Jordan Lucas

(910) 555-0148 jordan.lucas@protonmail.com
linkedin.com/example/jordanlucas Fayetteville, NC 28314

SUMMARY

Purple Team Lead and **Senior Vulnerability Assessment Analyst** with 10 years supporting authorized **penetration testing**, **adversary emulation**, CDAP missions, and **defensive validation** across DoD and federal environments. Leads network, web application, Active Directory, cloud, and endpoint assessments under approved Rules of Engagement, Army regulations, and DoD cybersecurity policies. Partners with Blue Team, Cyber Threat Intelligence, and incident response personnel to connect attacker behavior with MITRE ATT&CK, improve detection logic, and validate response and recovery procedures. Converts technical evidence into prioritized risk assessments and remediation plans for government stakeholders. Mentors junior analysts through assessment planning, evidence handling, reporting, and after-action reviews. Active DoD Secret clearance holder with CISSP, CASP+, and Security+ credentials, ready to help Meridian Defense Technologies strengthen mission assurance and customer security outcomes.

EXPERIENCE

Purple Team Lead
July 2022 - Present

Apex Federal Cyber Operations
Fort Liberty, NC

Leads Purple Team campaigns and CDAP missions for Army-aligned environments, coordinating offensive testing, defensive validation, reporting, and analyst development across network, endpoint, cloud, and Active Directory domains.

- Directed Army-aligned Purple Team campaigns across network, endpoint, cloud, and **Active Directory** environments.
- Planned CDAP NAV, NDA, and PPT missions under approved **Rules of Engagement** and customer decision points.
- Built controlled attack paths with **Cobalt Strike**, Impacket, BloodHound, Metasploit, and **Kali Linux**.
- Mapped adversary activity to **MITRE ATT&CK** and refined SIEM detections with **Blue Team** partners.
- Presented risk-ranked findings linking evidence, remediation owners, milestones, and residual risk.
- Mentored six junior analysts through planning, evidence handling, technical writing, and after-action reviews.

Senior Penetration Tester
January 2020 - June 2022

Cobalt Ridge Security Services
Raleigh, NC

Led federal penetration testing engagements across segmented networks, web applications, Active Directory, cloud workloads, and endpoint platforms, translating exploit evidence into remediation sequences and control improvements.

- Led **federal** penetration tests across segmented networks, applications, **Active Directory**, cloud, and endpoint platforms.
- Built threat-driven **adversary emulation** plans using **MITRE ATT&CK** techniques and controlled test windows.
- Validated authentication, authorization, segmentation, exposed services, and defensive coverage with leading assessment tools.
- Coordinated live testing with **security operations** and **incident response** teams during customer-approved windows.
- Produced executive summaries and technical reports separating exploitable weaknesses from control gaps.
- Guided junior testers through evidence checks, retesting standards, and secure artifact handling.

Cyber Defense Analyst
January 2018 - December 2019

Northstar Mission Assurance
Washington, DC

Supported vulnerability assessments and Purple Team engagements for federal infrastructure, combining authenticated scanning, manual validation, defensive telemetry review, risk analysis, and customer remediation planning.

- Supported federal Purple Team engagements through authenticated scanning, manual validation, and telemetry review.
- Assessed Windows, Linux, Active Directory, web applications, and network services with approved tools.
- Translated attacker behavior into **MITRE ATT&CK** mappings and Blue Team briefing material.
- Executed controlled credential, privilege, and **lateral movement** scenarios within documented **Rules of Engagement**.
- Prepared **NIST Cybersecurity Framework** risk assessments and prioritized **remediation recommendations** for system owners.
- Captured lessons from after-action reviews with **CTI** and incident response personnel.

Security Operations Analyst
June 2016 - December 2017

Ironwood Federal Systems
Alexandria, VA

Monitored federal network and endpoint telemetry while supporting vulnerability validation, **incident response** exercises, evidence preservation, and early **DoD cyber operations** responsibilities within approved customer boundaries.

- Monitored federal network and endpoint telemetry for authentication, execution, and **persistence** anomalies.
- Correlated network flows, Windows events, endpoint findings, and vulnerability data before escalation decisions.
- Performed supervised **Nmap** discovery and vulnerability validation against approved customer assets.
- Assembled incident timelines and compared analyst actions with response and recovery procedures.
- Mapped recurring alerts to **MITRE ATT&CK** and identified credential access detection gaps.

- Earned broader assessment responsibilities through reliable evidence handling and concise **technical reporting**.

PROJECTS

CDAP Mission Validation Framework 2024

Created a repeatable framework for NAV, NDA, and PPT planning, joining attack objectives, defensive telemetry, safety controls, and customer decision points.

Adversary Emulation Reporting Standard 2022

Built a reporting model that connects MITRE ATT&CK evidence, detection outcomes, residual risk, and practical remediation sequencing for federal stakeholders.

LEADERSHIP & AWARDS

- Federal Cyber Operations Excellence Award, Apex Federal Cyber Operations, 2024
- Customer Impact Recognition for Purple Team Reporting, Cobalt Ridge Security Services, 2021
- Facilitator, Purple Team Mentorship Circle, 2023 - Present

EDUCATION

Bachelor's Degree in Cybersecurity 2016

George Mason University GPA: 3.7 *Fairfax, VA*

Coursework: *Network security, digital forensics, ethical hacking, incident response*

CERTIFICATIONS

- CISSP 2023
- CompTIA Advanced Security Practitioner (CASP+) 2024
- CompTIA Security+ 2017

TECHNICAL SKILLS

- **Offensive Security Tools:** Cobalt Strike, Metasploit, Kali Linux
- **Network Assessment Tools:** Nmap, network discovery, service enumeration
- **Web Application Testing:** Burp Suite, authentication testing, authorization testing
- **Adversary Emulation:** MITRE ATT&CK, TTPs, threat modeling
- **Identity Security:** Active Directory, BloodHound, Impacket
- **Cloud Security:** Cloud workload assessment, cloud controls, cloud infrastructure
- **Endpoint Security:** Endpoint assessment, endpoint telemetry, persistence analysis
- **CDAP Operations:** Network Assistance Visits, Network Damage Assessments, Persistent Penetration Testing
- **Defensive Validation:** SIEM detections, alert logic, triage playbooks
- **Cybersecurity Frameworks:** NIST Cybersecurity Framework, DoD cyber operations, Army regulations
- **Governance and Scope:** Rules of Engagement, approved testing, customer decision points
- **Reporting and Remediation:** Risk assessments, technical findings, remediation planning

SKILLS

- Purple Team Operations
- Penetration Testing
- Adversary Emulation
- CDAP
- NAV
- NDA
- PPT
- Network Security
- Web Application Security
- Active Directory
- Cloud Security
- Endpoint Security
- Incident Response
- MITRE ATT&CK
- Risk Assessments

PROFESSIONAL AFFILIATIONS

- Purple Team Mentorship Circle, Facilitator, 2023 - Present; supports practical coaching and shared assessment methods.
- Federal Cybersecurity Practitioners Forum, Technical Speaker, 2022 - Present; shares testing lessons with practitioner teams.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST