```markdown

# Cybersecurity with Generative AI

## Course Overview

Duration: 10 months

---

# Term 1: Introduction to Cybersecurity

## Module 1: Cybersecurity Foundations

- Topic 1: Overview of Cybersecurity
- Topic 2: Key Concepts and Terminology
- Topic 3: Cyber Threats
- Topic 4: Defense Mechanisms

## Module 2: System Security

- Topic 1: Operating System Vulnerabilities
- Topic 2: Secure Configuration
- Topic 3: Patch Management
- Topic 4: Malware Protection

## Module 3: Network Security

- Topic 1: Network Fundamentals
- Topic 2: Firewalls and Intrusion Detection Systems
- Topic 3: VPNs
- Topic 4: Securing Wireless Networks

## Module 4: Cybersecurity Policies and Procedures

- Topic 1: Developing Security Policies
- Topic 2: Risk Assessment
- Topic 3: Incident Response Plans
- Topic 4: Compliance and Legal Issues

---
```

Term 2: Generative AI in Cybersecurity

Module 5: Introduction to Generative AI

- Topic 1: What is Generative AI?
- Topic 2: Applications of Generative AI
- Topic 3: AI-Based Security Tools
- Topic 4: Ethical Considerations

Module 6: Machine Learning for Threat Detection

- Topic 1: Basics of Machine Learning
- Topic 2: Supervised vs. Unsupervised Learning
- Topic 3: Using AI for Threat Intelligence
- Topic 4: Case Studies

Module 7: Leveraging AI for Incident Response

- Topic 1: Automated Incident Response
- Topic 2: AI-Powered Forensics
- Topic 3: Real-Time Threat Analysis
- Topic 4: False Positives and Negatives

Module 8: Future Trends in AI and Cybersecurity

- Topic 1: Trends Shaping the Future
- Topic 2: The Impact of AI on Cybersecurity Jobs
- Topic 3: New AI Technologies in Cybersecurity
- Topic 4: Preparing for Future Challenges

Term 3: Secure Coding Practices

Module 9: Understanding Application Security

- Topic 1: Software Development Lifecycles
- Topic 2: Threat Modeling
- Topic 3: Common Vulnerabilities
- Topic 4: Secure Coding Standards

Module 10: User Input Validation

- Topic 1: Input Sanitization Techniques
- Topic 2: Preventing SQL Injection
- Topic 3: XSS Prevention
- Topic 4: Security in APIs

Module 11: Secure Deployment Practices

- Topic 1: System Hardening
- Topic 2: Secure Deployment Pipelines
- Topic 3: Environmental Security
- Topic 4: Incident Handling and Reporting

Module 12: Testing and Auditing Applications

- Topic 1: Security Testing Methods
- Topic 2: Vulnerability Assessments
- Topic 3: Penetration Testing
- Topic 4: Secure Code Review

Term 4: Cybersecurity Tools and Technologies

Module 13: Overview of Cybersecurity Tools

- Topic 1: Types of Cybersecurity Tools
- Topic 2: Open Source vs. Commercial Tools
- Topic 3: Selecting the Right Tools
- Topic 4: Tools for Monitoring Networks

Module 14: SIEM Solutions

- Topic 1: Introduction to SIEM
- Topic 2: Deploying SIEM Systems
- Topic 3: SIEM Use Cases
- Topic 4: Integrating SIEM with Other Tools

Module 15: Endpoint Protection

- Topic 1: Endpoint Threats
- Topic 2: Endpoint Security Tools
- Topic 3: Strategies for Securing Endpoints
- Topic 4: Case Studies

Module 16: Encryption and Data Protection

- Topic 1: Understanding Cryptography
- Topic 2: Encrypting Data in Transit and at Rest
- Topic 3: Key Management Practices
- Topic 4: Data Loss Prevention Policies

Term 5: Cybersecurity Risk Management

Module 17: Risk Management Frameworks

- Topic 1: Understanding Risk Management
- Topic 2: NIST Risk Management Framework
- Topic 3: ISO 27001 Framework
- Topic 4: Risk Assessment Process

Module 18: Business Continuity Planning

- Topic 1: Importance of BCP
- Topic 2: Disaster Recovery Planning
- Topic 3: Developing BCP and DR Plans
- Topic 4: Testing and Maintaining BCP

Module 19: Third-Party Risk Management

- Topic 1: Evaluating Vendor Risks
- Topic 2: Security Assessments for Third Parties
- Topic 3: Contracts and SLA Considerations
- Topic 4: Auditing Third-Party Security Practices

Module 20: Governance, Risk, and Compliance (GRC)

- Topic 1: Understanding GRC
- Topic 2: Aligning Security with Business Objectives
- Topic 3: Regulatory Compliance
- Topic 4: Implementing GRC Solutions

