Swathi Tadepalli

(240)426-6012 | swatadepalli@gmail.com | Website

Summary

Results-oriented Cyber Security Professional with experience in information technology, including threat detection and incident response, cyber security architecture, and data analysis.

Professional Skills

- Adept at following each phase of the detection development lifecycle, including threat research, detection design, rule development, tuning, and continuous testing
- Built custom detections aligning with prevalent MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) through KQL queries and Sigma rules
- Researched emerging threats for detection rule concepts and analyzed application, cloud, network, and system logs to identify and troubleshoot issues
- Developed and integrated security tests for Atomic Red Team's open-source library to enhance the cyber community's capability to conduct threat emulation testing efficiently

Technical Skills

Frameworks	NIST SP 800-207, FISMA, MITRE ATT&CK 13.1, TSA Directive, PCI DSS 3.2.1, HIPAA,
Security Tools	Splunk, Microsoft Sentinel, ZeroFox, Dragos, Atomic Red Team, Carbon Black, LimaCharlie, Sigma, Yara, ELK Stack (Elasticsearch, Logstash, Kibana), Elastic, Chainsaw, Dradis, Nessus, Volatility, Wireshark, Pfsense, Autopsy, FTKImager, Chronicle, RSA Archer, NMAP, Burpsuite, Snort, Tcpdump, Metasploit, Microsoft Defender, Kerberos, AWS, Microsoft Azure
Programming Languages	Java, Python, KQL (Kusto Query Language), SQL, NoSQL, PL/SQL, HTML, CSS, XAML, Windows and Linux command line, PowerShell
Data Tools	Oracle, MySQL, Tableau, Excel, Google Analytics
Methodologies/tools	SAFe (Scaled Agile Framework), SDLC, Agile framework, OSINT, OWASP Top 10, IAM (Identity Access Management), Cybersecurity Mesh Architecture, Multi-Factor Authentication, ServiceNow, Jira, Confluence
Other	Cyber Law and Policy, Digital Forensics, Cryptography, Kubernetes, Git, Web Mapping, Cloud Computing
Operating Systems	Windows, Mac, Linux

Work Experience

Personal Project 5/24-Present

- Developed a home lab with Windows and Linux virtual machines, integrating the Elastic Stack SIEM for security monitoring and analysis
- Authored multiple cybersecurity articles on Medium on topics including Sysmon integration, keylogger attack simulation, and creating custom detection rules, featured in Zack Allen's Detection Engineering Weekly Newsletter
- Studied for industry-recognized cybersecurity certifications, including Security+
- Leveraged online educational platforms like Codecademy, TryHackMe, and TCM Security to enhance engineering and security skills

Cybersecurity Analyst,
Amtrak, Washington DC 9/23 – 5/24

- Leveraged open-source Python scripts to decrypt AES credentials within our environment in efforts to advocate for stronger authentication protocols, policies, and standards
- Participated in all phases of Amtrak's detection development lifecycle, including threat research, detection design, rule development, tuning, and continuous testing to enhance threat visibility and response effectiveness.
- Developed curated detections associated with common MITRE ATT&CK TTPs using KQL queries and Sigma rules
- Demonstrated proficiency in analyzing application, cloud, network, and system logs to detect threats, investigate anomalies, and optimize security defenses
- Developed a comprehensive cybersecurity mesh framework by integrating NIST SP 800-207 Gartner's Zero Trust Architecture, improving the cybersecurity model with automation and efficiency

- Utilized Dradis to enhance the readability, comprehension, and organization of imported Nessus/Tenable, Invicti, and Pentera data for over 100,000 assets
- Aided cyber threat intelligence efforts by administering OSINT and access management tools to disable compromised email accounts, ensuring a more secure environment
- Led a team of interns, offering valuable career guidance and handling administrative responsibilities to foster success

IT Specialist,
Internal Revenue Service, Washington DC 1/21 - 11/21

- Utilized SAS programming language for data mining and analyzing in the Oracle database.
- Developed applications using .NET framework in Visual Studio to enhance team productivity.
- Executed advanced SQL queries in the database using TOAD to identify data discrepancies.
- Reviewed and validated IT tax project specification documents to ensure accuracy and readability.

Chief Privacy Office Intern,
General Services Administration, Washington DC 6/19 - 8/19

- Reviewed Privacy Impact Assessments and System of Records Notices to support the Privacy team's mission.
- Validated customer facing website for compliance with GSA's privacy policy to ensure they are up to date.
- Developed knowledge of government guidelines, standards, and frameworks including NIST and FISMA.
- Utilized Google Analytics to track traffic on GSA's public-facing privacy websites.
- Edited the back-end code for GSA's public-use privacy forms using Google App Script.
- Supported IT security tasks by shadowing team members and performing assigned duties.

Certifications

CompTIA Security+ (Estimated April 2025)
Google Cybersecurity Professional Certificate – August 2023

Education

University of Maryland, Baltimore County, Baltimore, MD
Master of Science in Cybersecurity, August 2024
Bachelor of Science in Information Systems, Minor in Entrepreneurship, December 2019