GERANCE INFORMATIQUE

PFE Book

Édition 2026

Get Secure !

Vous protège depuis 2005

GERANCE INFORMATIQUE

Sommaire

GERANCE INFORMATIQUE

À propos de nous

Fondée en 2005, basée à Paris, à Tunis et à Abidjan et opérant principalement dans la région EMEA, GÉRANCE INFORMATIQUE est pionnière dans la fourniture de solutions et de services de sécurité informatique à forte valeur ajoutée.

Nous accompagnons les entreprises dans la définition, la mise en oeuvre, le suivi de la cybersécurité de leurs
Systèmes d'information reposant sur l'usage des meilleures technologies au monde.

Notre métier consiste à concevoir, déployer, intégrer, administrer, dépanner et manager la sécurité informatique de l'entreprise.

+750
PROJETS RÉALISÉS

+2000
CLIENTS DANS LE MONDE

+30
SOLUTIONS PARTENAIRES INNOVANTES

COMMENT POSTULER ?

Vous êtes à la recherche d'un stage de fin d'étude dans le cadre de votre cursus universitaire?

Vous êtes dynamique et ambitieux, Vous êtes passionné(e) par la cybersécurité ?

Vous savez prendre des responsabilités et avoir une vision large?

C'est vous? Alors rejoignez L'équipe de Gérance Informatique.

Pour postuler, veuillez suivre les étapes suivantes:

Étape 1 :

Choisir au maximum de 02 sujets parmi la liste sur le PFE Book.

Étape 2 :

Adressez votre dossier de candidature à l'adresse e-mail:
Emploi@geranceinformatique.com

Ou déposez-le directement à notre siège social sis au :
93, Avenue Louis Braille, Tunis 1003.

GERANCE INFORMATIQUE

NIVEAU D'ÉTUDE

BAC+5

Sujet n°1 : Plateforme de supervision avancée des événements de sécurité et détection d'anomalies basée sur Splunk et le Machine Learning.

Sujet n°2 : Mise en œuvre d'une solution de Monitoring et SIEM avec Elastic pour la supervision et la détection des incidents de sécurité.

Sujet n°3 : Conception d'une architecture réseau sécurisée par segmentation avancée.

Sujet n°4 : Detection Engineering avec Splunk Enterprise Security (SIEM) — conception, validation et amélioration des règles via campagnes Red Team / Pentest.

Sujet n°5 : Conception et intégration d'un écosystème Splunk ES, OpenCTI et TheHive pour renforcer les capacités de réponse aux incidents.

Sujet n°6 : Automatisation de la réponse aux incidents de sécurité avec Splunk Phantom (SOAR).

Sujet n°7 : Mise en place d'une stratégie de résilience aux attaques par ransomware dans les infrastructures critiques d'entreprise.

GERANCE INFORMATIQUE

Sujet 1 : Plateforme de supervision avancée des événements de sécurité et détection d'anomalies basée sur Splunk et le Machine Learning

Description du sujet :

Ce projet vise à concevoir et implémenter une solution technique pour détecter les comportements
anormaux et les menaces potentielles dans les Systèmes d'information de l'entreprise en s'appuyant
sur les capacités avancées de Splunk et les algorithmes de machine learning.
L'objectif principal est d'établir une surveillance proactive et intelligente des environnements informatiques afin d'identifier les activités malveillantes ou suspectes, incluant, mais sans s'y limiter :

- Détection de falsification des journaux d'audit Windows et altération des événements d'audit.
- Identification de téléchargements Web volumineux ou inhabituels (ex. téléchargement de payloads).
- Détection et classification de logiciels malveillants récurrents à partir de patterns comportementaux.
- Repérage d'attaques par force brute (lockouts, tentatives répétées de connexion).
- Surveillance des communications non chiffrées ou potentiellement risquées (HTTP, FTP, etc.).
- Analyse des commandes PowerShell suspectes (scripts, commandes obfusquées, etc.).
- Détection de suppression ou d'altération des journaux d'audit.
- Identification de scans réseau (scan de ports, balayage de sous-réseaux).
- Repérage de création de services Windows dans des chemins inhabituels ou non autorisés.
- Masquage de processus critiques via des techniques d'obfuscation ou injection.
- Supervision des scripts exécutés au démarrage ou à la connexion (startup, login scripts).
- Monitoring des modifications de base de registre critiques liées à la sécurité.

