Securing Applications and APIs with F5 Distributed Cloud Services

Category: Networking & Security | **Vendor:** F5

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

Tentatively named "Protecting Web Applications and APIs with F5 Distributed Cloud WAAP" this is a security course covering all major web application firewall, bot defense, DoS protection, and API discovery/protection components offered through the XC WAAP console with the exception of SOC-based DoS protection. The course explores the header and method elements of HTTP which must be recognized to configure protection from external client vectors. Students will exploit vulnerabilities in the target application in before-and-after learning scenarios. Major topics are web application firewall policies, attack signatures, threat campaigns, and differentiation between positive and negative security. We will address handling violations, false positives, and how to manage security events with exclusion rules. The course then takes a deep dive into controlling HTTP request flows at layer 7 with service policies. We will configure bot defense and threat mitigation using machine learning and artificial intelligence. Additional topics include discovery of public API endpoints and securing those endpoints. The course wraps up with API automation using Postman environments, collections, and variables.

About This Course

- Module 1: Introduction to Distributed Cloud WAAP and WAF Deployment
- Module 2: Setting the Stage: Analyzing Web Applications and HTTP
- Module 3: Exploiting Web Application Vulnerabilities
- Module 4: Mitigating Threats with Web Application Firewall Policies
- Module 5: Manage Security Events with Exclusion Rules
- Module 6: Mitigating Threats with Service Policies
- Module 7: Bot Defense
- Module 8: Mitigate Threats using Machine Learning and Artificial Intelligence
- Module 9: Protecting Your Public APIs
- Module 10: API Automation using Postman

Who Should Attend

The course is designed for DevOps, SecOps, NetOps, and application developers who have foundational knowledge of F5 Distributed Cloud services.

Prerequisites & Entry Requirements

General Prerequisites:

Administering Applications in F5 Distributed Cloud Services

Learning Outcomes

Upon successful completion of this course, participants will be able to:

By the end of this course, you will be able to:

- Deploy and manage F5XC WAAP to mitigate the OWASP Top 10 - via WAF Policy and via Service Policy
- Deploy F5XC WAAP to mitigate bot traffic
- Deploy F5XC WAAP to mitigate DDoS attacks at layers 3, 4, and 7
- Use F5XC WAAP to automatically discover and secure APIs

Detailed Course Outline

Intro

- Overview of how F5XC WAAP protects web apps in any cloud, edge, or on-premises environment
- Defining the core features: WAF, bot defense, DDoS protection, and securing APIs

Module 1: Introduction to Distributed Cloud WAAP and WAF Deployment

- Exploring the security flow through application proxy
- Lab: Deploy Juice Shop (target application) on an HTTP load balancer and configure API endpoint discover

- Create load balancer and connect origin pool to expose Juice Shop application
- Enable API discovery (so that we can discuss API protection and have ready examples)
- Run some traffic and review request log

Module 2: Setting the Stage: Analyzing Web Applications and HTTP

- Overview of web application communication elements

- Overview of HTTP message structure (headers and methods)

- Parsing HTTP requests

- Lab: Exploring the target application

Module 3: Exploiting Web Application Vulnerabilities

- A taxonomy of attacks: the threat landscape

- Common exploits against web applications (OWASP Top 10, OWASP API)

- Lab: Exploiting web application vulnerabilities

- SQL injection

- Cross-site scripting

- Poison byte

- Forceful browsing

Module 4: Mitigating Threats with Web Application Firewall Policies

- Defining web application firewall processing at layer 7

- Applying different protections to a load balancer

- Defining violations and false positives

- Reviewing RFC 2616 as it drives protocol compliance

- Differentiating positive and negative security

- Differentiating blocking and monitoring actions

- Reviewing security event logging

- Defining Threat Campaigns

- Defining Attack Signatures

- Lab: Create App Firewall, enable blocking mode, attach to load balancer

- Lab: Launch XSS attack and observe security processing in the log

- Lab: Launch SQL injection attack and observe security processing in the log

- Lab: Launch poison null byte attack and observe security processing in the log

Module 5: Manage Security Events with Exclusion Rules

- Defining exclusion rules
- Analyzing elements and contexts of exclusion rules
- Lab: Create an Exclusion Rule for Two Attack Signature IDs

Module 6: Mitigating Threats with Service Policies

- Differentiating protections at namespace vs. load balancer levels
- Exploring service policy rules, policies, and policy sets
- Handling traffic flow
- Enforcing layer 7 elements of HTTP processing
- Lab: Practicing service policy protections for geolocation enforcement, file types enforcement, method and path enforcement, and IP address enforcement.

Module 7: Bot Defense

- Classifying and categorizing bots (good/suspicious/malicious)
- Reviewing bot signatures
- Configuring bot defense on the XC load balancer
- Lab: Mitigating an attack from an automated agent (python scripts for bad traffic and credential stuffing/brute force)

Module 8: Mitigate Threats using Machine Learning and Artificial Intelligence

- Defining Malicious User Detection

- TLS fingerprinting
- JavaScript challenges/client side defense
- Lab: Deploying Machine Learning

Module 9: Protecting Your Public APIs

- Defining an API
- Defining API specifications
- Defining a RESTful API
- Recognizing API endpoints
- Defining Shadow APIs
- Defining OpenAPI 3.0 and the Swagger specification
- Analyzing API routing in F5XC
- Analyzing API protection in F5XC

- App firewall (OWASP vulnerabilities)
- CAPTCHA/JS challenges
- Network firewall
- API usage characterizations
- User anomaly detection
- API rate limiting (threshold configuration)
- API Learning
- Endpoint learning
- Schema learning
- Behavioral firewall/business logic markup
- Lab: Machine Learning Lab

- Review discovered APIs
- Configure malicious users mitigation
- Configure user identification
- Configure load balancer
- Test XSS (without WAF policy)

Module 10: API Automation using Postman

- Introduction to Postman

- Defining environments

- Defining collections

- Reviewing variables

- Lab: Use a postman collection to create a WAF policy for a namespace

- Lab: Use a postman collection to create service policies for a shared namespace

Skills You Will Learn:

By the end of this course, you will be able to:

- Deploy and manage F5XC WAAP to mitigate the OWASP Top 10 - via WAF Policy and via Service Policy
- Deploy F5XC WAAP to mitigate bot traffic
- Deploy F5XC WAAP to mitigate DDoS attacks at layers 3, 4, and 7
- Use F5XC WAAP to automatically discover and secure APIs

Frequently Asked Questions

Q: What delivery options are available for Securing Applications and APIs with F5 Distributed Cloud Services?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Securing Applications and APIs with F5 Distributed Cloud Services course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Securing Applications and APIs with F5 Distributed Cloud Services training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Securing Applications and APIs with F5 Distributed Cloud Services?

Yes, we provide corporate training, dedicated training, and closed classes for Securing Applications and APIs with F5 Distributed Cloud Services. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Securing Applications and APIs with F5 Distributed Cloud Services, F5 Networks, XC-WAAP

Q: Why choose Nexus Human for Securing Applications and APIs with F5 Distributed Cloud Services?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Securing Applications and APIs with F5 Distributed Cloud Services training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)