

## ArcSight Skills On-Demand: Administrator

*Experience transforms competence to expertise.* The training courses offered by ArcSight University provide the foundation knowledge and skills for the security professionals working with the ArcSight Technology and Solutions.

All organizations desire their security professionals to reach the *Expert* level, to be most effective. To achieve this, hands-on experience on various aspects of the technology and the security environment is required. In general this experience is acquired on-the-job, over a period of time. ArcSight Education has developed the Skills on-Demand offering to accelerate this journey.

Skills on-Demand Provides:

### **Cloud based Labs**

- ▶ Installed and configured to provide real-world experience of an ArcSight implementation
- ▶ Learners can perform the activities at their own pace and from any convenient location via standard browser and high-speed internet connection
- ▶ Safe for experimenting, refresh to original state with “a push of a button”

### **Prescribed Activities for Analysts and Administrators**

- ▶ Documented guides to ensure most important areas of expertise are covered. The learners use the guide to access the site as well as perform the prescribed activities

## ArcSight Skills On-Demand: Administrator - Advanced Network and Asset Modeling

- ▶ Based upon Use Cases for Analysts to provide exposure to most demanding areas of daily work
- ▶ Exposure to key tasks performed by Administrators and critical areas managed by Senior Administrators
- ▶ Valuable references to resources (documentation, white papers and quick guides)

### eMentors

- ▶ eMentors are experienced professionals and instructors dedicated to providing support related to the Prescribed Activities of Skills on-Demand
- ▶ Access to eMentors is via email, with a committed turnaround time of 24 hours maximum

#### Please Note:

Each Skills on-Demand (SKOD) module is designed to be **18 hours of hands-on activity spanned over 14 days of access to the Labs.**

### Delivery Options

- ▶ Eighteen hours web-based access over a fourteen day period

### Prerequisites

To be successful in the advanced activities in this Skills on-Demand, you will have:

- ▶ Successfully completed ArcSight ESM Administrator **and**
- ▶ At least one additional course such as the ArcSight SmartConnector Foundations and Tool Kit **or**
- ▶ ArcSight Security and Authentication Skills On-Demand module

## Advanced Network and Asset Modeling Module

The following module is intended to give an Administrator of an ArcSight ESM installation the opportunity to perform advanced Network and Asset modeling related configuration tasks in a hands-on, non-production environment.

Some common administrative tasks associated with Network and Asset modeling within ArcSight ESM are:

Using advanced correlation capabilities, you can:

- ▶ Organizing network segments into Zones and grouping them in a logical fashion
- ▶ Organizing and grouping Assets and assigning appropriate categories such as business impact and criticality
- ▶ Maintaining and reassigning Zones in accordance with network infrastructure changes

### Activities Included in this Module:

The activities in this module include:

- ▶ Build the Network Model and verify that Zones are applied to events so that outbreaks can be tracked across Zones
- ▶ Set up an ArcSight Nessus SmartConnector to automatically populate the Asset model and Vulnerability status
- ▶ Assign appropriate categories to mission critical Assets so that the CISO can see the business impact as outbreaks are happening
- ▶ Extend the Network Model to differentiate between two separate network segments with overlapping IP address ranges

## What are our customers saying?

*“The big difference between the traditional training classes and this training is that you get the exercise and the expected result – how you get to the result is up to you. The exercises are designed in a way where you have to work with the entire system.”*

*“The benefit of this training, from a cost perspective is that you don’t have to travel, you don’t have to use 3 full days but you can fit it into your daily work. I don’t see SKOD as a replacement for traditional training classes, but more as a great opportunity to get a “brush up” on already learned skills, where you meet challenges you might not meet in your daily environment.”*