Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

Securing Applications and APIs with F5 Distributed Cloud Services

CODE:	LENGTH:	PRICE:
F5N_F5XC-SAA	24 Hours (3 days)	£2,995.00

Description

Learn about all major web application firewall, bot defense, and API discovery/protection components offered through the F5XC WAAP console. Explore the header and method elements of HTTP which must be recognized to configure protection from external client vectors. Exploit target application vulnerabilities in before-and-after protection scenarios. Explore web application firewall policies, attack signatures, threat campaigns, and differentiation between positive and negative security. Address handling violations, false positives, and how to manage security events with exclusion rules. Take a deep dive into controlling HTTP request flows at layer 7 with service policies. Configure bot defense and threat mitigation using machine learning and artificial intelligence. Discover and secure public API endpoints. Complete the course working with API automation using Postman environments, collections, and variables.

Audience

This course is intended for those with little to no knowledge of F5 Distributed Cloud WAAP.

Prerequisites

Before taking *Securing Applications and APIs with F5 Distributed Cloud Services*, make sure you have completed the following:

-

Administering Applications in F5 Distributed Cloud Services (ILT)
Suggested Prework
In addition to meeting the prerequisite, the following skills are helpful:

- Experience with any cloud provider
- Basic networking skills including a basic understanding of routing, firewalls (application and network layer), proxies and load balancers
- Basic understanding of Kubernetes, pods, and containerization concepts

Programme

Introduction and Agenda

- Lesson Objectives
- Lesson Topics
- Overview of how F5XC WAAP protects web apps in any cloud, edge, or on-premises environment
- Defining core features and use cases

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: Overview of Web Application Processing

- Overview of web application communication elements
- Overview of HTTP message structure (headers and methods)
- Parsing HTTP requests
- Lab: Exploring the target application

Module 3: Overview of 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
    - Bypass security using a poison null 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: Deploying 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 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

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.