SOAR Advanced Implementation

Course Description:

This course is intended for experienced SOAR consultants who will be responsible for complex SOAR solution development and will prepare the attendee to integrate SOAR with Splunk as well as develop playbooks requiring custom coding and REST API usage.

Potential attendees have received a passing grade in all prerequisite courses and must ensure they can devote all of their attention to the class, as the course work is very challenging. Students will develop a custom solution with SOAR, Splunk and custom Python code. The labs provide requirements for the solution; the student must plan and execute the development. This will require thoughtful focus, experimentation, and problem-solving skills.

Course Duration:

2 Days

Prerequisites:

Attendees for this class must ensure that they meet all course prerequisites. This is a challenging, advanced class that draws on technical knowledge from many areas in Splunk and SOAR, and the demanding labs and course schedule leave little time to learn the basics.

To be successful, students should have a solid understanding of the following:

- Experience with Python programming
- Administering Splunk SOAR
- Developing Splunk SOAR Playbooks
- Enterprise Splunk Data Administration
- Enterprise Splunk System Administration
- Either Using or Administering Splunk Enterprise Security

Course Outlines:

Module 1 – Implementing Splunk and SOAR

- Review of SOAR UI and concepts
- Describe interactions between Splunk and SOAR
- Identify key concepts and data flows
- Prerequisites for integration

Module 2 – Forwarding Events from SOAR to Splunk

- Describe the benefits of sending events to Splunk
- Configure the SOAR instance for forwarding
- Configure the Splunk instance for forwarding
- Search for SOAR events and logs on Splunk

Module 3 – Sending Splunk Events to SOAR

- Configure the Splunk App for SOAR Export
- 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

Target Audience:

- SOAR Automation Engineers