JOÃO PEDRO ROSA CEZARINO

+55 11 96462-6395
joaopedrorosa03@gmail.com
SÃO PAULO, SP

PROFESSIONAL SUMMARY

- With a BSc in Computer Science from Centro Universitário FEI, I currently work as an Security Analyst at T-Systems Brazil. My role involves supporting Cyber Security initiatives, conducting detailed analyses, and developing solutions based on best market practices.
- Passionate about technology and innovation in information security, I am constantly seeking new improvements and training. With a proactive and analytical approach, I stay equipped to tackle the challenges of the digital environment and ensure the security and integrity of data.
- My main interests include Critical Infrastructure Security, Cyber Threat Intelligence (CTI), Threat Hunting, Detection Engineering, Cyber Defense and Coding.

WORK EXPERIENCE

IT Internship, **Kuka Systems**, Dec 2020 - Jun 2021, São Bernardo do Campo, SP

- Support in ticket management;
- Asset control;
- User support;
- Assistance for collaborators.

Cyber Security Intern, **T-Systems**, Jun 2021 - Oct 2021, São Bernardo do Campo, SP

- Assist in monitoring and analyzing security alerts from tools like SIEM, IDS/IPS, and endpoint protection systems;
- Support the implementation and management of cybersecurity solutions, including firewalls, antivirus, and VPNs;
- Participate in the development and maintenance of security policies, procedures, and documentation;
- Assist in managing user access controls, including account provisioning and deprovisioning.

Security Operations Center Technician, **T-Systems**, Oct 2021 - Apr 2024, São Bernardo do Campo, SP

- Assist in monitoring and analyzing security alerts from tools like SIEM, IDS/IPS, and endpoint protection systems;
- Support the implementation and management of cybersecurity solutions, including firewalls, antivirus, and VPNs;
- Investigate and document security incidents, providing recommendations for mitigation;
- Provide technical support for end-users related to cybersecurity concerns;
- Research the latest cybersecurity threats, vulnerabilities, and mitigation techniques.

Security Analyst, **T-Systems**, Apr 2024 - Current, São Bernardo do Campo, SP

- Collect, analyze, and disseminate intelligence on emerging threats using platforms like MISP and OpenCTI;
- Correlate threat intelligence feeds with internal telemetry to identify potential risks to the organization;
- Develop custom scripts to automate ingestion and enrichment of threat intelligence data;
- Design and implement detection rules;

- Collaborate with SOC and incident response teams to refine and validate detection logic;
- Develop and maintain frameworks for validating detection efficacy;
- Create custom tools in Python and Bash to automate repetitive security tasks or enhance team workflows;
- Build parsers, enrichment modules, and custom integrations for security platforms;
- Monitor, detect, and respond to threats targeting OT/ICS environments while ensuring minimal disruption to operations;
- Collaborate with engineering teams to integrate cybersecurity measures into industrial control systems;
- Implement and monitor network segmentation strategies for securing critical OT/ICS infrastructure;
- Research and simulate ICS-specific threat scenarios to improve incident response capabilities.

EDUCATION

High School Diploma — Dec 2019
ÁBACO School - São Bernardo Do Campo

Technological Degree, Machining — Dec 2019
SENAI - São Bernardo Do Campo
- Awarded Bronze Distinction Award at SENAI for outstanding performance and achievement.

Bachelor of Science, Computer Science — Dec 2023
Centro Universitário FEI - São Bernardo Do Campo, SP
- Awarded as one of the best Graduation Thesis in my Computer Science program.

SKILLS

- Proficiency in threat intelligence tools (MISP, OpenCTI) and frameworks;
- Knowledge of detection engineering tools and frameworks;
- Understanding of OT/ICS protocols;
- Reporting and documentation;
- Collaboration skills for working with cross-functional teams;
- Strong programming skills in Python and Bash for scripting and tool development;
- Experience with CI/CD tools like GitLab CI;
- Familiarity with cybersecurity frameworks;
- Strong analytical and problem-solving skills;
- Strong communication skills for presenting findings to stakeholders.

LANGUAGES

English, Upper intermediate (B2)

CERTIFICATIONS

- **B2 First – Score 173** , Cambridge University Press & Assessment English, 02/2021
- **NSE 1 - Network Security Associate** , Fortinet, 11/2021
- **NSE 2 - Network Security Associate** , Fortinet, 11/2021
- **Linux Essentials - 010-160V** , Linux Professional Institute (LPI), 01/2023

- **Certified in Cybersecurity (CC)** , ISC2, 05/2024
- **Security+** , CompTIA, In Progress...

COURSEWORK

- **Cybersecurity Analyst Bootcamp** , Institute of Management and Information Technology (IGTI), 08/2020
- **Linux Administrator Bootcamp** , Institute of Management and Information Technology (IGTI), 12/2020
- **Introduction to Cybersecurity** , Cisco Networking Academy, 02/2021
- **Ransomware: Identify, Protect, Detect, Recover** , ISC2, 08/2021
- **Cybersecurity Foundations** , IBSEC - Brazilian Institute for Cybersecurity, 02/2022
- **Virtual Industrial Control Systems Cybersecurity (301V) Training** , Cybersecurity and Infrastructure Security Agency, 03/2022
- **ICS Cybersecurity Landscape for Managers** , Cybersecurity and Infrastructure Security Agency, 03/2022
- **ICS Cybersecurity Analysis & Evaluation Virtual Training (401V)** , Cybersecurity and Infrastructure Security Agency, 03/2022
- **OT Sales Training** , Fortinet, 10/2022
- **MITRE ATT&CK Defender - ATT&CK Fundamentals Training** , Cybrary, 09/2023
- **MITRE ATT&CK Defender - Cyber Threat Intelligence Training** , Cybrary, 10/2023
- **Introduction to the Threat Intelligence Lifecycle** , IBM, 07/2024
- **Foundation Level Threat Intelligence Analyst** , arcX, 07/2024
- **Cybersecurity Awareness - CAPC** , CertiProf, 08/2024
- **Ransomware Attack Investigation** , Digital Forensics Academy, 08/2024
- **Threat Intelligence** , Digital Forensics Academy, 08/2024

ADDITIONAL INFORMATION

Served in the **Brazilian Army** (January 2021 – December 2021) in São Bernardo do Campo, SP, Brazil.

- Awarded **Best Combat Shooter of the Year ;**
- Received **Medal of Honor** for outstanding service.

HOBBIES

- **Coding;**
- **Machine Learning;**
- **Artificial Intelligence;**
- **AI Agents;**
- **Natural Language Processing (NLP).**

PROJECTS

- **MailHeaderDetective:** A powerful tool that can help dissect complex email headers, providing useful insights and valuable information about the provided email (https://github.com/akajhon/MailHeaderDetective).
- **TCP_MultiChat_Server:** Multi-chat and Multi-Rooms TCP chat server implementation. Inspired in IRC protocol (https://github.com/akajhon/TCP_MultiChat_Server).

PUBLICATIONS

- **From Tweet to Threat: A Study on Cyber Threat Detection Patterns Using Natural Language Processing.** *Available at:* https://repositorio.fei.edu.br/items/b9162ebf-30c0-430b-b1ff-3fc4b87cf00e

MY LINKS

- **LinkedIn:** https://www.linkedin.com/in/joaocezarino/
- **GitHub:** https://github.com/akajhon
- **E-mail:** joaopedrorosa03@gmail.com