Matheus Theodoro

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

ISO 27001 — SkillFront
SkillFront — *2025/05*

Experience

Offensive Security Engineer — Feb. 2025 – Present
Boltsec — *Paraná, Brasil*

- Led penetration testing engagements for 5+ clients, focusing on web applications, APIs, and cloud (AWS) security, uncovering and helping remediate high-impact vulnerabilities
- Functioned as a key security advisor to startup CTOs and founders, translating complex technical findings into clear business risks and developing prioritized remediation strategies for 8+ clients
- Authored and presented 5+ clear, concise, and developer-centric security assessment reports, prioritizing findings by real-world risk and providing actionable remediation guidance
- Provided post-assessment support to 5+ client development teams, ensuring effective implementation of security fixes and fostering a more security-aware culture
- Proactively identified and analyzed emerging threat vectors and business logic flaws specific to modern SaaS and platform architectures

Security Engineer (DevSecOps) — Sep. 2023 – Feb. 2025
Marketisa — *Campo Mourão, Paraná, Brasil*

- Restored a client website from near-total inaccessibility (90%+ open redirects to malicious sites) to full functionality by configuring Cloudflare and custom firewall rules, mitigating over 5,000 malicious requests
- Conducted penetration tests on 5 web applications, identifying and mitigating 20 vulnerabilities (DDoS, SQL injection, XSS)
- Configured Cloudflare WAF with custom rulesets to mitigate DDoS attacks and block malicious traffic patterns
- 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 40%
- Utilized Elastic Stack (Elasticsearch, Logstash, Kibana) for log aggregation, analysis, and visualization
- Integrated real-time threat intelligence feeds to enhance proactive threat hunting capabilities
- Implemented automated incident response workflows, reducing mean time to resolution (MTTR) by 30%

Cybersecurity Lab | *SIEM, Penetration Testing, 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 20+ simulated penetration testing attacks
- Configured pfSense for network segmentation, managing internal, isolated, and AD lab networks
- Practiced lateral movement and privilege escalation in an Active Directory environment with Windows Server

Technical Skills

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