

PROFESSIONAL SERVICES BOOT CAMP SYLLABUS

Course description and overview

The ArcSight Professional Services Boot Camp is a four-week immersion into ArcSight products and technologies as well as techniques for deriving maximum value from those products. This training is deeply technical and highly demanding, requiring that a significant amount of material be retained by the students within a short time period.

The range of topics include operating the ESM console, building content (rules, dashboards, etc.), installing the various ArcSight products, developing FlexConnectors, Compliance Insight Packages, advanced tools and techniques, Connector Appliance, Logger, Express, and integration of all ArcSight products to create a comprehensive solution. The “course details” section of this syllabus includes an outline of all topics to be covered.

All time during the course will be utilized to the fullest extent in order to cover all of the planned material.

In addition to the prerequisite reading described later in this syllabus each week will have a reading assignment to be completed over the prior weekend.

Throughout the course many hands-on exercises will be leveraged to reinforce the topics being covered. Each week will end with a mandatory exam; the fourth week’s exam will include a practical component which consists of a team exercise followed by individual presentations.

The “completion criteria” section of this syllabus describes the requirements for successful completion of the course; certificates of completion will *not* be distributed to students who fail to meet these criteria.

Prerequisite reading (to be done **PRIOR** to attending corresponding week of training)

Week 1

- ACIA course summary
- ESM Installation and Configuration Guide
- SIEM solutions whitepaper

Week 2

- ACSA course summary
- ESM 101
- ESM System Content Reference
- ArcSight Express Installation and Configuration Guide
- ArcSight Express Forwarding Connector Configuration Guide
- ArcSight Express QuickStart Guide

Week 3

- ArcSight Logger v3.0 Administrator's Guide
- ArcSight Connector Appliance v5.0 Administrator's Guide
- ArcSight Log Management Top 10 whitepaper
- SmartConnector User's Guide
- SmartConnector configuration guides
 - Nessus NSR
 - IBM AS/400 Audit Journal File
 - Oracle Audit DB
 - UNIX OS Syslog
 - Microsoft Windows Event Log
 - Check Point FW-1/VPN-1 OPSEC NG

Week 4

- FlexConnector Developer training course summary
- FlexConnector Developer's Guide
- Compliance Insight Package for PCI Compliance Solution Guide

Prerequisite skills

The following skills and experience are required in order to be successful in this course (prescreening will be performed by ArcSight staff to ensure that all students are prepared for success):

- Windows administration
- UNIX/Linux administration
- Understanding of virtualization (preferably VMware experience)
- Some level of security experience (network, host, web, etc.)
- Familiarity with relational databases (preferably Oracle)
- Familiarity with SQL
- Familiarity with regex
- Familiarity with scripting (i.e. shell, perl, etc.)

Required materials

- laptop running an OS that the student is comfortable administrating
 - Preferred*
 - 64-bit laptop with ≥ 60 GB free space and ≥ 3 GB RAM
 - SSH client
 - SCP client
 - Remote Desktop client

Course outline

Week 1

- Welcome to Boot Camp
 - expectations (working hours, course completion criteria, syllabus review, professional conduct, etc.)
- ESM capability demonstration
- ArcSight Certified Integrator/Administrator material (see included ACIA course outline for details; timelines may be slightly different than standalone course in order to accommodate overall boot camp schedule)
- ESM installation troubleshooting exercise

Week 2

- ArcSight Certified Security Analyst material (see included ACSA course outline for details; timelines may be slightly different than standalone course in order to accommodate overall boot camp schedule)
- ArcSight Express Installation & Configuration

Week 3

- SmartConnector Deep Dive
 - SmartConnector installation
 - File reader (Apache Access Log)
 - Folder follower (AS/400 (aka. iSeries))
 - Scanner (Nessus)
 - Database (Oracle audit)
 - Syslog (Unix syslog: file, FIFO, and daemon)
 - API (Check Point w/ SSL & Windows domain events)
- Logger
- Connector Appliance
- Advanced Topics
 - Importing zones and assets
 - Network Model Wizard
 - Asset Import Connector
 - Customizing console tools
 - ESM remote authentication
 - Case customization
 - Pattern Discovery
- Troubleshooting presentation by ArcSight Support

Week 4

- FlexConnector development (see included FlexConnector Training course outline for details; timelines may be slightly different than standalone course in order to accommodate overall boot camp schedule)
- Modifying stock connectors
 - Unobfuscating parsers
 - Map files
 - Parser overrides
- Compliance Insight Packages (focus on PCI)
- Integration exercise/final assessment
 - Knowledge of the products covered
 - Ability to implement and integrate products to build solutions

Completion criteria

- Successful completion of all weekly assessment quizzes (80% or better)
- Successful completion of all exercises (verified and signed off by instructors)
- Successful completion of final exam and practical (80% or better on exam and instructor evaluation of practical solution and presentation)

** Boot camp candidates who have already completed ACSA, ACIA, or FlexConnector Training may request additional information from their registration advisor with regard to placing out of some parts of the boot camp. Those candidates attempting to place out of boot camp segments will still be responsible for successfully passing the assessment quizzes that go with these segments and may also be responsible for completing some exercises outside of class.*