Position Title: Systems & Security Engineer
Location: IIT Tirupati Navavishkar I-Hub Foundation (IITTNiF)
Employment Type: Ad-hoc (12-month contract including 3 months probation)
Reporting To: Project Director
Working Days: Six days a week (Monday to Saturday)
Office Timings: 9:00 AM – 5:30 PM
Created by:

Role Overview

The Systems & Security Engineer will support the Geo-Intelligence (Geo-Intel) Lab, which works on large-scale geospatial, positioning, navigation, and precision technology data under the NM-ICPS program. The role will ensure secure, reliable, and high-availability infrastructure for handling sensitive spatial datasets, real-time sensor feeds, and research applications.

The Systems & Security Engineer will be responsible for managing and securing the organization's data center infrastructure, ensuring confidentiality, integrity, and availability of critical systems and research data. The role includes overseeing server, network, and application security, implementing monitoring and incident response mechanisms, and leading a small technical team to maintain secure and reliable operations aligned with NM-ICPS and DST guidelines.

Key Responsibilities

1. Data Center & Infrastructure Management

- Manage on-premise and cloud servers (Linux-based) used for research and production workloads.
- Oversee virtualization, storage, backup, and disaster recovery systems.
- Ensure high availability, performance monitoring, and capacity planning.

2. Cyber Security & Data Protection

- Implement and maintain security controls such as firewalls, IDS/IPS, access control, and network segmentation.
- Perform vulnerability assessments and coordinate remediation.
  Ensure secure configuration of servers, databases, and applications (hardening, patching, least privilege).
- Protect sensitive research and positioning data through encryption, access policies, and secure key management.

3. Security Operations & Monitoring

- Deploy and manage log monitoring, SIEM, and alerting systems.
- Detect and respond to security incidents, conduct root cause analysis, and prepare incident reports.
- Maintain audit trails and support compliance with government and DST security guidelines.

4. Application & API Security Support

- Work with development teams to review application security (OWASP Top 10, API security, authentication, authorization).
- Assist in secure deployment, SSL/TLS configuration, and secure CI/CD pipelines.

5. Team Leadership

- Lead and mentor at least one technical engineer for infrastructure and security operations.
- Define Standard Operating Procedures (SOPs) for data center operations and security.

Required Technical Skills

Core Security Skills

- Web & API Security (OWASP Top 10, Auth flaws, IDOR, XSS, CSRF, SQLi, SSRF etc)
- Vulnerability Assessment & Penetration Testing (VAPT)
- Incident Response & Log Analysis
- Risk Assessment & Security Policy Implementation

Infrastructure & Systems

- Linux Server Administration (hardening, patching, monitoring)
- Networking fundamentals (TCP/IP, firewalls, VPN, VLANs)
- Data Center Operations (backup, DR, high availability, monitoring)
- Virtualization & Containers (VMware/Docker)

Security Tools

- Burp Suite, Nmap, Nessus, Metasploit, Wireshark
- SIEM / Log Monitoring (ELK, Wazuh, or similar)
- Endpoint and server security tools (Fail2ban, Auditd, OSSEC, etc.)

Automation & Scripting

Python and Bash for security automation, monitoring, and reporting.

Qualifications & Experience

- Bachelor’s or Master’s degree in Information Technology, Computer Science, Cybersecurity, or a related field, or equivalent professional experience.