FRED ZIRBEL

414-916-1145 | me@fredzirbel.com | linkedin.com/in/fredzirbel | fredzirbel.com

EXPERIENCE

Critical Start Plano, TX

Principal Security Analyst *July 2026 - Present*

- Lead complex, customer requested deep dive investigations into phishing, malware, and identity intrusions across an MDR operation protecting 2,500+ customer environments. Correlate evidence from 30+ security products to determine scope, root cause, and required containment.
- Maintain a 16 minute average time to investigation while handling 300+ alerts monthly, enabling timely customer escalation and containment.
- Execute live containment and remediation actions, including host isolation, credential resets, session revocation, email deletion, and file quarantine, through a dual authorization workflow that removes attacker access and malicious artifacts.
- Translate technical findings into impact, response status, and remediation decisions for customer stakeholders, providing actionable recovery guidance during high priority incidents.
- Train and mentor L1 analysts to use the in-house AI platform effectively, improving investigation efficiency, correlation quality, and client ready writeups.

Senior Security Analyst *July 2025 - July 2026*

- Reconstructed attacker activity with custom KQL across evidence sources, including URL clicks, file downloads, identity activity, and process telemetry, to establish scope and root cause.
- Briefed customer stakeholders during three to five weekly high priority incident calls, delivering findings, attribution, and remediation guidance that informed response decisions.
- Correlated indicators across customer environments to identify shared phishing and malware campaigns, enabling coordinated response beyond individual alerts.
- Engineered 500+ suppression filters with KVP logic and regex, eliminating thousands of recurring false positives and improving analyst signal quality.
- Validated five or more suppression and orchestration changes daily before deployment, preventing faulty logic from reaching production.

Security Analyst *October 2024 - July 2025*

- Triaged identity, phishing, malware, and endpoint alerts across four EDR and SIEM platforms, producing scoped escalations for senior response.
- Developed custom KQL across identity, endpoint, and email telemetry to accelerate incident scoping in Microsoft Sentinel and Defender.
- Produced client ready escalations with attribution, investigation context, and remediation guidance, giving senior responders an actionable basis for customer communication.

AI & AUTOMATION

- Use an in-house AI platform daily across MDR workflows, including triage, investigation, correlation, and writeups, while validating findings against source telemetry. Apply AI to personal projects that accelerate hands on learning with new technologies.

TECHNICAL SKILLS

MDR & Incident Response: Alert triage and escalation, scope, impact, and root cause analysis, live containment and remediation, stakeholder communications, phishing, malware, and identity threat response

Endpoint & Detection: CrowdStrike Falcon, Palo Alto Cortex XDR, Microsoft Defender XDR/Endpoint, SentinelOne, detection tuning, suppression and orchestration QA

SIEM & Analytics: Microsoft Sentinel, Splunk Enterprise Security, Sumo Logic, KQL, regex, cross tenant campaign correlation

Identity, Cloud & Frameworks: Entra ID, Azure, identity and endpoint telemetry, MITRE ATT&CK, NIST SP 800-61

CERTIFICATIONS

CompTIA SecurityX (CASP+) | CompTIA CySA+ | CompTIA PenTest+ | CompTIA Security+ | ISC2 Certified in Cybersecurity (CC)

EDUCATION

Western Governors University January 2024 - December 2025

Master of Science in Cybersecurity and Information Assurance *Remote*

The University of Texas at Arlington August 2019 - December 2023

Bachelor of Science in Information Systems *Arlington, TX*