AVENTURE
INFINITE POSSIBILITIES

Cybersecurity Course Content

Module 1: Introduction to Cybersecurity

- Overview of Cybersecurity
- Importance and Impact of Cybersecurity
- Key Terminology and Concepts
- Cybersecurity Threat Landscape
- Historical Cyber Attacks and Case Studies

Module 2: Network Security

- Basics of Networking
- Network Protocols and Architecture
- Firewalls, VPNs, and Intrusion Detection/Prevention Systems (IDS/IPS)
- Network Security Measures and Best Practices
- Secure Network Design and Implementation

Module 3: Cryptography

- Fundamentals of Cryptography
- Symmetric vs. Asymmetric Encryption
- Hash Functions and Digital Signatures
- Public Key Infrastructure (PKI)
- Cryptographic Protocols and Applications

Module 4: Secure Software Development

- Secure Coding Practices
- Common Vulnerabilities (e.g., OWASP Top 10)
- Code Review and Static Analysis Tools
- Software Development Lifecycle (SDLC) Security
- Security Testing and Quality Assurance

Module 5: Web Security

- Web Application Architecture
- Common Web Vulnerabilities (e.g., SQL Injection, XSS)
- Web Security Testing Tools and Techniques
- Secure Web Application Development
- Content Security Policy (CSP) and HTTPS

Module 6: Operating System Security

- Security Features of Major Operating Systems (Windows, Linux, macOS)
- Access Control Mechanisms
- Hardening Operating Systems
- Patch Management
- Malware and Anti-Malware Strategies

Module 7: Identity and Access Management (IAM)

- Authentication and Authorization
- Multi-Factor Authentication (MFA)
- Identity Federation and Single Sign-On (SSO)
- Role-Based Access Control (RBAC)
- IAM Best Practices and Tools

Module 8: Threat Intelligence and Incident Response

- Threat Intelligence Gathering and Analysis
- Incident Response Planning and Execution
- Forensic Analysis and Digital Evidence
- Incident Handling Tools and Techniques
- Post-Incident Activities and Reporting

Module 9: Risk Management and Compliance

- Risk Assessment and Management Frameworks
- Security Policies, Standards, and Procedures
- Compliance Requirements (e.g., GDPR, HIPAA, PCI-DSS)
- Security Audits and Assessments
- Business Continuity and Disaster Recovery Planning

Module 10: Ethical and Legal Aspects of Cybersecurity

- Cyber Law and Regulations
- Ethical Hacking and Penetration Testing
- Privacy and Data Protection
- Intellectual Property and Cybercrime
- Ethical Issues in Cybersecurity

Module 11: Emerging Trends and Technologies

- Cloud Security
- Internet of Things (IoT) Security
- Artificial Intelligence and Machine Learning in Cybersecurity
- Blockchain Security

- Future Directions and Career Opportunities

Practical Labs and Projects

- Network Security Simulation
- Cryptography Implementation
- Web Application Penetration Testing
- Secure Software Development Project
- Incident Response Simulation

Capstone Project

- Real-world Cybersecurity Challenge
- End-to-End Security Solution Design
- Presentation and Defense of the Project

Assessment and Certification

- Quizzes and Exams
- Practical Lab Assessments
- Final Project Evaluation
- Certification of Completion