

TIMOTHY FLETCHER

IT Support & Security Analyst | SIEM · Alert Triage · Security Automation · Infrastructure as Code

Open to Remote, Any Shift · timfletcher.tech · linkedin.com/in/timcfletch · github.com/NotKornFlakes

SUMMARY

Help Desk Analyst at Upstate Medical University handling account access, ticketed incidents and escalations in an SLA-driven healthcare environment. In self-built Azure labs, I monitor and triage Microsoft Sentinel alerts, write and tune KQL detections, configure log collection, automate enrichment and containment through APIs, and deploy infrastructure as code with Terraform. I document every investigation with evidence, metrics and lessons learned. B.A. in Information Science; ISC2 Certified in Cybersecurity.

TECHNICAL SKILLS

SIEM & Security Ops: Microsoft Sentinel, KQL, Log Analytics, Logic Apps (SOAR), MITRE ATT&CK mapping, IOC triage, threat intel (AbuseIPDB, ThreatFox), honeypots (Cowrie, Endlesssh), detection tuning, evidence preservation, incident write-ups

Cloud & DevOps: Azure (VMs, Storage, NSG firewall rules, RBAC, managed identity, Azure Monitor Agent), Terraform, GitHub Actions (OIDC), Checkov, Cloudflare (DNS, TLS, CDN), Git

Systems & Identity: Windows, Linux (Ubuntu, Fedora), networking fundamentals, Active Directory accounts & permissions, Microsoft 365 / Outlook, least privilege

Support & ITSM: Ticketing and queue management, incident documentation, escalation & handoff, remote troubleshooting, knowledge-base-guided resolution, phishing awareness, remediation tickets for resolver teams

Scripting & Reporting: KQL, Python (pandas, Plotly), SQL, REST APIs (Azure, AbuseIPDB), dashboards (Sentinel workbooks, D3, Plotly), Tableau, Excel

PROFESSIONAL EXPERIENCE

Help Desk Analyst — Upstate Medical University

Oct 2025 – Present

- Provide Tier 1 support by phone and ticketing system, triaging and resolving hardware, software and account-access issues for clinical and administrative staff.
- Administer Active Directory accounts and permissions and Microsoft 365 / Outlook access (calendar sharing, delegation) under least privilege.
- Document incidents and resolution steps in the system of record, manage a personal ticket queue, and follow up to close within service-level targets.
- Escalate complex cases to resolver teams with initial findings and clear handoff notes, and flag recurring issues to improve the knowledge base.

Owner — Self-Employed Home Repair & Remodeling

Jan 2021 – Sep 2025

- Ran all client communication, scheduling and on-site diagnosis end to end while completing a B.A. in Information Science full-time.

Project Estimator / Coordinator — TPM General Contractors & Property Restoration

Jan 2019 – Jan 2021

- Built insurance claim estimates in Xactimate and tracked schedules and progress across contractors and clients in Excel.

SECURITY & CLOUD PROJECTS

SOC Home Lab: Azure Honeypots + Microsoft Sentinel

GitHub

- Deployed three honeypots (Windows RDP, Cowrie SSH, Endlesssh) and configured Azure Monitor Agent, data collection rules and a custom log table to feed Sentinel; captured 1.24M attack attempts from 75 IPs in 37 hours with zero compromises.
- Wrote 5 KQL analytics rules (incl. password spray, brute-force-then-success); tested coverage and rebuilt the low-and-slow rule after v1 missed an attacker guessing once every 12 minutes.
- Reconstructed an SSH intrusion chain from session logs, mapped 13 techniques to MITRE ATT&CK, preserved 13 captured attacker files in quarantine and identified Panchan, Mirai and Bashlite by hash; published defanged IOCs and a D3 dashboard.

Sentinel SOAR: Automated Brute-Force Response

GitHub

- Built and troubleshooted a Logic App playbook integrating Sentinel, the AbuseIPDB API and the Azure REST API to enrich incidents and auto-block high-risk IPs in an NSG, using a least-privilege managed identity.
- Cut triage to ~12 seconds on average (8–18 s) versus 10–15 minutes manually; blocked IPs made zero further attempts, and per-IP grouping reduced 65 alerts to 6 incidents (~91%).

Portfolio Site: Infrastructure as Code (Terraform, Azure, Cloudflare, GitHub Actions)

GitHub

- Provisioned an Azure Storage static site behind Cloudflare (custom domain, strict TLS) with Terraform; remote state in a locked, versioned Azure backend.
- Built CI/CD in GitHub Actions: enforced Checkov scan on every push, plan on pull requests, apply on merge to a production environment.
- No stored credentials: OIDC federation with RBAC scoped to one resource group; storage account keys disabled for Entra ID auth.

HHS Healthcare Breach Analysis (Python, pandas, Plotly)

GitHub

- Cleaned and analyzed 8,013 HHS OCR breach records (2009–2026), showing hacking grew to 81% of breaches by 2025; published a live dashboard and a security-budget memo for a 40-person clinic.

CERTIFICATIONS & EDUCATION

ISC2 Certified in Cybersecurity (CC) — Jul 2025 · TestOut Security Pro

B.A., Information Science — State University of New York at Oswego

2024

Coursework: cybersecurity, networking, systems analysis, databases. Ongoing TryHackMe labs (networking, Linux, defensive security).