💾 Cybersecurity Internship Submission Guidelines (2025)

📌 Organized by: **Digisuraksha Parhari Foundation**

🤝 Powered by: **Infinisec Technologies Pvt. Ltd.**

🗓️ **Final Project Submission Deadline: 12th May 2025**

📽️ **Live Project Presentation: 12th May Night (Meeting link will be shared via email)**

👷 **Submission Medium: *GitHub Repository (Mandatory)***

🔐 Overview

As part of this internship, all participants are required to submit a **complete cybersecurity research portfolio** through a **personal GitHub repository**.

You are expected to showcase your technical and research skills by:

- ✅ Developing a practical **project/tool**
- ✅ Submitting a **research paper** with factual depth
- ✅ Delivering a **presentation** in slide and video format
- ✅ Participating in a **live review meeting on 11th May night**

👥 Team Formation

- Work **solo** or in a **team of up to 3 members**.
- Each team must create **one GitHub repo** and **add collaborators**.

🎯 Research & Project Topics (Choose or Propose)

Participants may choose any topic relevant to modern cybersecurity trends, including:

🤖 AI-Driven Cybersecurity

- AI-Powered Malware and Evasion Techniques
- Weaponizing LLMs for Offensive Cybersecurity
- Prompt Injection Attacks on AI Systems
- LLM-based Red Team Simulations
- Deep Learning for Exploit Generation
- AI in Social Engineering and Phishing Campaigns
- Neuro-symbolic AI for Vulnerability Detection
- Building Autonomous Threat Hunting Agents
- AI vs AI: Defense Models Against Malicious AI Agents

- Federated Learning in Cybersecurity
- Ethical Challenges in AI-based Cyber Warfare
- Deepfake Malware and Detection Strategies
- Zero-Day Prediction using Graph Neural Networks
- Leveraging Reinforcement Learning for Exploit Chains
- AI-Enhanced Breach and Attack Simulation Tools
- Creating AI-Based Honeypots for Dynamic Threat Capture
- LLMs in Mobile Malware Detection and Prevention
- AutoML for Cyber Threat Intelligence
- Multi-Agent AI for Coordinated Cyber Offense and Defense

🌐 Global & Future-Forward Topics (2025 & Beyond)

- Post-Quantum AI-Driven Threat Modeling
- LLM-Driven Cyber Deception and Misinformation Warfare
- Explainable AI (XAI) for Transparent Cyber Defense
- AI in Cyber-Physical System (CPS) Security
- Generative AI for Malware Mutation & Sandbox Evasion
- AI in Insider Threat Prediction and Behavior Analysis
- AI in Digital Forensics and Attribution
- Data Poisoning and Backdoor Attacks in AI Pipelines
- AI-Augmented Threat Intelligence Fusion
- Red Team vs Blue Team AI Simulations

✈️ Other Research Topics:

- Drone Hacking: Signal Interference, Hijacking, GPS Spoofing
- Airlines Hacking: ADS-B vulnerabilities, In-flight WiFi, Maintenance system exploits
- Space Systems Cybersecurity: Satellite comms, Space traffic control, GNSS hacking

📁 1. Project Requirements

Your tool must:

- Be cybersecurity-focused and solve a real problem.
- Be original, ethical, and practical.

📌 Your GitHub Repo Must Include:

- Full Source Code
- README.md with:
  - Problem statement
  - Setup instructions
  - Screenshots/logs/diagrams
- License & disclaimer
- YouTube video demo link

📁 2. Research Paper Requirements

Required Sections:

1. **Title Page**
2. **Abstract** (100–200 words)
3. **Problem Statement & Objective**
4. **Literature Review**
5. **Research Methodology**
6. **Tool Implementation**
7. **Results & Observations**
8. **Ethical Impact & Market Relevance**
9. **Future Scope**
10. **References** (Minimum 10 genuine sources)

📌 **Upload as research_paper.pdf to your GitHub repo**

🖥️ 3. Presentation & Video Demo

You must submit:

- 🎞️ **Demo Video** (7–15 mins, YouTube link)
  - Tool walk-through & real-world relevance
  - Link must be added in README.md
- 📈 **Slide Deck**
  - 10–15 slides (PDF or PPT)
  - Must cover:
    - Introduction, Problem, Solution
    - Code/Tool Breakdown
    - Real-World Use Cases
    - Future Enhancements

📌 **Upload as presentation.pdf in your GitHub repo**

🗣️ 4. Live Presentation—12th May Night

- Format: **7-minute presentation + Q&A**
- Platform: Online meeting Microsoft Teams
- Participation in this live session is **mandatory**

✅ Final Deliverable Checklist (GitHub Submission)

Component	Filename	Required?
Source Code	Root or /src/	✅
Research Paper	research_paper.pdf	✅
Presentation	presentation.pdf	✅
Demo Video	YouTube link in README.md	✅
README File	Full project documentation	✅

📬 How to Submit

1. Create a **public GitHub repository**.
2. Add all team members as **collaborators**.
3. Email your **GitHub repo link** to:
   📧 support@digisuraksha.org: Subject: Internship Final Submission Name/Team Name

⚠️ Important Guidelines

- 🔍 Submissions must be **original** and technically sound.
- 📌 Research must be supported by **genuine references**.
- 💡 Tools should solve a **real cybersecurity problem**.
- ❌ No unethical or plagiarized content will be accepted.

🚀 **Build the future of ethical cybersecurity.'** Let's secure digital Bharat, one tool at a time.

— Digisuraksha Parhari Foundation

Powered by: Infinisec Technologies Pvt. Ltd.

Example:

```
📁 your-project-name/
├── 📁 research-paper/
│   └── final_research_paper.pdf
├── 📁 presentation/
│   └── project_presentation.pdf / .pptx
├── 📁 tool/
│   ├── source_code/
│   │   └── (your scripts, code, folders here)
│   ├── requirements.txt / setup.py
```

```
│   └── README.md
├── 📁 demo/
│   └── demo_video_link.txt (link to your YouTube video)
├── LICENSE
└── README.md
```

Fill this Form. 🙂 https://forms.gle/TCFg8hHgzsWyy7cc8