Techonquer Certified SOC Analyst

Start your learning journey without financial stress!

Course Details

Starting Date

The course begins on **28th July!**

Language

The course will be taught in **English only**.

Schedule

The batch will be on weekdays, with sessions on **Monday, Tuesday, and Wednesday after 8:30 pm to 10 pm**. Each class will be **1.5 hours long**.

Recording Access

Life time Recording Access after live class.

Budget-Friendly Course Fee

The course fee is just **₹3,500 INR**, making it budget-friendly for students. You can conveniently pay in two installments:

1

First Installment

₹2,500 at the time of enrollment

2

Second Installment

₹1,000 after 20 days

A) Introduction to Cybersecurity

- Need of Cybersecurity, CIA Triad, Threat, Vulnerability, Exploit and Risk
- Vulnerability Management and Risk Management
- Hacking and its types
- Types of Threats
- Security Controls: Preventive vs. Detective
- Defense in Depth, Offensive Security & Defensive Security

B) Introduction to Network & Security

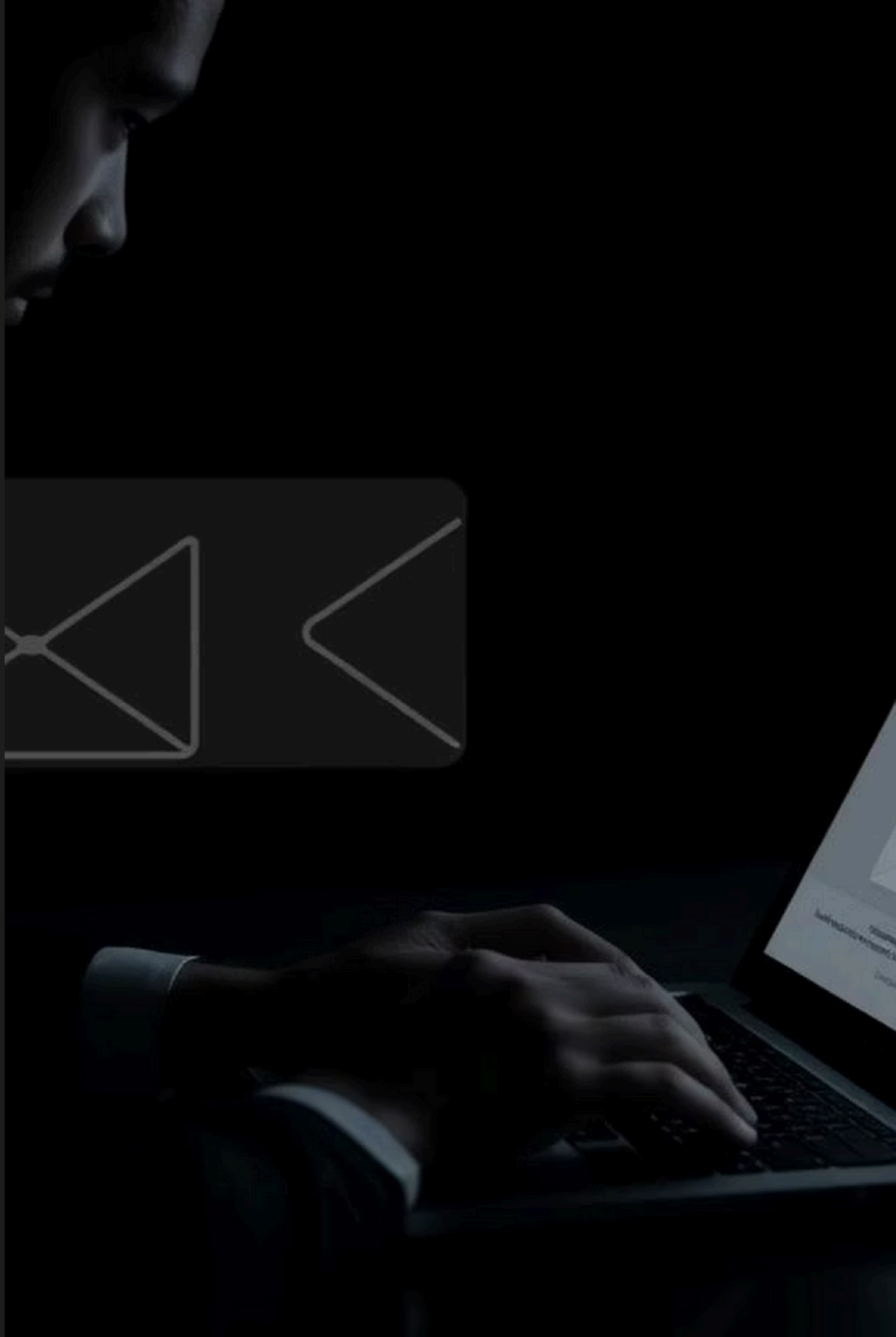
- OSI Models
- TCP/IP
- Types of Networks: LAN, WAN (Routers and Switches)
- Common Protocols: ARP, DNS, HTTP, TCP/IP
- Firewalls: Stateful, Next-gen Firewall
- Web Application Firewall
- IDS vs IPS

C) Introduction to Security Operations Centre Fundamentals (SIEM/SOC)

