Advanced Phantom Implementation 4.10

Module 1 – Implementing Splunk and Phantom

- Review of Phantom UI and concepts
- Describe interactions between Splunk and Phantom
- Identify key concepts and data flows
- Pre-requisites for integration

Module 2 – Configuring External Splunk Search

- Describe the benefits of externalizing search to Splunk
- Configure the Phantom instance for externalization
- Configure the Splunk instance for externalization
- Use the Splunk app for Phantom Reporting

Module 3 – Sending Splunk Events to Phantom

- Configure the Phantom Add-on for Splunk
- Map CIM fields to CEF
- Send Enterprise Security notables to Phantom
- Automatically trigger Phantom playbooks for Splunk notables

Module 4 – Accessing Splunk from Phantom

- Install and configure the Phantom App for Splunk
- Ingest Splunk events into Phantom
- Use Splunk search from playbooks
- Update Splunk notable events

Module 5 – Custom Coding in Playbooks

- Phantom coding best practices
- Writing, using and managing custom functions
- Using the Phantom API in custom code
- Store and retrieve persistent data

Module 6 – Using Phantom REST

- Use Django queries to search for data in Phantom
- Use REST from other systems to access Phantom data
- Use the HTTP app to execute REST from playbooks