Gautier Bielak

INGÉNIEUR CYBERSÉCURITÉ

CONTACT

Troyes

gautier.bielak@proton.me

07-81-88-79-30

Permis B

Gautier Bielak

Hackthebox: Gillbi

CryptoHack: Gillbi

root-me: Gillbi

COMPETENCES

Administration Système
ArchLinux, Debian, Ubuntu, Windows Server 2016, RedHat, Fedora, ESXi vsphre, VMWARE Workstation, Oracle Virtualbox

Administration reseau
Juniper, stormshield, cisco, Palo Alto, Infoblox

Langage de programmation
Python, C/C++, Rust, Typescript, PHP, bash, powershell, mysql, sqlite, mongodb

Forensique
Splunk, Graylog, KAPE, IDA, Ghidra, binaryninja, x64debugger, Eric Zimmerman's suite

Contenerisation
Docker, Kubernetes

Test intrusion
SQL injection, XXE, XSS, Kerberoasting, golden/silver ticket, brute force, Local File Inclusion...

Automatisation
Ansible

CI/CD
GitHub, Gitlab

Langes
Français: Natif
Anglais: C1
Polonais: A2, Gitlab

A PROPOS

Diplomé de l'École 2600, je participe activement à des CTFs chaque fois que l'occasion me le permet et je me prépare actuellement à la formation CPTS de HackTheBox.

EXPÉRIENCES

CONSULTANT CYBERSÉCURITÉ - ANALYSTE PSIRT
SII - Thales LAS (01/2025 - 07/2025)

- Analyses et veilles de vulnérabilités sur Dependancy Track
- Importation de SBOM pour veille vuln + exportation mensuelle de rapport pour Security Manager via Dependancy Track

APPRENTISSAGE : INGÉNIEUR CYBERSÉCURITÉ
Thales Global Services (10/2021 - 09/2024)

- Installation et administration d'un ESXi avec mise en rack et connexion réseau interne
- Analyse de risque avec la méthodologie EBIOS

STAGE : ADMINISTRATEUR RÉSEAU
Midrange Solution & Services (06/2021 - 09/2021)

- Automatisation des MAJ et backup des firewall via Ansible et crontab
- Chiffrage des données de connexions via Ansible-Vault

FORMATION

2021 - 2024 | Titre RNCP de Niveau 7 - Ecole 2600, Expert SDSR
2020 - 2021 | DUT Informatique, IUT d'Orsay
2018 - 2020 | Licence Informatique, Paris-Saclay

PROJETS

(Liste non exhaustive)

- Installation et configuration réseau ArchLinux
- Malware Windows en ASM x86 avec Process Hollowing
- mise en place d'un SOC miniature pour simulation d'attaque avec Splunk et Graylog