Ravi Nandan Ray

Threat Detection Engineer(Cyber Security)

Pune ravinandanray99@gmail.com **7600486822** My Portfolio Linkedin Github

Summary

Threat Detection Engineer with expertise in Sentinel, Devo SIEM and Qradar, log parsing, Linux, SQL and incident response automation.

Experience

Associate Consultant - Threat Detection Engineer (Capgemini) *Pune*
SEP 2022 – Present

- **Implemented and fine-tuned 500+ Log Analytics rules in Azure Sentinel**, improving threat detection and monitoring efficiency.
- **Developed workspace functions for accurate parsing of device-specific logs from Syslog and CEF**, ensuring seamless log ingestion and normalization.
- **Designed and automated incident response playbooks using Azure Logic Apps**, reducing manual intervention and accelerating response times.
- **Optimized 1298 SIEM rules in IBM QRadar, achieving a 50% reduction in weekly offense count (from 334 to 171) through enhanced correlation and rule tuning**.
- Created and fine-tuned 168 SIEM rules across QRadar and Sentinel, strengthening detection capabilities for diverse security devices.
- **Authored Standard Operating Procedures (SOPs) and developed automation playbooks for L1/L2 SOC teams**, streamlining incident triage and response workflows.
- **Utilized JIRA (JQL) for efficient task management and tracking** of security operations projects.

SDE (Intern) *Remote*
Capgemini - Cloud Infrastructure Security Services *FEB 2022 – JULY 2022*

- **SIEM rules translation** between **Sentinel, Splunk, and Qradar, Devo SIEM**.

Technical Skills

- **Coding Language**: **C++**, JavaScript, **Python**.
- **Skills**: **SIEM Threat detection and Fine-tuning**, **Security Log Analysis**, **SQL**, **AQL**, **KQL**, **JQL**, **LINQ**, **Python task automation**, **LINUX**, **Wireshark and tcpdump**, Incident Response.
- **SIEM Tools**: **Sentinel**, **IBM Qradar**, **Devo**
- **Certifications**: **Google Cybersecurity Professional Certificate(v.2)**, **GenAI for Cybersecurity**

Coursework

Network Concepts and protocols, Network Security, Cloud Infrastructure Security, Soft Computing, OOP Concepts, DBMS, Operating system, **GIT, GITHUB (VCS) and GITLAB**, Data Structure and Algorithms.

Education

Delhi Technological University - DTU(Formerly Delhi College Of Engineering - DCE) *Post-Graduation in* **Electrical Engineering** *SEPT 2020 – MAY 2022 (Delhi)*

Achievements

- GATE (IN) - 2020 - All India Rank 773
- Leetcode Contest Rating - 1661
- GFG Contest Rating - 1774
- Open Source Contribution - The OdinProject PR link