Premjit Sengupta

SOC Analyst Trainee

PERSONAL INFORMATION

Email
premjitsengupta44@gmail.com

Mobile
(+91) 8902725645

Total work experience
2 Years 1 Month

Social Link
https://www.linkedin.com/in/premjit-sengupta-96a48793/

KEY SKILLS

- SOC
- SIEM
- Azure Sentinel
- Threat Intelligence
- Threat Management
- Threat Hunting
- Threat Detection
- Incident Response
- Incident Investigation
- Soar Automation

OTHER PERSONAL DETAILS

City	Kolkata
Country	INDIA

PROFILE SUMMARY

Dedicated and detail-oriented SOC Analyst with hands-on experience in monitoring, detecting, analyzing, and responding to cybersecurity incidents within enterprise environments. Proficient in utilizing SIEM tools like Splunk Enterprise Security and Azure Sentinel to identify threats, perform deep-dive investigations, and enhance security posture. Skilled in creating and fine-tuning detection rules, threat hunting, and incident response. Strong understanding of network protocols, log analysis, malware analysis, and cloud security monitoring. Effective communicator with the ability to collaborate with cross-functional teams to mitigate risks and improve incident handling processes.

EDUCATION

2013 — BSC
Calcutta University

WORK EXPERIENCE

Feb 2025 - Present — SOC Analyst Trainee
Purplesynapz

Dedicated and detail-oriented SOC Analyst with hands-on experience in monitoring, detecting, analyzing, and responding to cybersecurity incidents within enterprise environments. Proficient in utilizing SIEM tools like Splunk Enterprise Security and Azure Sentinel to identify threats, perform deep-dive investigations, and enhance security posture. Skilled in creating and fine-tuning detection rules, threat hunting, and incident response. Strong understanding of network protocols, log analysis, malware analysis, and cloud security monitoring. Effective communicator with the ability to collaborate with cross-functional teams to mitigate risks and improve incident handling processes.

INTERNSHIP

41 Days — **PURPLESYNAPZ**

72 Days — **QOS Technology**

72 Days — **PURPLESYNAPZ**

LANGUAGES

- english
- hindi
- bengali

Projects

41 Days

Malware Detection via Sysmon & SIEM Integration

To enhance detection of malware activity by integrating Sysmon logs with SIEM tools. Tools & Technologies: Sysmon, Splunk, Azure Sentinel.

41 Days

Insider Threat Detection

Objective: To detect anomalous user behavior suggesting potential insider threats. Tools & Technologies: Splunk User Behavior Analytics (UBA), Azure Sentinel, Windows Security Logs.

31 Days

BRUCEFORCE ATTACK ON vm

ANALYZING BRUCEFORCE ATTACK WITH SPLUNK ENTERPRISE SECURITY AND CONTINOUS MONITORING WITH SEARCH QUERIES

31 Days

ANALYZE MAIL PHISING ATTACK

PHISING ATTACK ANLAYSIS WITH EMAIL HEADER ANALYSIS

72 Days

Monitoring & Detecting Windows Security Log Deletion (Event ID 1102)

To implement effective detection and alerting mechanisms for unauthorized or suspicious Windows Security Log deletions (Event ID 1102) to enhance endpoint security and ensure audit trail integrity.

COURSES & CERTIFICATIONS

- doeacc a level
- networking fundamentals
- palo alto administration