# Abdurrahman Balsus

AbduBalsus@Gmail.com (657)-239-7237 Irvine, CA LinkedIn

*__Cybersecurity professional__ with a solid foundation in __network security__, __cloud security__, and __threat detection__. Holds the __CompTIA Security+__ and __Google Cybersecurity Professional Certificate__, with hands-on experience in __SIEM monitoring__, __log analysis__, and __incident response__. Demonstrated ability to __assess risks__, __implement controls__, and __enhance security__ in both production and simulated environments. Skilled in __Splunk__, __Wireshark__, __AWS IAM__, and __Active Directory__, with a passion for defending digital systems through __automation__, __research__, and __continuous learning__.*

## RELEVANT EXPERIENCE

**Software Engineering Intern - Fair-Observer Inc.** Aug - Dec 2024

- Documented **UI logic** and **component usage patterns**, reducing onboarding time for future interns by ~ **50%**.
- Participated in weekly **sprint reviews**, Git-based **version contro**l, and **PR** workflows to support **Agile delivery**.
- Contributed to **two major** feature rollouts, helping transition the platform to a more **scalable** and **modular architecture**.
- **Researched and documented** 10+ vulnerability types, contributing to the organization's **incident response playbook** and increasing response preparedness.
- **Recommended and implemented** encryption strategies for handling **PII**, reducing exposure risks by ~ **40%**.

**Home Depot** - Sales Associate (Multiple Departments) Jan 2022 - Present

- Served as a **Subject Matter Expert (SME)** for in-store technology, providing **technical support** for hardware, software, and network issues across departments.
- **Assisted 500+ customers weekly**, offering guidance on product selection, **DIY solutions**, and tech products.
- Supported daily operations in a high-traffic location, handling 1000+ of SKUs with peak shifts generating **$35K+** in department sales.
- **Resolved 95% of escalations** independently by troubleshooting **POS systems** and network-connected equipment

## RELEVANT PROJECTS

**Cloud-Based Log Monitoring with SIEM** Jan - May 2025

- Deployed **log collection pipelines** using **CloudTrail**, **CloudWatch**, and **Guard Duty** on **cloud-hosted systems**.
- Collaborated with a **cross-functional team** to present findings and **risk mitigation** strategies.
- Tuned **alert rules** to reduce **false positives** and orchestrated **auto-response workflows** using **AWS Lambda**.

**Nimble Engine for Routine Operations (NERO), The AI Assistant** Oct 2024 - Present

- **Built** a smart assistant with **FastAPI**, **React**, and **OpenAI API**; enabling optimal scheduling & task management.
- **Integrated secure authentication** using **JWT**, **OAuth**, and **RBAC**, achieving **100% protection** against unauthorized test access.
- Implemented **real-time logging** with **Splunk** and **Sysmon**, cutting debug time by **40%**.
- Planning enhancements including **MFA** and **penetration testing** for robust defense.

**Virtual Network Security Simulation** Aug 2024 - Oct 2024

- **Designed and configured** a multi-router, multi-subnet topology in **Cisco Packet Tracer**.
- Implemented **VLANs**, **ACLs**, and **static IPs** across 15+ devices, validated via **Wireshark packet captures**.
- Simulated misconfigurations and unauthorized access attempts, training for **SOC-level diagnostics**.

## SKILLS & STRENGTHS

- **Security & Monitoring:** Splunk, Chronicle, Sysmon, Wireshark, tcpdump, Event Tracing for Windows (ETW)
- **Network Security & Tools:** Firewalls, ACLs, VLANs, NetFlow, DHCP, ARP Poisoning, CPT, GNS3, pfSense
- **Cloud & SIEM:** AWS IAM, S3 Encryption, AWS Lambda, Azure Security Center, SIEM Integration
- **Identity & Access Management (IAM):** Active Directory, OAuth, Role-Based Access Control (RBAC), MFA
- **Threat Detection & Analysis:** Windows Event Logs, Anomaly Detection, MITRE D3fend
- **Offensive Security & Pentesting:** Nmap, Metasploit, Ettercap, Wireshark, TryHackMe Labs, Netcat
- **Programming & Scripting:** Python, C++, Bash, PowerShell, MySQL, JavaScript
- **Dev & Automation Tools:** FastAPI, React.js, Linux, Git, VS Code, MongoDB

## EDUCATION & CERTIFICATIONS

**B.S. Computer Science, California State University, Fullerton** - May 2025

Certifications:

- Google – Google Cybersecurity Professional Certificate - June 2024
- **CompTIA – Security + - July 2024**
- Cisco Certified Network Associate (studying) - July 2025
- AWS Certified Cloud Practitioner (studying) - July 2025

## RELEVANT LABS & TRAINING

- **Completed 15+ TryHackMe labs:** ARP Poisoning, Snort IDS, Kerberos Attacks, Metasploit
- **Advanced Networking Projects**: MAC spoofing, Wi-Fi cracking (WPA), honeypot setup, Nmap scanning
- **Digital Forensics Foundations**: Sysmon-based analysis, ETW trace logging, malicious .NET detection