

Tajae Johnson

Security Analyst

Relevant experience: **2 years**

Total experience: 4 Years

+1 (213) 316 8984

TajaeJohnson@proton.me

Houston, Texas



Summary



As a Computer Science connoisseur, I specialize in Object-Oriented Programming, web development, and server-side technologies, with strong

knowledge of network security and encryption. Transitioning into cybersecurity, I leverage my development background to address challenges with a focus on incident response, prioritizing both efficiency and security.

Work Experience

SANS Institute

Sep 2023 - Nov 2024

1 Year

Cybersecurity Trainee | Cyber Immersion Bootcamp

- Gained practical knowledge of hardware components, memory structures, and **virtualization** technologies like **Docker** and **VMware**.
- Mastered essential **Linux** and **Windows CLI** commands, **UAC**, and networking to secure systems.
- Conducted **memory forensics** and disk analysis using **Volatility**, focusing on **attacker persistence**, **lateral movement**, and **data exfiltration**.
- Acquired proficiency in **TCP/IP**, **DNS**, and the **OSI model**. Used **Wireshark** for traffic analysis and **Nmap** for network scanning.
- Applied cryptographic techniques (**symmetric/asymmetric encryption**, **PKI**, **VPNs**) and **steganography** for secure communication.
- Implemented layered security strategies using **firewalls**, **HIDS**, and **NIDS**, applying principles of **defense in depth** to protect systems.
- Configured and monitored **SIEM** systems like **Splunk** and **Zeek** for log analysis and **RITA** real-time threat detection.
- Applied the **PICERL** process to handle incidents, and **mitigated post-exploitation attacks** (e.g., persistence, exfiltration) across network and cloud environments using **LivingOffTheLand (LOTL)** and **PowerShell**.
- Performed penetration testing using **Metasploit**, **Mimikatz**, **Hydra**, and **NetCat** to detect and remediate network and host vulnerabilities.
- Simulated **drive-by attacks** and applied mitigation strategies.
- Secured cloud infrastructures in **Azure** and **AWS** using **Azure Security Center** and **CloudTrail**.
- Applied **Windows Group Policy** and Linux hardening techniques to secure systems.
- Protected web applications against **SQL Injection**, **XSS**, and **CSRF** using secure coding practices and **SSL/TLS encryption**.

2U Inc.

Nov 2021 - present

3 Years

Instructional Specialist

- Led penetration testing workshops with **Metasploit**, **Burp Suite**, and **OWASP ZAP**, covering **SQL Injection**, **XSS**, and **CSRF**. Integrated **OWASP Top Ten** for secure coding and vulnerability prevention.
- Conducted labs with **Autopsy**, enabling students to perform memory and disk forensics. Taught **chain-of-custody** protocols and evidence integrity practices for **incident response**.
- Instructed on securing **Azure** infrastructures, configuring **Azure Security Center** and **Azure Sentinel**. Integrated **Splunk** for **SIEM** and real-time log analysis, emphasizing **NSG** setup and automated deployment via Azure CLI and **ARM templates**.
- Led training on **MITRE ATT&CK** and threat modeling, mapping **CVEs** to mitigation strategies. Taught CVE research and **NIST CVSS** vulnerability assessment, aligning vulnerabilities with patching priorities.
- Facilitated **security awareness** programs on social engineering, phishing, and data protection. Delivered mitigations such as **MFA**, **RBAC**, and **EDR** to strengthen organizational security posture.

Career Objective

I aim to build expertise in reverse engineering and assembly language to enhance my threat-hunting skills and protect enterprise systems from evolving threats. Passionate about emerging technologies, I am committed to staying at the forefront of cybersecurity and aspire to manage enterprise-level security infrastructures. With rapid advancements, including quantum computing, I plan to leverage my development background to streamline security processes and adapt to the fast-changing landscape.

Technical expertise

Python	<div></div>
PowerShell	<div></div>
Java	<div></div>
Rust	<div></div>
Assembly	<div></div>
OWASP	<div></div>

Skills / Exposure

Linux	Windows	Azure	AWS
Ghidra	Splunk	Hydra	Redis

Methodology/Approach

Defensive Programming	Blue Team		
Zero Trust	PICERL	GRC	OSINT

Tools

MITRE ATT&CK	Vim	Git
--------------	-----	-----

Education

BA, MS - Computer Science	
Texas Southern University	Jan 2018 - present

Certificates and Awards

- Completed **Full Stack & Cybersecurity** Boot Camps at **UT Austin**, with proficiency in programming, web development, network security, encryption, and incident response.
- Currently attending **SANS Institute** on scholarship. Obtained: **GSEC**, **GFACT**.
- Currently pursuing **GCIH - Testing Nov 2024**