Term 6: Cyber Threat Intelligence

Module 21: Introduction to Threat Intelligence

- Topic 1: The Role of Threat Intelligence
- Topic 2: Types of Threat Intelligence
- Topic 3: Sources of Threat Intelligence
- Topic 4: Integrating Threat Intelligence

Module 22: Analyzing Threat Intelligence

- Topic 1: Threat Assessment Techniques
- Topic 2: Tools for Analyzing Threats
- Topic 3: Collaborating on Threat Intelligence
- Topic 4: Threat Intelligence Frameworks

Module 23: Building a Threat Intelligence Program

- Topic 1: Steps to Building a Program
- Topic 2: Challenges in Implementation
- Topic 3: Measuring Effectiveness
- Topic 4: Case Studies

Module 24: Cyber Intelligence Sharing

- Topic 1: Sharing Models
- Topic 2: Contingencies For Sharing
- Topic 3: Legal Issues
- Topic 4: Industry Best Practices

Term 7: Penetration Testing and Red Teaming

Module 25: Introduction to Penetration Testing

- Topic 1: What is Penetration Testing?
- Topic 2: The Benefits of Pen Testing
- Topic 3: Penetration Testing Types
- Topic 4: Methodologies

Module 26: Tools and Techniques

- Topic 1: Tooling for Penetration Testing
- Topic 2: Reconnaissance Techniques
- Topic 3: Exploit Development
- Topic 4: Post-Exploitation Tasks

Module 27: Developing a Red Team Strategy

- Topic 1: The Role of Red Teams
- Topic 2: Creating Red Team Exercises
- Topic 3: Measuring Impact and Outcomes
- Topic 4: Post-Engagement Analysis

Module 28: Threat Simulation

- Topic 1: Simulating Cyber Attacks
- Topic 2: Behavioral Analysis
- Topic 3: Detecting Anomalies
- Topic 4: Reporting and Documentation

Term 8: Cybersecurity for Emerging Technologies

Module 29: Cybersecurity in Cloud Computing

- Topic 1: Overview of Cloud Security
- Topic 2: Protecting Cloud Resources
- Topic 3: Data Protection in the Cloud
- Topic 4: Compliance in the Cloud

Module 30: IoT Security

- Topic 1: Understanding the IoT Landscape
- Topic 2: IoT Vulnerabilities
- Topic 3: Securing IoT Devices
- Topic 4: Standards and Regulations

Module 31: Blockchain and Cybersecurity

- Topic 1: Blockchain Basics
- Topic 2: Security Implications of Blockchain
- Topic 3: Use Cases in Cybersecurity
- Topic 4: Challenges and Future

Module 32: Ethical Hacking and Response

- Topic 1: The Role of Ethical Hackers
- Topic 2: Legal Considerations
- Topic 3: Ethics in Hacking
- Topic 4: Career Paths

Term 9: Cybersecurity Leadership and Management

Module 33: Building a Cybersecurity Culture

- Topic 1: Role of Leadership in Security
- Topic 2: Creating a Security Culture
- Topic 3: Employee Training and Awareness
- Topic 4: Measuring Culture Effectiveness

Module 34: Cybersecurity Team Management

- Topic 1: Structuring Security Teams
- Topic 2: Team Leadership Skills
- Topic 3: Performance Metrics
- Topic 4: Conflict Resolution

Module 35: Financial Aspects of Cybersecurity

- Topic 1: Budgeting for Cybersecurity
- Topic 2: Cost-Benefit Analysis
- Topic 3: ROI Measurement
- Topic 4: Cyber Insurance

Module 36: Strategic Cybersecurity Planning

- Topic 1: Aligning Goals with Business Strategy
- Topic 2: Long-term Security Planning
- Topic 3: Incident Management Planning
- Topic 4: Evaluating Strategies

Term 10: Capstone Project

Module 37: Project Planning

- Topic 1: Selecting a Project Topic
- Topic 2: Defining Project Scope
- Topic 3: Resource Allocation
- Topic 4: Creating a Timeline

Module 38: Execution of the Project

- Topic 1: Building the Project
- Topic 2: Project Management Techniques
- Topic 3: Risk Management in Projects
- Topic 4: Quality Assurance

Module 39: Presentation and Defense

- Topic 1: Preparing the Presentation
- Topic 2: Engaging the Audience
- Topic 3: Responding to Questions
- Topic 4: Feedback Collection

Module 40: Project Evaluation

- Topic 1: Evaluating Project Success
- Topic 2: Lessons Learned
- Topic 3: Future Recommendations
- Topic 4: Documenting Outcomes

Conclusion

This comprehensive curriculum structure aims to develop skills in cybersecurity and its intersection with generative AI, preparing participants for challenges in this evolving field. ```

The content has been saved successfully and is ready for direct use.