Thomas Birt

Tyler, TX 75707
TBirt2000@proton.me (903) 714-8827
Portfolio LinkedIn GitHub

PROFESSIONAL SUMMARY

Cybersecurity Analyst with 17 months of Tier 2 SOC experience investigating security incidents, performing threat hunting, vulnerability management, analyzing SIEM/EDR alerts, and building ServiceNow dashboards for security reporting. Willing to relocate for the right opportunity.

EDUCATION

Bachelor of Science in Computer Information Systems

- Graduated *Cum Laude* from Stephen F. Austin State University (Nacogdoches, TX) Jan 2021 - May 2023

Associates Degree in Business

- Tyler Junior College (Tyler, TX) Aug 2019 - Dec 2020

CERTIFICATIONS

- CompTIA SecAI+ (`067b97817bd4437d8d85af618b8ad653`) Mar 2026
- Certified in Cybersecurity (CC) (`2303539`) Sep 2024
- AWS Certified Cloud Practitioner (`69a25b42f8e04c589dcd2bcd9668165a`) Jan 2024
- CompTIA Security+ (`06C5ZVWZ1FFQ1EK0`) Oct 2023

TECHNICAL SKILLS

Security Tools:

- Splunk, Proofpoint, SentinelOne, Mandiant Advantage, Zimperium, Palo Alto Cortex XSOAR and XPANSE, Tenable, Armis

Security Operations:

- Incident triage, threat hunting, vulnerability management, attack surface management, OSINT, IOC analysis, MITRE ATT&CK, malware sandbox analysis

Programming Languages:

- PowerShell, Bash, Python, Java, C++, Visual Basic, SQL, HTML, JavaScript, CSS, MySQL, TypeScript, Angular, Spring Boot, MySQL Workbench, Postman, APIs, Microservices, JUnit, Selenium WebDriver

Computer Systems & Cloud:

- Experience with Azure AD, AWS Lightsail, GitHub, ServiceNow, Microsoft SharePoint, Microsoft Windows, macOS, Linux, Oracle VirtualBox and VMWare Workstation, Microsoft Office Suite (Word, PowerPoint, Excel, Access)

Network:

- Windows PC deployment and configuration using PXE booting, Knowledge of TCP/IP and data protocols

EMPLOYMENT HISTORY

Provalus — Detection Assessment Analyst (SOC Tier 2)
Henderson, TX | Jun 2024 - Nov 2025

- Investigated Tier 1 escalations by analyzing SIEM, EDR, email security, OSINT, and threat intelligence data to determine severity, scope, escalation requirements, and remediation actions.
- Conducted proactive threat hunting to identify Indicators of Compromise (IOCs), analyze emerging threats, and implement mitigation strategies.
- Streamlined vulnerability management workflows in ServiceNow, ensuring critical vulnerabilities were prioritized and patched within SLA windows.
- Assisted with remediation calls by organizing and formatting monthly remediation workbooks.
- Conducted ASM (Attack Surface Management) mapping across Tenable, SentinelOne and Armis to eliminate blind spots in asset coverage by brand, region, and function.
- Applied MITRE ATT&CK Tactics and Techniques during security investigations, mitigation planning, and forensic analysis.

GenSpark — Java Full Stack Developer
Mar 2024 - Jun 2024

- Developed diverse projects leveraging foundational Java concepts, Spring Boot, Hibernate, MySQL, TypeScript, and Angular.
- Applied object-oriented programming and test-driven development principles to build maintainable applications.
- Built backend services and database integrations using Spring Boot, Hibernate, and MySQL.
- Used GitLab, Postman, JUnit, and Selenium WebDriver during development and testing workflows.

Stephen F. Austin State University — IT Internship, Tech Shop Group Member
Nacogdoches, TX | May 2022 - Aug 2022

- Provided computer lab assistance and implemented new technical solutions
- Provided technical support for workstations and software products to various departments

PROJECTS

Android Proxy Botnet IOC Scanner
Jul 2026 - Present

- A detection tool that checks Android TV boxes, phones, or emulator images for indicators associated with Popa/NetNut-style proxy abuse, risky apps, suspicious network IPs, and proxy behavior.

HoneyRadar - Honeypot/SIEM Dashboard
Jun 2026

- Designed and deployed a Linux-based honeypot and SIEM lab using Cowrie, OpenCanary, Python, WebSockets, Tailscale. Captured attacker probes and login attempts, normalized JSON security logs, enriched public source IPs and malware with threat reputation data, and visualized activity through a live attack map dashboard.

SOC Dashboard - ServiceNow
Feb 2025 - Nov 2025

- Implemented a ServiceNow SOC Dashboard for monitoring and sharing reports, data visualizations and trends with internal stakeholders.

**Additional projects and work samples are available on my portfolio website, LinkedIn and GitHub links.*