- People, Processes, and Technology
- Understand the SOC Fundamentals
- Introduction to Logs Management
- Types of Alerts, Alert Triage in SIEM (SOC)
- Linux log analysis
- Understand the Implementation of SOC
- SIEM Architectures (ArcSight, Splunk, Seceon)
- Log Correlation in Cybersecurity
- SOC Terminologies
- Windows log Analysis

D) Phishing Analysis

- Types of Phishing Attacks
- How Phishing Works
- How to Analyze a Phishing Email
- Email Phishing Analysis
- Phishing Attack Types
- Phishing Attack Techniques
- Phishing Attack Analysis Methodology

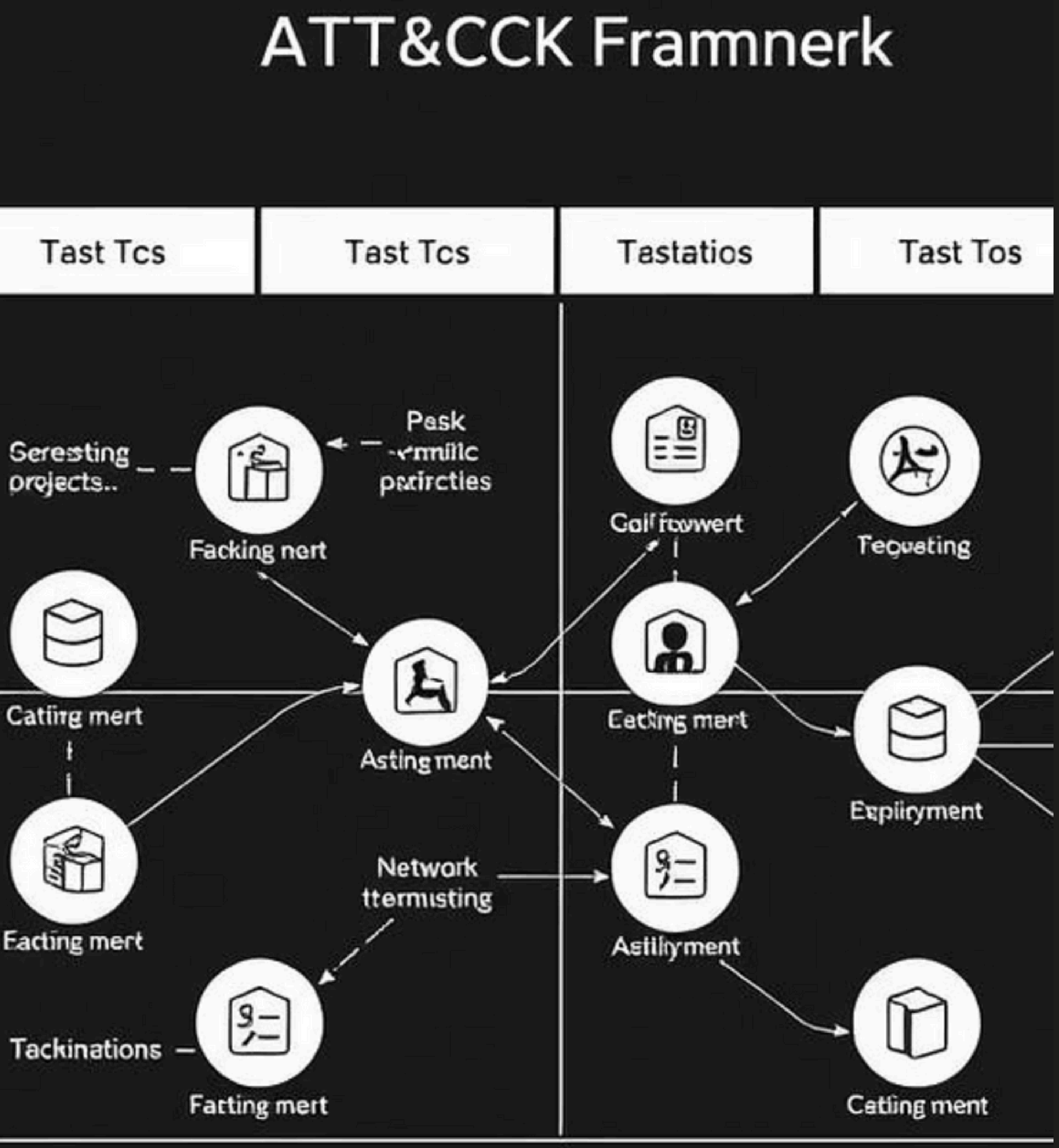


E) Endpoint Security

- Introduction to Endpoint Security
- Windows Core Processes
- What is Windows Networks Analysis
- Windows Process Analysis
- Endpoint Forensics

F) Threat Intelligence

- Introduction to Threat Intelligence
- TYPES OF THREAT INTELLIGENCE
- THREAT HUNTING METHODOLOGIES
- THREAT INTELLIGENCE LIFECYCLE
- SOURCES OF THREAT INTELLIGENCE
- Indicators of Compromise (IOCs)
- Indicators of Attack (IOAs)
- Tactics, Techniques, and Procedures (TTPs)



F) Threat Intelligence

1 **MITRE ATT&CK Framework**

2 **USE CASES OF THREAT INTELLIGENCE**