Indicative list of Topics for NCIIPC Internship Program 2023

Domains (Indicative)

I. Cyber Security Audits, Risk Assessments, Enterprise Risk Management
II. Vulnerability Assessment and Penetration Testing
III. Network/Architecture, Gap analysis and Recommendations
IV. Cyber Incident Response and Root Cause Analysis
V. Cyber Threat Intelligence: Automated through scripts/programs
VI. Malware Reverse engineering through static and dynamic analysis
VII. IT, OT, Cloud, IoT Security
VIII. Legal Framework in CII Security: Cyber and CII Laws
IX. Traffic/Log analysis: Scripts, Platforms, Tools
X. Digital forensics: Open source tools usage, Development of scripts/tools
XI. Threat hunting, link analysis and deployment
XII. Global Policy and Regulatory Frameworks in CII Security
XIII. Global Cybersecurity Industry- Outlook and Prospects
XIV. Geopolitics, Emerging Technology and Cyber Security Strategies
XV. AI/ML
XVI. Zero Trust Architecture
XVII. SBOM

Problem Statement (Indicative)

a) Software/Application Development/Cyber Technology

I. Phishing Mitigation and Email Security Technology
II. OSINT on Indicators of Compromises (IoCs)
III. Parsers for log analysis, Network Traffic Analysis
IV. Threat assessment and dissemination Framework/Platform
V. Stakeholder Survey automation, database and dashboard prototypes
VI. Prototype Infrastructure as a Code (IaC) solution using Ansible platform
VII. Secure privilege user- remote access solution
VIII. Automation of incident report and management capabilities

b) Security Testing

I. Innovative Test Methods conforming to global standards for IT equipment
II. Testing scenarios of IoT equipment security
III. Simulation of IT/OT for tolerances, vulnerabilities, device overrides etc.
IV. Automatic Fuzz testing test bed for IT equipment
V. Malware Analysis using Sandboxing environments and result integration

c) International and Security Studies

I. Global CII protection framework and Best Practices
II. Global SOPs, Best Practices and comparisons
III. Global approach and Emerging Technology in CII Security
IV. Strategic Affairs- Technology and Policy

d) Legal Studies

I. Examining legalities around CII protection
II. Liability, Insurance, Claims
III. Legal architecture around CII protection
IV. Examining Indian and Global case laws and implications
V. Invoking of sections under IPCs for Cyber incidents. Global arrangements for tackling attacks on CIIs of the country.
VI. Data Governance Frameworks for NCIIPC and CII entities

e) Design and Content Creation

I. Designing and developing websites with new age designs and features
II. Generating high resolution graphics for logos and designs
III. Creative design/ animation for social media content repository
IV. Video Content Creation
V. Layout, Web and Application Designs

f) Statistical Inference

I. Approaches in Mathematics and Statistical theory- Cybersecurity
II. Examining literature of sampling based research on cyber security
III. Regression analysis
IV. STATA/R based programming approaches and applications to cyber security

g) AI/Machine Learning

I. Survey and Prototyping Machine Learning approaches to CII security
II. AI/ML approaches in Threat hunting, Cyber kill chain mapping, link analysis
III. Prototyping solutions to key technical challenges in this domain
IV. Optimizing, scaling and fine tuning existing ML solutions in cyber defence
V. National language Processing for Data Extraction and Topic Modelling