Marcos Luchetti

Cybersecurity Intern

mluchettim@gmail.com | https://mluchetti.com

Profiles

marcos-luchetti

mluchettii

Summary

Driven Cybersecurity Intern experienced in integrating and managing diverse systems spanning cybersecurity, cloud platforms, networking, and automation. Proficient in designing and optimizing secure, scalable environments leveraging virtualization, containerization, and advanced security tools. Demonstrates a strategic approach to problem-solving, process improvement, and collaboration across technical disciplines. Passionate about continuous learning and applying innovative solutions to meet evolving organizational needs.

Experience

Zolon Tech Inc.

June 2025 - Present

Cybersecurity Intern

Herndon, VA

https://www.zolontech.com/

- Take full ownership of assigned projects with minimal supervision, effectively managing setup, configuration, and troubleshooting.
- Learn and implement security tools including IBM QRadar, CrowdStrike Falcon, Nessus, driving enhanced detection capabilities.
- Conduct self-directed research and hands-on testing of new technologies.
- Build and configure lab environments simulating real-world infrastructure with secure segmentation and optimized resource allocation.
- Write detailed technical documentation and knowledge base articles, improving team onboarding efficiency.
- Develop automation scripts reducing repetitive task time by up to 30%.
- Monitor system logs to validate functionality and fine-tune configurations, identifying and mitigating security gaps.
- Troubleshoot complex issues through log analysis, research, and iterative testing.
- Present progress and findings to mentors, incorporating feedback to refine techniques.

Projects: Zolon Tech Inc. / Homelab

Homelab Infrastructure and Documentation

2023 - Present

- Maintain a homelab to apply and extend IT, networking, virtualization, and cybersecurity knowledge through practical hands-on experience.
- Set up Raspberry Pi and Proxmox server environments for containerization and virtualization learning.
- Deploy containerized applications through Docker; design Docker Compose YAML files, manage and monitor containers.
- Deploy and maintain a Zensical documentation site through automated builds and global distribution using Cloudflare Pages connected to a GitHub repository.

Projects: Zolon Tech Inc. / Homelab

Networking and Zero-Trust Architecture — 2025 - Present

- Configure Tailscale VPN to provide zero-trust secure access, enforcing least-privilege access control lists.
- Set up Cloudflare domain with DNS configured to route subdomains via VPN and VPS IPs.
- Deploy and manage web servers (Nginx, Caddy) with automated Let's Encrypt TLS certificates via Cloudflare DNS validation.
- Deploy and manage a DigitalOcean VPS hosting a Pangolin tunneled reverse proxy, utilizing WireGuard for secure, firewall-bypassing connections to the homelab, enabling private, authenticated access to internal services.
- Implement AdGuard DNS server to block ads and trackers, with custom local DNS rewrites.

Identity and Access Management — 2025 - Present

- Configure Cisco Duo IAM for lab user authentication simulations.
- Deploy open-source OAuth provider (Authentik) for secure sign-in management for applications.
- Set up Vaultwarden password manager with zero-trust Tailscale IP access and MFA protection.

SIEM — 2025 - Present

- Deploy IBM QRadar CE on VirtualBox; ingest logs from Windows/Linux systems via WinCollect and rsyslog.
- Develop and tune rules and alerts for security offenses based on event IDs.
- Operate Squid web proxy logging TCP packets to QRadar with NxLog forwarding.
- Deploy Wazuh for intranet agent monitoring.
- Generate and analyze compliance reports referencing DISA STIGs, CIS Benchmarks, NIST standards, MITRE ATT&CK, and PCI DSS.

EDR — 2025 - Present

- Deploy CrowdStrike Falcon sensors on Windows, Linux, and Android devices.
- Monitor Falcon events and configure customized dashboards.
- Fine-tune detection with IOC configuration and exceptions managing false positives.
- Conduct malware alert triage, improving workload prioritization

Vulnerability and Compliance Management — 2025 - Present

- Utilize SCAP/OSCAP with DISA STIGs and CIS Benchmarks to automatically detect and remediate vulnerabilities on Windows/Linux.
- Use Nessus and OpenVAS to scan home network, generating detailed vulnerability reports.

Self-Hosted Services and Monitoring — 2025 - Present

- Configure OpenCloud server on Raspberry Pi for secure remote document editing and access.
- Implement GoAccess for server log visualization, creating actionable charts and graphs.
- Deploy and maintain RustDesk remote desktop server for secure server management.

Projects: Old Dominion University

Cybersecurity Assessment 2022

- Delivered executive briefing and board presentation for a company's cybersecurity strategy.
- Conducted comprehensive risk management analysis, utilizing qualitative and quantitative risk analysis methods.
- Developed a risk matrix and recommended mitigation strategies based on NIST and industry standards.

Cybersecurity Labs 2022

- Analyzed malicious network traffic using Wireshark for threat detection.
- Performed network attacks using Metasploit and explored various attack vectors.
- Utilized password-cracking tools such as John the Ripper, Cain and Abel, and aircrack-ng.
- Ran vulnerability scans on subnets with Nessus, used Nmap for network reconnaissance.

Advanced Network and Server Configuration 2022

- Deployed Windows Server 2019.
- Implemented Hyper-V and rapid server deployment.
- Collaborated with team members on Active Directory configuration, account management, and access control.
- Configured and managed data storage, network services, and printing.

Network Infrastructure Design 2021

- Collaborated in designing a secure network infrastructure mock-up for a college campus.
- Specified configurations for domain controllers, file servers, routers, and switches.
- Developed firewall policies and incident response strategies, including disaster recovery planning.

Network Case Analysis 2021

- Designed wired and wireless network architectures for a high school building.
- Developed floor plans and network topology diagrams.
- Specified hardware, cabling, and network configuration requirements.

Skills

Operating Systems
Windows, Linux, macOS

Virtualization & Containers
Windows Server 2019, VirtualBox, VMware, Proxmox, Docker

Cloud Platforms & Hosting
DigitalOcean, VPS, Cloudflare, Cloud Security Fundamentals

Network & Security
Zero-Trust Architecture, VPNs, TCP/IP, DNS, TLS/SSL, Tailscale, WireGuard, Nginx/Caddy, AdGuard DNS Server, Firewall Configuration, Network Segmentation

Network Analysis
Wireshark, Nmap

EDR/SIEM
IBM QRadar, Wazuh, CrowdStrike Falcon

Skills

Vulnerability & Compliance
Nessus, OpenVAS, SCAP, DISA STIGs, CIS Benchmarks

Identity and Access Management (IAM)
Cisco Duo, Authentik

CI/CD & Automation
GitHub Actions, Cloudflare Pages, Docker, Bash scripting, Automated Builds and Deployments

Incident Response & Threat Detection
Security Incident Handling, Log Analysis, Threat Modeling

Security Frameworks & Standards
NIST, GDPR, HIPAA, MITRE ATT&CK

Open Source Intelligence (OSINT)
VirusTotal, Any.Run, Who.is, Webroot BrightCloud, Authentic8 Silo

Office & Productivity Tools
Microsoft Office 365, Google Workspace

Soft Skills
Documentation, Troubleshooting, Research, Communication, Team Collaboration

Education

Old Dominion University — 2022
Cybersecurity — Bachelor of Science

Certifications

Security+ — Expected 11/2025
CompTIA

A+ — 2024
CompTIA

Languages

English
Native

Spanish
Fluent