1. Environnement technique : Splunk, Active Directory, Sysmon, Splunk Machine Learning Toolkit, Python.
2. Profil recherché : Étudiant en Ingénierie | Master en TIC | Sécurité Réseau
3. Compétences requises :

Un bon niveau en analyse du log, création des scripts Powershell, connaissance, python, Splunk, connaissance en Windows/Linux, indexer des fichiers et des répertoires via l'interface Web,
CLI, par fichiers de configuration, obtenir des données via ports réseau, scripts ou entrées modulaires.
Mise en oeuvre de l'expéditeur universel (Universal Forwarder).

4. Équipe : Équipe Technique
5. Durée : 06 mois
6. Niveau d'étude : Bac+5
7. Nombre de stagiaire : 01

Sujet n°2 : Mise en œuvre d'une solution de Monitoring et SIEM avec Elastic pour la supervision et la détection des incidents de sécurité

Description du sujet :

Ce projet vise à étudier et à déployer une plateforme de Monitoring et de SIEM basée sur la suite Elastic (Elasticsearch, Kibana, Logstash, Beats) afin de renforcer la visibilité, la supervision et la sécurité de l'infrastructure informatique de l'entreprise.
Dans un contexte où la détection des menaces, l'analyse des journaux et la surveillance en temps réel sont essentielles, l'objectif de ce projet est de démontrer comment Elastic permet de collecter, centraliser, analyser et corréler efficacement les logs issus des serveurs, postes clients, équipements réseau et applications, afin d'identifier rapidement les anomalies et incidents de sécurité.

1. Compétences requises:

A. Compétences Techniques:
   - Connaissance des concepts SIEM et Monitoring.
   - Administration Windows / Linux.
   - Maîtrise ou compréhension d'Elastic (Elasticsearch, Kibana, Beats).
   - Analyse des logs et détection d'incidents.
   - Notions de sécurité réseau et système.

B. Compétences Analytiques et Organisationnelles
   - Capacité d'analyse des événements de sécurité.
   - Conception et mise en œuvre de stratégies de surveillance.
   - Création de tableaux de bord et reporting.
   - Documentation et communication technique.

2. Environnement technique : Elastic Stack, Réseaux, Systèmes et Sécurité.
3. Profil recherché : Étudiant en Master en TIC | Sécurité Réseau.
4. Équipe : Équipe Technique
5. Durée : 04 mois
6. Niveau d'étude : Bac+5
7. Nombre de stagiaire : 01

GERANCE INFORMATIQUE

Sujet n°3 : Conception d'une architecture réseau sécurisée par segmentation avancée

Description du sujet :

Ce projet vise à concevoir une architecture réseau où tout trafic est bloqué par défaut. L'étude se concentrera sur la segmentation poussée du réseau et la définition de politiques d'accès granulaires basées sur les applications, les utilisateurs et le contenu. Le projet intégrera des solutions de sécurité pour endpoints et applications web afin de renforcer la protection globale et de contenir les menaces potentielles.

Résultats attendus :

- Architecture réseau segmentée avec zones de sécurité définies
- Politiques d'accès granulaires et cartographie des flux autorisés
- Procédures d'intégration des solutions de sécurité
- Plan de déploiement progressif avec validation par tests

2. Environnement technique : Segmentation réseau, Pare-feu nouvelle génération, Politiques de sécurité, Solutions EDR et WAF

3. Profil recherché : Etudiant en Ingénierie | Master en TIC | Sécurité Réseau.

4. Compétences requises :

- Maîtrise des techniques de segmentation réseau
- Connaissance des architectures de sécurité
- Expérience avec les solutions de sécurité modernes

5. Équipe : Équipe Technique

6. Durée : 04 mois

7. Niveau d'étude : Bac+5

8. Nombre de stagiaire : 01

Sujet n°4 : Detection Engineering avec Splunk Enterprise Security (SIEM) — conception, validation et amélioration des règles via campagnes Red Team / Pentest

GERANCE INFORMATIQUE

Description du sujet :

Le SIEM (Splunk ES) dote le SOC d'alertes, mais la valeur réelle dépend de la qualité des règles de détection.

