Pandipally Madhu

**Security Analyst-L1**

# Email: [madhusoc6@gmail.com](mailto:madhusoc6@gmail.com) Contact: +91 8985905028

**Career Objectives:**

Information Security professional seeking a career position within an organization, where my professional experience, education and abilities would be an advantage for the growth of employer and myself.

# Professional Summary:

* Over all 4.4 years of experience in Information Security and currently working as Security Analyst (Security Operation Centre team)
* Hands on experience on Threat analysis, Remediation of malware and **Security Monitoring and Operation.**
* Experience on **SIEM (Security Information and Event Management) tools** like Monitoring real- time events using **HP ArcSight, IBM Q Radar, Splunk** tools.
* Preparing daily, weekly and monthly report as per client requirement.
* Investigating and creating case for the security threats and forwarding it to Onsite SOC team for further investigation and action.
* Experience on performing log analysis and analyzing the crucial alerts at immediate basis.
* Filling the Daily health checklist.
* Installation of Application Software and Antivirus software.
* Installing the Operating Software such as Windows.
* Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.
* Good understanding of security solutions like Firewalls (Palo alto, checkpoint, Fortinet, Cyber am), DLP, Anti- virus, IPS, Email Security etc.
* Hands on experience with Qradar SIEM tool for logs monitoring and analysis.

# Work History:

**SECURITY ANALYST– Cognizant (May 2018 – April** **2021) – Hyderabad**

**SECURITY ANALYST- Wells Fargo (May 2021 – Till Date) Hyderabad.**

# Project Roles and Responsibilities:

* Served as Security Analyst in SOC operations for real-time monitoring, analyzing logs from various security/Industrial appliances by using HP ArcSight ESM console, ArcSight Logger and troubleshooting of logging issues.
* Administrating various incidents/security alerts triggered in SIEM tool.
* Carrying out log monitoring and incident analysis for various devices such as Firewalls, IDS, IPS, database, web servers and so forth.
* Monitoring 24x7 for Security Alerts and targeted phishing sites by using SIEM tool with the help of technologies such as Watermark, Referrer, Abuse mailbox and similar sounding domains.
* Website Anti-Malware and Defacement monitoring and real-time alerting based on anomalies detected.
* Created filters, active channels, queries, Rules, Dashboard in ArcSight for monitoring purpose.
* Configured reports in ArcSight ESM and ArcSight Logger as per the requirement.
* Maintenance of HP’s ArcSight Products (ESM and Logger) like its Health check which also includes ArcSight content developments i.e. rules, reports, dashboards.
* Knowledge of Installation, Configuration and up gradation of various connectors, and its troubleshooting.
* Work closely with business units to ensure that they know what and how to feed data into

HP Arcsight and to create network hierarchy, classify Log Sources within the HP Arcsight SIEM.

* Monitoring the customer network using IBM SIEM tool– HP ArcSight
* Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
* Maintain keen understanding of evolving internet threats to ensure the security of client networks.
* Escalating the security incidents based on the client&#39; s SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
* Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.
* Co-ordinate extensively with networking teams to maintain and establish communication to Remote HP Arcsight Collectors/Processors.
* Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
* 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.

* Creation of reports and dashboards and rules fine tuning.
* Mostly worked on Broken authentication, Sensitive data exposure, Broken access control, XSS, Using components with known vulnerabilities, Insufficient logging and monitoring.
* Creation of reports and dashboards and rules.
* Maintain & Document the application support strategy.

# Technical Skills:

* + **SOC** (Security Operation Center)
  + SIEM (Security Information and Event Management) Tool: HP ArcSight, IBM Qradar, Vulnerability Assessment Phishing Email Analysis, NMAP.
  + Create, Modify and Update Security Information Event Management (SIEM) Tools.
  + Perform Cyber and Technical Threat Analyses.
  + Experienced and proficient in Security Framework of OWASP, with expertise in OWASP Top 10.

# Education:

* + B.Tech from Nalla Narasimha Reddy Engineering college, JNTUH - 2017.

# Personal Details:

Father Name : Pandipally Madhu Date of Birth : 24/11/1994

Languages : English, Telugu , Hindi

Address : D no: 14-64,Adarsha nagar, Bachannapet (V/M), Warangal dist. Telangana

# Declaration:

I Madhu declare that the above-mentioned information is correct to the best of my knowledge and belief.

Date: Madhu

Place: