Busireddy Pavankumarreddy
Email Id: - **pavanvikram5@gmail.com**
Contact no: - +**91-9440181668**

Professional Summary:

- Having 5.8 years of experience in I.T Industry and 4.5 years of experience in cybersecurity currentlyworking as Security Analyst (Security Operation Center team).
- Hands on experience on Threat analysis and Security Monitoring and Operations.
- Specialized in proactive network monitoring of SIEM (sentinel).
- Have a deep knowledge in identifying & analyzing suspicious event.
- Working on the detailed analysis of the malware and to identify the point of infection using the logsfrom the tools such as Firewall logs.
- Experience in SOC monitoring and investigation through SIEM tools like Sentinel and Splunk.

Technical Skills:

- **SIEM Tools : Azure Sentinel & Splunk.**
- **Email Security : Proof Point & O365**
- **EDR : MDE**
- **Cloud Services : AWS, AZURE.**

Work Experience:

Currently working as **security Analyst** with TCS from **JUN 2024** to **till Date.**

Project-4

NAME: TCS **DURATION: JUN-2024 to till now**
ROLE : Security Engineer

- **Proficiently triaged and responded to cyber security incidents triggered by use cases derived from Windows event logs and application logs.**
- **Utilized Splunk for advanced log analysis, incident search, and effective triaging, ensuring timely identification of potential security threats.**
- **Monitored and managed cyber security and compliance dashboards in Splunk to maintain real-time awareness of cyber security events and potential risks.**
- **Employed AWS services to triage DDoS alerts, block malicious domains and IPs using WAF (Web Application Firewall), and maintain a secure cloud environment.**
- **Expertise in using CrowdStrike to detect and investigate malicious activities on client endpoints, taking appropriate actions to remediate alerts.**
- **Provided training and mentorship to junior SOC analysts on the use cases and best practices related to incident triaging and security monitoring.**
- **Collaborated with cross-functional teams to enhance security measures.**
- **Successfully optimized incident response processes through runbook, and strengthened overall security posture**

Project-3

NAME: Becton Dickinson **DURATION: AUG-2021 to JUN-2024**

ROLE : Security Analyst

Responsibilities:

- Responsible for handling tickets and dispatching within Security operations.
- Responsible for performing regular health checks as per the standard procedure.
- Responsible for creating incidents for Security Operation and providing 24x7 eventmonitoring and analysis support for pro-active trend analysis of events.
- Providing timely reports to the stakeholders.
- Analyzing Phishing and Spam related activities and notifying the users.
- Preparing daily and weekly dashboard on the security threats and trends on the network. Working on Real Lime network traffic by analyzing the logs from IDS and Firewalls.
- IT experience in monitoring log sources, correlating, analyzing security events and integrating the security devices with SIEM tools like Azure Sentinel.
- Integrating Microsoft Native data source, security network devices, Endpoints, Applications and third-party devices with Azure Sentinel and validate for event of interest.
- Implementing KQL use cases based on device types and attack vector to identify security events based on risk level and impact, Mapping with MITRE Attack Framework.
- Fine-tuning the KQL use cases based on the false positive detection to detect specific security threats or anomalies.
- Working on Email security tools like Proof Point.
- Worked with core teams to investigate the false and true positive alerts.
- Experience in collaborating with cross-functional teams, including security operations, incident response, and IT operations, to ensure timely and effective incident response.
- Proficiency in documenting incident response procedures, playbooks, and workflows to ensure consistency and repeatability of incident response processes.
- Responsible for following all the steps in Incident Response Process.
- Will document the tickets fully with all the action taken for the incident and update it on frequent basis and maintain ticket quality by documenting it with all the required comments.
- Responsible for monitoring infrastructure health, security and capacity, and make decisions on the security incidents that occurs in the environment.
- Determine the scope of security incident and its potential impact to Client network recommend steps to handle the security incident with all information and supporting evidence of security events.

Project-2

NAME: MYER **DURATION: MAR-2020 to AUG-2021**

ROLE: Splunk Consultant

Responsibilities:

- Coordinating all application teams to migrate the Splunk Forwarders to new Splunk environment.
- Parsing, Indexing, searching concepts Hot, Warm, Cold, Frozen bucketing and Splunk clustering.

- Setup and configuration of search head cluster with search head nodes and managing the search head cluster with deployer.
- Responsible with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management.
- Experience in Splunk GUI development creating Splunk apps, searches, Data models, dashboards, and Reports using the Splunk query language.
- Involved in Installation, Administration and Configuration of Splunk Enterprise and integration with local legacy systems.
- Created and configured management reports and dashboards in Splunk for application log monitoring.
- Extensive experience in setting up the Splunk to monitor the customer volume and track the customer activity.
- Worked on Splunk upgradations, troubleshooting Splunk Enterprise.
- Expertise in customizing Splunk for Monitoring, Application Management, and Security as per customer requirements and industry best practice.

Project-1

NAME: VERIZON **DURATION: FEB-2019 to MAR-2020**

ROLE: Linux System admin

Responsibilities:

- **Experience in configuring Yum server.**
- **Handling of tickets based on the priorities.**
- **Response to incident tickets and resolves them with SLA.**
- **Implement the changes based on requests.**
- **Managing file system and resolve the file system problems.**
- **Install and upgrade the packages with YUM & RPM.**
- **Monitoring system Performance of Virtual memory, Disk utilization and CPU utilization.**
- **Performance tuning, restart and kill the process.**
- **File System Creation, deletion and modifications.**
- **Providing 24*7 Support to the customer environment**

Certification:

- KQL (Microsoft E - Learning)
- SC-200
- NSE1(Fortinet)
- NSE2(Fortinet)

Educational Qualification:

- Graduation in B-tech from JNTU- University

Place:
Date: Pavan Kumar Reddy