|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Project Title:** | Wasmpot2 | | | |
|  |  |  |  |  |
| **Project Sponsor:** | Aucun |  | **Date Prepared:** | 15/10/2023 |
|  |  |  |  |  |
| **Project Manager:** | JB Jail |  | **Project Customer:** | Frédéric Paillart |

|  |
| --- |
| **Project Purpose or Justification, Context:** |
| Dans un paysage numérique où les cyberattaques et les menaces informatiques évoluent de manière exponentielle, la nécessité de détecter, d'analyser et de prévenir ces dangers est devenue vitale pour la sécurité des entreprises et des organisations. C'est dans ce contexte que Wasmpot2 a été conceptualisé. Wasmpot2 est bien plus qu'un simple outil de défense ; c'est un système innovant conçu pour répondre aux défis complexes et dynamiques posés par les cybermenaces contemporaines. |

| **Project Description:** |
| --- |
| Wasmpot2 est un honeypot c’est-à-dire un système informatique conçu pour simuler des vulnérabilités et attirer les cybercriminels, en leur faisant croire qu'ils ont accès à de véritables données sensibles ou à des systèmes informatiques. L'objectif principal d'un honeypot est de surveiller et d'analyser les attaques potentielles, permettant ainsi aux experts en sécurité de mieux comprendre les tactiques des cybercriminels et de renforcer la sécurité des réseaux et des systèmes informatiques.  En tant que honeypot avancé, Wasmpot2 simule fidèlement des environnements critiques tels que Keycloak et GitLab, jouant ainsi un rôle crucial dans la détection et l'analyse des activités malveillantes. Son objectif principal est de renforcer la sécurité des entreprises en leur fournissant des informations précieuses sur les menaces émergentes et les techniques d'attaque dont elle pourrait être victime. En combinant une simulation réaliste, une analyse proactive et une infrastructure sécurisée, Wasmpot2 s'impose comme une solution essentielle dans la lutte contre les menaces numériques et la préservation de la sécurité des données sensibles des entreprises. |

| **Use Case:** |
| --- |
| Contexte :  Une entreprise, "SecureCorp", cherche à renforcer sa cybersécurité pour protéger ses systèmes contre les attaques malveillantes. Pour ce faire, SecureCorp décide de mettre en œuvre Wasmpot2 dans son infrastructure afin de détecter et d'analyser les activités suspectes.  Scénario :   1. Intégration de Wasmpot2 : L'équipe de sécurité de SecureCorp déploie sur son réseau Wasmpot2 grâce aux scripts automatisés fournis. 2. Attirer les Attaquants : Les honeypots de Wasmpot2 sont déployés à des emplacements stratégiques dans le réseau de SecureCorp. Les attaquants ciblant l'entreprise sont redirigés vers ces honeypots, croyant avoir accès à des cibles légitimes. 3. Détection d’activités suspectes : Un groupe de cybercriminels lance une attaque par force brute contre le Keycloak de SecureCorp perçu comme le point central de l’entreprise, cherchant à compromettre les comptes utilisateur. Lorsqu'ils interagissent avec le honeypot, leurs actions sont enregistrées par Wasmpot2. 4. Analyse des données : Wasmpot2 enregistre en temps réel les activités des attaquants, y compris les tentatives de connexion infructueuses, les scans de ports et les tentatives d'exploitation de vulnérabilités. Les données sont analysées pour identifier les schémas d'attaque et les tactiques utilisées. 5. Alerte et réponse : L'équipe de sécurité de SecureCorp est alertée dès qu'une activité suspecte est détectée par Wasmpot2. Ils prennent alors des mesures pour bloquer les attaquants, renforcer les défenses du réseau et remédier aux vulnérabilités identifiées.   Résultat :  En utilisant Wasmpot2, SecureCorp parvient à détecter et à contrer efficacement les attaques malveillantes dirigées contre son infrastructure. La surveillance proactive des activités des attaquants permet à l'équipe de sécurité de prendre des mesures rapides pour protéger les systèmes et les données de l'entreprise contre les menaces en ligne. |

|  |
| --- |
| **High-Level Requirements:** |
| Mettre en place une architecture Kubernetes sécurisée pour le déploiement des honeypots  Créer des honeypots reproduisant fidèlement les interfaces de Keycloak et GitLab  Récupérer et à analyser les logs générés par les honeypots afin de comprendre les activités malveillantes et de renforcer la sécurité |

