multisoft
Systems

Incapsula (Imperva Cloud WAF) Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

Incapsula (Imperva Cloud WAF) Training by Multisoft Systems is designed to help professionals gain practical expertise in securing web applications, APIs, and enterprise websites against modern cyber threats. This training provides in-depth knowledge of Imperva Cloud Web Application Firewall (WAF), DDoS protection, bot mitigation, CDN integration, SSL security, and advanced traffic filtering techniques used by global enterprises.

Module 1: Web Application Security Fundamentals

- ✓ Overview of web application architecture
- ✓ Common vulnerabilities (OWASP Top 10)
- ✓ SQL Injection, XSS, CSRF, file inclusion attacks
- ✓ Role of Web Application Firewall (WAF)
- ✓ Signature-based vs behavior-based protection
- ✓ Introduction to cloud-based security models

Module 2: Introduction to Imperva Cloud WAF (Incapsula)

- ✓ Platform overview and capabilities
- ✓ Incapsula architecture and components
- ✓ Reverse proxy and traffic inspection flow
- ✓ CDN + WAF + DDoS protection integration
- ✓ Global PoPs and traffic routing
- ✓ Security layers and request lifecycle

Module 3: Application Onboarding & Deployment

- ✓ Adding a website to Incapsula
- ✓ DNS redirection and proxy setup
- ✓ SSL/TLS certificate configuration
- ✓ Domain validation and verification
- ✓ Traffic cutover strategy
- ✓ Initial security profile setup
- ✓ Testing and validation of protected applications

Module 4: WAF Policy Configuration

- ✓ Default security rules and policies
- ✓ Custom rule creation (URL, headers, IP, country)
- ✓ IP whitelisting and blacklisting

- ✓ Geo-location blocking
- ✓ Rate limiting configuration
- ✓ Session and cookie-based controls
- ✓ Virtual patching concepts

Module 5: Bot Protection & Access Control

- ✓ Bot detection mechanisms
- ✓ Good bots vs malicious bots
- ✓ CAPTCHA and JavaScript challenges
- ✓ Device fingerprinting techniques
- ✓ User behavior analysis
- ✓ API protection strategies
- ✓ Login protection and brute-force prevention

Module 6: DDoS Protection & Traffic Filtering

- ✓ Types of DDoS attacks (L3, L4, L7)
- ✓ Layer 7 DDoS mitigation strategies
- ✓ Traffic filtering rules
- ✓ Challenge-response mechanisms
- ✓ Automatic attack detection
- ✓ Traffic anomaly identification
- ✓ Real-time mitigation techniques

Module 7: CDN & Performance Optimization

- ✓ CDN fundamentals
- ✓ Content caching strategies
- ✓ Cache rules and TTL settings
- ✓ Dynamic vs static content handling
- ✓ Load balancing basics
- ✓ Failover and high availability

- ✓ Performance monitoring and tuning

Module 8: Monitoring, Logs & Reporting

- ✓ Dashboard overview
- ✓ Traffic analytics and insights
- ✓ Security event logs
- ✓ Attack reports and trends
- ✓ Log export and SIEM integration
- ✓ Alert configuration and notifications
- ✓ Compliance and audit reporting

Module 9: Advanced Security Features

- ✓ API security and protection
- ✓ Data masking and sensitive data protection
- ✓ Custom security policies
- ✓ Integration with DevSecOps pipelines
- ✓ Automation using APIs
- ✓ Multi-site and multi-domain management

Module 10: Troubleshooting & Best Practices

- ✓ Identifying and resolving false positives
- ✓ Debugging blocked requests
- ✓ Traffic bypass scenarios
- ✓ Performance vs security tuning
- ✓ Best practices for WAF deployment
- ✓ Incident response strategies
- ✓ Real-world use cases and case studies