


João Pedro Rosa Cezarino

Cybersecurity Analyst

Threat Intelligence; Detection Engineering; ICS/OT Security

São Paulo, Brazil 

+55 11 96462-6395 

joaopedrorosa03@gmail.com 

linkedin.com/in/joaocesarino 

Summary

- Cybersecurity Analyst with practical experience in Threat Intelligence, Detection Engineering, and OT/ICS Security. Skilled in developing custom tools in Python and Bash, automating security workflows, and correlate threat data to strengthen cyber defense strategies
- Collaborates effectively across teams to implement detection rules, investigate incidents, and support secure architectures in critical infrastructure environments. Continuously seeks innovation and improvement, bringing analytical thinking and a proactive mindset to every challenge. Recognized for academic excellence and military discipline.

Skills & Tools

- **Threat intelligence platforms:** MISP, OpenCTI.
- **Detection engineering:** rule development, validation, threat correlation.
- **Programming:** Python, Bash (automation, tooling, scripting).
- **CI/CD:** GitLab CI for security automation.
- **OT/ICS:** protocol awareness, segmentation, industrial system monitoring.
- **Frameworks:** MITRE ATT&CK, NIST, ISO 27001.
- **Incident Response:** alert triage, investigation, documentation, mitigation.
- **SOC Operations:** SIEM monitoring, log analysis, endpoint security, escalation support.
- **Network Security:** firewalls, VPNs, IDS/IPS, proxies.
- Strong documentation, analytical thinking, and cross-team collaboration.
- Clear communicator with both technical and non-technical stakeholders.

Certifications

- **B2 First** (Score 173) | Cambridge University Press & Assessment English | Feb 2021
- **Certified in Cybersecurity (CC)** | ISC2 | May 2024

- **NSE 1 - Network Security Associate** | Fortinet | Nov 2021
- **NSE 2 - Network Security Associate** | Fortinet | Nov 2021
- **Linux Essentials - 010-160V** | Linux Professional Institute (LPI) | Jan 2023
- **Cybersecurity Awareness - CAPC** | Certiprof | Oct 2024
- **Security+** | CompTIA | In Progress...

Education

- **Post-Graduate degree in Cyber Threat Intelligence** - IDESP, São Paulo
Jan 2025 - PRESENT
- **Bachelor's degree in computer science** - Centro Universitário FEI, São paulo
Jan 2020 - Dec 2023
Awarded as one of the best Graduation Thesis in my Computer Science program.
- **Technical Degree in Machining** - SENAI, São Paulo
Jan 2019 - Dec 2021
Awarded Bronze Distinction Award at SENAI for outstanding performance and achievement.
- **High School Diploma** - Ábaco, São Paulo
Jan 2017 - Dec 2019

Experience

Cybersecurity analyst II (Tier 2) - T-Systems Brazil, São Paulo

Apr 2024 - PRESENT

- Correlate internal telemetry with threat feeds using MISP/OpenCTI;
- Collect, analyze, and disseminate intelligence on emerging threats;
- Develop custom automation scripts in Python/Bash;
- Design and implement detection rules and validate logic;
- Collaborate with SOC and incident response teams during investigations;
- Monitor and respond to SIEM, IDS/IPS alerts and EDR/XDR Alerts;
- Support and Administration of Firewalls, Proxies and VPN solutions;
- Monitor and secure OT/ICS environments with segmentation strategies.

Security Operations Center Technician - T-Systems Brazil, São Paulo

Oct 2021 - Mar 2024

- 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;
- Provide technical support for end-users related to cybersecurity concerns.

Cyber Security Intern - T-Systems Brazil, São Paulo

Jun 2021 - Oct 2021

- Participate in the development and maintenance of security policies, procedures, and documentation;
- Assist in managing user access controls, including account provisioning and deprovisioning.

Soldier - Brazilian Army, São Paulo

Jan 2021 - Dec 2021

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

Service Desk Analyst - KUKA Systems Brazil, São Paulo

Dec 2020 - Jun 2021

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

Projects

- **MailHeaderDetective:** A tool to dissect and analyze email headers for security insights and investigations (github.com/akajhon/MailHeaderDetective).
- **TCP_MultiChat_Server:** Multi-room TCP chat server inspired by the IRC protocol (github.com/akajhon/TCP_MultiChat_Server).

Publications

- **From Tweet to Threat: A Study on Cyber Threat Detection Patterns Using Natural Language Processing** - Published as part of graduation thesis at FEI University.
 - <https://repositorio.fei.edu.br/items/b9162ebf-30c0-430b-b1ff-3fc4b87cf00e>

Languages

- **English** - Upper Intermediate Level (B2)

My links

- **LinkedIn:** <https://www.linkedin.com/in/joaocezarino/>
- **Blog:** <https://akajhon.github.io/>
- **GitHub:** <https://github.com/akajhon>

Training

- **Fundamentals of Malware Analysis and Remediation** | Skillsoft | Mar 2025
- **Fundamentals of Threat Intelligence with OpenCTI** | Filigran | Mar 2025
- **ICS/SCADA Hacker Intelligence** | ADINT School | Jan 2025
- **Threat Intelligence** | Academia de Forense Digital | Aug 2024
- **Ransomware Attack Investigation** | Academia de Forense Digital | Aug 2024
- **Foundation Level Threat Intelligence Analyst** | arcX | Jul 2024
- **Introduction to the Threat Intelligence Lifecycle** | IBM | Jul 2024
- **MITRE ATT&CK Defender - Cyber Threat Intelligence Training** | Cybrary | Oct 2023
- **MITRE ATT&CK Defender - ATT&CK Fundamentals Training** | Cybrary | Nov 2023
- **OT Sales Training** | Fortinet | Oct 2022
- **ICS Cybersecurity Analysis & Evaluation Virtual Training (401V)** | CISA | Mar 2022
- **ICS Cybersecurity Landscape for Managers** | CISA | Mar 2022
- **Virtual Industrial Control Systems Cybersecurity (301V) Training** | CISA | Mar 2022
- **Cybersecurity Foundations** | IBSEC | Feb 2022
- **Ransomware: Identify, Protect, Detect, Recover** | ISC2 | Aug 2021
- **Introduction to Cybersecurity** | Cisco Networking Academy | Feb 2021
- **Linux Administrator Bootcamp** | IGTI | Dec 2020
- **Cybersecurity Analyst Bootcamp** | IGTI | Aug 2020