

## PROFILE

Cybersecurity engineer with **3+ years of SIEM experience** (Splunk & Azure Sentinel), focused on **automation, documentation, and reliable log management** to improve detection, reduce false positives, and enhance SOC efficiency.

## KEY SKILLS

**SIEM Platforms:** Splunk, Azure Sentinel

**Cloud & Infra:** Azure, GCP, Linux, Windows, Proxmox, LXC

**Automation:** Python, Go, Bash, Ansible Tower, CCA for Splunk

**DevOps & Tools:** Git, Azure DevOps

**Core Strengths:** Documentation, incident handling, data pipeline optimization

## PROFESSIONAL EXPERIENCE

### **Orange Cyberdefense — SIEM Specialist**

*Sep 2022 – Present | Brussels*

Operate and optimize SIEM platforms (Splunk & Sentinel), improving detection quality, automation, and SOC workflows through reliable ingestion and documentation.

### **Orbid — System Engineer**

*May 2019 – Aug 2022 | Merelbeke*

Provided infrastructure support and administration (Linux/Windows/virtualization) for SMEs.

### **ICT Talents (Next-ICT) — IT Consultant**

*May 2019 – Jul 2020 | Belgium*

Delivered outsourced IT support in Microsoft environments while achieving certifications in Linux and virtualization.


## PROJECTS


**Portfolio Website:** Built siemforge.xyz to showcase projects.

**Proxmox Homelab:** Designed a virtualized multi-environment test lab for automation and SIEM use cases.


**Splunk Instance:** Deployed and customized Splunk to develop apps, add-ons, and detection logic.

## CONTACT

 available on request

 benny@siemforge.xyz

 siemforge.xyz

 9420 Vlekkem, Belgium

 Driver's license: Category B

## RECENT CERTS

Cribl Certified Admin

Splunk Enterprise Certified Admin

Comptia Linux+

## LANGUAGES

Dutch

- Native

English

- Professional working proficiency

French

- Intermediate

