# Sandeep Reddy Pulyala Email Id: [sandypulyala@gmail.com](mailto:sandypulyala@gmail.com) Contact: +91- 9059034354

To associate with an innovative and vibrant organization, allowing me to put my competencies to the best use, to add value to the organization and contribute to my overall growth as an individual

# SKILLS & COMPETENCIES

* **SIEM tools** – IBM QRadar, Splunk
* **EDR tools** – CrowdStrike and MS Defender
* **Security** – Good knowledge on Network and security devices like IPS, IDS, Firewalls, Switches, Routers.
* **Email Security** – Proofpoint TAP& TRAP
* **Ticketing tools** – Service now, Wolken
* **SOAR -** Cortex XSOAR
* **Operating Systems** – Windows, Linux

# WORK EXPERIENCE

**Organization : Infosys Limited (**March 2024 – Till date)

**Role : Senior Associate Consultant**

# Responsibilities :

• Total **5 years** of experience as an Information Security Analyst (Security Operation Centre team).

• Proactively monitored security alerts using IBM QRadar, investigating and analyzing security events

from multiple devices, including servers, firewalls, Office 365, endpoints and workstations, ensuring

early detection and mitigation of security threats.

• Worked extensively on IBM QRadar for rule creation, customizing rules to correlate and prioritize

alerts, minimizing false positives and optimizing incident response efficiency.

• Experience in Threat Analysis and Threat Hunting.

• Raised, tracked, and managed incidents related to security alerts received from multiple security

devices, ensuring proper escalation to higher-level teams when critical threats were identified.

• Experience in generating Daily, Weekly & Monthly Reports.

• Experience of working in 24x7 operations of SOC team, offering log monitoring, security information management, global threat monitoring.

• Automated incident triage workflows using Cortex XSOAR, reducing incident resolution time by 40%

through security orchestration and response playbooks, improving SOC operational efficiency.

• Strong knowledge on Incident Management, Event Life Cycle and its Phases.

• Utilized CrowdStrike and Microsoft Defender to identify and analyze security risks on endpoints,

performing risk assessments based on alert severity and ensuring comprehensive endpoint detection

and response (EDR).

• Experience in handling multiple clients as a part of MSSP.

• Delivered training sessions for internal employees on security best practices, increasing overall

awareness and response to potential threats and improving incident handling capabilities across the

organization.

**Organization : Syberzen Infosec Private Limited (**December 2020 – September 2023)

**Role :**  **Security Analyst**

# Responsibilities :

• Proficiency in using various security tools and technologies, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, proxy, SIEM (Security Information and Event Management), and threat intelligence platforms

• Analyse the nature and source of security threats, understanding their tactics, techniques, and procedures (TTPs)

• Handling alerts from Crowd strike EDR and investigation.

• Investigate phishing emails, domains and IP's using open-source tools and recommend proper blocking based on analysis.

• Good understanding of OWASP Top 10, IDS, IPS, Cyber Attacks like DOS, DDOS, MITM, SQL XSS and CSRF.

• Skill in responding to security incidents, including identifying, containing, and mitigating the impact of security breaches.

• Knowledge of security architecture best practices and the ability to design and implement security measures to protect critical assets.

• Keeping up to date with the latest threats and trends in the cybersecurity landscape and utilizing threat intelligence to proactively defend against emerging threats.

• Configure and fine-tune security technologies to enhance detection and prevention capabilities.

• Maintain detailed records of security incidents, investigations, and response activities.

• Prepare incident reports and recommendations for improving security practices.

**Organization : BluSapphire Cyber Systems** (December 2019 – December 2020)

**Role : Security Analyst**

# Responsibilities :

• Email forwarding for alerts, timely acknowledge and forwarding email alerts.

• Experience of working in 24x7 operations of SOC team, offering log monitoring, security information

management, global threat monitoring.

• Monitor and acknowledge alerts in the console as per the internal OLAs (Low and Medium)

• ensure that all incidents were investigated and resolved in a timely manner.

• Tickts status to be updated on daily basis.

• Experience on performing log analysis and analyzing the crucial alerts at immediate basis through SIEM.

• Strong in team coordination and managing tasks.

• Preapration of Shift Handover reports at the end of the shift to provide situational awareness to the incoming shift.

**CERTIFICATION/LICENSES**

• CEH Trained

• SECEON Certified

• Infosys Certified Security Operation Center Associate

# EDUCATIONAL QUALIFICATION

* 2011-2015- B. TECH (ECE) –Vivekananda Institute of Technology & Science – 70%
* 2009-2011- 12th Standard – SVV Junior college – 74%
* 2008-2009 - 10th Standard – VBGP HIGH SCHOOL – 75%

# PERSONAL DETAILS

**Name** : Sandeep Reddy Pulyala

**Gender** : Male

**Marital Status** : Married

**Nationality** : Indian

**Languages Known :** English, Hindi &Telugu.

# DECLARATION

I hereby declare that all the information provided here is too true to my knowledge and belief.

**Place: Hyderabad.**

**Signature: Sandeep Reddy Pulyala**