

Thomas Birt

Tyler, TX 75707

[\(903\) 714-8827](tel:(903)714-8827)

TBirt2000@proton.me

[Portfolio](#)

[LinkedIn](#)

[GitHub](#)

OBJECTIVE:

Pursuing employment as a Cybersecurity Analyst with Tier 2 SOC, threat-hunting, incident response, vulnerability management experience and hands-on proficiency with SIEM, EDR, and XSOAR platforms.

EDUCATION

Bachelor of Science in Computer Information Systems

- Graduated *Cum Laude* from Stephen F. Austin State University (Nacogdoches, TX) 01/21 - 05/23

Associates Degree in Business

- Tyler Junior College (Tyler, TX) 08/19 - 12/20

CERTIFICATIONS

- CompTIA SecAI+ (067b97817bd4437d8d85af618b8ad653) 03/26
- Certified in Cybersecurity (CC) (2303539) 09/24
- AWS Cloud Certified Practitioner (69a25b42f8e04c589dcd2bcd9668165a) 01/24
- CompTIA Security+ (06C5ZVWZ1FFQ1EK0) 10/23

TECHNICAL SKILLS

Security Tools:

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

Programming Languages:

- Python, Java, C++, Visual Basic, SQL, HTML, JavaScript, CSS, MySQL, JSX, TypeScript, Angular
- Worked with Hibernate, Spring, Spring Boot, MySQL Workbench, Postman, GitKraken, GitLab, JSX, APIs, Microservices, JUnit, Selenium WebDriver

Cloud Development

- Amazon Web Services, Lightsail

Computer Systems & Support:

- Experience with Azure AD, Windows, macOS, Ubuntu, Arch Linux, Microsoft Office Suite (Word, PowerPoint, Excel, Access)
- Installation, configuration, maintenance, and upgrades of hardware and software, peripheral device integration
- Virtual machine management through VirtualBox and VMware Workstation
- Built, repaired, configured, and installed workstations to meet end user needs
- Experienced in GitHub, ServiceNow, SharePoint

Network:

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

Graphic Design and Media Arts:

- YouTube content creation using Magix Vegas
- Adobe Photoshop and Illustrator for graphic design projects

ADDITIONAL SKILLS

- Effective teamwork and project management abilities
- Proven ability to reduce incident resolution times and develop custom dashboards for security metrics.
- Strong technical support and troubleshooting skills
- Teamwork experience on multiple projects
- Metrics to Visuals skills
- Rapid Skill Acquisition and Adaptability

EMPLOYMENT HISTORY

Stephen F. Austin State University IT Internship, Tech Shop Group Member 05/22 - 08/22
Nacogdoches, TX

- Collaborated with a team of 6 to improve technical support for faculty clients
- Provided computer lab assistance and implemented new technical solutions
- Provided technical support for workstations and software products to various departments
- Trained new interns on the complexity of hardware and software installation

GenSpark Java Full Stack Developer 03/24 - 06/24

- Executed assignments leveraging foundational Java concepts encompassing Loops, Arrays, Collections, Classes, Object-Oriented Programming (OOP), Exceptions, IO Files, and Functional Programming principles
- Applied Test Driven Development (TDD) methodologies to ensure the creation of robust, maintainable code.
- Developed diverse projects including "Humans vs Goblins" and a Simple Slot Machine application, employing Java and integrating various Java concepts.
- Engineered the backend of an application utilizing Java, Spring Boot, and Hibernate to establish seamless connectivity with a MySQL database.
- Explored TypeScript fundamentals, covering Basic Types, Type Annotations and Inference, Functions, Interfaces, Classes, Generics, Modules, Namespaces, and Decorators.
- Engaged in foundational Angular Development tasks, encompassing Components, Templates and Data Binding, Directives, Services and Dependency Injection, Modules, Routing, Forms, HTTP Client, Pipes, and RxJS Basics.
- Orchestrated the development of a comprehensive Full Stack Employee Management System using Java, Spring Boot, Hibernate, MySQL, and Angular.

Provalus Detection Assessment Analyst (SOC Tier 2) 06/24 - 11/25
Henderson, TX

- Further investigated and performed deeper analysis on Security Incidents escalated from Tier 1 Alert Triage Analysts, and if needed escalate higher priority alerts to Tier 3.
- Conducted proactive threat hunting to identify Indicators of Compromise (IOCs), analyze emerging threats, and implement mitigation strategies.
- Utilized OSINT sources, Malware Analysis Sandboxes, and SOC tools including ServiceNow, Splunk (SIEM), Proofpoint, SentinelOne (EDR), Mandiant, Recorded Future, Zimperium, and Palo Alto Cortex XSOAR and Xpanse, Tenable to investigate and remediate security incidents.
- Responsible for the development, review, and deployment of ServiceNow Dashboard for monitoring and sharing reports, data visualizations and trends with people across the organization.
- Streamlined vulnerability management workflows in ServiceNow, ensuring critical vulnerabilities were prioritized and patched within SLA windows.

- Assisting with remediation calls by organizing and formatting monthly remediation call workbooks, saving time for pre-meeting preparations.
- Conducted ASM (Attack Surface Management) mapping across Tenable, SentinelOne and Armis to eliminate blind spots in asset coverage by brand, region, and function.
- Adhered to MITRE ATT&CK Frameworks involving Tactics and Techniques when performing investigations, mitigations, and forensics.

PROJECTS

SOC Dashboard	Implemented a ServiceNow SOC Dashboard for monitoring and sharing reports, data visualizations and trends with internal stakeholders.	02/25
WordPress Portfolio	Deployed and hosted a highly-available WordPress application using Amazon Lightsail.	02/24
MyPantry app	Developed an app as a team using Android Studio.	08/22 - 12/22
ASUS Zenbook UX331 Macintosh	Successfully installed & configured full functionality of Mac OS on a Windows laptop.	08/20 - 01/21

ACHIEVEMENTS

- The National Society of Leadership and Success 08/23
- 1st Place - SentinelOne Proactive Services Capture the Flag Exercise (8372102773) 02/25
- Participated in:
 - Stephen F Austin State University 47th Annual Computer Science Programming Contest
 - National Cyber League Individual Game Spring 2022

REFERENCES

Paul Gault, Provalus Senior Director, Meridian Program	Email: paulgault@provalus.com	Cell: (850) 876-9233
Morgan Gibson, ReliaQuest GreyMatter Engineer	Email: gibsonmc@hotmail.com	Cell: (903) 413-5973
Sam Bowman, Brookshire Grocery Company Systems Administrator I	Email: sambow23@gmail.com	Cell: (903) 270-4201
David Townsend, Provalus SOC Tier 3 Shift Lead	Email: davidpaultownsend@gmail.com	Cell: (972) 953-6523
Christian Brunning, Provalus TVM Analyst	Email: christianbrunning@gmail.com	Cell: (318) 366-3634
Matthew Beauregard, Stephen F. Austin State University, Professor & Chair of the Department of Computer Science	Email: beauregama@sfasu.edu	Work: (936) 468-2508