Dallas Gallegos

(973) 555-0148 dallas.gallegos@email.com
linkedin.com/example/dallasgallegos Newark, NJ 07102

SUMMARY

Red Team Engineer with four years delivering authorized penetration tests, adversary-emulation exercises, and threat-informed assessments across enterprise applications, infrastructure, cloud platforms, and identity environments. Builds realistic attack paths from **MITRE ATT&CK** and current intelligence, then works with security operations, detection engineers, incident responders, technology teams, and business owners to validate defensive readiness. Develops Python and PowerShell utilities, adapts established security tools, and preserves safe-testing boundaries through clear authorization, scope, **rules of engagement**, and risk-acceptance practices. Translates technical evidence into audit-ready findings, practical remediation plans, and concise executive readouts. OSCP, **AWS Certified Security – Specialty**, and CompTIA Security+ credentials support hands-on work across AWS, Azure, Active Directory, Linux, Windows, networks, endpoint telemetry, **vulnerability management**, detection engineering, and incident response. Ready to help strengthen Meridian Harbor Financial's resilience through disciplined, intelligence-driven testing and trusted collaboration.

EXPERIENCE

Red Team Engineer

September 2024 - Present

Northstar Cyber Defense

Newark, NJ

Lead authorized red-team engagements across AWS, Azure identity services, internal networks, and customer-facing applications. Own threat-informed planning, controlled execution, purple-team validation, evidence preservation, reporting, and remediation guidance for technical and risk stakeholders.

- Led AWS and **Azure adversary emulation** under approved scope, rules, and risk acceptance controls.
- Mapped **MITRE ATT&CK** paths to credential access, privilege escalation, lateral movement, and cloud persistence.
- Tested applications and infrastructure with **Burp Suite**, Nmap, BloodHound, Metasploit, and cloud utilities.
- Coordinated purple-team sessions that exposed endpoint, identity, and network detection gaps for remediation.
- Built **Python** and **PowerShell** helpers for reconnaissance, evidence collection, and repeatable validation tasks.
- Delivered audit-ready findings linking exploitable conditions, business risk, control domains, and treatment plans.

Penetration Tester

September 2022 - August 2024

Cedar Ridge Security Services

Jersey City, NJ

Executed authorized penetration tests across web applications, APIs, Windows and **Linux** infrastructure, corporate networks, and AWS environments. Combined technical testing, finding analysis, detection validation, and stakeholder communication to support practical risk decisions and durable corrective action.

- Executed authorized tests across web applications, APIs, **Windows**, Linux, corporate networks, and **AWS**.
- Mapped findings to **MITRE ATT&CK** and vulnerability classifications, clarifying root causes for engineering teams.
- Investigated access control, segmentation, exposed services, and cloud weaknesses with leading assessment tools.
- Created Python and PowerShell scripts for discovery, HTTP testing, evidence capture, and fix validation.
- Replayed attack behaviors with monitoring teams, verifying **SIEM** alerts and incident-response playbook improvements.
- Presented technical and executive readouts that converted complex findings into practical treatment options.

PROJECTS

Threat-Informed Purple-Team Validation 2026

Partnered with security operations and detection engineers on controlled attack scenarios mapped to MITRE ATT&CK. Shared evidence openly, adjusted testing after defensive feedback, and helped teams improve visibility across identity, endpoint, and network telemetry.

Cloud Identity Attack-Path Assessment 2025

Reviewed AWS and Azure identity relationships with infrastructure owners and defenders. Built safe attack paths, documented authorization boundaries, and connected privilege findings with remediation choices business stakeholders could act on.

LEADERSHIP & AWARDS

- Received Northstar Cyber Defense recognition for clear, audit-ready red-team reporting and practical remediation guidance.
- Earned team recognition at Cedar Ridge Security Services for dependable purple-team coordination and stakeholder communication.
- Led peer knowledge sessions on MITRE ATT&CK mapping, safe testing, and evidence preservation.

EDUCATION

Bachelor's Degree in Cybersecurity 2022

Rowan University GPA: 3.7 *Glassboro, NJ*

Coursework: *Network security, ethical hacking, digital forensics, secure software development*

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP) 2024
- AWS Certified Security – Specialty 2025
- CompTIA Security+ 2023

TECHNICAL SKILLS

- **Offensive Security Tools:** Burp Suite, Metasploit, SQLMap
- **Network Assessment:** Nmap, Nessus, Wireshark
- **Cloud Platforms:** AWS, Azure, AWS Security Hub
- **Identity Systems:** Active Directory, Azure AD, BloodHound
- **Operating Systems:** Linux, Windows, PowerShell
- **Scripting Languages:** Python, PowerShell, Bash
- **Attack Frameworks:** MITRE ATT&CK, adversary emulation, threat intelligence
- **Detection Platforms:** SIEM, endpoint telemetry, detection engineering
- **Security Testing:** Penetration testing, purple teaming, vulnerability assessment
- **Governance Controls:** Rules of engagement, authorization controls, risk acceptance
- **Incident Response:** Incident response, alert validation, response playbooks
- **Reporting Practices:** Audit-ready reporting, risk analysis, remediation planning

SKILLS

- Adversary Emulation
- Red-Team Operations
- Infrastructure Testing
- Web Application Testing
- Cloud Security
- MITRE ATT&CK
- Purple Teaming
- Detection Engineering
- Incident Response
- Vulnerability Management
- Risk Reporting
- Rules of Engagement
- Python
- PowerShell
- Identity Security

PROFESSIONAL AFFILIATIONS

- Member, Information Systems Security Association, participating in security education and peer exchange.
- Member, OWASP community, following application security research, testing practices, and responsible disclosure discussions.

LANGUAGES

- English (Native)
- Spanish (Proficient)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST