Antoinette"Toni" Valdez

| LinkedIn - Toni Valdez
GitHub/Aval12T

CYBERSECURITY ANALYST

Cybersecurity professional with a Master of Science in Cybersecurity and CompTIA Security+ certification. Experience includes security monitoring, incident response, threat analysis, vulnerability assessment, and risk management through graduate coursework, hands-on projects, and IT leadership experience. Skilled in Splunk, Wireshark, Snort, and Nmap, and other cybersecurity tools used for monitoring, threat detection, and incident response. Seeking a Cybersecurity Analyst, SOC Analyst, or Information Security Analyst position supporting threat detection, incident response, and risk reduction efforts.

Areas of Expertise:

- Digital Forensics & Investigations
- Cyber Threat Intelligence & Situational Awareness Training
- Incident Detection & Escalation
- Risk Assessment, Vulnerability, Mitigation & Compliance (SOC 2, NIST, ISO 27001)
- Malware Analysis
- Vulnerability Assessment & Management
- Security Controls Testing
- SIEM Monitoring & Log Analysis (Splunk & Snort)
- Threat Detection and Data Privacy Protection
- Intelligence Reporting & Briefings (Analytical Summaries, Alerts)
- Stakeholder Communication & Cross-Functional Collaboration
- Audit Support & Evidence Collection
- Network Security Monitoring

TECHNICAL PROFICIENCIES & CERTIFICATIONS

Cybersecurity Tools & Platforms: Splunk (SIEM), Wireshark, Nessus, Metasploit, Kali Linux, FTK, Imager Nmap, Snort, Burp Suite, VirusTotal
Networking & Security: TCP/IP, DNS, DHCP, VPNs, Firewalls, IDS/IPS, Network Traffic Analysis, Packet Analysis, Security Monitoring
Risk & Vulnerability Management: Vulnerability Scanning, Penetration Testing, Risk Assessment, Threat Intelligence Monitoring, OSINT, Threat Actor Analysis, Indicators of Compromise (IOCs), Remediation Reporting
Incident Response: Log & Event Analysis, Malware Analysis, Evidence Collection, Incident Response, Containment & Recovery Procedures, Intelligence Reporting, Security Event Investigation
Operating Systems: Windows Server, Linux (Ubuntu, CentOS), macOS
Security Frameworks & Standards: NIST CSF, NIST 800-61, CIS Controls, MITRE ATT&CK, SOC 2, ISO 27001, GLBA, HIPAA

CompTIA Security+ (SY0-701): Earned March 2026

Education

Master of Science, Cybersecurity | Southern New Hampshire University

- Gained hands-on experience with security tools and practices, including incident response, intrusion network analysis, and digital forensics. Developed skills in SIEM log monitoring, vulnerability assessment, penetration testing, and risk management using NIST frameworks.

Bachelor of Science, Agriculture | Virginia State University

CYBERSECURITY PROJECTS AND SIMULATIONS

Incident Detection & Response Simulation

- Configured Snort IDS/IPS rules and analyzed SIEM logs to identify anomalous network activity and potential security threats.
- Applied NIST 800-61 IR lifecycle to contain and recover from a simulated cyberattack.
- Authored incident reports that improved escalation workflows and reduced response time in exercises by 30%.
- Triaged and prioritized security alerts based on severity, identifying true positives and escalating critical threats.

Antoinette"Toni" Valdez

LinkedIn - Toni Valdez

GitHub/Aval12T

TryHackMe Cybersecurity Labs| 2025- Present

- Completed hands-on labs covering network security, incident response, vulnerability assessment, digital forensics, web application security, and threat detection
- Practiced identifying indicators of compromise (IOCs), analyzing network traffic, investigating security events, and responding to simulated cyber incidents.
- Utilized tools including Wireshark, Nmap, Metasploit, Burp Suite, Linux command line, and
- SIEM-based analysis environments.

Digital Forensics & Risk Management Case Study

- Collected and preserved evidence with FTK Imager and analyzed packet captures using Wireshark.
- Conducted vulnerability assessments with Nmap and Metasploit, linking findings to organizational risk.
- Delivered a remediation and compliance plan aligned with SOC 2 and NIST standards, reducing high-risk exposures by 40% and strengthening overall risk posture.

Deloitte Australia Cyber Job Simulation (Forage) - August 2025

- Conducted OSINT investigations and analyzed network and log data to identify IOCs, and suspicious activity.
- Correlated findings across multiple data sources to assess potential risk and support threat intelligence
- reporting.
- Produced intelligence briefings highlighting threat indicators, attack patterns, and recommended mitigation strategies.

PROFESSIONAL EXPERIENCE

IT Manager (Volunteer) (AwakenHer Wellness**)** Charlotte, NC 2024 – 2026

- Implemented multi-factor authentication (MFA), password security standards, and access control
- practices to strengthen protection of sensitive organizational data.
- Developed and documented IT policies, cybersecurity procedures, and data protection guidelines to support secure nonprofit operations.
- Provided technical support for staff and leadership by resolving user access, software, device, and system-related issues while maintaining security best practices.
- Delivered cybersecurity awareness training and guidance on phishing prevention, password hygiene, and safe handling of sensitive information.
- Evaluated technology risks and recommended security improvements to support data privacy, system reliability, and organizational growth

Customer Specialist II| Risk Compliance Focus (Principal) Charlotte, NC 2024 – Present

- Analyzed sensitive financial activity and operational risk indicators in a controlled, compliance-driven environment.
- Supported control testing, issue remediation, and audit evidence collection in partnership with compliance and technology stakeholders.
- Investigated anomalies and potential risk indicators, documented findings, and escalated concerns in accordance with internal control and governance requirements.
- Recommended process improvements that supported compliance objectives and reduced operational risk.
- Protected sensitive data through access controls, secure data handling procedures, and security-focused operational practices

Customer Specialist| Business & Consumer Accounts (Verizon) Charlotte, NC 2019 – 2023

- Performed Know Your Customer (KYC) and Know Your Business (KYB) checks by validating customer identities, reviewing tax IDs, and verifying business documentation.
- Investigated discrepancies in account information, escalating suspicious activity cases to fraud and risk teams.
- Delivered fraud awareness and account security guidance to customers, reducing account compromise

Licensed Insurance Agent (Allstate) Charlotte, NC 2017-2019

- Secured sensitive client information in alignment with GLBA and HIPAA compliance standards.
- Conducted identity verification and customer due diligence during onboarding, mitigating fraud and identity theft risks.
- Partnered with compliance teams to assess suspicious claims activity and support investigative escalation processes.