Service Description

Cisco Technical Security Assessment Service Subscription

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. Summary

The Cisco Technical Security Assessment Service subscription ("Services") provides Customers access to a portfolio of security assessment activities which Customer can use to evaluate its cybersecurity.

Activities may include one or more of the following:

- Penetration Testing
- Red Teaming
- Threat Modeling
- Configuration / Build Assessment
- Security Architecture Assessment
- DevOps Security Assessment
- Security Operations Assessment

2. Services Credits

The quantity of services credit units ("Credits") purchased is as set forth in the Quote. You may redeem Credits for the delivery of Cisco Technical Assessment Service activities. You are entitled to redeem the number of Credits as set forth in the Quote in each year of the Services Term. If You choose a non-standard Services Term, then Your Credits will be calculated on a pro-rata basis. For example, a one hundred (100) Credit subscription with a thirty (30) month Services Term will entitle You to the following:

- Year 1 (12 months) – 100 credits
- Year 2 (12 months) – 100 credits
- Year 3 (6 months) – 50 credits

For reference, each activity below will require five (5) Credits:

- Cisco will perform an objective-led internal penetration test of an environment with up to five hundred (500) live IP addresses, or
- Cisco will perform an external penetration test of up to sixty-four (64) live IP addresses, or
- Cisco will perform an application penetration test of up to fifteen (15) dynamic pages / endpoints and one (1) role, or
- Cisco will perform a build/configuration review of up to five (5) devices.

When Customer requests an activity, Cisco will work with Customer to define the activity scope and Credit requirements. The required Credits correspond to the length and complexity of the activity Cisco will perform. Cisco will document the activity scope and Credit requirements in a Solution Requirements Document ("SRD"). Customer will approve the SRD before Cisco will commence any activity. If Customer's Credit balance is not sufficient for the proposed activity scope, Cisco will work with Customer to refine the activity scope (where applicable) or suggest alternative options to meet Customer objective, which may include the purchase of additional Credits.

3. Notes and Limitations

The following notes and limitations apply to the Services:

3.1 Cisco will make efforts to allocate resources evenly throughout the Services Term.

3.2 Once the Credits in any year are consumed, Cisco may suspend work until additional Credits are purchased or other arrangements are agreed in writing.

3.3 Unused Credits expire at the end of their corresponding one-year subscription Services Term.

3.4 Activities must be requested by Customer and scheduled at least ninety (90) days before the end date of the Services Term.

3.5 Customer will respond to any SRDs within ten (10) Business Days and no later than five (5) Business Days in advance of any proposed delivery start dates.

3.6 Customer expressly provides Cisco with permission to conduct penetration testing or other forms of simulated cyber-attacks on the Customer's environment as set forth in the SRD for that activity. Customer will provide Cisco a letter of agency or similar documentation as proof of this permission upon Cisco's request.

3.7 Customer may not report any of Cisco's testing activities, tools, or infrastructure used in connection with the Services as malicious to any third party.

3.8 Customer will provide Cisco with prerequisites for each activity as set forth in the corresponding approved SRD. This may include connecting Cisco devices to networks, configuring devices to allow Cisco access, or providing requested credentials to access systems.

3.9 Cisco will make reasonable efforts to provide findings and an issue resolution plan.

3.10 The Services can provide insight into vulnerabilities, weaknesses, and capability gaps, but resolving these is outside the scope of the Services.

3.11 If, during an activity, a serious fault or problem in Customer's environment is discovered that Cisco believes could affect the operational status of the environment or the delivery of the engagement, Cisco may generate a Security Fault Notice ("SFN"). In such event, Cisco may suspend activities until Customer has reviewed the SFN and Customer has instructed Cisco to resume activities. In this event, Cisco may generate a Change Request which may require additional Credits.

3.12 Work may occur after Business Hours in Cisco's discretion.

3.13 Travel will be determined in Cisco's discretion.

3.14 Cisco will use commercially reasonable processes and technologies to assess Customer's cybersecurity, but Cisco does not guarantee that all vulnerabilities and weaknesses in Customer's environment will be detected.

3.15 All information Cisco collects from Customer in relation to the Services is considered Systems Information, and we will treat it as set forth in the Services Guide.

3.16 Information on Cisco's corporate policy on the disclosure of Security Vulnerabilities discovered as part of Cisco's Services is posted at: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#dsvdpcsd