Aiden Knecht

(225) 253-2457 | knechtaj@mail.uc.edu | Cincinnati, OH | linkedin.com/in/aiden-knecht | github.com/AidenKnecht

SUMMARY

CompTIA Security+ certified Cybersecurity student (4.0 GPA) with hands-on cybersecurity experience in threat detection, phishing analysis, and cloud security automation within a regulated healthcare environment.

EDUCATION

University of Cincinnati | B.S. Cybersecurity | GPA: 4.00 | Dean's List (All Semesters) | Expected: Summer 2028

Relevant Coursework: Network Security, Database Management, Network Infrastructure Management, System Administration

WORK EXPERIENCE

IT Security and Infrastructure Co-op | AtriCure | Mason, OH | May 2026 – August 2026

- Uncovered a dangling DNS record exposing the organization's production environment to subdomain takeover by engineering an Azure Function App that ingests 51 Cloudflare security insight classes into Microsoft Sentinel via webhook and a custom Data Collection Rule
- Reduced phishing investigation turnaround by ~35% across 200+ monitored mailboxes by triaging and dispositioning suspicious emails daily using Microsoft Defender XDR Threat Explorer, ANY.RUN, and VirusTotal
- Improved executive visibility into phishing risk across 40+ departments by building a KnowBe4 simulation analytics dashboard presented to VP leadership, which was escalated to the executive leadership team
- Identified and blocked a Chinese cloud storage application (Nutstore) posing data exfiltration risk by auditing 200+ unsanctioned cloud applications with Microsoft Defender for Cloud Apps and McasShadowItReporting KQL queries
- Assessed enterprise identity posture by auditing SSO configuration and authentication protocol (SAML/OIDC) across 335 Entra-integrated cloud applications, identifying 4 apps with expired SAML certificates and 8 operating without SSO

Shift Leader | Graeter's | West Chester, OH | July 2025 – Present

- Reduced new hire ramp-up time by ~50% by designing and delivering structured onboarding and training programs for 13 rotating team members covering compliance protocols, operational procedures, and performance standards
- Sustained 97% customer satisfaction across 500+ weekly interactions by leading real-time shift operations, delegating tasks under high-volume conditions, and resolving escalations before they impacted service quality

TECHNICAL SKILLS

Microsoft Defender XDR, Microsoft Sentinel, Microsoft Azure, Cloudflare, Stellar Cyber, KnowBe4, Zscaler, ANY.RUN, VirusTotal, Microsoft Defender for Cloud Apps, Microsoft Purview, Entra ID, Identity & Access Management (IAM), SIEM, KQL, PowerShell, Microsoft Graph API, Python, Linux/Unix, Windows Server Administration, TCP/IP, DNS, DHCP, SSL/TLS, Incident Response, Threat Detection, Phishing Analysis, Log Analysis, Risk Assessment, Compliance

CERTIFICATIONS

- CompTIA Security+ (May 2026)
- Microsoft Certified: Azure Fundamentals (AZ-900) (August 2026)
- TestOut Ethical Hacker Pro
- TestOut Hybrid Server Pro: Core

PROJECTS

Azure Sentinel Honeypot | June 2026

- Captured 3,500+ brute-force authentication attempts from 7 countries within 24 hours by deploying a cloud-based Azure honeypot and ingesting logs into Microsoft Sentinel
- Built a live attacker geolocation map using KQL and API enrichment within Sentinel Workbooks

Pi-hole DNS Server | March 2026

- Eliminated network-wide ad and tracker traffic by deploying and self-hosting Pi-hole on an Ubuntu Server VM
- Delivered DNS-level filtering, real-time query logging, and traffic visibility across all home network devices

Python Document Processing Automation | December 2025

- Accelerated document processing speed by 80% by developing a custom Python automation script
- Successfully parsed and extracted data from 1,000+ insurance documents for a small insurance business