Zayden Strickland

(630) 555-1847 | zayden.strickland@example.com | linkedin.com/example/zaydenstrickland | Naperville, IL 60540

SUMMARY

Cybersecurity engineering executive with 16 years directing enterprise security architecture, **cloud protection**, **application security**, identity programs, vulnerability management, incident response, and security operations. Leads distributed engineering teams across manufacturing, logistics, and technology environments, translating security risk into funded roadmaps and measurable outcomes. Established zero-trust architecture, secure software development, SIEM modernization, **threat-informed risk management**, and cloud guardrails across AWS and Azure. Partners with infrastructure, product, legal, operations, audit, and business leaders to improve resilience without slowing delivery. Develops technical leaders, manages strategic vendors, and communicates investment priorities clearly to executives and boards. Ready to help Redwood Industrial Systems strengthen **enterprise security capabilities**, protect business systems and data, and build resilient operations through focused engineering leadership.

EXPERIENCE

Vice President of Cybersecurity Engineering

March 2021 - Present

Northstar Manufacturing Technologies

Chicago, IL

Direct a 42-person cybersecurity engineering organization supporting 18 manufacturing sites, enterprise applications, cloud platforms, and connected production environments. Set security strategy, prioritize investment, develop leaders, and align engineering standards with enterprise risk and **resilient operations**.

- Aligned 42-person engineering roadmaps with enterprise risk priorities across 18 manufacturing sites and cloud platforms.
- Established **zero-trust architecture** across identity, privileged access, endpoints, and network segmentation for infrastructure leaders.
- Modernized AWS and Azure guardrails with **infrastructure as code** and **centralized logging** across 300 accounts.
- Introduced threat modeling and **software composition analysis**, moving application security validation earlier in product delivery.
- Consolidated vulnerability intelligence and risk exceptions into executive reporting for critical exposure prioritization.
- Built **incident response** playbooks, tabletop exercises, escalation paths, and partnerships for ransomware readiness.

Senior Director, Security Engineering

July 2017 - February 2021

BlueCrest Logistics Group

Oak Brook, IL

Led **security architecture**, **cloud security**, identity engineering, and security operations for transportation, warehouse, and customer-facing platforms. Coached managers and architects while guiding enterprise initiatives, vendor decisions, remediation governance, and secure product delivery.

- Replaced fragmented **SIEM** tooling with **Splunk** detection workflows using endpoint, identity, firewall, and cloud telemetry.
- Delivered privileged access management for administrators, service accounts, and third-party personnel across business-critical systems.
- Chaired API, mobile, and warehouse automation architecture reviews with documented abuse cases and control decisions.
- Established **vulnerability management** councils that converted scan findings into accountable remediation and risk-acceptance plans.
- Coached six engineering managers and senior architects through career expectations and succession planning.
- Connected **security operations** priorities with regional platform owners, improving investigation context and stakeholder confidence.

Director of Cybersecurity Engineering

January 2014 - June 2017

Meridian Cloud Services

Austin, TX

Managed a 19-person team responsible for cloud security architecture, application security enablement, identity controls, and security automation for hosted business services. Partnered with engineering, legal, compliance, and customer assurance teams on secure delivery and audit readiness.

- Designed **AWS** reference architectures covering IAM, encryption, network boundaries, logging, **key management**, and recovery.
- Launched product security training, code-review guidance, **dynamic testing**, and risk-based remediation service levels.
- Implemented automated security checks in Jenkins and **Terraform** workflows before **infrastructure** changes reached production.
- Prepared **SOC 2** evidence with legal, compliance, and customer assurance teams while retaining engineering ownership.
- Directed post-incident improvements involving secrets rotation, token monitoring, access reviews, and lessons-learned tracking.
- Translated customer security requirements into architecture decisions that supported reliable hosted service delivery.

Security Engineering Manager

August 2011 - December 2013

Apex Digital Retail

Dallas, TX

Supervised a seven-person security engineering team supporting e-commerce **applications**, corporate identity, payment integrations, and customer **data** platforms. Improved application risk review, access controls, vulnerability prioritization, incident investigations, and team readiness.

