Tyler Will *Security-Focused Engineer | Security Threat Analysis*

tylerwill.dev@gmail.com 512-767-4456 Austin, Texas Portfolio Tyler Will

Profile

Security-driven engineer with hands-on experience in telemetry systems, incident detection, and system monitoring across Azure environments. Strong foundation in threat response, email security, compliance workflows, and vulnerability analysis. Skilled in Microsoft security tools, Python automation, and root-cause investigation. Focused on building secure systems and contributing to proactive defense strategies

Skills

Security & Analysis: Phishing Analysis, Threat Pattern Recognition, OSINT Tools, Log Analysis, Python Scripting, Microsoft Defender

Cloud & Infrastructure: Azure (Storage, DevOps, Functions), GitHub Actions, Grafana

Data Engineering: ETL/ELT Pipelines, LiteDB, REST APIs, CI/CD, SQL

Expanding Expertise In: Email Security Analysis, Log Triage, Threat Detection, Vulnerability Scanning, SIEM Tools, Palo Alto Basics, Proofpoint, Compliance Documentation

Professional Achievements

Azure Monitor Health Checks
- Created automated health checks that mimic endpoint detection behaviors, aligning logs to detection logic in Azure Monitor and Defender

Backend Service Optimizations
- Improved simulation performance by 86% by refactoring backend data processing; Optimizing telemetry ingestion

Grafana-Based Notification System
- Built a real-time observability pipeline using Grafana, Azure Monitor, and C# to monitor health metrics to trigger alerting events in Kubernetes

Projects

Malware Analysis Labs
Reverse engineering malware samples using Ghidra. Analyzing PE file structures, packer behaviors, and ML-triggered detections. Writing Python scripts to automate signature extraction

Education

Bachelor of Science – Computer Science,
Colorado State University
02/2019 – 07/2021

Professional Experience

Software Engineer, *Contract Projects*
01/2025 – present | Austin, Texas
- Built automated scripts in Python to identify abnormal log patterns and contain suspicious behavior in simulated environments
- Integrated build tools and log analysis frameworks to validate system health and trigger alerting logic
- Developed tooling to isolate failure patterns in simulation telemetry, flagging potential malicious/erroneous behavior from binary inputs
- Built internal tools that supported self-service deployment of test environments and cloud containers
- Analyzed telemetry and Defender logs to surface early-stage threat signals and support simulated incident workflows

Full-Stack Software Developer, *General Motors - Motorsports*
09/2022 – 12/2024 | Austin, Texas
- Engineered internal data integration pipelines using Python, SQL, and YAML to process telemetry data and support simulation workflows
- Created CI/CD pipelines using YAML for automated builds and Azure deployments, integrating telemetry ingestion workflows
- Developed internal build/release tooling with YAML and C# to support telemetry-aware deployment workflows for simulation engine
- Created tools for debugging and performance tuning backend services, including SQL optimization and integration validation
- Collaborated with cross-functional teams to develop internal platform features, including secure API endpoints and telemetry-integrated workflows

Software Engineer - Quality Assurance,
General Motors - Manufacturing
06/2021 – 09/2022 | Austin, Texas
- Automated data validation workflows across 80+ facilities using Python scripts and Excel macros, ensuring compliance with telemetry data rulesets
- Reported data defects, documented results, and worked to ensure validated business logic and data flow accuracy
- Led test automation for critical manufacturing applications across 80+ facilities globally, improving test coverage