|  |
| --- |
| **Constraints :** |
| Honeypot déployé sur une architecture Kubernetes  Mise en place de micro-services  Honeypot codés en Rust  Compilation avec WebAssembly  Architecture déployée sur 4 serveurs Linux |

| **The 5 High-Level Risks (perform the risk matrix to identify the 5 highest risks) :** |
| --- |
| Défaillance de l’infrastructure Kubernetes  Vulnérabilité non prévue sur les honeypots  Attaques contre les honeypots  Pas de log collectés  Problème éthique concernant la gestion des données |

|  |  |  |
| --- | --- | --- |
| **Project Objectives** | **Success Criteria** | **Person Approving** |

|  |  |  |
| --- | --- | --- |
| **Scope:** |  |  |
| Avoir 2 honeypots déployés sur une infrastructure Kubernetes sécurisée grâce a des technos imposée et d’autres libres. Récupérer, analyser et interpréter les logs de ces honeypots afin de renforcer la sécurité du système sur lesquels ils seront déployés. | Honeypots réalistes et fonctionnels avec des vulnérabilités connues.  Récupération de vrai log si déploiement possible avant la présentation | Frédéric Paillart |

|  |  |  |
| --- | --- | --- |
| **Time:** |  |  |
| Présentation les 24 et 30 mai  Documentation technique  Projet déployé et fonctionnel | 100% des deadlines respectées | Jury presentation technique  Jury presentation SHES Reponsable SHES |

|  |  |  |
| --- | --- | --- |
| **Cost:** |  |  |
| Nom de domaine pour héberger le projet (4€ par an) | Cout total en dessous de 10€ | Fréderic Paillart |

|  |  |
| --- | --- |
| **Summary Milestones (must appear on your planning too)** | **Due Date (not confirmed)** |
| Présentation et choix du projet | 15/09/2023 |
| Choix des technos | 02/11/2023 |
| Serveurs fonctionnels | 01/12/2023 |
| Installation de proxmox | 14/12/2023 |
| Faux Keycloak prêt (interface web) | 11/01/2024 |
| Jury de mi parcours | 26/01/2024 |
| Générateur de honeypot foncitonnel | 03/05/2024 |
| Serveurs sécurisés et cloudflare configuré | 26/04/2024 |
| Déploiement des honeypots | 26/04/2024 |
| Jury final | 24/05/2024 |

**Team Organization:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Position** | **Role** | **Contact Information** | **Requirements** |
| Agathe |  | Membre de l’equipe de dev, récupération des logs et membre de l’équipe SHES | agathe.mullot@isen.yncrea.fr | S’occuper de la partie dev, récupération des logs et de la documentation SHES |
| Jean-Baptiste Jail |  | Chef de projet, membre de l’équipe serveur, récupération des logs | jean-baptiste.jail@isen.yncrea.fr | S’occuper de la mise en place et de la gestion des serveurs, de la récupération des logs et de coordonner tout le monde |
| Jean-Baptiste Relave |  | Membre de l’équipe dev, récupération des logs | jean-baptiste.relave@isen.yncrea.fr | S’occuper de la partie dev et de la récupération des logs |
| Duncan Sayn |  | Membre de l’équipe serveur | duncan.sayn@isen.yncrea.fr | S’occuper de la mise en place et de la gestion des serveurs et notamment de l’automatisation du déploiement |
| François Palayer |  | Membre de l’équipe serveur, gestion du réseau | francois.palayer@isen.yncrea.fr | S’occuper de la mise en place et de la gestion des serveurs et de la gestion du réseau avec l’exposition sur internet des honeypots |

|  |
| --- |
| **Etimated Budget:** |
| 4€/an : Hébergement des micro services |

|  |  |
| --- | --- |
| **Stakeholder(s)** | **Role** |
| Frédéric Paillart | Client |
| Willy Duquenoy | Support réseau |
| Equipe Wasmpot2 | Réaliser le projet |
| Equipe SHES | Réaliser la documentation |
|  |  |
|  |  |

**Approvals:**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Project Manager Signature |  | Sponsor or Originator Signature |
|  |  |  |
| Project Manager Name |  | Sponsor or Originator Name |
|  |  |  |

Date Date