Matheus Theodoro

55 44999522514 | dev.matheustheodoro@gmail.com | linkedin.com/in/matheustheodoro1 | github.com/matheusht

Professional Summary

Aspiring cybersecurity professional with hands-on experience in SIEM implementation, threat detection, and incident response. Skilled in using industry-standard tools like Elastic Stack, pfSense, and Wireshark. Seeking an internship to apply my knowledge and contribute to a dynamic security team.

Education

CS-340 Intro to Computer Networking — Youtube
Networking Course — *October 2024*

Technical School in System Analysis and Computing — Campo Mourão, Paraná
Certified in System Analysis and Computing — *2025*

Security+ Certification — CompTIA
Certified in Security+ — *2025/05*

Experience

Software Developer — Sep. 2023 – Present
Marketisa — *Campo Mourão, Paraná, Brasil*

- Developed full-stack applications with secure coding practices, including input validation and encryption
- Automated CI/CD pipelines, integrating vulnerability scanning tools like Nessus
- Collaborated on access control and authentication systems
- Performed manual penetration testing on web apps

Projects

Synkro | *Enterprise SIEM Implementation, Elastic Stack, Kubernetes* — Feb. 2025 – Present

- Addressed the challenge of implementing a robust SIEM solution for enterprise-level threat detection and response
- Utilized Elastic Stack (Elasticsearch, Logstash, Kibana) for log aggregation, analysis, and visualization
- Deployed the solution on Kubernetes for scalability and resilience
- Integrated real-time threat intelligence feeds to enhance proactive threat hunting capabilities
- Implemented automated incident response workflows, significantly reducing mean time to resolution (MTTR)

Cybersecurity Lab | *SIEM, Kali Linux, Active Directory, Vulnerable VMs, pfSense* — Start Date – Present

- Created a controlled environment to practice offensive and defensive cybersecurity techniques
- Configured pfSense for network segmentation, managing internal, isolated, and AD lab networks
- Used Kali Linux to exploit vulnerabilities in VMs
- Practiced lateral movement and privilege escalation in an Active Directory environment with Windows Server 2019 and Windows 10 Enterprise
- Gained hands-on experience in network security, penetration testing, and incident response

Malware Analysis Lab | *REMnux, FlareVM, Sandboxing Tools* — Start Date – Present

- Set up a safe environment to analyze and understand malware behavior
- Utilized REMnux and FlareVM for static and dynamic malware analysis
- Employed sandboxing tools, disassemblers, and debuggers to investigate malware samples
- Developed skills in reverse engineering, behavioral analysis, and identifying indicators of compromise (IOCs)

Technical Skills

Tools: Elastic Stack, Suricata, Nessus, Splunk, Wireshark, Snort, REMnux, FlareVM
Frameworks: MITRE ATT&CK, ISO 27001, NIST
Languages: Python, C/C++, Javascript, Bash