

SilentRunner Fundamentals

Intermediate • Three-day Instructor-led Class



AccessData®

This class is designed for security administrators, security auditors, data center managers, IT managers, system administrators, and law enforcement investigators who are responsible for responding to and investigating network irregularities. It is designed to show the student how to collect and analyze network data from a single point of control using AccessData® SilentRunner®.

During this three-day hands-on class, participants perform the following tasks:

- Identify and plan the requirements to install SilentRunner in a network environment.
- Install SilentRunner and configure the system.
- Identify the components in the SilentRunner Collector.
- Use the SilentRunner Collector interface and the tools to capture network data.
- Identify the components of the SilentRunner Data Manager.
- Use the SilentRunner Data Manager to create:
 - Database Queries
 - Columnar Queries
 - Email Evaluation Queries
 - A Graphical Evaluation Query
 - A Query with a Query Template
- Identify the components and tools in the SilentRunner Analyzer.

Prerequisites

To obtain the maximum benefit from this class, the student should also meet the following requirements:

- Knowledge and understanding of TCP/IP and Ethernet network security
- In-depth knowledge of the Open Systems Interconnection (OSI) model
- Knowledge of typical network security roles, responsibilities, and practices

Class Materials and Software

You will receive the student training manual and CD containing the training material, lab exercises and class-related information.

Module 1: Introduction

Topics

- Introduction
- Class materials and software
- Prerequisites
- Class Outline

Module 2: Installation and Deployment

Objectives

- List the features and describe the functionality of SilentRunner
- List the components of SilentRunner
- Outline the pre-installation and planning process
- Install the Standard Edition of SilentRunner

Lab

- Install the AccessData CodeMeter driver and License Manager
- Install the Microsoft SQL Server 2005 software (Optional)
- Install Silent Runner software

Module 3: Collector Interface**Objectives**

- Navigate the Collector interface
- Describe the function of the tools available in the Collector

Lab

- Navigate the SilentRunner Collector

Module 4: Configure the Collector**Objectives**

- Launch the SilentRunner Collector
- Set up automatic segmenting
- Configure the SilentRunner Collector
- Use alerts

Lab

- Use the SilentRunner Collector to:
 - Configure the sensor manager
 - Configure session options
 - Configure filtering options
 - Configure services, ports, and protocols to capture data packets
 - Create a TCPDump file
 - Use the KnowledgeBase options
 - Configure and set alert options

Module 5: Working with Network Data**Objectives**

- Collect Network Data
- Browse the KnowledgeBase
- Work with Network Data
- View the Network Topology
- View Information about Transitive Relations
- View and Record Sessions

Lab

- Perform a live collection
- Interpret the KnowledgeBase
- Search the Knowledgebase
- Print Reports
- View network topology
- Interpret network display
- View information about Transitive relations
- View packet information
- View session data

Module 6: Data Manager**Objectives**

- Summarize the Data Manager functionality
- Describe the Data Manager tool functions
- Summarize the SilentRunner Analyzer functionality
- Describe the Analyzer functions

Lab

- Navigate the SilentRunner Data Manager tools
- Navigate the SilentRunner Analyzer tool

Module 7: Query the Database**Objectives**

- Create Database Queries
- Create Columnar Queries
- Create Email Evaluation Queries
- Create a Graphical Evaluation Query
- Create a Query with a Query Template

Lab

- Use the SilentRunner Database Manager to perform the following functions:
 - Extract transactions and session data
 - Extract graphics
 - Extract and reconstruct email
 - Extract and reconstruct web usage
 - Extract and reconstruct IM sessions
- Create a graphical representation of network traffic and usage with the SilentRunner Analyzer
- Create report

For a complete listing of scheduled courses or to register for available courses, see www.accessdata.com.

© 2009 AccessData Corporation – All rights reserved.

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, Forensic Toolkit, FTK, FTK Imager, Known File Filter, KFF, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are either registered trademarks or trademarks of AccessData Corporation in the United States and/or other countries. Other trademarks referenced are property of their respective owners.