SURYA VARMA MANDAPATI

Security Operation Centre Analyst
suryavarmamandapati@gmail.com
91+ 8897597757

PROFESSIONAL SUMMARY

Dedicated **Cybersecurity Analyst** with expertise in **threat detection**, **incident response**, and **vulnerability management**. Proficient in **SIEM tools** like **Azure Sentinel** and **Splunk** along with **EDR** solutions such as **Sentinel One** and **CrowdStrike**. Skilled in **firewall** management **Palo Alto**, **Fortinet** and **email security Abnormal, Proofpoint** and **O365** to safeguard against threats. Experienced in **DLP** technologies like **Forcepoint** and log analysis for data protection. Strong communicator with a commitment to continuous learning and cybersecurity best practices.

EMPLOYMENT HISTORY

Senior Executive SOC- L1, Apollo Hospitals, Chennai

02/2025 – Present

- Monitored and analyzed security events using **SIEM tools Azure Sentinel**, investigating threats and incidents in real-time.
- Managed **CrowdStrike & Defender EDR**, detecting and responding to endpoint threats to safeguard organizational assets.
- Configured and maintained **Fortinet firewalls**, enforcing security policies and protecting network perimeters.
- Implemented and monitored **Forcepoint DLP solutions** to prevent data breaches and ensure compliance with security policies.
- Conducted **incident investigations and threat hunting**, correlating logs from SIEM, EDR, and firewall sources.
- Managed and monitored **O365 Email Gateway**, analyzing email threats, phishing attempts, and spam to enhance email security.
- Optimized security alerts and detection rules to reduce false positives and enhance threat visibility.

Cyber Security Analyst, Jubilee Information Technology Pvt Ltd, Hyderabad

12/2022 – 12/2024

- Monitored and triaged security alerts using **Azure Sentinel** and **Splunk**, ensuring timely threat response.
- Conducted **incident analysis**, log reviews, and collaborated with **L3 analysts** for escalation.
- Utilized **Jira** for incident tracking and compliance documentation.
- Managed and troubleshot **endpoint protection** tools like **CrowdStrike** and **Sophos** for device security.
- Performed **phishing analysis** with **Abnormal**, **Proofpoint** and contributed to **user awareness campaigns**.
- Assisted in **DLP deployment** Symantec and conducted **vulnerability scans** using **Qualys**.
- Monitored **EDR alerts CrowdStrike, Sentinel One** supported **firewall/IDS integration**, and participated in **on- call rotations**.
- Contributed to the creation of **runbooks** and **incident response SOPs**, enhancing team efficiency and security operations.
- Participated in **security training sessions**, educating **L1 team members** on **incident response protocols** and **best practices**.

CERTIFICATION

- Cisco Certified Network Associate (CCNA 200-301) – NETWORKERS HOME, Bangalore
- Cisco Certified Network Professional Enterprise (CCNP Enterprise) - NETWORKERS HOME, Bangalore
- Certified Palo alto Training – NETWORKERS HOME, Bengaluru
- **Microsoft Certified**: Security Operations Analyst Associate (**SC200**)
  Credential ID: E7E391906CE61F89

EDUCATION

Bachelor’s in computer science, Andhra University

TOOLS

- Security Information and Event Management (SIEM): **Azure Sentinel & Splunk**
- Endpoint Detection and Response (EDR): **Defender, Crowdstrike**
- Firewalls**: Palo Alto, Fortinet**
- Email Security**: Abnormal, Proofpoint, O365**
- Vulnerability Management**: Qualys**
- Anti-Virus Solutions**: TrendMicro, McAfee**
- Data Loss Prevention (DLP): **Symantec, Forcepoint**
- Ticketing Tools**: ServiceNow, Jira**
- Network Security Tools**: IDS, IPS**
- Phishing and Email Analysis**: Proofpoint, O365**
- Cloud: **Azure**
- Security Frameworks**: MITRE ATT&CK**

TECHNICAL SKILLS

- Proficient in using SIEM tools like Azure Sentinel and IBM QRadar for monitoring, analyzing, and responding to security events.
- Skilled in managing firewalls such as Palo Alto and Cato Networks to control and secure network traffic.
- Hands-on experience with EDR solutions including CrowdStrike Falcon, Microsoft Defender for Endpoint, and Sentinel One for detecting and responding to endpoint threats.
- Experienced in email security using Proofpoint and Abnormal to protect against phishing, malware, and spam.
- Familiar with email gateways like Proofpoint and Microsoft 365 for secure email delivery and filtering.
- Knowledgeable in cloud security and operations on Microsoft Azure.
- Experienced in using ticketing tools like ServiceNow and Jira for incident tracking and workflow management.
- Skilled in using KQL (Kusto Query Language) for querying and analyzing data in Azure Sentinel and Log Analytics.
- Basic experience with Security Orchestration, Automation, and Response (SOAR), including hands-on exposure to CrowdStrike SOAR.
- Practical experience with IDS/IPS systems for detecting and preventing network intrusions.
- Proficient in implementing DLP (Data Loss Prevention) strategies to protect sensitive data from unauthorized access or leaks.
- Familiar with basic networking concepts (TCP/IP, DNS, VPN, ports, protocols).
- Understanding of cybersecurity frameworks like NIST, MITRE ATT&CK, and ISO 27001.
- Knowledge of incident response processes, including detection, analysis, containment, and recovery

DECLARATION

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

Surya Varma. M