2013-2014

IPS APPLIANCE

Projet de Veille Technologique

Sébastien DESZCZ

Thomas DURAK

Grégoire MEURILLON

Marianne STALTER

EPSI

**Sommaire**

[1. Présentation 3](#_Toc386736403)

[1.1. Introduction 3](#_Toc386736404)

[1.2. Présentation du Groupe 3](#_Toc386736405)

[1.3. Présentation du Sujet 3](#_Toc386736406)

[1.4. Gantt 3](#_Toc386736407)

[2. Technologie 4](#_Toc386736408)

[2.1. IPS Applicance 4](#_Toc386736409)

[2.1.1. Définition 4](#_Toc386736410)

[2.1.2. Fonctionnement 4](#_Toc386736411)

[2.1.3. Avantage 4](#_Toc386736412)

[2.2. NIPS 4](#_Toc386736413)

[2.2.1. Définition 4](#_Toc386736414)

[2.2.2. Fonctionnement 4](#_Toc386736415)

[2.2.3. Avantage 4](#_Toc386736416)

[2.3. HIPS 4](#_Toc386736417)

[2.3.1. Définition 4](#_Toc386736418)

[2.3.2. Fonctionnement 4](#_Toc386736419)

[2.3.3. Avantage 5](#_Toc386736420)

[2.4. KIPS 5](#_Toc386736421)

[2.4.1. Définition 5](#_Toc386736422)

[2.4.2. Fonctionnement 5](#_Toc386736423)

[2.4.3. Avantage 5](#_Toc386736424)

[2.5. Localisation sur un Réseau 5](#_Toc386736425)

[3. Acteur du marché 6](#_Toc386736426)

[3.1. Identification des constructeurs 6](#_Toc386736427)

[3.2. Identification des Produits 6](#_Toc386736428)

[3.3. Identification des OS et machines physiques 6](#_Toc386736429)

[4. Part de marchés 7](#_Toc386736430)

[4.1. Répartition sur le marché Mondial 7](#_Toc386736431)

[4.2. Répartition sur le marché Européen 7](#_Toc386736432)

[4.3. Répartition sur le marché Français 7](#_Toc386736433)

[5. Implantation 8](#_Toc386736434)

[5.1. Mondiale 8](#_Toc386736435)

[5.2. Europe 8](#_Toc386736436)

[5.3. France 8](#_Toc386736437)

[6. Référence 9](#_Toc386736438)

[6.1. Identification des types de clients 9](#_Toc386736439)

[6.2. Les grands noms parmi les clients 9](#_Toc386736440)

[7. Annexes 10](#_Toc386736441)

[7.1. L’historique de l’IPS 10](#_Toc386736442)

[7.2. Les types d’attaques 10](#_Toc386736443)

[7.3. Les chiffres Clés 10](#_Toc386736444)

[7.4. Etudes des offres proposés par les Acteurs 10](#_Toc386736445)

[7.5. Exemple concret d’implantation 10](#_Toc386736446)

[7.6. Rentabilité de l’IPS 10](#_Toc386736447)

[7.7. Bibliographie 10](#_Toc386736448)

[7.8. Glossaire 10](#_Toc386736449)

[8. Synthèse 11](#_Toc386736450)

[8.1. Français 11](#_Toc386736451)

[8.2. Anglais 11](#_Toc386736452)

[9. Conclusion 12](#_Toc386736453)

# Présentation

## Introduction

De nos jours, l’informatique est un élément vital pour chaque société et entreprise. Cet informatique est en constante évolution et permet de facilité le travail de chacun. Mais toutes ces évolutions ne sont pas que positive. En effet, si des outils de plus en performant pour la gestion des réseaux et des applications se créés, des failles tout aussi puissante apparaisse ce qui fait le bonheur des pirates informatique. Les pirates n’ont aucune pitié pour les outils et machines qui peuvent exister sur réseau. Ils n’hésiteront à se servir d’elle pour s’attaquer aux serveurs présents sur ce même réseau. Donc pour combattre ces attaques de nouveaux outils sont créer et amélioré chaque jours. C’est le cas de l’outil que nous allons présenter dans cette étude. Le système de prévention d’intrusion (Intrusion Prevention System « IPS ») permet au administrateur système et réseau d’installer un outil qui va analyser le comportement des machines de leurs réseaux et d’agir automatiquement cas d’attaque d’un pirate informatique.

## Présentation du Groupe

## Présentation du Sujet

Il a été demandé à notre groupe de rédiger un rapport sur la technologie IPS APPLIANCE. Nous devons donc présenter cette technologie en précisant son but et ses différentes formes. De plus, nous devons réaliser une étude de marché. (A revoir)

## Gantt

# Technologie

## IPS Applicance

### Définition

### Fonctionnement

### Avantage

## NIPS

### Définition

### Fonctionnement

### Avantage

## HIPS

### Définition

### Fonctionnement

### Avantage

## KIPS

### Définition

KIPS « Kernel Intrusion Prevention System »

Cet outil permet aux administrateurs réseau de configurer une ou plusieurs réactions ainsi que de bloquer certaine action sur la partie système d’exploitation d’une machine.

Le KIPS agit directement sur le « Noyaux » d’un système ce qui permet de réguler les actions et de prévenir toute défaillance ou attaque. En effet, le KIPS va vérifier chaque appel vers le système et va ainsi permettre de détecter un comportement anormal et interdire ces actions.

Le KIPS permet par exemple de protéger un serveur web en restreignant la lecture et l’écriture des fichiers juste à la partie du service web et ainsi empêcher toute possibilité d’ouverture de shell de commande et de lecture sur le reste du serveur.

L’outil KIPS peut aussi détecter toutes les modifications de performance de la machine telle qu’une utilisation trop importante de mémoire et stopper le logiciel ou l’outil entrainant cette utilisation.

### Fonctionnement

1. La machine initialise une action système
2. L’outil KIPS analyse la commande
3. KIPS vérifie dans sa base de règle si la commande est autorisé

### Avantage

## Localisation sur un Réseau

# Acteur du marché

## Identification des constructeurs

## Identification des Produits

## Identification des OS et machines physiques

# Part de marchés

## Répartition sur le marché Mondial

## Répartition sur le marché Européen

## Répartition sur le marché Français

# Implantation

## Mondiale

## Europe

## France

# Référence

## Identification des types de clients

## Les grands noms parmi les clients

# Annexes

## L’historique de l’IPS

## Les types d’attaques

## Les chiffres Clés

## Etudes des offres proposés par les Acteurs

## Exemple concret d’implantation

## Rentabilité de l’IPS

## Bibliographie

## Glossaire

# Synthèse

## Français

## Anglais

# Conclusion