

Raesah Hernandez

raesah.hernandez@gmail.com | www.linkedin.com/in/raesah-hernandez-4792bb203 |
<https://github.com/RaeHernandez> | North Richland Hills | (469) 583-8342

SUMMARY

Driven cybersecurity professional with hands-on SOC lab experience in threat detection, incident response, and SIEM monitoring. Certified in Security+, CySA+, and Splunk Core Certified User, with practical skills in Python scripting and network analysis. Experienced in risk assessment, vulnerability management, and compliance frameworks including GDPR, CCPA, and PCI-DSS. Analytical, proactive, and collaborative, dedicated to applying technical expertise to strengthen organizational security posture.

EDUCATION

The University of Texas at Arlington | Arlington, TX
Bachelor of Science in Information Systems

December 2025

- Relevant Coursework: Network and Data Communications and Cybersecurity.

EXPERIENCE

Cybersecurity Intern | DoJoGa

August 2025 - Present

- Audited the dojoga.io web application, identifying gaps in encryption, headers, third-party integrations, and vulnerabilities aligned with OWASP Top 10, achieving a 40% improvement in risk mitigation and compliance posture.
- Developed remediation strategies and recommendations to align systems with GDPR/CCPA and strengthen overall security practices.
- Documented findings to support organizational compliance, internal controls, and security policy enforcement.

Cybersecurity Intern | TLT – Tomorrow's Leaders Today

May 2025 - July 2025

- Assessed internal cybersecurity controls and conducted risk assessments to identify vulnerabilities in access management, data integrity, and compliance processes.
- Developed and documented incident response and disaster recovery procedures to enhance organizational resilience and cyber threat readiness.
- Collaborated with 40+ interns to apply security best practices and support team-based cyber defense strategies.

TRAINING AND CERTIFICATIONS

CompTIA CySA+ | CompTIA Security+ | Splunk CCU | Google Cybersecurity Professional Certificate | TryHackMe SOC L1

PROJECTS

Telstra Cybersecurity Job Simulation - Forage | Remote

Individual Project

- Simulated live malware incident response within a SOC environment for Australia's largest telecom provider.
- Triaged a malware alert, analyzing logs to identify indicators of compromise (IOCs) and assess lateral movement.
- Conducted malware behavior analysis and created a Python-based firewall rule to block propagation.
- Produced a detailed incident postmortem documenting root cause, containment strategy, and remediation actions.
- Developed applied skills in threat analysis, malware forensics, scripting, and detection engineering aligned with enterprise SOC operations.

SKILLS

SIEM (Splunk) | Incident Response & Disaster Recovery | Risk Assessment & Vulnerability Analysis | Compliance Assessment (GDPR/CCPA, PCI-DSS, NIST CSF familiarity) | Internal Controls Evaluation | Security Policy Enforcement | Networking & Protocols (TCP/IP, DNS, HTTP/S, VPNs, Firewalls) | Programming/Scripting (Python, Java, C, Bash/PowerShell)