Module 1 – Introduction to ES

Overview of ES features and concepts

Module 2 – Security Monitoring & Incident Investigation

Use the Security Posture dashboard to monitor the statues of ES

Use the Incident Review dashboard to monitor the statues of ES

Take ownership of an incident and move it through the investigation workflow

Create notable events

Suppress notable events

Examine the investigation journal

Module 3 – Analyst Tool & Data Sources

Identify ES security analyst tools

Map security tools to data sources

Examine management tools for analyste dashboards

Module 4 – ES Deployment

Identify deployment topologies

Examine the deployment checklist

Understand pre-deployment requirements

Module 5 – Installation

List ES pre-installation requirements

Identify steps for downloading and installing ES

Test a new install

Module 6 – Initial Configuration

List ES pre-installation requirements

Identify steps for downloading and installing ES

Test a new install

Module 7 – Validating ES Data

Verify data is correctly configured for use in ES

Validate normalization configurations

Install additional add-ons

Module 8 – Custom Add-ons

Use custom data in ES

Create an add-on for a custom sourcetype

Describe add-on troubleshooting

Module 9 – Tuning Correlation Searches

Describe correlation search operation

سرفصل دوره splunk enterprise security

Customize correlation searches

Describe numeric vs. conceptual thresholds

Discuss the Event Sequencing Engine

Module 10 – Creating Correlation Searches

Create a custom correlation search

Manage adaptive responses

Manage content import and export

Module 11 – Lookups and Identity Management

Identify ES-specific lookups

Describe the interaction of lookups with correlation searches and other ES functions

Configure asset and identity lookups

Module 12 – Threat Intelligence Framework

Describe threat lists and threat list administration tools

Configure a new threat list