Tejeswar Ponnathota

Oak Point, TX | 315.291.6026 | tejeswarponnathota@outlook.com

Website: tejeswar.ponnathota.com

Objective

Seeking to leverage expertise in cloud, cybersecurity, IAM and Insider Threat to build innovative and reliable security architecture helping organizations to mitigate risk and enhance threat detection goals that align with business objectives

Experience

Securonix Inc. | Sr.Manager, SIEM Engineering **Jun 2021 – Jan 2025**

- Built and led a high performing team of security architects responsible for end-to-end design and deployment of enterprise grade cloud based Securonix SIEM / UEBA solution on AWS
- Pioneered a standardized global deployment framework for cloud based Securonix SIEM / UEBA and implemented automation solutions, reduced product delivery time by 45% and significantly improved operational efficiency while optimizing implementation consistency
- Leveraged experience with AWS, Azure, GCP to architect and implement scalable data pipelines in the cloud using native cloud technologies to ensure minimal latency
- Automated cloud infrastructure scaling in GCP / AWS to improve resource utilization and reliability of the system to accommodate for heavy load and failover
- Spearheaded a collaborative effort with pre-sales teams to revamp and automate post-sales deployment handoff process significantly improving the onboarding experience for customers
- Developed and implemented comprehensive security programs on Microsoft cloud including IAM, data classification, data loss prevention and insider threat mitigation strategies
- Led a MITRE ATT&CK based gap analysis initiative to identify critical detection gaps resulting in a 20% increase in attack detection coverage across key log sources improving the security posture
- Orchestrated the design, implementation, and optimization of Securonix SOAR solution, boosting the efficiency of SOC teams by over 25% and significantly enhancing threat response capabilities
- Improved the speed and efficiency of incident response through creation of detailed SOAR playbooks to respond to critical events in a timely manner

Securonix Inc. | Solutions Architect – Cyber Security **Apr 2020 – Jun 2021**

- Successfully integrated Securonix SaaS Solution for a diverse customer base, enhancing their security logging and monitoring capabilities and strengthening the overall security posture
- Collaborated with SOC analysts to enhance cyber threat detection and response capabilities by developing and implementing tailored security use cases and threat models
- Played a key role in mitigating insider threats at various organization by partnering with Data loss and Fraud prevention teams to develop and deploy robust Insider threat programs tailored to organizations needs
- Enhanced detection accuracy through complex threat models using cross correlation of data from multiple log sources

Securonix Inc. | Principal Technical Lead – Cyber Security **Apr 2019 – Apr 2020**

Securonix Inc. | Senior Security Engineer **Feb 2018 – Apr 2019**

Securonix Inc. | Security Engineer **Mar 2016 – Feb 2018**

Syracuse University | Information Security Analyst **Nov 2014 – Dec 2015**

Education

Syracuse University, MS Computer Science **Jan 2014 – Dec 2015**

BITS Pilani, B.E(Hons) Computer Science and Engineering **Aug 2009 – Jun 201**

Skills & abilities

- Cloud Services – AWS, Azure, GCP
- Cloud Security
- SIEM
- Cybersecurity
- Vulnerability Management
- Insider Threat and UEBA
- Identity and Access Management
- SOAR
- Incident Management
- Threat Intelligence
- Endpoint Security
- Threat Modeling
- Python
- Bash scripting