Advanced SOAR Implementation

Module 1 – Implementing Splunk and SOAR

- Review of SOAR UI and concepts
- Describe interactions between Splunk and SOAR
- 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 SOAR instance for externalization
- Configure the Splunk instance for externalization

- Use the Splunk app for SOAR Reporting

Module 3 – Sending Splunk Events to SOAR

- Configure the SOAR Add-on for Splunk
- Map CIM fields to CEF

- Send Enterprise Security notables to SOAR
- Automatically trigger SOAR playbooks for Splunk notables

Module 4 – Accessing Splunk from SOAR

- Install and configure the SOAR App for Splunk
- Ingest Splunk events into SOAR

- Use Splunk search from playbooks
- Update Splunk notable events

Module 5 – Custom Coding in Playbooks

- SOAR coding best practices

- Writing, using and managing custom functions

- Using the SOAR API in custom code
- Store and retrieve persistent data

Module 6 – Using SOAR REST

- Use Django queries to search for data in SOAR

- Use REST to access SOAR data

- Use the HTTP app to execute REST from playbooks