Ce stage vise à renforcer la couverture et la qualité des détections en confrontant les règles existantes à des scénarios offensifs (tests manuels et frameworks d'émulation), puis en corrigeant et en développant les règles manquantes.

1. Missions & tâches:
   - Inventaire & priorisation des règles Splunk ES et mapping MITRE.
   - Conception de scénarios de Pentest / Red Team pour chaque règle sélectionnée.
   - Exécution des scénarios (manuelle + Atomic Red Team / MITRE Caldera / outils offensifs autorisés).
   - Mesure des résultats via KPIs (TPR, FPR, MTTD, couverture Mitre ATT&CK, etc.)
   - Tuning & correction des règles existantes selon les résultats.
   - Création de nouvelles règles si nécessaire et documentation complète.
2. Environnement technique : Splunk Enterprise Security, atomic Red Team, MITRE Caldera, Mitre Att&ck,

Outils offensifs au choix.

3. Livrables:
   - Rapport de couverture MITRE et catalogue des règles testées.
   - Scénarios documentés (playbooks Atomic/Caldera + procédures manuelles).
   - Tableau KPI avant/après et rapport d'analyse.
   - Ensemble de règles corrigées et nouvelles règles.
4. Profil recherché : Étudiant en Ingénierie | Master en Sécurité des réseaux.
5. Compétences requises :
   - Connaissances de base Splunk / SPL
   - Notions d'Active Directory, réseaux et Windows internals
   - Curiosité pour l'offensive security (red team basics)
6. Équipe : Équipe Technique
7. Durée : 06 mois
8. Niveau d'étude : Bac+5
9. Nombre de stagiaire : 01

GERANCE INFORMATIQUE

Sujet n°5 : Conception et intégration d'un écosystème Splunk ES, OpenCTI et TheHive pour renforcer les capacités de réponse aux incidents.

Description du sujet :

La valeur d'un Centre des Opérations de Sécurité (SOC) ne réside pas dans le volume d'alertes traitées, mais dans sa capacité à neutraliser rapidement les menaces réelles. Ce stage vise à transformer un SOC traditionnel en une cellule de réponse "haute-fidélité". L'objectif est de construire une architecture où chaque alerte est automatiquement qualifiée, enrichie et priorisée, permettant aux analystes de concentrer leur expertise uniquement sur ce qui compte. Pour cela, nous intégrerons le SIEM Splunk ES pour la détection, la plateforme CTI OpenCTI pour le contexte, et TheHive comme plateforme centrale de gestion d'incident pour piloter

- l'investigation
- Missions & tâches :
- Qualifier à la source (Splunk ES) : Déployer le SIEM et affiner ses règles de corrélation. L'objectif n'est pas de tout voir, mais de détecter avec une haute probabilité les signaux faibles d'une attaque.
- Contextualiser la menace (OpenCTI) : Mettre en place la plateforme de CTI pour répondre instantanément aux questions : "Cette menace me vise-t-elle ?", "Est-elle connue ?", "Quel est le mode opératoire de l'attaquant ?".
- Piloter l'investigation (TheHive) : Déployer TheHive pour servir de cockpit aux analystes. C'est ici que les incidents sont gérés de manière structurée, de leur création à leur clôture.
- Automatiser le flux de travail de l'analyste :
- De l'alerte au plan d'action : Mettre en place un workflow où une alerte Splunk ES ne se contente pas de créer un ticket, mais génère un cas complet dans TheHive avec un plan de réponse initial (checklist de tâches).
- L'investigation augmentée : Intégrer TheHive avec Cortex et OpenCTI pour que l'enrichissement des preuves (observables) soit réalisé en quelques secondes, et non en quelques heures.
- oLa capitalisation du savoir : S'assurer que chaque nouvel indicateur de compromission découvert lors d'une enquête dans TheHive est automatiquement enregistré dans OpenCTI, rendant le SOC plus intelligent après chaque incident.

Mesurer pour améliorer : Mettre en place des indicateurs de performance (KPIs) c

lairs dans TheHive (MTTD, MTTR) pour quantifier l'apport de l'automatisation et identifier les p

rochains goulots d'étranglement à optimiser.

