Joseph Belcher

Cybersecurity Analyst · Security Operations · Risk & GRC

Dayton, OH ☎ 937-654-6625 joebelcher94@gmail.com linkedin.com/in/joseph-belcher-infosec

About

Security analyst with an enterprise IT background and hands-on experience in endpoint security, Zero Trust, incident investigation, networking, and systems administration. I'm strongest when the work sits between technical troubleshooting and practical risk decisions.

Certifications

SecurityX (CAS-005, formerly CASP+) • **CySA+** • **Network+** • **Security+**

Core skills

Security Endpoint investigation · alert triage · EDR/MDR · Splunk/SIEM · log analysis · incident response · ThreatLocker
Risk & controls NIST CSF/RMF concepts · HIPAA · PCI DSS · least privilege · Zero Trust · control evidence · documentation
Systems Windows/Server · Active Directory · Linux · TCP/IP · DNS · VPN · Cisco · Palo Alto · Wireshark · M365 · Azure/Intune
Infrastructure Proxmox · Hyper-V · Docker · Tailscale · Git/GitHub · JIRA · Python · SQL · systemd · SSH

Experience

ThreatLocker · Security Analyst II Orlando, FL • 2025–Present

- Investigate escalated endpoint and application-control issues in customer Zero Trust environments using process activity, logs, network context, and application behavior.
- Build and tune allowlisting and Ringfencing policies around least privilege while accounting for business continuity and legitimate software behavior.
- Document findings and remediation for customers and internal teams; escalate higher-risk cases with the evidence and reasoning needed for the next analyst.

TransCore · IT Systems Administrator / In-House Support Orlando, FL • Jan 2024–May 2025

- Supported 100+ enterprise users across endpoints, identity, software, networking, conferencing, and security updates; helped administer Cisco and Palo Alto environments.
- Improved operational follow-through with clearer JIRA workflows, inventory tracking, issue documentation, and coordination across infrastructure projects.

Geek Squad · Advanced Repair Technician / Senior Hardware Technician Florida • Aug 2019–2024

- Diagnosed malware, operating-system failures, hardware faults, and data-loss risks in a high-volume repair environment while protecting customer data and documenting work clearly.

Secure Cyber Defense · Security Analyst Intern Ohio • May–Aug 2019

- Worked in a DoD-focused SOC environment with Splunk/SIEM, network-defense telemetry, log review, alert triage, and incident-response workflows.

Selected technical work

Home lab — Proxmox/Debian/Docker environment with hardened SSH, internal DNS, reverse proxying, monitoring, Tailscale remote access, and GitHub-backed infrastructure documentation.

Endpoint detection lab — Isolated Hyper-V attacker/target systems used to study DNS C2, LOLBin activity, controlled transfer/exfiltration patterns, shadow-copy deletion, and the resulting analyst telemetry.

Linux incident response — Socket-to-process investigation and persistence analysis with ss, ps, systemctl, journalctl, and lsof/netstat; stop malicious services and verify remediation.

Education

University of Cincinnati — B.S., Cybersecurity & Networking Systems • Cum Laude • GPA 3.67 • 2019–2022
Sinclair Community College — A.A.S., Computer Information Systems & Network Engineering