

AKSHAY M S

Cyber Security Analyst

+919207177323 • akshaymsatheesh@gmail.com • linkedin • Palakkad, Kerala, 678597

Summary

Entry-level Cybersecurity Analyst with 1.5 years of hands-on experience in cybersecurity operations and infrastructure monitoring within a 24/7 SOC environment. Proficient in identifying and responding to security incidents, analyzing logs, and supporting threat detection activities. Skilled in networking concepts like TCP/IP, DNS, and DHCP, and experienced with SIEM tools such as Splunk and Microsoft Sentinel. CEH and CSA certified, with a strong understanding of firewall configurations and endpoint security measures. Detail-oriented, analytical, and a quick learner with effective communication and problem-solving skills.

Technical Skills

SIEM • Sentinel • Elastic • Logpoint • Splunk • SentinelOne • Jira • VirusTotal • AbuseIP • IBM X-Force • MxToolbox • Any.run • Mac OS • OSI • MITRE • Cyber Kill Chain ISO 27001 • NIST • TCP/IP • DNS • SMTP • HTTP • FTP • SSH • Windows • Linux • Wireshark • Firewall

Experience

Junior SOC Analyst

Oct 2024-Feb 2025

Encyb Security Services Pvt Ltd, Thrissur, Kerala

- Monitored and analyzed security events to identify intrusions and malicious activities.
- Reported alerts and investigated issues identified during live traffic monitoring.
- Escalated incidents to the L2 SOC team, when necessary.
- Followed up on remediation activities to ensure resolution.
- Performing phishing email analysis to identify potential threats.
- Maintained and troubleshooted SIEM systems.
- Assessed SIEM health by monitoring key metrics such as RAM, storage, and processor performance to gain insights on system stability.
- Verified log transmission from assets to ensure data accuracy and integrity.
- Prepared daily, weekly, and monthly reports for clients.
- Collected threat advisories and compiled reports three times a month.
- Conducted dashboard reviews to monitor and report any malicious activities.

SOC Analyst Trainee

Apr 2024-Sep 2024

Encyb Security Services Pvt Ltd, Thrissur, Kerala

- Monitored real-time event logs 24x7 using SIEM tools; performed analysis, investigation, and mitigation.
- Handled incidents, reviewed alerts, and conducted in-depth log analysis.
- Detected suspicious activity and raised tickets with relevant teams.
- Adhered to SLAs and standard procedures.
- Followed up and closed tickets based on client feedback.
- Gained hands-on experience in daily monitoring and incident investigation.
- Worked with SIEM tools including Logpoint, Elastic, and Azure Sentinel.

Cyber Security Intern

Jul 2023-Dec 2023

Techbyheart Pvt Ltd, Kochi, Kerala

- Monitored event logs using the SIEM tool Splunk.
- Learned about various cyberattacks and their mitigation techniques.
- Gained foundational knowledge of the ELK stack.
- Hands-on experience with Snort.

Education

Rajadhani Institute of Science and Technology

BTech • Computer Science Engineering

Palakkad, Kerala

2019 – 2023

D.B.H.S.S Thachampara

Higher Secondary • Computer Science

Palakkad, Kerala

2017 – 2019

D.B.H.S.S Thachampara

SSLC

Palakkad, Kerala

2017

Certifications

- Certified Ethical Hacker (CEH), EC-Council
- Certified SOC Analyst (CSA), EC-Council
- Certified Network Security Practitioner (CNSP), SecOps
- FCA-Fortigate 7.4 Operator Self-Paced, Fortinet
- The Absolute Guide to MITRE ATT&CK, Picus Security
- Operationalizing MITRE ATT&CK for SOCs, Picus Security
- 210W-04 Cybersecurity Within IT and ICS Domains, CISA
- 100W Cybersecurity Practices for Industrial Control Systems, CISA
- CSI Linux Certified Investigator, CSI Linux
- Ethical Hacker, CISCO

Achievements

TryHackMe Rank: Top 1% | Level: 13 (LEGEND)