TRITON AP-DATA
v8.0 Course 201

OVERVIEW
During this three day training course, you will learn how to install, configure, administer, and support TRITON AP-DATA. Through instruction, demonstrations, and hands-on lab practice exercises, you will learn the requirements and recommendations to successfully deploy TRITON AP-DATA in a variety of network environments. You will develop expertise in creating data security policies, fingerprinting structured and unstructured content, data discovery, endpoint configuration and deployment, incident management, reporting, and system architecture.

COURSE OBJECTIVES
- Understand the fundamentals of DLP technology
- Use Policy Wizard and PreciseID Fingerprinting
- Understand Data Discovery
- Review Incidents and Reports
- Configure initial setting
- Configure the Protector
- Create different policy levels
- Understand the integration between TRITON AP-DATA and TRITON AP-WEB
- Test TRITON AP-DATA policies on TRITON AP-WEB
- Perform a backup of the management server
- Understand best practices for configuration and implementation

INTENDED AUDIENCE
- Channel Partners: Consultants, system architects, integrators and planners who help customers with TRITON AP-DATA implementations
- Websense Sales Engineers: Websense personnel who provide pre-sales and post-sales support for TRITON AP-DATA

DURATION
- 3 Days

FORMAT
- Instructor-Led Training (ILT)

PREREQUISITES
- TRITON APX 101 Online Technical Training
- TRITON AP-DATA 101 Online Technical Training

CERTIFICATION REQUIREMENTS
- Instructor-Led Training (ILT)
- 201 Part 1 Exam (Multiple Choice)
- 201 Part 2 Exam (Hands-On Lab)
Day 1

1) Introductions
   a) Participant introductions
   b) Logistics
   c) Course Objectives

2) TRITON APX Solution Overview
   a) TRITON AP-DATA, TRITON AP-ENDPOINT, TRITON AP-EMAIL and TRITON AP-WEB

3) Introduction to TRITON AP-DATA
   a) Data Loss Prevention (DLP)
   b) Cost of a data breach
   c) Websense Data Security solution

4) TRITON AP-DATA Product Architecture
   a) Manager, Policy Engine, PE Package, Protector, DSS Server
   b) Deployment process
   c) Integration with TRITON AP-WEB and TRITON AP-EMAIL
   d) Agents & Endpoint

5) Installation and Initial Setup
   a) System requirements
   b) Port configuration
   c) Basic deployment process
   d) Task distribution and load balancing
   e) Component architecture

6) Understanding Policies
   a) Policies and Rules
   b) Creating Policies

Day 2

7) Stateful DLP
   a) Cumulative Rules

8) Classifiers
   a) Content Classifiers

9) Unstructured Fingerprinting
   a) Fingerprinting components
   b) Types of File Fingerprinting
   c) PreciseID
   d) Fingerprinting Task

10) Structured Fingerprinting
    a) Database records
    b) Configuring

11) Machine Learning
    a) Overview
    b) Configuring
    c) Outliers

12) Conditions
    a) Conditional policy logic
    b) Configuration

13) Resources
    a) Data Security policy resources
    b) Rule Source and Destination
    c) Action Plans
    d) Remediation
    e) Creating Rules
    f) Policy Levels
14) The Protector Module
   a) Classic Protector
   b) Installation
   c) Monitoring and configuration
   d) Bypass and troubleshooting

15) Mobile Agent
   a) Mobile Agent architecture
   b) Status and Configuration

16) ISA/TMG, Printer and SMTP Agents
   a) Agent Overview
   b) Agent architecture
   c) Agent setup and configuration

17) FCI Agent
   a) FCI Agent architecture
   b) FSRM installation and configuration
   c) FCI discovery tasks

18) Data Endpoint
   a) Endpoint overview
   b) Endpoint application monitoring
   c) Endpoint discovery
   d) Creating & deploying the Endpoint package
   e) Endpoint Profiles, Properties, Resources and Action Plans

19) Data Discovery: Data at Rest
   a) Crawler
   b) Configuring file system discovery
   c) Discovery policy templates