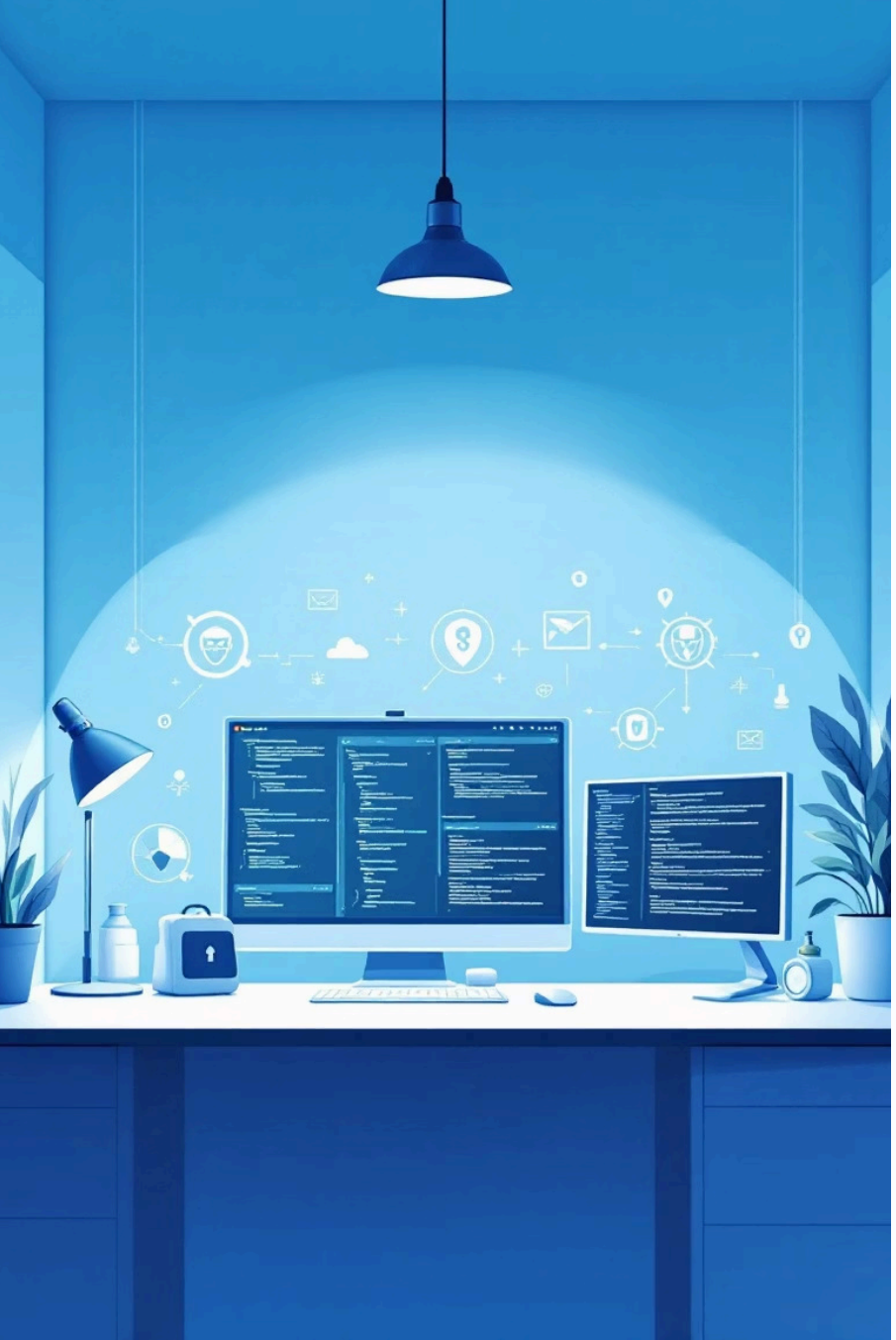


Portfolio de Projets en Cybersécurité

Une collection de 13 projets démontrant l'expertise en sécurité informatique, développement et infrastructure réseau.

FORENSIQUE

Analyse Forensique Post-Incident

Investigation complète d'un incident de sécurité virtuel avec analyse de la mémoire vive, du disque et des témoignages. Utilisation d'Autopsy et Volatility pour retracer les actions des acteurs de menace.

Résultats clés

- Identification du chemin d'attaque complet
- Restauration des traces supprimées
- Scripts Python pour corrélation RAM/disque
- Collecte de preuves et rapport détaillé

MALWARE

Analyse Avancée du Trojan njRAT

Analyses Multiples

Statique, dynamique, mémoire vive et code source complet

Threat Intelligence

Règles YARA et SIGMA pour détection SOC

Capacités Identifiées

Commandes à distance, keylogging, effacement MBR

Rapport complet incluant mécanismes de défense et règles de détection pour environnements SOC.

