Advanced Bot Protection Course

Course Duration: 8 Hrs. **Course code: ABP**

Course Overview

The Advanced Bot Protection course equips security professionals with the knowledge and skills to detect, mitigate, and manage sophisticated automated threats targeting web applications, APIs, and mobile apps. Participants will learn how to leverage advanced bot mitigation tools, configure detection rules, and implement proactive defense strategies to safeguard critical digital assets and ensure business continuity.

What you'll learn?

- Understand modern bot threats, attack types, and their business impacts.
- Configure and deploy advanced bot protection solutions.
- Detect and classify malicious versus legitimate automation traffic.
- Integrate both protection with security operations and incident response workflows.
- Analyze bot attack reports to optimize defense strategies.

Target Audience

Security Engineers and SOC Analysts.

- Application Security Specialists.
- Network and Cloud Security Professionals.
- IT Operations Teams managing digital platforms.
- Professionals responsible for protecting online services from automation abuse.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Pre-Requisites

Basic understanding of cybersecurity principles.

- Familiarity with HTTP, APIs, and web application architecture.
- Experience with security tools or traffic monitoring is beneficial but not mandatory.

Course content

Module 1: Introduction to Advanced Bot Threats

- Types of bots: malicious, benign, and mixed purpose
- Common attack vectors (credential stuffing, scraping, DDoS, etc.)
- Business risks and industry case studies

Module 2: Bot Detection Techniques

- Behavioral analysis and machine learning models
- Device fingerprinting and browser challenges
- Identifying evasion techniques used by advanced bots

Module 3: Deploying Advanced Bot Protection Solutions

- Architecture and integration with existing security stack
- Configuring bot protection rules and thresholds
- Securing APIs and mobile applications

Module 4: Incident Response and Mitigation Strategies

- Real-time bot attack response workflows
- Automation of bot mitigation with SOAR platforms
- Reducing false positives and ensuring user experience

Module 5: Reporting, Analytics, and Continuous Optimization

- Using dashboards and attack analytics
- Reviewing and fine-tuning detection policies