FORCEPOINT
POWERED BY Raytheon

AP-DATA

ADMINISTRATOR COURSE (ILT)

OUTLINE

TRAINING BY

NEWBERRY GROUP

REGISTRATION

Online: www.newberrygroup.com/Training/Websense-Training.aspx
E-mail: training@thenewberrygroup.com
Phone: 636.442.5766

TRITON AP-DATA Administrator Course

COURSE SPECIFICS

Intended audience

- **End-User/Customers:** System administrators, network security administrators, IT staff
- **Channel Partners:** Sales Engineers, consultants, implementation specialists

Format

- Instructor-Led training (Classroom training)

Duration

- 3 days

Pre-requisites

- None

Certification requirements

- Completion of all course sessions
- Configured lab exercises
- Certification exam (multiple choice)

Overview

During the three days, you will learn how to test existing deployment, how to administer policies and reports, handle incidents and endpoints, upgrade and manage the AP-DATA system. You will develop skills in creating data policies, building custom classifiers and using predefined policies, incident management, reporting, and system architecture and maintenance.

Course objectives

- Understand the deployment
- Create and use custom classifiers
- Use predefined classifiers, rules and policies
- Control various channels – network, file discovery and endpoint agents
- Review Incidents and Reports
- Perform the backup and restore for logs and other data
- Perform semi-automatic failover
- Archive incidents and forensics

Day 1

1) **Intercepting with AP-WEB and AP-EMAIL**
   a) Checking the WCG configuration
   b) Checking the AP-EMAIL configuration
   c) Monitoring vs. blocking mode
   d) Intercepting TLS traffic
2) **Intercepting traffic with Protector**
   a) Protector deployment types
   b) ICAP mode
3) **Discovery with AP-DATA Servers**
   a) Classical discovery with crawler
   b) Discovery with FCI Agent
   c) OCR for image analysis
4) **Transaction Lifecycle**
   a) Processing order
   b) Custom extractors and steganography
   c) Traffic logs
5) **Methodology of DLP policy creation**
   a) Building AUP (Acceptable Use Policy)
   b) Monitoring vs blocking
   c) Classifiers, rules, c-logic, exception rules
6) **Simple classifiers**
   a) Keywords and phrases, dictionaries
   b) Regular expressions
   c) File properties

Day 2

1) **Scripts and predefined classifiers**
   a) Region-specific classifiers
   b) Industry-specific classifiers
   c) Data theft
2) **Fingerprinting and ML**
   a) Unstructured fingerprinting
   b) Structured fingerprinting
   c) Machine Learning
3) **Data Endpoint**
   a) Endpoints controlling applications and file discovery
   b) Endpoint profiles, policies and alerts
4) **Incidents and reporting**
   a) Incident lifecycle
   b) Incident reports
5) **Advanced incident workflow**
   a) Force-release feature
   b) Email based incident workflow
6) **Delegated Admins**
   a) Notifications data owners
   b) Tiered Incident Management
   c) Pseudonymization of source and destination data
   d) Setting up incident response teams

Day 3

1) **Custom action plans**
   a) Deploying simple remediation scripts
   b) SIEM Integration
2) **High Availability of AP-DATA Manager**
   a) Database partitions and file shares
   b) Full backup and restore of a AP-DATA configuration
   c) Semi-automatic failover
3) **Resource Management**
   a) Archiving old incidents and forensics
   b) Distributing fingerprints, policies and AP-DATA resources
   c) System health logs and dashboards
4) **Alerts, System Events**
   a) Configuring system alerts
   b) Scheduling reporting and maintenance
5) **Upgrades**
   a) AP-DATA Manager and AP-DATA Server upgrades
   b) Protector and Endpoint upgrades

For more information, contact Forcepoint Technical Readiness and Training at salestraining@Forcepoint.com