RSA NetWitness Platform Foundations 11.3

Course Objectives

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

- Describe the RSA NetWitness® Platform architecture
- Describe the NetWitness core components and their functions
- Describe how metadata is created
- Differentiate between meta keys, meta values, sessions and events
- Investigate data using queries and customized displays
- Filter data using rules
- Create new meta values using rules and feeds
- Deploy RSA-provided reports
- Create alerts using ESA and reporting rules
- Describe the use of the Endpoint Insights Agent
- Describe the basic concepts of RSA NetWitness UEBA
- Create and manage incidents

Course Outline

RSA NetWitness Platform Overview
- RSA NetWitness Platform components and architecture
- RSA NetWitness Data
- RSA NetWitness Interface

Investigation Basics
- What is metadata?
- Differentiating between packets and logs
- Differentiating between data and metadata
- Customizing the investigation screens
- Viewing reconstructed events
- Writing simple and complex queries
- Describing the purpose of meta key indexing
- Customizing data and meta data displays
- Creating data visualizations
- Creating meta groups
- Creating custom column groups
- Using complex queries, drills and views to perform investigations
- The Context Hub

Refining the Dataset
- Filtering data with rules
- Taxonomy concepts for metadata
- Using Application rules to create new meta
- Using Correlation rules to create new meta
- Deploying content from RSA Live to create new meta
- Describing how parsers populate meta keys

- Creating feeds
- Using alerts and metadata to investigate potential threats

Reporting and Alerting

- Configuring the Reporting Engine and RESPOND
- Creating reports
- Creating alerts to identify future threats

Event Stream Analysis

- Configuring ESA
- Creating ESA alerts
- Best practices and approaches

Incident Management and Respond

- Components of the RESPOND module
- Viewing alerts and incidents
- Incident Rules

Endpoint Insights Agent

- Insight configurations
- Endpoint investigation
- Hots/Files

UEBA Concepts

- How UEBA works
- Analyzing logon activity