Automating and Programming Cisco Security Solutions v1.0 (300-735)

Exam Description: Automating and Programming Cisco Security Solutions v1.0 (SAUTO 300-735) is a 90-minute exam associated with the CCNP Security Certification and DevNet Professional Certification. This exam tests a candidate's knowledge of implementing Security automated solutions, including programming concepts, RESTful APIs, data models, protocols, firewalls, web, DNS, cloud and email security, and ISE. The course, Implementing Cisco Security Automation Solutions, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

10% 1.0 Network Programmability Foundation

- 1.1 Utilize common version control operations with git (add, clone, push, commit, diff, branching, and merging conflict)
- 1.2 Describe characteristics of API styles (REST and RPC)
- 1.3 Describe the challenges encountered and patterns used when consuming APIs synchronously and asynchronously
- 1.4 Interpret Python scripts containing data types, functions, classes, conditions, and looping
- 1.5 Describe the benefits of Python virtual environments
- 1.6 Explain the benefits of using network configuration tools such as Ansible and Puppet for automating security platforms

35% 2.0 Network Security

- 2.1 Describe the event streaming capabilities of Firepower Management Center eStreamer API
- 2.2 Describe the capabilities and components of these APIs
  - 2.2.a Firepower (Firepower Management Center and Firepower Device Management)
  - 2.2.b ISE
  - 2.2.c pxGRID
  - 2.2.d Stealthwatch Enterprise
- 2.3 Implement firewall objects, rules, intrusion policies, and access policies using Firepower Management Center API
- 2.4 Implement firewall objects, rules, intrusion policies, and access policies using Firepower Threat Defense API (also known as Firepower Device Manager API)
- 2.5 Construct a Python script for pxGrid to retrieve information such as endpoint device type, network policy and security telemetry
- 2.6 Construct API requests using Stealthwatch API
  - 2.6.a perform configuration modifications
  - 2.6.b generate rich reports

30% **3.0** **Advanced Threat & Endpoint Security**

3.1 Describe the capabilities and components of these APIs

- 3.1.a Umbrella Investigate APIs
- 3.1.b AMP for endpoints APIs
- 3.1.c ThreatGRID API

3.2 Construct an Umbrella Investigate API request

3.3 Construct AMP for endpoints API requests for event, computer, and policies

3.4 Construct ThreatGRID APIs request for search, sample feeds, IoC feeds, and threat disposition

25% **4.0** **Cloud, Web, and Email Security**

4.1 Describe the capabilities and components of these APIs

- 4.1.a Umbrella reporting and enforcement APIs
- 4.1.b Stealthwatch cloud APIs
- 4.1.c Cisco Security Management Appliance APIs

4.2 Construct Stealthwatch cloud API request for reporting

4.3 Construct an Umbrella Reporting and Enforcement API request

4.4 Construct a report using Cisco Security Management Appliance API request (email and web)