Cisco Technical Security Assessment Service Subscription

This document must be read in conjunction with How Cisco Provides Services, which is incorporated into this document by reference.

The Cisco Technical Security Assessment Service subscription (“Services”) provides Customers access to a set of security assessment services which Customer can use to evaluate its cybersecurity.

Cisco Technical Security Assessment Service

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

Intended activities are reviewed and updated quarterly by Customer and Cisco.

Subscription Entitlement Consumption

The quantity of subscription credit units (“Credits”) purchased is as set forth in the Quote.

Each of the following items will consume five (5) Credits:

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

When Customer requests activities, Cisco will validate that Customer has sufficient Credits for such activities. If Customer’s Credit balance is not sufficient, Cisco will work with Customer to define and refine, where required, the activity scope. Credits required will be proportional to length and complexity of the assessment being performed. Cisco will document activity scope and credit requirements in a Solution Requirements Document (“SRD”) to be approved by Customer before commencing any activity.

Notes and Limitations

The following notes and limitations apply to the Services:

- Cisco will make efforts to allocate resources evenly throughout the Services subscription term.
- Once the Credits are used, Cisco may suspend work until additional Credits are purchased or other arrangements are agreed in writing. Any unused Credits expire at the end of a subscription term.
- Activities must be requested by Customer and scheduled at least ninety (90) days before the end date of the subscription.
- 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.
- 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.
- 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.
- Cisco will make reasonable efforts to provide findings and an issue resolution plan.
- The Services can provide insight into vulnerabilities, weaknesses, and capability gaps, but resolving these is outside the scope of the Services.
- 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.
- Work may occur after Standard Business Hours in Cisco's discretion.
- Travel will be determined in Cisco's discretion.
- Customer remains responsible for the security of its environment(s).
- 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.
- Vulnerability, weakness, and other related information that Cisco collects from Customer in relation to the Services is considered Systems Information, and we will treat it according to our security and privacy program referenced in How Cisco Provides Services.
- 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