Formaliser l'excellence : Produire une documentation de qualité (schémas, procédures, guides) qui servira de fondation pour les opérations quotidiennes du SOC.

2. Environnement technique
   - SIEM : Splunk Enterprise Security
   - CTI Platform : OpenCTI
   - Incident Management System (IMS) : TheHive, Cortex
   - Systèmes & Conteneurisation : Linux (Debian/Ubuntu), Docker, Docker-Compose
   - Scripting & API : Python, API REST
3. Compétences requises
   - Solides connaissances en administration système Linux et en concepts réseaux.
   - Maîtrise du scripting en Python et aisance avec les API REST.
   - Compréhension des concepts de la réponse à incident, de la CTI et du framework MITRE ATT&CK.
   - Autonomie, rigueur et une forte appétence pour l'automatisation des processus de sécurité.
   - Une expérience avec Docker est un avantage significatif.
4. Profil recherché :

Étudiant en dernière année d'école d'Ingénieur ou Master spécialisé en Cybersécurité.

5. Durée : 06 mois
6. Nombre de stagiaires : 01

Sujet n°6 : Automatisation de la réponse aux incidents de sécurité avec Splunk Phantom (SOAR)

Description du sujet :

Le but de ce projet est de configurer Splunk Phantom afin d'automatiser la gestion et la réponse aux incidents de sécurité détectés dans un environnement d'entreprise vulnerable.

Dans ce cadre, le stagiaire devra :

A. Détecter et analyser les comportements malveillants tels que :

1. Propagation de ransomware
    - Attaques brute-force
    - Anomalies réseau ou système
    - Scripts malveillants ou activités suspectes sur les endpoints
2. Concevoir et développer des playbooks automatisés permettant de :
    - Bloquer automatiquement un utilisateur compromis
    - Isoler une machine via EDR ou firewall
    - Enrichir automatiquement les IOC (IP, URL, hash)
    - Réinitialiser des mots de passe
    - Notifier les équipes via email/Teams
    - Exécuter des requêtes Splunk ou API pour compléter l'analyse
3. Simuler des incidents de sécurité réels (avec outils gratuits) pour valider les playbooks SOAR: Le stagiaire utilisera des outils open-source pour générer des incidents contrôlés, tels que :
    - Hydra (attaque brute force contrôlée sur un service local)
    - Caldera de MITRE ATT&CK (simulations automatisées d'attaques adversaires)
    - Infection Monkey (test de latéralisation, vulnérabilités, mouvements internes)
    - Atomic Red Team (exécute des tests ATT&CK en local)
4. Mettre en place un processus de bout en bout, incluant ingestion, automatisation, actions humaines, journalisation.
5. Créer un tableau de bord Splunk dédié au SOAR, permettant :
    - Suivi des workflows Phantom
    - Dashboard incidents en temps réel
    - KPIs (MTTR, distribution des incidents, actions automatisées)

Ce projet vise à renforcer les capacités de réponse aux incidents et valider la pertinence de l'automatisation via des scénarios réalistes.

1. Environnement technique :
   - Splunk Phantom, Splunk Enterprise, Python 3, REST API, MITRE Caldera, Atomic Red Team,
   - Infection Monkey.
2. Profil recherché :
   - Étudiant en TIC (Ingénierie | Master) spécialisé en cybersécurité ou sécurité réseaux.
3. Compétences requises :
   - SOAR & Splunk Phantom
   - Python (développement d'actions automatisées)
   - API REST
   - Connaissance des incidents de sécurité (MITRE ATT&CK)
   - Bonne compréhension des environnements Windows/Linux et réseaux
   - Capacité à documenter des procédures & playbooks
4. Équipe :
   - Équipe Technique / SOC
5. Durée: 06 mois
6. Niveau d'étude: Bac+5
7. Nombre de stagiaire: 01

Sujet n°7 : Mise en place d'une stratégie de résilience aux attaques par ransomware dans les infrastructures critiques d'entreprise

Description du sujet :

Ce sujet porte sur le développement d'une stratégie pour protéger les infrastructures critiques des entreprises contre les attaques par ransomware. Cela implique d'identifier les vulnérabilités et d'évaluer les risques. La stratégie se concentre sur des approches telles que la segmentation du réseau pour limiter la propagation des ransomwares et l'utilisation de solutions de sauvegarde pour assurer la continuité des activités.

1. Environnement technique :
   - Infrastructure réseau (switches, pare-feu, etc.).
   - Splunk pour la gestion des logs et l'analyse des incidents.
   - ESET EDR pour la détection et la réponse aux menaces.
   - Outils de sauvegarde et de récupération de données.
   - Systèmes d'exploitation et logiciels de sécurité.
2. Profil recherché : Étudiant en Master | Ingénierie en informatique | Cybersécurité.
3. Compétences requises :
   - Compréhension des menaces liées aux ransomwares.
   - Compétences en segmentation de réseau et en sauvegarde de données.
   - Connaissance des outils Splunk et ESET EDR.
   - Familiarité avec les meilleures pratiques de Cybersécurité.
4. Équipe : Équipe Technique
5. Durée : 06 mois
6. Niveau d'étude : Bac+5
7. Nombre de stagiaire : 01

GERANCE INFORMATIQUE

NIVEAU D'ÉTUDE

BAC+3

Sujet n°8 : Implémentation et administration d'une solution EDR .

Sujet n°9 : IInstallation, Configuration et Administration d'un Next-Generation Firewall (NGFW).

Sujet n°10 : Implémentation et administration d'une solution de backup et de réplication VEEAM.

Sujet n°11 : Implémentation et configuration d'une solution PAM.

Sujet n°12 : Mise en Place d'une Solution de Scanner de Vulnérabilités Automatisée dans une Infrastructure d'Entreprise.

Sujet n°8 : Implémentation et administration d'une solution EDR.

Description du sujet :

Le projet commence par l'étude de l'architecture et la validation des prérequis, suivies de l'installation et de la configuration de l'EDR et des solutions Endpoint. Ensuite, vérifier que les tâches et politiques sont configurées. Pour terminer, une simulation d'attaque réseau sera réalisée pour tester la détection.

1. Environnement technique : Windows /Linux/MS SQL Server /Apache.
2. Compétences requises :
   - Maîtrise des systèmes d'exploitation (Windows, Linux).
   - Active Directory, GPO, Windows installer.
   - Les fondamentaux de la sécurité informatique.
3. Profil recherché : Étudiant en Licence appliquée en TIC.
4. Équipe : Équipe Technique.
5. Durée : 04 mois
6. Niveau d'étude : Bac+3
7. Nombre de stagiaire : 01

Sujet n°9 : Installation, Configuration et Administration d'un Next-Generation Firewall (NGFW)

Description du sujet :

Ce projet consiste à installer, configurer et administrer un pare-feu de nouvelle génération (NGFW) afin de renforcer la sécurité du réseau de l'entreprise.

L'objectif est de déployer une solution de sécurité réseau capable d'offrir une protection avancée contre les menaces, tout en permettant un contrôle précis du trafic et une visibilité en temps réel.

Parmis vos objectifs:

- Analyse des besoins et définition de l'architecture :
  - Identification des zones réseau à protéger et des flux critiques à sécuriser.
  - Analyse des menaces potentielles et des politiques de sécurité nécessaires.
  - Définition de l'architecture réseau et des emplacements stratégiques pour le NGFW.
- Installation et configuration du NGFW
- Mise en œuvre des fonctionnalités avancées :
  - Activation des modules avancés : IPS (Intrusion Prevention System), antivirus, sandboxing, et filtrage DNS.
  - Détection et blocage des menaces basées sur des signatures et des comportements.

1. Environnement technique : Palo Alto.
2. Compétences requises :
   - Maîtrise des protocoles réseau (TCP/IP, VLAN, VPN).
   - Connaissance des concepts de sécurité réseau et des pare-feux.
   - Les fondamentaux de la sécurité informatique.
3. Profil recherché : Étudiant en Licence appliquée en TIC
4. Équipe : Équipe Technique
5. Durée : 04 mois

Sujet n°10 : Implémentation et administration d'une solution de backup et de réplication VEEAM

Description du sujet :

Ce sujet porte sur l'implémentation et l'administration de VEEAM, une solution reconnue pour la sauvegarde et la réplication des données.

