**Cahier des Charges – AutoSocDeploy**

1. **Contexte du projet**

Mise en place d'un lure (honeypot) monitorée par un SIEM automatiquement déployé : Splunk. Détecter l'attaque, travail, d'analyse et identification d'attaques.

1. **Périmètre du projet**

Virtual Machines : 3

* Windows AD 2020 : (1069€)
* Windows 10 Pro : (259€)
* Linux Debian : (0€)

Splunk Enterprise (1800€/an)

Splunk Forwarder (0€/an)

3 développeurs (20€/h)

1. **Budget**

|  |  |  |
| --- | --- | --- |
| Fonctionnalités | Heures de travail estimé | Prix |
| Serveur AD : Mise en place de Splunk Entreprise | 5 | 300€ + 2869€ (software) |
| Serveur Web : Mise en place d'un Linux avec un Honeypot Wordpress | 15 | 900€ |
| Serveur Windows : Mise en place d'un Windows 10 pro avec un Honeypot | 20 | 1200€ + 259€ |
| Serveur Windows : Sysmon configuré sur le poste W10 pro client | 5 | 300€ |
| Serveur Web : Auditd configuré sur le Serveur Web | 5 | 300€ |
| Serveur AD : Splunk server reçoit des logs des 2 machines | 10 | 600€ |
| Serveur AD : Début construction de règles, alertes sur splunk | 35 | 2100€ |
| Début mise en place d'une solution qui test nos alertes Splunk | 20 | 1200€ |
| Réalisation d'une analyse d’infra (nmap) | 10 | 600€ |
| Tester une attaque sur AD (smbexec ou autre ... ) | 25 | 1500€ |
| Amélioration infra | 25 | 1500€ |
| Total | 205 | 13628€ |