# AKHIL CEEPATHI

SOC ANALYST

akhilcpi3897@gmail.com | www.linkedin.com/in/akhil-ceepathi | +91-8328368561

## PROFILE SUMMARY

Security Operations Center analyst with 4.8 years of experience in identifying and mitigating cybersecurity risks. Experience in Information security which includes security log management technologies, Network Security, Web Security, Endpoint security and malware analysis. Well-versed with analysis and Vulnerabilities and threats. Having good communication and interpersonal skills. Experience of working in 24x7 operations of SOC team, offering log monitoring, security information and Event management.

## WORK EXPERIENCE

**SOC ANALYST** Oct 2022-Dec 2023
**R4 SOLUTIONS** **NOIDA**

- Monitored and analyzed security alerts generated by SIEM tool Microsoft 365 Defender to detect potential security breaches and incidents.
- Responded to cybersecurity incidents, including malware outbreaks, phishing attacks, and suspicious network activity.
- Conducted in-depth analysis of malicious emails and attachments to identify indicators of compromise (IoC's) and applied defensive measures.
- Using AV and other analysis tools to perform Malware Analysis and complete removal of malware from the client's environment.
- Ensure all organizational endpoints are equipped with the latest antivirus (AV) updates by regularly monitoring endpoint security status. For endpoints lacking the latest AV versions, perform remote installations and updates using Remote Desktop Protocol (RDP) to maintain consistent security across the network.
- Installing Microsoft Defender for Endpoint on user's machines and performing full device scan as per requirements.
- Add and manage indicators of compromise (IoC's) such as suspicious URLs, IP addresses, and file hashes in the Microsoft 365 Defender portal, ensuring proactive blocking and response according to client requirement.
- Initiate live response sessions in Microsoft 365 Defender using command-line tools to investigate and permanently remediate suspicious files from user machines, ensuring prompt threat mitigation.
- Revoke user and Multi-Factor Authentication (MFA) sessions in Microsoft Azure when a device is detected to be out of compliance, enforcing security policies to prevent unauthorized access.

**SOC ANALYST** Oct 2018- April 2022
**COGNIZANT TECHNOLOGY SOLUTIONS** **HYDERABAD**

- Worked in Security Operation Centre (24*7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Real time Monitoring of Alerts using SIEM Tool like IBM Qradar.
- Analyze and investigate the alerts in SOC monitoring tool to report any abnormal behaviors, suspicious activities, traffic anomalies etc.
- Perform incident response tasks, including containment, eradication, and recovery, ensuring timely and effective resolution.
- Creating an incident ticketing, analyzing, managing and tracking security incidents to closure by coordinating with different teams.

- Extensive knowledge of email security threats and security controls, with hands-on experience in analyzing email headers, attachments, and URLs to identify phishing attempts, malware, and other malicious activities.
- Experience working with email security gateways such as Mimecast, filtering malicious emails, and monitoring for phishing and spam threats to enhance organizational email security.
- Executed live response actions using Sentinel One, including isolating compromised endpoints, terminating malicious processes, and performing forensic analysis to understand the nature of threats.
- Using various security tools to perform monitoring and analysis of security events to detect security risks and threats within established customer Service Level Agreements.
- Raising true positive incidents to respective stack holders and take appropriate actions to block suspicious and poorly reputed IP addresses on the firewall, ensuring swift threat containment and mitigation.
- Development of reports and dashboards in Qradar.
- Generating reports based on cases triggered on a weekly, monthly basis and providing it to the clients.
- Knowledge on integration of log sources like windows and Linux with IBM Qradar tool.

---

## SKILLS

- IBM Qradar
- Microsoft 365 Defender
- Service now
- Palo alto firewall
- Sentinel one
- Mimecast

---

## Analysis Tools

- Virus Total
- Hybrid Analysis
- Browserling
- MX Toolbox
- IBM X-Force
- Urlscan.io
- URLVOID
- IPVOID

---

## EDUCATION

| | | |
|---|---|---|
| Bachelor of Engineering | Kshatriya College of Engineering | 2014-2018 |
| Board of Intermediate Education | Narayana Junior College | 2012-2014 |
| Board of Secondary Education | Narendra High School | 2011-2012 |