Group Formation Rules

 - You may work individually or in a group of up to 3 members.

- Team collaboration is encouraged, but solo projects are equally allowed.

- Every participant is responsible for their contribution.

Blue Team (Defensive Security)

• Adaptive Threat Intelligence Co-Pilot (ATICoPilot)

 • Shadow-IT Detection & Local-Control Gateway

 • Atomic Coverage Health Scanner (ACHS)

• Zero-Day Exposure Radar (ZDER)

• IoT Behavioral Whitelisting Gateway

• Resilience-Oriented Cyber Hygiene Simulator Purple Teaming (Red + Blue Collaboration)

• Simulate & Detect PowerShell Attacks

• Credential Dumping Monitoring (e.g., Mimikatz)

 • Malware Behavior Analysis (AnyRun/Cuckoo)

 • USB Drop Attack Detection

• Phishing Simulation & Email Header Review

• Build Detection Rules using MITRE mapping

• Honeypot Setup & Log Analysis

• Full Kill Chain Simulation

Network Security & Cybercrime Investigation

• Dark Web Threat Intelligence Platform

• IoT Forensic Toolkit

• OSINT Aggregator for Investigations

• AI-based Cybercrime Reporting Portal

 • Cyberstalking Detection System

Purple Teaming (Red + Blue Collaboration)

 • Simulate & Detect PowerShell Attacks

• Credential Dumping Monitoring (e.g., Mimikatz)

 • Malware Behavior Analysis (AnyRun/Cuckoo)

• USB Drop Attack Detection

• Phishing Simulation & Email Header Review

• Build Detection Rules using MITRE mapping

• Honeypot Setup & Log Analysis

• Full Kill Chain Simulation

Red Teaming (Offensive Security)

• AI-Based Phishing Simulator

- Browser Credential Harvester Extension

- USB Payload Builder

- Active Directory Attack Lab

- Wi-Fi Evil Twin Simulator

- Insider Threat Emulation Toolkit

- Covert C2 Channels Framework

- Social Engineering Toolkit

Project Proposals

- You are not restricted to the above ideas.

- You are free to propose your own unique project ideas if you are confident and comfortable doing so.

- The project must align with cybersecurity, OSINT, digital forensics, or threat intelligence.

Tools & Description Requirement

For every tool or technology used in the project, the following must be included:

- Tool Name

- Brief Description of its Purpose

- How it will be used in the project

• Mention any alternative tools considered for the same task or domain. This helps reflect your research and decision-making process

Final Submission Checklist

• Project Title

 • Abstract / Summary

• Tools & Tech Used

• GitHub Repo

• Final PPT/PDF Presentation

• Project Demo (video/report/screenshots)