Prithul Raj M R

Ernakulam, Kerala, India
+91 9188869274 • prithulrajmr@gmail.com
linkedin.com/in/prithulraj • github.com/prithul21

Profile

Recent Cyber Forensics graduate with hands-on experience in SIEM Monitoring, Incident Response, and Threat Intelligence. Proficient in Splunk Enterprise Security, analyzing security alerts, and identifying potential threats such as DDoS, APT Lifecycle, and Data Exfiltration Attempts. Passionate about cybersecurity, forensic analysis, and security operations.

Areas of Expertise

Security Operations (SOC): SIEM Log Analysis, Incident Response, Alert Triage, Threat Intelligence

Threat Detection & Analysis: Splunk Enterprise Security, IDS/IPS, Malware Analysis, Threat Hunting

Security Event Management: Triage, Correlation, Enrichment of Security Events, Incident Escalation

Vulnerability Management: Risk Assessment, SOC Compliance, Threat Vector Identification

Forensic Investigation: Traffic Analysis, Security Event Correlation, SOC Efficiency Improvement

Security Metrics & Reporting: Dashboard Design, Asset Monitoring, Security Incident Reporting

Projects

Ernakulam, Kerala

Project: Security Monitoring with Splunk *01/2025*

- Developed a SIEM-based security monitoring system using Splunk Enterprise Security.
- Configured custom security alerts for threat detection, including:
  - **Failed Logins:** Detection of brute force attempts and unauthorized access.
  - **APT Lifecycle Monitoring:** Alerts for persistent threats and data exfiltration.
  - **Malware Infection Detection:** Identification of compromised assets.
  - **DDoS Attack Indicators:** Correlation of anomalous traffic patterns.
- Designed interactive Splunk dashboards for security teams to visualize real-time threats.
- Improved incident response efficiency by 30% through enhanced log correlation and enrichment.

Internship Experience

Prodigy Infotech **Remote**

Cybersecurity Intern *09/2024 – 10/2024*

- Performed SIEM log analysis and monitored security events for potential threats.
- Worked on network packet analysis, keyloggers, and security automation tools.
- Developed a password complexity checker, image encryption tool, and custom brute-force testing scripts.
- Gained hands-on experience in SOC operations, threat detection, and forensic analysis.

Certifications

- EC-Council - Certified Ethical Hacker
- Google - Foundations Of Cybersecurity
- EC-Council - Certified SOC Analyst
- TechByHeart - Certified SOC Analyst
- EC-Council - Ethical Hacking Essentials
- EC-Council - Python Beginners' Certificate
- Red Team - Ethical Hacking Essentials
- CISCO - Introduction to Cybersecurity
- FCF - Introduction to the Threat Landscape 2.0
- Tata Group - Cyber Security Analyst Job Simulation
- Splunk - Introduction to Enterprise Security

Education

Mahatma Gandhi University, Kochi, Kerala
BSc in Cyber Forensics *2020 – 2024*
Focus: Cybersecurity, Digital Forensics, Network Security.

TechByHeart, Kochi, Kerala
Diploma in Cybersecurity, SOC Analyst, and Cyber Forensics *2024 – Present*
Focus: Threat Analysis, Security Monitoring, Cybersecurity Fundamentals.

Skills

- **Cybersecurity:** Security Information and Event Management (SIEM), Threat Intelligence, Incident Response, Vulnerability Management
- **SIEM:** Splunk Enterprise Security, Log Analysis, Alert Triaging, Threat Correlation
- **Tools:** Wireshark, Metasploit, Burp Suite, Kali Linux, Nmap, Nessus, Splunk, Aircrack-ng, John The Ripper, Gobuster, Hydra, Maltego
- **Threat Detection:** APT Lifecycle, Data Exfiltration, Malware Detection, DDoS Indicators
- **Security Metrics & Reporting:** Dashboard Design, Security Incident Reports, Risk Assessment
- **Operating Systems:** Windows, Linux

Languages

English: Fluent

Malayalam: Native

Hindi: Intermediate