
G KARTHIK

Pune, ♦ 7013716540 ♦ karthikgummuluri4@gmail.com

PROFESSIONAL SUMMARY

Driven SOC Analyst with a robust background in deploying and maintaining SOAR & SIEM solutions, including Azure Sentinel & Splunk, at a leading tech firm. Excelled in configuring advanced email fraud defense mechanisms and enhancing incident response capabilities.

SKILLS

- SIEM: Splunk, Microsoft Sentinel
- EDR: MS Defender Endpoint EDR
- DLP: Purview DLP – MIP
- Defender for Cloud: CSPM, Entra ID, Azure ID
- CASB Netskope MCAS
- Vulnerability Management: Qualys Cloud, Tenable Nessus
- Malware Analysis: Any run, Virus total, Hybrid Analysis for Static and Dynamic Analysis.
- Email Security: o365 email security, Proofpoint
- Incident Management: JIRA, ServiceNow

PROFESSIONAL EXPERIENCE

SOC Analyst | Persistent Systems

Aug 2023 to Current, Pune

- Designed and fine-tuned workbooks, playbooks, and analytic rules to streamline investigations and threat visibility.
- Investigated, analyzed, and responded to SOC alerts and security incidents within Azure Sentinel, conducting root cause analysis and mitigation.
- Identified security gaps and optimized Defender ATP policies, improving endpoint visibility and response effectiveness.
- Provided guidance on best practices for Defender XDR deployments, advising customers on policy tuning, use case management, and performance optimizations.
- Created and maintained security documentation on Defender ATP policies, configuration guides, playbooks, and incident response procedures.
- Performed investigations and audits using eDiscovery and Communication Compliance, ensuring policy adherence and legal hold requirements.
- Collaborated with cross-functional teams, including data engineers, compliance officers, and security analysts, to align data governance strategies with business objectives.
- Familiarity with Splunk security management technologies (SIEM).
- Good familiarity with techniques like threat hunting and malware analysis.
- Created and maintained workbooks and playbooks to improve SOC visibility, investigation workflows, and incident response efficiency.

- Investigated and responded to security incidents, leveraging Azure Sentinel's automation, playbooks, and KQL-based analytics for in-depth analysis and mitigation.
- Familiarity with vulnerability scanning tools like Nessus.
- Nessus is used to generate reports for vulnerability assessments.
- Determine which systems, networks, and business applications are vulnerable, and rank them accordingly.
- Configured and managed device enrollment and compliance policies, ensuring secure access to corporate applications and data.
- Troubleshoot Intune security policy conflicts affecting Defender ATP configurations, ensuring uninterrupted policy enforcement.
- Familiarity with tracking and ticketing systems like ServiceNow.
- Strong grasp of security operations, protocols, and processes, particularly as they relate to threat intelligence and incident response.
- Compliance, ensuring compliance with legal and regulatory requirements.
- Worked closely with compliance and security teams to establish data governance frameworks, retention policies, and access controls.
- Provided advisory on Microsoft Purview best practices, helping organizations align data security strategies with business and regulatory requirements.
- language and the use of Splunk DB Connect health dashboards to monitor the health Familiarity with the Splunk query of database connections.
- Strong background in log management, central logging, and Splunk SIEM design.

EDUCATION

Bachelor of Science: 07/2023

Adikavi Nanaya University