Macharla Akhil Kumar

Security Analyst

+91-9849640522

Macharlaakhil9817@gmail.com

*To obtain a challenging and rewarding position as **SOC Analyst** with organization this recognizes my true potential and provides me sufficient avenues for professional growth through nurturing my technical skills and competencies with **2+ years** of experience as **Information Security Analyst**.*

PROFESSIONAL SUMMARY

- Having **2+ years** of IT experience working in a large-scale **SOC (Security Operations Center)**
- 2 years of experience as a SOC Analyst (L1).
- Hands-on experience in log and monitoring management systems, security event monitoring using **SIEM Elastic (ELK), Splunk** and **working knowledge of Azure Sentinel**.
- Exposure to Ticketing tools like service now, Uniview ticketing tool.
- Experience in generating Daily, Weekly & Monthly Reports.
- Participating in weekly review meetings.
- Experience to support in-depth investigations, Incident response and 'hunting' activities.
- Proficient in fine-tuning security systems and alerts to optimize accuracy and reduce false Positives.
- Skilled in developing and implementing playbooks to standardize incident response procedures and enhance efficiency.
- Experience on performing **Incident response, Malware analysis**.
- Provide daily summary reports of events and activity relevant to cyber defense practices.
- Strong technical skills and the ability to work independently as well as in a team environment.

Have strong written and verbal communications skills, and the ability to create complex technical reports on analytic findings.

WORK EXPERIENCE

Company: CyberNX Technologies Pvt Ltd, Mumbai
Role: SoC Analyst ***Dec 2022 - Till Now***

Roles and Responsibilities:

- Monitoring and analyzing the logs and alerts from Sophos XDR, Azure, AWS, Cloudflare WAF, CrushFTP, Google Workspace, and GCP(Google Could Platform) using **Elastic** to identify and triage security incidents affecting customers.
- Evaluate the severity of security alerts and unusual network traffic, and collaborate with customers and internal teams to implement appropriate measures to address the identified risks.
- Adding **Indicators of Compromise (IOCs)** to the **MISP** server, including threat signatures, IP addresses, domains, and hashes, to enhance threat intelligence.
- Sending emails for false positive alerts, ensuring prompt communication with stakeholders and providing clarification on non-malicious incidents.
- Provide suggestions for **fine-tuning** security systems and alerts based on the analysis of false positive incidents, contributing to improved accuracy and efficiency

- Assess security alerts and incidents, identifying situations where **exceptions** or **whitelisting** may be necessary due to legitimate or known safe activities.
- Add exceptions to the alerting rules in Elastic, ensuring that false positive alerts are reduced and legitimate activities are not flagged unnecessarily.
- Create alerts or tickets using **Uniview ticketing tool** and Elastic SIEM, following defined processes to ensure timely response and resolution of security incidents.
- Develop and document **playbooks** for different types of security alerts, outlining step-by-step procedures and recommended actions to streamline incident response and ensure consistency.
- Prepare and deliver daily/weekly reports summarizing key security findings, incidents, and trends to management and stakeholders
- Conduct **phishing email analysis**, examining email headers, content, and attachments to identify and report potential phishing attacks.
- Collaborate with incident response teams to take appropriate actions against identified phishing threats, such as phishing email takedown or user awareness campaigns.
  Successfully worked in a 24x7 shift-based system, adhering to rotation schedules to provide continuous security monitoring and incident response using Elastic for all incoming security alerts.
- Effectively tracked and updated incident requests based on client updates and analysis results using Uniview ticketing tool and Elastic, ensuring accurate documentation and timely resolution.

Technical Skills / Key Skills:

- **SOC** (**Security Operation Centre**)
- **SIEM** (**Security Information and Event Management**) Tool: **Elastic**, **Splunk, Azure Sentinel.**
- Application Security - **Email security O365**.
- **Phishing Email Analysis, ProofPoint**
- **Endpoint protection - Sophos XDR, CrowdStrike EDR**
- **Vulnerability Assessment (Qualys Guard)**
- **Ticketing Tool used - Service Now, Uniview**
- **Phishing Email Analysis, Spam Mails, Check point, Playbook Development**
- **Perform Cyber** and **Technical Threat Analysis**

EDUCATION

- Acharya Nagarjuna University 2022
  B.com(Computers), Bachelor's Degree

DECLARATION

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear that responsibility for the correctness of the above-mentioned.

Macharla Akhil Kumar