Sommaire :

Mission

Introduction

Fonctionnement

Services

**Missions :**

**Intro : pkoi je suis ici**

Parler des attaques en France 80% des attaques blabla et combien dans la sécurité repartition par petite ou grande entreprise

Analogie un peu macabre mais adaptée: Cancer on croit que ça ne nous arrivera jamais

Parler des Bots qui scan la toile

Parallèle avec la norme ISO 27001

Problématique : quels sont les moyens de défense face à ces attaques ?

**Fonctionnement :**

Listing des moyens : Firewall (ce que l’on a a l’heure actuelle Juniper) généralement placé en tête de réseau mais requiert ACL humain.

(Mettre photo de l’infra)

Il nous faudrait un moyen d’automatiser ces ACL et de relever des alertes en cas de cas de force majeure et c’est là ou l’IDS entre en jeu. De plus ISO 27001 parler de la partie concernée.

Qu’Est-ce qu’un IDS ? Organe de sécurité, une sonde que l’on va placer à un endroit de l’infrastructure que l’on souhaite protéger.

2 types d’IDS :

* HIDS : sonde sur un équipement (switch, serveur…) : anomalie au niveau de la charge, intégrité des fichiers…
* NIDS : sonde sur le réseau : moi

2 types de sondes :

* Anomalie : détection d’une anomalie comportementale (Failles 0 days, appel au machine learning actuellement)
* Signature : comparaison des trames avec une base de données (80% des attaques – attaques standards) 30000 signatures à l’heure actuelle maintenu constamment par qui ?
* Mode IDS/IPS

Parler des alertes :

Parler de OSI 7 couches avec les différentes attaques (réseau, applicative…) 3 4 5

Cette sonde va remonter des alertes en cas de « problèmes » ex : mot de passe en clair, injection SQL, conformité RFC…la sonde relève tout et n’importe quoi (parler des faux positifs)

Que faire de toutes ces alertes ensuite ?

Le SIEM constitue l’intelligence et va corréler tout ça afin de diminuer le nombre de fausses alertes

(parler faux négatifs faux positifs..)

SIEM : difficile à mettre en place difficultés à corréler + open source nouveaux

Parler de ou on va placer l’IDS + le fait que c un serveur physique

**Services :**

(En pratique :)

Services : Suricata + Graylog + Capture d’écran avec démo

Fonctionnalités : cahier des charges ?

* Redondance sur PA2 PA3
* Alerting Centreon via les alertes définis par l’équipe
* Reporting
* LDAP

Parler de là où ça en est + les niveaux d’alertes qui ont été définis.

Parler du fait que cest un truc qui doit être maintenu dans le temps pour être vraiment efficace

Lien Wiki docs

Screens de suricata d’une alerte de graylog