Orlando David Hernandez Jr.

odhernandezjr@gmail.com | (847) 971-9568 | Chicago, IL | GitHub | LinkedIn | Portfolio

Early-career security engineer with hands-on experience detecting, investigating, and documenting real attack scenarios. Built end-to-end SOC workflows using SIEM and SOAR, authored publishable case studies mapped to **MITRE ATT&CK T1110** and **OWASP Top 10 A01**, and validated detections through controlled adversary simulation.

TECHNICAL SKILLS

- **Detection & Response:** Wazuh (SIEM), Shuffle (SOAR), DFIR-IRIS, alert correlation, authentication & authorization controls
- **Scripting & Automation:** Python (API enrichment), Bash, Git
- **Platforms & Frameworks:** Windows, Linux, AWS (EC2/IAM), MITRE ATT&CK (T1110), OWASP Top 10 (A01), NIST CSF

SECURITY ENGINEERING & SOC CASE STUDIES

Security Operations Engineering Environment Jan 2024 – Present

- Designed and operated a multi-host SOC lab integrating Wazuh, Shuffle, and DFIR-IRIS; validated detection coverage through controlled Atomic Red Team simulations and iterative SIEM tuning.
- Authored and published a Windows brute-force attack investigation mapped to MITRE ATT&CK T1110, incorporating SIEM detection logic, alert correlation, and SOAR-based enrichment and response workflows. Performed basic static and dynamic malware analysis in isolated lab environments (FLARE-VM, REMnux) to observe execution behavior, indicators of compromise, and detection-relevant artifacts.

Application Security Case Study – Broken Access Control (IDOR) Jan 2026

- Identified and validated a Broken Access Control / IDOR vulnerability aligned with OWASP Top 10 A01 by exploiting insecure object-level authorization between authenticated users.
- Demonstrated unauthorized cross-user resource access by manipulating direct object references while preserving session context, confirming missing server-side ownership enforcement.
- Documented attack methodology, affected authorization logic, and remediation controls including authorization middleware, ownership validation, and deny-by-default access patterns.

PROFESSIONAL EXPERIENCE

Island Party Hut Chicago, IL

General Manager Jul 2023 – Nov 2025

- Improved internal operations by implementing role-based access controls (RBAC), reconfiguring network infrastructure, and documenting technical SOPs, applying security and authorization principles in a real production environment.

Additional Experience

Hospitality Operations & Management 2019 – 2023

- Leadership, training, process documentation, and operational troubleshooting.

EDUCATION

- **Northeastern Illinois University** | *B.S. Computer Science*
- **William Rainey Harper College** | *A.A. Arts*

CERTIFICATIONS

- CompTIA Security+ (*Dec 2023*)
- Oracle Cloud Foundations Associate (*Oct 2023*)
- Google Cybersecurity Certificate (*Sep 2023*)