HARISH DONDAPATI

**Mobile:** +91 8217689583 **Email** : **[harishdondapati07@gmail.com](mailto:vijaychandratk@gmail.com)**

**Objective:**

To be an integral part of a professional Information Security team for applying my knowledge and Professional skills to add value to the organization’s business and also achieve the corporate objectives whilst getting valued exposure and professional satisfaction along with personal growth.

# Profile Summary:

* Having 2 Years of Experience in security Analyst.
* Having sound knowledge on SIEM Tools and reporting any security breaches, attacks, malicious activities, unauthorized accesses to the concerned team.
* Acknowledges and responds on various security threats and notifications.

# Educational Qualifications:

* B.COM from S.V University Tirupati in 2018.

# Professional Experience:

* + Company **EASY BI Solutions**(2019 – Till Date)
  + Designation Software Engineer ( Security Analyst)
  + Work Unit Cyber security Unit

# Technical Skills:

* Having sound knowledge on Security Tools and reporting any security breaches, attacks, malicious activities, unauthorized accesses to the concerned team
* Recognizes successful intrusions and compromises through review and analysis of relevant event detail information.
* Proactively manages IT security on behalf of customer to reduce the impact of security incidents and system compromises.
* Good understanding of OSI Model, TCP/IP, IP address and classes of IP address.

# Project Details:

**Project Name :** SOC Operations.

**Role :** Security Analyst.

**Duration :** 2019 to till Present.

# Description:

Security incident and event management (SIEM) is the process of identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment. It provides a comprehensive and centralized view of the security scenario of an IT infrastructure.

# Roles & Responsibilities:

* Real Time Log analysis from different network security devices such as Firewalls, IDS/ IPS, Operating Systems like Windows, Proxy Servers, Windows Servers, System Application, Databases, Web Servers and responding to intrusion
* Escalates and hands off to team members and leadership based on defined threat and priority determination.
* Creating an incident ticket with device owners and Tracking Security incidents to closer by coordinating with different teams.
* Create and run search queries in SIEM tool to help with identifying and troubleshooting security issues
* Conducts technical analysis on impacted systems to determine impact, scope, and recovery from active and potential cyber incidents.
* Documents results of cyber threat analysis and subsequent remediation and recovery in an effective and consistent manner.
* Ensure software is patched and able to protect from threats.
* Develop use cases for some security devices with correlation rule.
* Provide threat analysis and security logs for security device.
* Utilize Threat intelligence tools.
* Ability to interact effectively with different infrastructure teams like network, systems, compliance, database, Firewall etc.
* Preparing daily/Weekly/Monthly reports and security advisory covering both management and compliance specific devices.

HARISH . D