L'implémentation comprend la planification et la configuration de VEEAM, avec l'installation des composants nécessaires, comme VEEAM Backup & Réplication, et la définition des stratégies de sauvegarde en fonction des besoins de l'organisation.

Parmis vos objectifs:

- Analyse des besoins et de l'infrastructure existante :
  - Identification des systèmes, applications et bases de données critiques nécessitant une sauvegarde.
- Évaluation de la capacité de stockage, de la fréquence de sauvegarde et des objectifs de temps de récupération (RTO/RPO).

  Installation et configuration de Veeam Backup & Replication.
- Optimisation et sécurisation de la plateforme.
  - Mise en œuvre des meilleures pratiques pour protéger les sauvegardes contre les menaces (ex. : ransomware, accès non autorisés).
  - Intégration des fonctionnalités avancées comme le monitoring des sauvegardes et la vérification automatique des restaurations (SureBackup).

1. Environnement technique : Windows, Linux, Virtualisation/VMWARE, VEEAM.
2. Compétences requises :
   - Connaissance des concepts de sauvegarde, réplication et reprise après sinistre.
   - Bonne maîtrise des environnements Windows Server, virtualisation (VMware, Hyper-V) et des systèmes de stockage.
   - Sensibilité aux bonnes pratiques de sécurité des données.

Sujet n°11 : Implémentation et configuration d'une solution PAM

Description du sujet :

Ce projet consiste à mettre en place et configurer une solution de Gestion des Accès Privilégiés (Privileged Access Management - PAM) pour renforcer la sécurité des comptes à privilèges et limiter les risques liés aux accès non autorisés ou abusifs aux ressources critiques de l'entreprise.

Parmis vos objectifs :

Analyse des besoins et de l'environnement existant :

- Identification des comptes à privilèges et des ressources sensibles (serveurs, bases de données, applications critiques).
- Évaluation des risques associés à une gestion inadéquate des accès privilégiés.

- Implémentation de la solution PAM : Installation et configuration de la solution PAM (ex. : Wallix).
- Configuration des contrôles et des audits :
  - Mise en œuvre de politiques de gestion des accès (basées sur le principe du moindre privilège).
  - Activation des fonctionnalités de surveillance et d'enregistrement des sessions pour garantir la traçabilité des actions.

1. Environnement technique : Windows, Linux, Virtualisation/VMWARE, Wallix / One Identity.
2. Compétences requises :
   - Connaissance des concepts de gestion des accès et des privilèges.
   - Maîtrise des environnements Windows, Linux, et des réseaux d'entreprise.
   - Notions en sécurité des Systèmes d'information et conformité réglementaire.
3. Profil recherché : Étudiant en Licence appliquée en TIC.
4. Équipe : Équipe Technique
5. Durée : 04 mois
6. Niveau d'étude : Bac+3
7. Nombre de stagiaire : 01

Sujet n°12 :Mise en Place d'une Solution de Scanner de Vulnérabilités Automatisée dans une Infrastructure d'Entreprise

Description du sujet :

Ce projet consiste à déployer une solution de scanner de vulnérabilités Qualys au sein d'une infrastructure d'entreprise. L'objectif est d'automatiser la détection des vulnérabilités sur l'ensemble des serveurs, applications et périphériques réseau. Le projet inclura la configuration des rapports, la planification des scans réguliers et l'intégration des résultats avec une plateforme de gestion des vulnérabilités.

1. Compétences requises
    - Compétences Techniques
        - Connaissances en Cybersécurité et Gestion des Vulnérabilités.
        - Infrastructure et Systèmes d'Entreprise.
        - Gestion des Accès et Sécurité des Données.
        - Rapports et Analyse des Vulnérabilités.
    - Compétences Analytiques et Organisationnelles
        - Analyse de Risques et Priorisation des Vulnérabilités.
        - Documentation et Communication Technique.
        - Conformité et Respect des Normes.
2. Environnement technique : Réseaux, Système et sécurité.
3. Profil Recherché : Étudiant en Master en TIC | Sécurité Réseau.
4. Équipe : Équipe Technique
5. Durée : 04 mois
6. Niveau d'étude : Bac+3
7. Nombre de stagiaire : 01

GERANCE INFORMATIQUE

Get Secure!

Vous protège depuis 2005