Kanuri Ramakrishna

Security Analyst

• +91 7396978139 • kanuriramakrishna18@gmail.com • linkedin.com/in/Kanuri Ramakrishna • Hyderabad

Summary

Experienced Security Analyst with over 3 years of expertise in threat detection and incident response. Proficient in leveraging Microsoft Sentinel, Azure, and Splunk for optimizing security measures. implemented Azure CA policies, resulting in a 25% reduction in the organizations exposure to cyber threats. Capable in analyzing IOCs to mitigate risks. Collaborate across teams to enhance SOC processes and strengthen overall security posture.

Technical Skills

- **Security Tools:** Microsoft Sentinel, Microsoft Defender for Cloud Apps, Microsoft Defender for O365, Microsoft Defender for Endpoint, Cloud Security, Splunk, Qualys.
- **Cloud Platforms:** Azure
- **Identity Management:** Active Directory, Azure Active Directory, SSO
- **Development Tools:** Postman, PowerShell Scripting
- **Query Languages:** KQL, SPL

Work Experience

Accenture — February 2022 – Present
Security Analyst — Hyderabad

- Monitored and analyzed security systems, leveraging SIEM tools, to detect and respond to potential threats, resulting in decrease in mean time to detect (MTTD) security incidents.
- Documented and responded to security incidents, utilizing SIEM tools to ensure timely resolution and minimize the impact on business operations, achieving a 20% reduction in mean time to respond (MTTR).
- Implemented Azure CA policies and analyzed IOCs to detect and mitigate security risks, reducing the organization's exposure to cyber threats.
- Optimized SIEM queries and correlation rules, resulting in a 40% reduction in false positives and enabling the prioritization of critical alerts for investigation.
- Prepared detailed reports on security events, incidents, and responses, providing management with actionable insights to strengthen the organization's security posture.
- Researched and learned the latest threat intelligence to defend against emerging threats, enhancing the resilience of the organization's security infrastructure.
- Collaborated cross-functionally to enhance SOC processes, optimizing security measures and operations.
- Scheduled and monitored vulnerability assessment scans using Qualys.
- Hands-on experience with Incident Response activities, including malware, phishing, and endpoint analysis.
- Good understanding of firewalls, IDS/IPS and TCP/IP protocols.

Projects

Threat Intelligence Platform Development

- Engineered a SIEM platform amalgamating data from many sources such as dark web forums, security feeds, and internal logs, achieving a data aggregation efficiency.
- Empowered security teams to defend against cyber attacks by providing comprehensive, timely insights, leading to a 50% decrease in successful breach incidents.

Education

- Bachelor of Technology in Electrical Engineering — June 2016 – October 2020
  Pragati Engineering College, Kakinada

Certifications

- Completed Microsoft's AZ500 for Azure security.
- Achieved Microsoft's AZ104 for Azure administration.
- Earned Microsoft's SC200 for security operations.
- Attained EC-Council's CEH for ethical hacking.