VENKATA MURALI KRISHNA REDDY

SOC ANALYST

✉ venkatamuralikrishnareddy111@gmail.com BANGALORE ✆ +91-9908973214

Profile Summary:

Having 3 years of experience in security practices, I have effectively managed the organization's Security Operations Center (SOC) and Cyber Security Incident Response Team. I monitor security events across the network, implementing proactive measures to prevent breaches and ensure compliance with industry standards. My role involves analyzing phishing and spam emails, as well as alerts related to risky sign-ins and impossible time travel incidents reported by users. Additionally, I actively track global outbreak alerts, taking necessary actions to protect the organization from emerging threats. I oversee 24/7 monitoring of security tools and SIEM systems, conducting malware analysis on suspicious files and collaborating with antivirus vendors to ensure timely updates of threat signatures. My comprehensive knowledge of security practices enables me to maintain a secure operational environment while enhancing the organization's overall cybersecurity posture.

Summary of Skills:

- 3.6 years of experience in SOC monitoring and incident response, demonstrating expertise in real-time security monitoring and incident management within a 24/7 Security Operations Center environment.
- Having experience on SIEM, SOAR, EDR, Sandbox…etc.
- Experience on performing log analysis and analyzing the crucial alerts at immediate basis through SIEM.
- Utilized Microsoft Azure Sentinel for security event monitoring, incident detection, and response coordination.
- Monitoring the alerts triggered from Sentinel and by analyzing logs and by taking necessary action with respect to alerts and remediate the alert by meeting the Service Level Agreement (SLA).
- Efficiently created and managed tickets using industry-standard ticketing tools to track incident resolution progress.
- Fine tuning the Use case based on the false positive detection.
- Good understanding on key customer infrastructure components Proxy, Firewall, Antivirus.
- Conducted thorough investigations into phishing and spam incidents, utilizing analysis tools to identify and mitigate threats.
- Developed comprehensive SOPs and runbooks for various security alerts, enhancing team response efficiency and consistency.
- Actively participated in incident response activities, coordinating with cross-functional teams to effectively manage security breaches.
- Prepared detailed daily, weekly, and monthly reports tailored to client requirements, highlighting key security metrics and incidents.
- Having Knowledge of the Cyber Kill Chain, the MITRE attack framework, various TTPs described within and commonly used by attackers as well as how to write detection rules for them in SIEM and EDR solution.

Work Experience:

Security Operation Center [Security Analyst] **Mphasis [2021 AUG – Till Date]**

- Monitoring 24x7 for Security Alerts and targeted phishing sites by using SIEM tool with the help of technologies such as Abuse mailbox and similar sounding domains.
- Analyze security alerts triggered by Microsoft Sentinel, distinguishing true positives from false positives.
- After analyzing alert raising incident in ticketing tool for true positive incidents and follow up the team up to incident closure.
- Manage the lifecycle of security incidents using ServiceNow (SNOW) from incident creation to resolution.
- Oversee all stages of incident management, ensuring accurate recording, prioritization, and adherence to Service Level Agreements (SLAs).

- Identifying False-Positive offences and perform fine tuning over them with the help of TEAM
- Adjust detection rules in Microsoft Sentinel to minimize unnecessary alerts and improve response efficiency
- Working on incidents and reviewing the alerts and do detailed analysis on alerts.
- Collaborate with L1 and L2 support teams, providing guidance on incident response and resolution strategies.
- Develop detailed Standard Operating Procedures (SOPs) for various security use cases to enhance incident handling.
- Ensure well-documented procedures to maintain consistency in incident management and reduce downtime.
- Analyze current security setups, identifying vulnerabilities and providing actionable recommendations for improvement.
- Create targeted use case queries within Azure Sentinel to identify specific threats based on environmental requirements.
- Facilitate regular training sessions for team members on incident response protocols and emerging threats.
- Maintain up-to-date documentation of incident response processes to ensure team readiness during incidents.
- Participate in post-incident reviews to analyze responses and improve future incident handling procedures
- Analyzed and reported security threats or incidents within established SLAs, ensuring timely communication.
- Handling the different issues like Phishing, Spam, Scam and Malicious email.
- Analyzed phishing emails reported by internal users to mitigate potential threats.
- Conducted thorough analysis of phishing and spam emails to enhance organizational defenses.
- Resolved security incidents raised by team and clients in accordance with defined SLAs, providing justified evidence for actions taken.
- Analyzed and reported security threats or incidents within established SLAs, ensuring timely communication.
- Preparing RCA documents and daily/weekly/monthly Reports
- Submitted Root Cause Analysis (RCA) reports to customers for critical incidents, detailing findings and remediation steps.
- Responsible to investigate the health checkup.
- Report alerts and investigate issue identified during monitoring the live traffic.
- Coordinates with all the teams to Mitigate/Remediate the issue
- Providing 24/7 support and coordinating with required team to resolve the issues.

SKILLS:

Tools	
Microsoft Azure Sentinel	SIEM, Incident Response, Cloud Security
ServiceNow	ITSM, Incident Management, Ticketing
Varonis	Data Security, Insider Threat Detection
Barracuda Email Protection	Email Security, Spam Filtering, Phishing Protection
JIRA	Project Management, Issue Tracking
Splunk SOAR	Security Orchestration, Automation, Incident Response
Abnormal Security	Fraud Detection, Behavioral Analysis, Threat Intelligence

Education:

- Completed degree in GITAM INSTITUTE OF TECHNOLOGY & MANANGEMENT – 2021