Jaden Chandler

(614) 555-0184 | jaden.chandler@example.com | linkedin.com/example/jadenchandler | Columbus, OH 43215

SUMMARY

Mid-level **Cybersecurity Engineer** with nearly five years strengthening security operations, cloud environments, enterprise networks, and identity services. Leads practical detection, response, **vulnerability management**, endpoint protection, and control improvements across Azure workloads and business applications. Tunes Microsoft Sentinel, Splunk, and **Defender for Endpoint** telemetry, then turns findings into clear remediation plans that infrastructure teams can act on. Builds PowerShell and Python automation for alert enrichment, indicator validation, log analysis, and ticket creation. Partners with service desk, application owners, technology leaders, and audit teams during investigations, change reviews, and control assessments. Holds CompTIA Security+ and **Microsoft Certified: Azure Security Engineer Associate** credentials. Ready to help Cedar Ridge Systems protect its people, platforms, and services through thoughtful engineering and dependable security operations.

EXPERIENCE

Cybersecurity Engineer

June 2025 - Present

Blue Harbor Logistics

Columbus, Ohio

Owns security engineering across Azure workloads, **corporate endpoints**, **identity services**, and enterprise investigations for more than 1,800 employees and contractors. Guides detection improvements, vulnerability reviews, automation, incident evidence, and secure infrastructure changes while keeping technology leaders and operational teams aligned.

- Tuned **Microsoft Sentinel** analytics for suspicious authentication activity and clearer investigation signals.
- Updated Defender for Endpoint policies to expose malware and lateral movement across corporate devices.
- Built **PowerShell** alert enrichment workflows that shortened analyst handoffs and improved investigation consistency.
- Created Python indicator validation and ticket automation for repeatable **security operations**.
- Ranked Nessus findings with asset criticality and exploit context for infrastructure remediation plans.
- Preserved incident logs and timelines, giving technology leaders concise evidence for containment decisions.
- Published **privileged access** and Azure configuration guidance for safer infrastructure change reviews

Security Engineer

September 2023 - June 2025

Pioneer Municipal Services

Dayton, Ohio

Supported security operations across a multi-site public services environment by connecting Splunk monitoring, endpoint defense, Azure access reviews, vulnerability remediation, **incident response**, and audit preparation. Worked closely with service desk, infrastructure personnel, application owners, and reviewers to reduce exposure without slowing delivery.

- Built Splunk correlation rules for Windows, network, cloud, and **authentication telemetry**.
- Investigated phishing and **credential misuse** with service desk partners, containing affected accounts and devices.
- Managed Nessus scans and converted exposed services into risk-ranked release work items.
- Onboarded about 900 workstations into Microsoft **Defender for Endpoint** with documented exceptions.
- Reviewed Azure role assignments and **conditional access** settings, guiding least-privilege corrections.
- Maintained incident playbooks and control evidence for quarterly security reviews and audit preparation.
- Documented containment actions and recovery lessons after **anomalous administrative activity** investigations

Cybersecurity Analyst

October 2021 - September 2023

Redwood Technology Cooperative

Cincinnati, Ohio

Monitored security telemetry for small and midsize clients while supporting vulnerability validation, access reviews, investigation automation, tabletop exercises, and risk reporting. Translated technical evidence into practical next steps that helped client teams prioritize threats, close control gaps, and plan service improvements.

- Monitored **SIEM** alerts and endpoint activity, escalating confirmed threats with actionable event summaries.
- Validated **Windows**, network appliance, and web application findings through configuration review.
- Created PowerShell queries for log parsing and asset inventory checks during investigations.
- Developed **Python** utilities for indicator matching and repeatable security analysis.
- Reconciled privileged account records with approved ownership during access review cycles.
- Facilitated **ransomware** and compromised credential **tabletop exercises**, assigning practical recovery actions.
- Prepared weekly reports linking alert trends, open findings, and remediation status to client risks

PROJECTS

Azure Security Control Program 2025

Partnered with infrastructure owners on Azure resource configuration, privileged access guidance, and evidence collection. Conversations stayed practical, helping teams adopt safer controls without disrupting delivery.

Endpoint Detection Coverage Rollout 2024

Coordinated Defender for Endpoint onboarding across a large workstation population. Shared exceptions clearly, checked coverage with peers, and helped service teams resolve deployment concerns.

Client Ransomware Readiness Exercises 2022

Supported tabletop sessions for ransomware, lost devices, and compromised credentials. Captured recovery gaps with care, then helped client teams assign realistic follow-up actions.

LEADERSHIP & AWARDS

- Cyber Defense Challenge Finalist, University of Cincinnati, 2021
- Cybersecurity Capstone Excellence Award, University of Cincinnati, 2021
- Dean's List, University of Cincinnati, 2020
- Peer Mentor, College of Information Technology, 2021

EDUCATION

Bachelor's Degree in Cybersecurity 2021

University of Cincinnati GPA: 3.7 *Cincinnati, Ohio*

Coursework: *Network security, incident response, cloud security, digital forensics, vulnerability management*

CERTIFICATIONS

- CompTIA Security+ 2022
- Microsoft Certified: Azure Security Engineer Associate 2024

TECHNICAL SKILLS

- **SIEM Platforms:** Microsoft Sentinel, Splunk, correlation rules
- **Endpoint Security:** Microsoft Defender for Endpoint, endpoint policies, malware detection
- **Cloud Security:** Microsoft Azure, Azure workloads, resource configuration
- **Vulnerability Tools:** Nessus, vulnerability scans, exploit context
- **Scripting Languages:** PowerShell, Python, query scripting
- **Identity Security:** Conditional Access, role assignments, privileged access
- **Incident Response:** Phishing investigations, containment, incident timelines
- **Network Monitoring:** Network telemetry, authentication telemetry, lateral movement detection
- **Security Governance:** Change management, security standards, implementation guidance
- **Audit And Compliance:** Control evidence, security reviews, audit preparation

SKILLS

- Security engineering
- Incident response
- Vulnerability management
- SIEM
- Microsoft Sentinel
- Splunk
- Defender for Endpoint
- Azure security
- Access management
- Endpoint protection
- Network monitoring
- Nessus
- PowerShell
- Python
- Threat detection

PROFESSIONAL AFFILIATIONS

- Cybersecurity Club Workshop Coordinator, University of Cincinnati, 2020 - 2021
- Volunteer Tabletop Exercise Facilitator, Ohio Cyber Range Student Program, 2021
- Peer Mentor, College of Information Technology, 2021

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST