
Sandhya Surada

2-130/A, near Krishna temple, mulapeta, u kothapalli mandal, kakinada district, Andhra Pradesh, India. 533448
9014821964 | sandhyasurada21@gmail.com
in <https://www.linkedin.com/in/sandhya-surada>

PERSONAL DETAILS

- Date of Birth : 21/06/2002
- Marital Status : Single
- Nationality : Indian
- Passport : Yes
- Gender : Female
- Place : Mumbai

OBJECTIVE

A detail-oriented and proactive SOC Analyst with expertise in monitoring, detecting, and responding to security incidents. Experienced in utilizing industry-leading tools such as SIEM, XDR, EDR, and firewalls to protect organizational assets. Seeking to leverage strong analytical skills, threat intelligence, and incident response experience to enhance the security operations of a forward-thinking organization. Eager to contribute to reducing vulnerabilities, improving threat detection, and ensuring timely responses to emerging security threats

LANGUAGES

- English
- Telugu
- Hindi

EDUCATION

- | | |
|------|--|
| 2023 | <ul style="list-style-type: none">• Adikavi nanaya university
Bachelor of degree (BSC-Computer science)
9.0 |
| 2020 | <ul style="list-style-type: none">• Sri Sai Aditya jr. College
Intermediate (MPC)
9.0 |
| 2018 | <ul style="list-style-type: none">• State board of Andhra Pradesh
Ssc
9.5 |

SKILLS

- Threat Intelligence (TI): Experience in aggregating and analyzing threat intelligence using platforms like Cyware
- Extended Detection & Response (XDR) & Endpoint Detection & Response (EDR): Skilled in leveraging XDR/EDR solutions to enhance endpoint visibility and threat response.
- Firewalls & Security Appliances: Palo Alto Networks Firewall Checkpoint Firewall TippingPoint IPS/IDS F5 WAF Imperva WAF
- Security Monitoring & Incident Response: Experience with SIEM monitoring and incident detection.
- Proficient in sandbox analysis to detect and analyze malicious threats.
- Monitored and analyzed WAF traffic to identify and mitigate potential security threats targeting web application. Utilized F5 WAF logs and analytics to identify trends, vulnerabilities, and attack patterns, providing actionable insights for improving security posture. Reviewed WAF logs to detect attack patterns, vulnerabilities, and suspicious activity, ensuring timely threat response
- SIEM & SOAR Tools: Azure Sentinel, Devo SIEM, Grey Matter SOAR
- Endpoint Detection & Response (EDR): Panda EDR Microsoft Security Solutions:

EXPERIENCE

Sep 2023 - Till
date

- **Soc analyst**

Ltimindtree

I worked as a soc analyst role L1 in Ltimindtree organisation.

SOC Analyst L1

Monitored and analyzed security events and alerts from various sources, including SIEM tools, network devices, and endpoint security systems.

Performed initial triage and investigation of security incidents to determine their severity and impact on the organization.

Managed and responded to security alerts by escalating potential threats to higher-tier SOC teams as necessary.

Supported incident response procedures and maintained detailed documentation of events, including timelines and actions taken.

Assisted in the development and execution of security policies, procedures, and guidelines to improve the organization's security posture.

Worked collaboratively with other IT and security teams to ensure rapid identification and mitigation of threats.

Provided regular reporting on security trends, incident response efforts, and system health.

Skills & Tools:

Security Information and Event Management (SIEM) tools (Securonix, IBM QRadar)

Security orchestration, automation, and response (SOAR) tools (Cortex)

Used Palo Alto Cortex XSOAR as a SOAR platform to automate security workflows.

Managed incident mirroring between ServiceNow and XSOAR, ensuring real-time synchronization of data for efficient incident response.

Integrated and streamlined incident management processes between XSOAR and ServiceNow to enhance operational efficiency.

Incident management and ticketing systems (e.g., Jira, ServiceNow, Data Service Center)

Network protocols and traffic analysis

Basic knowledge of cybersecurity principles (e.g., threat actors, attack vectors, vulnerability management, Threat Intelligence).

Experience with Cyware Platform for Threat Intelligence

Utilized the Cyware platform to aggregate, analyze, and share threat intelligence to enhance security operations.

Integrated Cyware TI feeds into security systems to improve threat detection and response capabilities.

Leveraged Cyware to automate threat intelligence workflows and facilitate collaboration across security teams.

Cyber Threat Intelligence Analyst

Conducted thorough analysis of security threats by monitoring and evaluating malicious hashes, IP addresses, domains, and URLs.

Collaborated with security teams to identify and assess emerging cyber threats, including malware, phishing attempts, and other attack vectors.

Generated actionable intelligence based on threat analysis and provided recommendations for network defense strategies.

Took ownership of the approval and implementation process for blocking identified malicious domains, IP addresses, and URLs across various systems and firewalls.

Utilized threat intelligence platforms (Threat Intel platform-Cyware, Citrix, and SOAR)

platform-cortex) to track, analyze, and report on security incidents.
Contributed to improving the organization's cybersecurity posture by ensuring timely response to evolving threats.

Utilized Azure Sentinel for advanced security monitoring, log management, and threat intelligence.

Configured and optimized Microsoft Defender to provide endpoint security across a hybrid environment.

Implemented and managed Panda EDR to detect and respond to advanced threats across the organization's endpoints.

Managed and integrated Devo SIEM for real-time log analysis and incident response automation within a SOAR framework, improving operational efficiency.

Worked with Grey Matter SOAR to automate incident response and enhance security operations workflows

CERTIFICATION

- Microsoft Certified: Security Operations Analyst Associate (SC-200) – [12/2024-12/2025]