

GADDIPATI LOHIT

lohiggaddipati@gmail.com | (425)-494-9600 | [LinkedIn](#) | [Blog](#) | [GitHub](#)

Skills

Technologies: Azure, AWS, GCP, Terraform, Splunk, Sentinel, Wireshark Defender, tcpdump, SQL, Linux.
Languages: Python, C
Skills: Monitoring & Analysis, Threat Detection, Patching solutions, Incident Response, Log Analysis, SIEM, Cloud Security, IAM, Security controls & Framework like TLS, Zero-trust, Vulnerability assessment, Adaptable.

Professional Experience

T-Mobile

Bothell, WA
present

Cloud Security Detection and Response Team

- Collaborated with cross-functional teams to establish and optimize AWS IAM processes, enhancing security and compliance which resulted in reduced vulnerabilities by almost 25%
- Implemented and streamlined authentication and SSO protocols, including SAML, resulting in a secure access experience for over 2,000 users, reducing login errors by 40%
- Integrated Azure for federated Single Sign-On (SSO) and Multi-Factor Authentication (MFA), strengthening access controls.
- Developed a solution to filter out false positive in Macie Logs using automation which was 90% effective and Implemented patching solutions across cloud platforms integrating with Git.
- As part of Cloud Center of Excellence, fostered collaboration with diverse teams, including infrastructure engineering, client groups, and network engineers, leading to well-architected and secure IAM solutions.

University at Buffalo

Buffalo, NY
2023

Cybersecurity Student

Azure SSO Configuration

- Configured Single Sign-On (SSO) using SAML in Azure, streamlining user access to applications.
- Implemented Multi-Factor Authentication (MFA) and Self-Service Password Reset (SSPR) in Azure for enhanced security and Integrated Azure for federated Single Sign-On (SSO) strengthening access controls.

Microsoft Sentinel Implementation

- Configured Microsoft Sentinel to ingest data and detect threats.
- Created analytic rules, automation rules, and customized dashboards to enhance threat detection capabilities.

Building an Dev Environment in AWS using terraform

- with a unique vision of learning and experimenting with AWS, created a small dev environment with an internet gate and a route table in a vpc and all the configurations are done utilizing Infrastructure as a code with terraform.

Vulnerability Assessment and Patching

- Created a website with vulnerabilities for SQL Injection and conducted comprehensive testing.
- Successfully identified vulnerabilities and implemented patches, enhancing website security.

Azure Firewall Configuration and Deployment

- Spearheaded configuration of Azure Standard Firewall, fortifying network security and ensuring optimal traffic flow.
- Meticulously orchestrated the application and network rules, along with NAT and Threat Intelligence implementation, proactively mitigated threats, culminating in a robust security infrastructure.

Server Hardening and vulnerability management

- Championed server hardening and vulnerability management, significantly reducing potential breach exposure by 85%. This strategic intervention fortified defenses and enhanced data protection.

Packet Analysis and Network Reconnaissance

- Uncovered a brute force attack that targeted a user's account. Post-breach analysis revealed the attacker's interest in various commands, including "ftp" possibly indicating data exfiltration intentions.
- This project shows my expert incident investigation skills, along my interest in incident investigation and Log analysis

K7 Computing

Chennai, India
2021

Security Analyst Intern

- Implemented advanced firewall configurations, mitigating cybersecurity threats effectively. This initiative resulted in a significant reduction in security risks, fortifying data protection.
- Utilized virtual environments and pfSense for comprehensive network testing, bolstering vulnerability assessment and optimizing network efficiency.
- Strategically reorganized a vital segment of the firewall infrastructure and simplifying operations

Certifications

Google Cybersecurity Professional Certificate	2023
AWS Solutions Architect (Est. Dec)	2023
CompTIA Security Plus (Est. Jan)	2023