers
- Ouverture d'une partie de la technologie en licence Apache

Endiguard.VAC (VAC algo. - XDR) et routage BGP décisionnel

Merci de votre attention,
avez-vous des questions ?

icodia