- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
    1. Documentation
    2. Offer Letter
    3. Joining Date/ Timeline of Joining

What to Choose After this **Course:**

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course **Curriculum:**

Module 01: Implementing Internet Security Antivirus

- ✓ Lesson 01: Importance of Internet Security
- ✓ Lesson 02: Malware
- ✓ Lesson 03: Antivirus protection
- ✓ Lesson 04: Internet security tips to know

Module 02: Multi Factor Authentication

- ✓ Lesson 01: Three Main Types of MFA Authentication Methods
- ✓ Lesson 02: How Multi-Factor Authentication Works
- ✓ Lesson 03: MFA Examples
- ✓ Lesson 04: Two-Factor Authentication (2FA)
- ✓ Lesson 05: Adaptive Authentication or Risk-based Authentication

Module 03: Mobile Device Management For Industry

- ✓ Lesson 01: What is mobile device management
- ✓ Lesson 02: How mobile device management works
- ✓ Lesson 03: Application security
- ✓ Lesson 04: Identity and access management (IAM)
- ✓ Lesson 05: Endpoint security
- ✓ Lesson 06: BYOD mobile device management

Module 04: Data Loss Prevention (DLP)

- ✓ Lesson 01: DLP Basics
- ✓ Lesson 02: Who use DLP
- ✓ Lesson 03: Why we need DLP

- ✓ Lesson 04: How does DLP works
- ✓ Lesson 05: DLP solutions

Module 05: **Security Information and Event Management**

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Indexing
- ✓ Lesson 03: Analysis logs and Alerts
- ✓ Lesson 04: Dashboard creation
- ✓ Lesson 05: Event Type

Module 06: **APT Attack**

- ✓ Lesson 01: What is APT Attack
- ✓ Lesson 02: Advanced persistent threat (APT) progression
- ✓ Lesson 03: APT security measures
- ✓ Lesson 04: Application and domain whitelisting
- ✓ Lesson 05: Access control

Module 07: **Mitre Attack Framework**

- ✓ Lesson 01: Introduction to Mitre
- ✓ Lesson 02: Matrix
- ✓ Lesson 03: Tactics
- ✓ Lesson 04: Techniques and Sub-Techniques
- ✓ Lesson 05: Mitigation

Module 08: **EDR and XDR**

- ✓ Lesson 01: EDR/XDR Introduction
- ✓ Lesson 02: Common EDR/XDR Products
- ✓ Lesson 03: Kill Processes
- ✓ Lesson 04: Managing Endpoints with EDR/XDR
- ✓ Lesson 05: Use Case with SIEM, EDR and XDR

Module 09: **Unified Threat Management**

- ✓ Lesson 01: Introduction to Unified Threat Management
- ✓ Lesson 02: Feature of UTM
- ✓ Lesson 03: Benefit of using UTM Solution

Module 10: **Firewall**

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Reason to have a firewall
- ✓ Lesson 03: Modern Firewall Design
- ✓ Lesson 04: Common Firewall Technologies
- ✓ Lesson 05: Next Generation Firewall

Module 11: **ISO 27001**

- ✓ Lesson 01: Introduction to ISO
- ✓ Lesson 02: Updation in ISO 27001
- ✓ Lesson 03: Clauses
- ✓ Lesson 04: Controls