SRINATH K K

SOC Engineer

7012804014 ◇ Gurugram, IN ◇ srinathkk99@gmail.com ◇ linkedin.com/in/srinathkk ◇ Portfolio

CAREER OBJECTIVE

BCA graduate and SOC Engineer L1 with 1.6 years of experience in SOC infrastructure, SIEM administration, server administration, network security, and cybersecurity technologies. Experienced in managing Docker containers, Linux and Windows servers, log collection and parsing, security tool integrations, Active Directory, DNS, and network infrastructure. Strong understanding of SIEM technologies, system administration, and cybersecurity operations, with a track record of responsibly securing 35+ websites through vulnerability research and disclosure.

EXPERIENCE

SOC Engineer L1 *CDC* *On-site at Power Grid Corporation of India, Gurugram* *Jul 2025 – Present*

- Manage **Docker containers** used for SOC applications and services, including container deployment, monitoring, and troubleshooting.
- Create and manage **watchers, playbooks, and dashboards** to monitor security events, automate workflows, and improve SOC visibility.
- Manage **SOC/SIEM servers and infrastructure**, ensuring stable operation and continuous security monitoring.
- Manage **High Availability (HA) servers** to ensure services continue running when a primary server goes down.
- Create **custom log parsers using Regex** to process and normalize logs from different sources for better monitoring and detection.
- Manage and maintain **Active Directory and DNS environments**, along with configuring **Group Policy (GPO) settings and DNS records**.
- Handle **security tool and endpoint integrations**, ensuring proper configuration, log collection, and monitoring.
- Configure **switches and firewalls** by creating ACL and VLAN rules on switches and access-control and NAT rules on firewalls.
- Configure and manage **Squid and Nginx proxy services** for secure network traffic and application access.
- Manage **Linux and Windows servers using tools such as Windows Admin Center and Zabbix**, including OS installation, VM creation, patching, monitoring, and troubleshooting.

SOC Analyst Intern *Ciber Digita Consultants (CDC)* Remote *Apr 2025 – Jul 2025*

- Completed hands-on training in **IT networking, SOC operations, alert triage, incident monitoring, and basic incident response** using CDC's SIEM tool, with practical experience in **Docker, Tmux, and Watcher creation**.

SKILLS

Tools & Technologies - CDC-ON, Burp Suite, Docker, Tmux, Zabbix, RegEx, Veeam, HAProxy, Squid, Nginx, ManageEngine, Windows Admin Center, Antivirus.

Systems & Networking - Linux, Windows Server, Active Directory, DNS, Firewalls, VLAN, ACL, NAT, Virtual Machines

Programming - Python, Bash, JavaScript, SQL, JSON

EDUCATION

Bachelor of Computer Applications, Kannur University *June 2020 - March 2023*

Diploma in Cyber Security, Bsoft Education *June 2024 - December 2024*

PROJECTS

INNOVORA SIEM. Customized an open source security platform into a dedicated SIEM solution, adding custom security monitoring, threat detection, log analysis, and investigation capabilities.

- Built lightweight endpoint agents across Linux, Windows, and macOS to capture host metrics, process activity, and authentication logs for centralized SIEM ingestion.
- Created an interactive pipeline builder with automatic log parsing and custom field mapping per index to standardize raw syslog events into Elastic Common Schema format.
- Developed a custom SIEM Query Language (IQL) with pipe based syntax that compiles into Elasticsearch DSL for high speed log search, bucket aggregations, and security event analysis.
- Implemented a sliding window correlation engine aggregating real time authentication telemetry over 5 minute intervals to detect SSH brute force attacks and unauthorized privilege escalation.
- Configured Elasticsearch Index Lifecycle Management (ILM) with 1 click index rollover and automated 90 day retention policies to manage high volume heartbeat and security event indices.
- Integrated real time detection rules and incident triage workflows mapped to the MITRE ATT&CK framework across Credential Access, Privilege Escalation, and Initial Access tactics.

AWARDS / ACHIEVEMENTS

- Recognized in **NASA's Hall of Fame** and awarded **2 Letters of Recognition** for reporting critical vulnerabilities.
- Earned a **Letter of Recognition** from the **U.S. Department of Homeland Security** for identifying and reporting a high-severity vulnerability.
- Recognized by **Google** with **two awards** for reporting P4-level vulnerabilities, demonstrating proficiency in identifying and documenting security issues.
- Received **20+ Hall of Fame recognitions** from organizations including BIA, FHFA, USAGM, RMIT, Unilever, Rakuten, Monash University, CIGIE, FRTIB, EXIM, EPA, and others.
- Responsibly identified and disclosed vulnerabilities across **30+ websites and organizations**, including Indian Army, AWS, Uber, DoD, Klarna, NBA, Land Rover, Jaguar, Upwork, Blackbaud, and Northwestern Mutual.
- Developed an AR effect and won **$300** in the **Meta Spark** competition, securing a position in the **top 500 globally**.

CERTIFICATIONS & TRAINING

- **Certified Ethical Hacker (CEH v13)** — EC-Council
- **Network Security: Core Security Concepts** — LinkedIn Learning
- **Introduction to Ethical Hacking** — Offenso Hackers Academy
- **Introduction to Cybersecurity** — Cisco