

ArcSight Education: Computer-Based Training (CBT)

ArcSight Self-Study Environment for Operators version 4.5

ArcSight Self-Study Environment for Operators provides comprehensive training for users of ArcSight Enterprise Security Management (ESM)/ArcSight Express release 4.5 software, with exercises specifically intended for SOC operators. This media driven course includes a comprehensive virtual SOC environment complete with rich sample data. It includes interactive, hands-on training on common functionality and procedures needed to quickly retrain or cross train a broader group of SOC operators. The modular format of this course enables users to select the topics and lessons applicable to their jobs and allows them to return to lessons at any time to refresh what they have learned.

In particular, organizations with large and evolving SOC operator teams will find the *ArcSight Self-Study Environment for Operators* self-paced course to be an effective complement to their existing ArcSight ACSA certified core analyst group.

For those that have previously owned or used the *ArcSight Self-Study Environment for Operators version 4.0*, the 4.5 version includes additional and updated content. See the training outline below for complete details.

BENEFITS

Lower Cost of Training

- Reduce downtime through self paced scheduling flexibility
- Eliminate travel costs
- Eliminate per student pricing – buy once and train any number of operators
- Eliminate training lab costs – bundled virtual SOC provides a “ready to use” training environment

Comprehensive Content

- Equivalent to 2 days of classroom instruction
- Includes the same “Virtual SOC” environment and comprehensive exercises as the operator modules of instructor led training

Self Contained Training Environment

- Includes full training instance of ArcSight Manager, database, and connectors
- Includes multi-source rich sample data sets for training exercises
- Virtual machine fail-proof with no impact on the production environment

TRAINING MODULES	<p>Module 1: Getting Started An overview of the virtual training system, including an introduction to ArcSight ESM software as well as how to use the training modules.</p> <p>Module 2: Console Views Introduction to the main features of the ArcSight Console</p> <p>Module 3: Navigating the Console Using ArcSight Console menus and toolbars</p> <p>Module 4: Working with Resources Descriptions and concepts behind packaged content and the use of resources within ArcSight ESM 4.5</p> <p>Module 5: Filtering Events How to use filter facilities to view, prioritize and focus in on security issues</p> <p>Module 6: Examining Events How to use grid views to both broaden and narrow event examination and conduct detailed investigations</p> <p>Module 7: Analyzing Potential Threats</p>
-------------------------	---

Detail about both investigative and reference tools to pursue potential security threats and determine how to handle them

Module 8: Documenting Events

Workflow framework for documenting and escalating incidents determined to be potential security threats

Module 9: Using Dashboards and Data Monitors

How to use tabular and graphic dashboards to monitor and investigate security issues and system status

Module 10: Reporting

How to use the report production, distribution and archiving features

Module 11: Customizing Your View

Additional ways to use ArcSight presentation features to improve event display and analysis

Module 12: Getting Started with ArcSight Web

Introduction to the Web-based ArcSight interface for remote access to ArcSight ESM

Module 13: Investigating Events (Web)

How to use the ArcSight Web-based active channels and dashboards to monitor and inspect events

Module 14: Documenting Operations (Web)

ArcSight Web-based access to reporting, workflow case and alert notification facilities

To order ArcSight CBT for Operators 4.0, please contact ArcSight Sales

Part Number	Description
CBT-100-45	ArcSight CBT for Operators 4.5
CBT-100-45MEDIA	Additional Media (DVDs) for ArcSight CBT for Operators 4.5

Minimum System Requirements

CPU	Intel P4 2+ GHz (Duo core or multiple CPUs for best results)
RAM	2 GB
HDD	30 GB HD space
Resolution	1024 x 768