ETHICAL HACKING

Infiltration et Exploitation Active Directory

Reconnaissance

Password-spraying et scan réseau

Accès Initial

Exploitation RDP et BloodHound

Escalade

Vulnérabilité Zerologon exploitée

Domain Admin

Contrôle total du domaine

Utilisation de PowerView, AdMiner et BloodHound pour cartographier et exploiter les chemins d'attaque menant aux administrateurs du domaine.

DÉVELOPPEMENT

Rootkit Python Furtif

Fonctionnalités Développées

- Connexion socket client-serveur
- Exécution de commandes à distance
- Transfert bidirectionnel de fichiers
- Persistance aux redémarrages
- Propagation aux supports amovibles
- Backdoor supplémentaire

Résultat : Infiltration discrète réussie sans détection par les mécanismes de sécurité de la cible.

Projets Infrastructure Réseau

Topologie Sécurisée

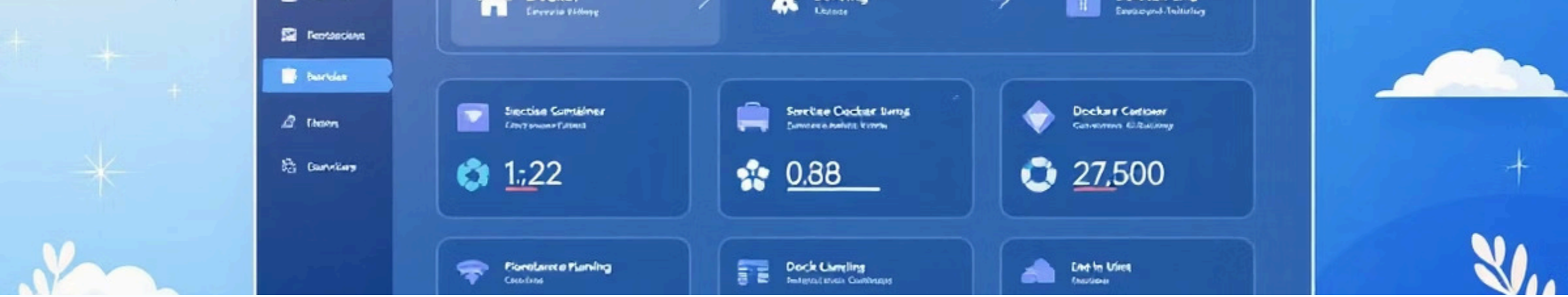
VLAN, NAT, AAA avec Packet Tracer. Amélioration sécurité +15%, efficience réseau optimisée.

FAI & Firewalls

GNS3/QEMU, iptables DNAT/SNAT, DHCP. Translation d'adresses et règles de sécurité réussies.

PKI & HTTPS

OpenSSL, certificats CA/serveur/client, Nginx, CRL. Sécurisation connexions et gestion confiance.



DEVOPS

Solutions Conteneurisées

Gestion de Parc GLPI

Docker, GLPI, Joomla, MariaDB, phpMyAdmin. Simplification gestion -40%, gain de temps significatif.

Chat Professionnel Synapse

Synapse, PostgreSQL, Traefik HTTPS. Communication temps réel sécurisée, gestion stack -20%.

AUTOMATISATION

Scripts d'Automatisation Système

Scripts Développés

Bash : Partage clés SSH, prise en main à distance des périphériques

Python : Analyse automatique de logs avec export des résultats

Impact Mesurable

- Réduction interventions manuelles : **-50%**
- Identification comportements à risque
- Automatisation tâches répétitives

IOT & FULL STACK

Système de Tri de Balles Intelligent

01

Vision & Identification

Détection visuelle des balles roses et jaunes

02

Backend Node.js

Express.js, modélisation BD, triggers SQL, procédures stockées

03

Communication Temps Réel

AJAX pour interactions sans rechargement, Raspberry Pi

04

Interface Web

Tablette, Chart.js pour graphes historiques

Projet intégrant construction physique, câblage électrique, systèmes embarqués et développement web full-stack.

IAM & SÉCURITÉ

AuthPlayground : Solution de Formation IAM

SWA

Secure Web Authentication implémentée

OIDC

OpenID Connect configuré

SAML

Security Assertion Markup Language intégré

Stack technique : FastAPI (Python), React, Okta. Solution multi-instance avec UI intuitive pour formation utilisateurs aux protocoles de fédération.

Ce portfolio démontre une expertise transversale en cybersécurité offensive/défensive, développement full-stack, infrastructure réseau et DevOps, avec 13 projets couvrant l'analyse forensique, le développement de malwares, l'ethical hacking et l'automatisation.