

# DILEEP SIRAM

Hyderabad | 9849702494 | siramdileep30@gmail.com

## Summary

Certified SOC Analyst (CSA) and Certified Ethical Hacker (CEH) with over three years of hands-on experience in **Security Operations, Incident Response, and Vulnerability Management** across enterprise environments. Skilled in **Splunk Enterprise Security (ES)** and **IBM QRadar** for proactive detection, correlation, and mitigation of threats. Experienced in conducting **security risk assessments, vulnerability analysis, and threat modelling** aligned with **NIST and ISO 27001** frameworks. Strong understanding of **cloud security, identity management, and governance best practices**. Adept at communicating security risks and collaborating with technical and business stakeholders to enhance resilience and compliance

## Skills

- **SOC Operations & Incident Response**  
Real-time threat monitoring, triage, and investigation  
Use case creation, tuning, and validation (Splunk, QRadar)  
Playbook design and SOAR workflow automation
- **Threat Hunting & Vulnerability Management**  
Vulnerability scanning, risk-based prioritization, and remediation tracking  
Threat intelligence correlation and patch management coordination  
MITRE ATT&CK mapping and adversary simulation
- **System & Identity Security**  
Active Directory security, Microsoft Identity technologies  
Linux administration, cryptography fundamentals
- **Frameworks & Standards**  
OWASP, ISO27001, NIST, CIS, PCI DSS  
Cloud log management (AWS CloudTrail, Azure Monitor)
- **Tools:** Splunk ES, QRadar, Burp Suite, Nessus, Nmap, ServiceNow, Cisco ThousandEyes, LogicMonitor, and XDR tools( Sentinel, wazuh).

## Experience

- |   |   |
|---|---|
| <b>Security Operations Center (SOC) Analyst</b><br><b>Symbiosys Technologies</b>  | <b>11/2023 to Current</b><br><b>India</b>     |
| <ul style="list-style-type: none"><li>• Monitored enterprise networks, endpoints, and cloud workloads using <b>Splunk ES</b> and <b>QRadar</b>, detecting and mitigating potential threats.</li><li>• Conducted <b>risk assessments and vulnerability validation</b>, recommending compensating controls and remediation measures.</li><li>• Built and refined <b>correlation rules and detection logic</b>, improving alert fidelity and reducing false positives by 35 %.</li><li>• Created and maintained <b>incident response playbooks</b> to streamline investigations and improve readiness.</li><li>• Supported <b>security investigations and root-cause analyses</b> for phishing, malware, and unauthorized-access events.</li><li>• Participated in <b>post-incident reviews</b>, contributing to stronger control design and operational maturity.</li></ul> |   |
| <b>Cyber Security Specialist</b><br><b>Woolworths Group</b>   | <b>08/2022 to 09/2023</b><br><b>Australia</b> |
| <ul style="list-style-type: none"><li>• Supported the enterprise cybersecurity operations team, assisting in vulnerability management and incident handling for critical systems.</li><li>• Monitored digital infrastructure health and performance using Splunk Observability, LogicMonitor, and Cisco ThousandEyes.</li><li>• Conducted vulnerability scans and remediation follow-ups, coordinating with IT and development teams to close high-risk exposures.</li><li>• Assisted in incident escalation, ensuring timely containment and root cause analysis in coordination with the SOC.</li></ul>   |   |

- Worked closely with business continuity and risk teams to align vulnerability findings with operational impact.
- Gained deep understanding of enterprise-grade cybersecurity operations, governance, and compliance frameworks.

**Online Manager**

**07/2021 to 07/2022**

**Woolworths Group**

**AU**

- Led cross-functional operations of the Woolworths online store, ensuring accurate delivery, customer experience, and inventory alignment.
- Managed a team of 25, coordinating supply chain, IT, and customer service teams for seamless delivery.

**Application Development Associate**

**06/2018 to 07/2019**

**Accenture**

**India**

- Addressed security alerts and escalated critical issues as needed.
- Acquired foundational skills in system monitoring, log analysis, and debugging, contributing to cybersecurity monitoring.

## Education and Training

---

**MBA: E-business And Supply Chain Management**

**07/2021**

Deakin University

Melbourne

**Bachelor of Technology: Electronics And Communications Engineering**

**05/2018**

Amrita University

Coimbatore

## Certifications

---

**CEH v13 – Certified Ethical Hacker**, EC-Council (ECC0143265789)

**CSA v2 - Certified SOC Analyst**, EC-Council (ECC4150628379)