INV110 – Introduction to ArcSight Investigate

Adoption Readiness Tool (ART)

The Adoption Readiness Tool (ART) provides initial and ongoing enablement to your users to ensure that you get the most out of your software. ART is a cost-effective, comprehensive IT education, documentation and performance support solution. ART provides pre-built simulation-based courses in Micro Focus software that can be accessed by users anytime, anywhere.

ART content provides easy access to self-paced learning content enabling your users to not only dive into an online course, but also to gain direct access to individual components to quickly master specific tasks.

- Access printable job aids targeted towards specific application tasks.
- View or practice a task in a simulated environment.
- Experience full learning with key terms and concepts, product demonstrations and selfassessments by viewing the entire course.

Regardless of which route chosen, users will gain an understanding of the important key concepts, as well as gain competency in both the navigation and functionality of the application.

Course Description

This course is a good starting point for a security analyst who is new to the ArcSight Investigate product to learn the fundamentals of ArcSight Investigate. You learn how to search and analyze event data for anomalies using the pre-defined query searches (and fieldsets) that are specific to security and threat investigating. Also, you learn how to create visual graphics that provide further insights to your search results. This course includes hands-on simulations that take you through real-life scenarios that occur when security threats arise in your organization.

Audience/Job Roles

This course is intended for Incident Response Managers, Hunt Teams, and Level 1 Analysts that monitor an organization's operations for security threats.

Course Objectives

Upon successful completion of this course, you should be able to:

- Describe the concept of security investigation
- Recognize the components and capabilities of ArcSight Investigate
- Recognize the views a L1 analyst has in a Security Operations Center and ArcSightInvestigate
- Within the user interface: o Set up users, groups and roles
  - Search, analyze, navigate and manage different types of data
  - Produce some fundamental search techniques
  - Create visual graphics and chart the search results

Prerequisites / Recommended Skills

To be successful in this course, you should have the following prerequisites or knowledge.

- High speed Internet connection
- Web browser (IE9+ or Firefox 8.5+), note: Chrome is not compatible
- Understanding of ArcSight ESM
- Basic understanding of web technologies, such as IP addresses, network assets
- Have an interest in cybersecurity

Course Topics

Modules	Objectives
Introduction to ArcSight Investigate	
Module 1: Introduction to Security Investigation	• Security Operations (SecOps) Role • Conducting a Security Investigations • Creating a Successful Security Investigation • Gathering Data for Analysis • Importance of Automation
Module 2: Introduction to ArcSight Investigate	• Basic Investigate Architecture and ADP Integration • Search Components and Capabilities • Investigate User Interface • Level 1 Analyst Workflow

Module 3: Users and Roles	• Security Hunt Teams • Users • User Profile • Create a User** • User Groups • Add Users to a Group** • Remove a User from a Group** • Delete a Group** • Roles • Create Roles with Permissions**
Module 4: Analyst Workflow	• Interface and Features • Dashboard and Widgets • Searching Event Data • Setting a Time Range • Setting Fieldsets • Charting Data • Managing Search Results • Compare Outbound Data** • Analyze URLs** • Network Flow-type Analysis** • Search and Display the McAfee Detections
Module 5: Fundamental Searches	• Search Types • Create Full Text Search** • Create Filed Based Search** • Create Hashtag Search** • Create a Bar Chart of your Search Results** • Create a Comparison Line Chart** • Exporting Search Results
Module 6: What's new in Investigate 2.1	• Describe the New Features • Create Visualizations** • Find a User** • Look up Lists** • Create Searches** • Save Searches**

* Indicates a simulation.