Carlos Alexandre Menezes

Junior Cybersecurity Analyst | SOC • Blue Team • SecOps

Sátão, Viseu, Portugal • cbittencourt1980@gmail.com • +351 915739684
linkedin.com/in/carlos-alexandre-bittencourt-de-menezes-66a99165 • github.com/camenezesdev

Professional Summary

Professional with a solid transition into Software Development and Cybersecurity, focused on SOC operations, Blue Team practices, and incident response automation. Currently developing the Zoomie ecosystem (xMDR/SOAR), secure system administration, and the integration of visibility, detection, and active containment. Combines an analytical background, documentation discipline, and hands-on technical skills in Python, C#, Java, Bash, Splunk, and Linux security to deliver solutions aligned with compliance and cyber resilience.

Core Competencies

- Splunk, SPL, SOC dashboards, detection engineering, and playbooks
- SOAR / xMDR, response workflows, and active containment
- Suricata and Snort, rule tuning and alert analysis
- Linux security: UFW, Fail2ban, hardening, and monitoring
- OpenLDAP, PAM/SSSD, RBAC, and password policy enforcement
- Native Portuguese, fluent English, intermediate Spanish
- Python, Java, SQL, Bash, C and C#, .NET

Professional Experience

Cybersecurity & Developer | Rootsystems

2025 – Present

- Development of the “Zoomie” SOAR/xMDR ecosystem for real-time threat mitigation across Layers 4 and 5.
- Incident response automation and telemetry with Splunk, Bash, and dedicated forwarder components.
- Implementation of Linux hardening, access control, and identity management with LDAP.

Administrative Assistant | CUF (Call Center)

2022 – 2024

- Customer support, administrative operations, information handling, and problem solving in a healthcare environment.
- Strengthened clear communication, document discipline, and response under pressure.

Call Center Supervisor | Intelcia

2017 – 2019

- Team leadership, onboarding, and training of new employees.
- KPI follow-up, quality improvement, and operational coordination.

Administrative Assistant and Management Support | BeiraZoo Veterinary Hospital

2017 – 2019

- Administrative and financial support, customer service, and process organization for daily operations.

Education and Certifications

Technical Programmer Course | IEFP

Status: Completed

Technical training in software development, algorithms, databases, and programming best practices.

CompTIA Security+ | Professor Messer

Status: Completed

Structured preparation covering security fundamentals, networking, risk management, and defensive operations.

Cisco CCST Cybersecurity / Networking | Cisco Networking Academy

Status: In progress

Training in cybersecurity, networking, and operations fundamentals.

Junior SOC Analyst / CJCA | Hack The Box Academy

Status: Completed

Hands-on path focused on SOC operations, log analysis, threat hunting, and incident response.

Law Degree | Universidade Estácio de Sá

Status: Completed

Strong foundation in critical analysis, logical reasoning, argumentation, and regulatory interpretation.

Key Projects

ZOOMIE — SOAR / xMDR (Rootsystems)

Orchestration and active response architecture

Description: Development of a SOAR/xMDR ecosystem focused on threat detection, analysis, and active mitigation. A C# engine processes telemetry and triggers mitigation, while Python forwarder and file watcher components execute defense actions.

Technical highlight: Dedicated forwarder for real-time malicious flow blocking, with a modular CLI and continuous telemetry that sharply reduces MTTR.

Stack: Python, C#, .NET, Bash, Splunk API, ILogger, Linux Hardening

SIEM & Detection Engineering (Splunk)

Advanced monitoring and Blue Team automation

Description: Implementation of a Splunk-based SOC for security event ingestion, correlation, and analysis, with analytical dashboards for operational visibility.

Technical highlight: Use cases for brute force and network anomalies, with playbooks that integrate directly with UFW for immediate blocking.

Stack: Splunk (SPL), Syslog, Python, Netfilter/UFW

Identity and Access Management (IAM/LDAP)

Centralized authentication and Zero Trust security

Description: Architecture of a centralized authentication system using OpenLDAP to consolidate users and permissions across a multi-host environment.

Technical highlight: PAM/SSSD integration, strong password policy enforcement, RBAC, and automated directory management via LDIF.

Stack: OpenLDAP, PAM, SSSD, Linux Security Modules

MEI — Management System (Java + SQL)

Software engineering and data persistence

Description: Operational management application for self-employed workflows, focused on data integrity and user experience.

Technical highlight: MVC implementation and full CRUD with SQL persistence to support consistent and modular transactions.

Stack: Java, MySQL/PostgreSQL, JDBC, Design Patterns