- Developed threat-modeling sessions for checkout, account, and partner integrations during product design.
- Implemented centralized authentication and multifactor access for administrative systems with service-owner rollout plans.
- Built vulnerability triage using scanner findings, asset criticality, exploit intelligence, and business ownership.

- Coordinated web application and endpoint investigations while preserving evidence and corrective action records.
- Created playbooks and mentoring plans that expanded junior analyst contributions across monitoring and access reviews.
- Partnered with help desk operations to resolve adoption issues during administrative access changes.

Security Engineer

June 2010 - July 2011

HarborPoint Software

Columbus, OH

Supported security assessments, **vulnerability management**, cloud identity reviews, incident investigations, and operational documentation across SaaS applications and internal infrastructure. Built practical automation under senior architectural guidance for Windows, Linux, and AWS environments.

- Supported SaaS security assessments by documenting weaknesses, affected assets, and practical remediation recommendations.
- Configured vulnerability scans and tracked findings through owner verification and closure across platform risks.
- Developed **Python** and **PowerShell** utilities for log enrichment, access reviews, and routine security checks.
- Assisted AWS **IAM**, security group, and CloudTrail reviews for development and production accounts.
- Collected endpoint and authentication evidence during incident investigations, maintaining timelines for engineering managers.
- Authored secure configuration and evidence collection procedures for recurring operational use.

PROJECTS

Enterprise Zero-Trust Architecture 2024

Directed phased identity, privileged access, endpoint, and network segmentation planning across manufacturing operations. The program gave leaders a practical investment sequence and clearer security ownership.

Cloud Security Standards Modernization 2023

Unified AWS and Azure security standards with infrastructure-as-code guardrails, centralized logging, and posture reviews across production accounts and subscriptions.

Security Operations Modernization 2020

Reframed detection and response around Splunk, endpoint, identity, firewall, and cloud telemetry, giving analysts stronger investigation context.

LEADERSHIP & AWARDS

- Security Leadership Excellence Award, Northstar Manufacturing Technologies, 2024
- Enterprise Risk Partnership Award, BlueCrest Logistics Group, 2020
- Customer Trust Impact Award, Meridian Cloud Services, 2016

EDUCATION

Bachelor's Degree in Information Technology

2010

Ohio University GPA: 3.5

Athens, OH

Coursework: *Cybersecurity, Database Systems, Network Administration, Systems Analysis*

CERTIFICATIONS

- CISSP 2015
- Certified Information Security Manager (CISM) 2018
- AWS Certified Security - Specialty 2022
- Microsoft Certified: Cybersecurity Architect Expert 2024

TECHNICAL SKILLS

- **Cloud Security:** AWS, Azure, CloudTrail
- **Identity Security:** IAM, Privileged Access Management, Multifactor Authentication
- **Security Operations:** SIEM, Splunk, Detection and Response
- **Application Security:** Threat Modeling, Software Composition Analysis, Dynamic Testing
- **Infrastructure Security:** Terraform, Infrastructure as Code, Network Segmentation
- **Automation Languages:** Python, PowerShell, Jenkins
- **Secure Development:** Secure SDLC, Code Review, DevSecOps
- **Vulnerability Management:** Vulnerability Scanning, Remediation, Risk Exceptions
- **Incident Response:** Tabletop Exercises, Ransomware Response, Evidence Collection
- **Security Architecture:** Zero Trust, Encryption, Key Management
- **Governance and Compliance:** SOC 2, Security Standards, Audit Evidence

- **Security Monitoring:** Centralized Logging, Endpoint Telemetry, Token Monitoring

SKILLS

- Cybersecurity Engineering
- Security Architecture
- Zero Trust
- Cloud Security
- Application Security
- Threat Modeling
- Identity and Access Management
- Privileged Access Management
- Vulnerability Management
- Incident Response
- Security Operations
- Risk Management
- Executive Communication
- Vendor Management
- Secure SDLC

PROFESSIONAL AFFILIATIONS

- Advisory Member, Midwest Cybersecurity Executive Forum, 2022 - Present
- Mentor, Chicago Information Technology Leadership Network, 2019 - Present
- Volunteer Instructor, Illinois Cybersecurity Workforce Initiative, 2017 - 2021

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST