Cel szkolenia:

The BIG-IP Application Security Manager course gives participants a functional understanding of how to deploy, tune, and operate BIG-IP Application Security Manager (ASM) to protect their web applications from HTTP-based attacks. The course includes lecture, hands-on labs, and discussion about different ASM components for detecting and mitigating threats from multiple attack vectors such as web scraping, Layer 7 Denial of Service, brute force, bots, code injection, and zero day.

Audience:
This course is intended for security and network administrators who will be responsible for the installation, deployment, tuning, and day-to-day maintenance of the Application Security Manager.

Course is based on the system version v13.1.

Plan szkolenia:

- Setting Up the BIG-IP System
  - Introducing the BIG-IP System
  - Initially Setting Up the BIG-IP System
Archiving the BIG-IP Configuration
Leveraging F5 Support Resources and Tools

Traffic Processing with BIG-IP
Identifying BIG-IP Traffic Processing Objects
Understanding Network Packet Flow
Understanding Profiles
Overview of Local Traffic Policies and ASM

Web Application Concepts
Anatomy of a Web Application
An Overview of Common Security Methods
Examining HTTP and Web Application Components
Examining HTTP Headers
Examining HTTP Responses
Examining HTML Components
How ASM Parses File Types, URLs, and Parameters
Using the Fiddler HTTP proxy tool

Web Application Vulnerabilities
OWASP Top 10 Vulnerabilities

Security Policy Deployment
Comparing Positive and Negative Security
Using the Deployment Wizard
Deployment Wizard: Local Traffic Deployment
Deployment Wizard: Workflow
Reviewing Requests
Security Checks offered by Rapid Deployment
Configuring Data Guard

Policy Tuning and Violations
Post-Configuration Traffic Processing
Defining False Positives
How Violations are Categorized
Violation Ratings
Enforcement Settings and Staging: Policy Control
Defining Signature Staging
Defining Enforcement Readiness Period
Defining Learning
Violations and Learning Suggestions
Learning Mode: Automatic or Manual
Defining Learn, Alarm and Block settings
Interpreting Enforcement Readiness Summary
Configuring the Blocking Response Page

Attack Signatures
Defining Attack Signatures
Creating User-Defined Attack Signatures
Attack Signature Normalization
Attack Signature Structure
Defining Attack Signature Sets
Defining Attack Signature Pools
Updating Attack Signatures
Understanding Attack Signatures and Staging

Positive Security Policy Building
Defining Security Policy Components
Choosing an Explicit Entities Learning Scheme
How to learn: Add All Entities
Staging and Entities: the Entity Lifecycle
How to Learn: Never (Wildcard Only)
How to Learn: Selective
Learning Differentiation: Real Threats vs. False Positives

Cookies and Other Headers
ASM Cookies: What to enforce
Understanding Allowed and Enforced Cookies
Configuring Security Processing on HTTP Headers

Reporting and Logging
Reporting Capabilities in ASM
Viewing DoS Reports
Generating an ASM Security Events Report
Viewing Log files and Local Facilities
Understanding Logging Profiles

User Roles and Policy Modification
Understanding User Roles & Partitions
Comparing Policies
Editing and Exporting Security Policies
Examples of ASM Deployment Types
- Overview of ASM Synchronization
- Collecting Diagnostic Data with asmqview

Lab Project
- Lab Project 1

Advanced Parameter Handling
- Defining Parameters
- Defining Static Parameters
- Understanding Dynamic Parameters and Extractions
- Defining Parameter Levels
- Understanding Attack Signatures and Parameters

Automatic Policy Building
- Overview of Automatic Policy Building
- Choosing a Policy Type
- Defining Policy Building Process Rules
- Defining the Learning Score

Web Application Vulnerability Scanners
- Integrating ASM with Vulnerability Scanners
- Importing Vulnerabilities
- Resolving Vulnerabilities
- Using the Generic XML Scanner Output

Login Enforcement & Session Tracking
- Defining a Login URL
- Defining Session Awareness and User Tracking

Brute force and Web Scraping Mitigation
- Defining Anomalies
- Mitigating Brute Force Attacks
- Defining Session-Based Brute Force Protection
- Defining Dynamic Brute Force Protection
- Defining the Prevention Policy
- Mitigating Web Scraping
- Defining Geolocation Enforcement
- Configuring IP Address Exceptions

Layer 7 DoS Mitigation
- Defining Denial of Service Attacks
- Defining General Settings L7 DoS profile
- Defining TPS-Based DoS protection
Defining Operation Mode
Defining Mitigation Methods
Defining Stress-Based Detection
Defining Proactive Bot Defense
Using Bot Signatures

ASM and iRules
Defining Application Security iRule Events
Using ASM iRule Event Modes
iRule Syntax
ASM iRule Commands

XML and Web Services
Defining XML
Defining Web Services
Configuring an XML Profile
Schema and WSDL Configuration
XML Attack Signatures
Using Web Services Security

Web 2.0 Support: JSON Profiles
Defining Asynchronous JavaScript and XML
Defining JavaScript Object Notation
Configuring a JSON Profile

Review and Final Labs

Wymagania:

Before attending the Troubleshooting, ASM, DNS, APM, AAM, AFM, VIPRION or iRules courses is mandatory:

- to take part in the BIG-IP Admin or LTM course
- or possession of F5-CA or F5-CTS LTM certification
- or pass special assessment test with score 70% or greater.

To take assessment test:

**Step 1: get an account on F5 University** [https://university.f5.com](https://university.f5.com)
**Step 2: goto My Training and find Administering BIG-IP Course Equivalency Assessment**
Take the test. Pass mark is 70%
**Step 3: take a screen shot as proof of results**
If this prerequisite is not met, F5 Networks have the right to refuse entry to the class.
Poziom trudności

Certyfikaty:

The participants will obtain certificates signed by F5 Networks (course completion). This course also will help to prepare you for the F5 Networks ASM Specialist certification (F5-CTS) exams Exam 303 - ASM Specialist, which is available through the Pearson VUE test centers.

Prowadzący:

Certified F5 Networks Trainer.