Automating Cisco Security Solutions v1.1 (300-735)

Exam Description: Automating Cisco Security Solutions v1.1 (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 Automation for Cisco Security 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 Use 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 Terraform for automating security platforms

35% 2.0 Network Security

- 2.1 Describe the event streaming capabilities of Cisco Secure Firewall Management Center (formerly Firepower Management Center) eStreamer API
- 2.2 Describe the capabilities and components of these APIs
  - 2.2.a Cisco Secure Firewall Management Center and Cisco Secure Firewall Device Manager
  - 2.2.b Cisco Identity Services Engine (ISE)
  - 2.2.c pxGRID
  - 2.2.d Cisco Secure Network Analytics (formerly Stealthwatch) Enterprise
- 2.3 Implement firewall objects, rules, intrusion policies, and access policies using Cisco Secure Firewall Management Center API
- 2.4 Implement firewall objects, rules, intrusion policies, and access policies using Cisco Secure Firewall 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 Cisco Secure Network Analytics 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 Cisco Cloud Security APIs (such as Umbrella APIs, Investigate APIs)
- 3.1.b Cisco Secure Endpoint (formerly AMP for Endpoints) API
- 3.1.c Cisco Secure Malware Analytics (formerly ThreatGRID) API
- 3.1.d Cisco XDR solution APIs (such as SecureX API and Threat Response API)

3.2 Construct an Umbrella Investigate API request

3.3 Construct Cisco Secure Endpoint API requests for event, computer, and policies

3.4 Construct Cisco Secure Malware Analytics API request for search, sample feeds, IoC feeds, and threat disposition

3.5 Construct Cisco XDR solution API calls

3.6 Describe the orchestration capabilities of Cisco XDR solution

25% 4.0 Cloud, Web, and Email Security

4.1 Describe the capabilities and components of these APIs
- 4.1.a Umbrella APIs
- 4.1.b Cisco Secure Cloud Analytics (formerly Steathwatch Cloud) APIs
- 4.1.c Cisco Secure Email and Web Manager (formerly Security Management Appliance) APIs

4.2 Construct Secure Cloud Analytics API request for reporting

4.3 Construct an Umbrella API request for Reports and Policies

4.4 Construct a report using Secure Email and Web Manager API request