Matheus Theodoro

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

Education

Technical School in System Analysis and Computing — Campo Mourão, Paraná
Integrated High School with Technical Diploma in IT — *2025/12*

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

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

Experience

Full Cycle / Security Analyst — Sep. 2023 – Present
Marketisa — *Campo Mourão, Paraná, Brasil*

- Conducted penetration tests on 5 web applications, identifying and mitigating 20 vulnerabilities (SQL injection, XSS)
- Developed applications with OWASP Top 10 mitigations (input validation, encryption, RBAC) and validated security through manual penetration testing, ensuring resilience against common threats
- Integrated security into the full development lifecycle (SDLC) through threat modeling and secure code reviews
- Automated vulnerability scans in CI/CD pipelines using Nessus, blocking deployments with common CVEs
- Implemented MFA and session hardening to mitigate credential stuffing attacks
- Architected SIEM infrastructure (Elastic Stack/Wazuh) to centralize logs from 5+ systems and automate threat detection with custom correlation rules

Projects

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

- Enhanced threat detection in an enterprise SIEM by integrating Elastic Stack on Kubernetes, reducing incident response time by 30%
- 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* — March 2025 – Present

- Designed a SOC-like lab environment using pfSense (IDS/IPS) and SIEM tools to detect, analyze, and respond to simulated Kali Linux attacks
- 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* — March 2025 – Present

- Established a malware analysis environment with REMnux and FlareVM, enabling safe dissection of malware samples and skill development in reverse engineering
- 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, Powershell