OJT Program - 6-Month Engagement Plan

Objective: The goal of this program is to equip fresh graduates with hands-on experience in IT Infrastructure services and cybersecurity, providing exposure to live projects and critical self-learning activities.

Note: This is a generic training plan that may be adjusted based on internal project needs and specific client requirements.

Module 1: Introduction to Networking and Basic IT Infrastructure

- **Topics Covered:**
  - IP Addressing (IPv4/IPv6), DNS Basics
  - Basic Networking Concepts (Subnetting, NAT, DHCP)
  - Introduction to Domain Registration (Godaddy, BigRock)
  - Basics of Web Hosting Control Panels
- **Self-Learning:**
  - Complete Udemy courses on IP addressing and DNS basics.
  - Study domain registration processes and providers.
- **Tasks:**
  - Set up a local DNS server and configure domain names for testing.
  - Register a sample domain using different domain registrars.
- **Live Implementation:**
  - Create basic network architecture and configure DNS zones for internal projects.

Module 2: Web Hosting and Cloud Security

- **Topics Covered:**
  - Open-source Web Hosting Control Panel (ISPConfig)
  - Setting up Web, Email, and Database services
  - Securing Websites with Cloudflare
  - Introduction to SSL Certificates and Implementation
- **Self-Learning:**
  - Explore tutorials and Udemy courses on hosting services, especially ISPConfig.
  - Understand Cloudflare’s features for security, CDN, and DNS.
- **Tasks:**
  - Install and configure ISPConfig to manage web hosting, email, and databases.
  - Secure a hosted website using Cloudflare and SSL.
- **Live Implementation:**
  - Deploy a WordPress site with SSL and Cloudflare integration.

Module 3: Advanced Web Hosting, Application Security & Cybersecurity Introduction

- **Topics Covered:**
  - WordPress Hosting and Security (Plugins, SSL, Firewalls)
  - Securing Websites and Web Applications
  - Introduction to Cybersecurity: EDR (Endpoint Detection & Response), XDR (Extended Detection & Response)
- **Self-Learning:**
  - Study WordPress security best practices and EDR/XDR principles.
  - Learn about EDR and XDR technologies and their importance in cybersecurity.
- **Tasks:**
  - Implement security features for WordPress sites.
  - Deploy and configure basic EDR/XDR tools for internal environments.
- **Live Implementation:**
  - Perform real-world tests on WordPress security and monitor environments with EDR/XDR solutions.

Module 4: LAN, WAN Setup & Advanced Cybersecurity Tools

- **Topics Covered:**
  - Vendor Identification and Procurement (LAN/WAN hardware)
  - Internal Data Center Setup
  - LAN/WAN Configuration and Failover Management
  - Introduction to SIEM (Security Information and Event Management)
- **Self-Learning:**
  - Study firewall and network configuration practices.
  - Learn the basics of SIEM and its role in monitoring network security.
- **Tasks:**
  - Set up LAN and WAN networks, configure firewalls.
  - Implement SIEM tools to monitor network traffic and detect security incidents.
- **Live Implementation:**
  - Deploy a small-scale internal data center and configure SIEM for security alerts.

Module 5: Firewall Security, VPNs, and XSOAR Implementation

- **Topics Covered:**
  - Firewall Configuration and Advanced Network Security

    - VPN Setup and Configuration
    - Introduction to XSOAR (Security Orchestration, Automation, and Response)
- **Self-Learning:**
    - Learn VPN and firewall best practices.
    - Explore XSOAR and its role in automating cybersecurity responses.
- **Tasks:**
    - Configure firewalls for internal and external networks, set up VPNs for secure connections.
    - Implement XSOAR to streamline incident response processes.
- **Live Implementation:**
    - Deploy a firewall and VPN solution and integrate XSOAR for security automation.

Module 6: M365 Implementation and Cybersecurity Best Practices

- **Topics Covered:**
    - M365 Tenant Creation, License Assignment
    - User Role and Permissions Management
    - Implementing Security Measures at the Tenant Level (MFA, Conditional Access)
    - Final Cybersecurity Wrap-up: Integrated EDR/XDR, SIEM, and XSOAR
- **Self-Learning:**
    - Study M365 tenant management and security configurations.
    - Review integrated security strategies using EDR/XDR, SIEM, and XSOAR.
- **Tasks:**
    - Create and manage M365 tenants, assign licenses, and implement multi-factor authentication (MFA) and conditional access.
    - Configure a complete security stack using EDR/XDR, SIEM, and XSOAR tools.
- **Live Implementation:**
    - Secure a full M365 tenant with advanced security measures and deploy integrated cybersecurity solutions.

Continuous Evaluation:

- **Monthly Evaluations:** Ongoing assessments based on task performance, technical understanding, and skill application.
- **Major Reviews:** At the end of Module 3 and Module 6 to assess progress and readiness for post-probation confirmation.