Service Description: Advanced Services – Fixed Price

Cloud Security Assessment Service for XaaS Adoption (ASF-DCV2-XAAS-SEC)

This document describes Advanced Services Fixed Price: Cloud Security Assessment Service for XaaS Adoption.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) Glossary of Terms; (2) List of Services Not Covered. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement") If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at http://www.cisco.com/web/about/doing_business/legal/terms_conditions.html. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at: http://www.cisco.com/web/about/doing_business/legal/terms_conditions.html. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cloud Security Assessment Service for XaaS Adoption

Service Summary

Cisco will provide the Cloud Security Assessment Service for XaaS Adoption to Customer during Standard Business Hours. Cisco will conduct a workshop as a forum to understand the Customer's cloud architecture with an emphasis on the infrastructure that is interfacing with the cloud and service provider, gathering data based on control sets, conducting tools-based data validation, conducting analysis, and developing recommendations that the Customer can use as reference when the Customer is evaluating security considerations when moving to cloud. Cisco will work with Customer to develop a security assessment report for XaaS cloud adoption. The Cloud Security Assessment Report deliverable will include findings, gap analysis, recommendations and guidelines to secure the cloud environment. Cisco will evaluate and benchmark the technical controls of the security infrastructure interfacing with the cloud environment, against a pre-defined set. Cisco will consider the following industry standard controls: Network Security, Host Level Security, Application Level Security, Management and Monitoring Systems, Access, and Identity Management ("Services").

Services are limited to one (1) customer site for the workshop and security assessment.

Deliverables

- Cloud Security Assessment Report
- Summary Presentation Slide Deck

Location of Services

Services are provided remotely and up to three (3) onsite visits, as necessary.

Security Workshop

Cisco Responsibilities

- Work with Customer to establish scheduling and agenda for the workshop to be held remotely or onsite.

- Work with Customer to confirm list of all Customer stakeholders, including security and cloud subject matter experts (SMEs) participating in the workshop.
- Conduct a workshop for up to five (5) days to understand the Customer's technical controls of the security infrastructure interfacing with the cloud environment.

Customer Responsibilities

- Review with Cisco the workshop scheduling and agenda, identifying either remote or onsite location for the workshop.
- Provide a list of all Customer stakeholders participating in the workshop.
- Provide to Cisco network, security, and application infrastructure documentation and any other relevant information.
- Provide industry regulatory and non regulatory compliance requirements which may be specific to the Customer's business.

Cloud Control Set based Data Gathering and Analysis

Cisco Responsibilities

- Develop Customer specific security information gathering and assessment questionnaires.
- Conduct up to ten (10) customer interviews to collect information on the network and server architecture and security control sets.
- Review with Customer the discovery methodology and associated information gathering activities.
- Request Customer to provide the necessary network configurations and customer environment information for network device security assessment.
- Conduct security posture assessment for up to ten (10) public IP's interfacing the cloud in the Customer environment to identify and understand potential vulnerabilities in the Customer's public IP addresses interfacing the cloud.
- Document findings and analysis in the Cloud Security Assessment Report.

Customer Responsibilities

- Review with Cisco the discovery methodology and associated activities, including commands to be executed on the network devices for configuration collection during discovery and identifying the public IP address interfacing the cloud.
- Provide the necessary network configurations and environment information to Cisco for network device security assessment.
- Customer will identify the appropriate schedule for the range of times to run the security posture assessment of the public IP addresses.
- Assign a dedicated technical contact to work with Cisco, participating in security assessment discussions, and validating assumptions, business constraints, and security discovery results.
- Work with Cisco to validate the discovery results, identifying and resolving any issues discovered from the information gathered during customer interviews.
- Provide the IP address for performing the security posture assessment and required approvals from the device owners and communications as per customer policies.

Documentation and Reporting

Cisco Responsibilities

- Integrate all project documents, including information on findings and recommendations from interviews on the security control set, analysis of configuration on network devices, security posture assessment; and, document the information in the Cloud Security Assessment Report to include:
  - summary on key observations and recommendations of the assessment;
  - detailed assessment of security readiness, including cloud architecture, configuration best practices, and the viability of secure cloud approaches;
  - detailed vulnerability assessment of the publically exposed IP addresses facing the cloud;
  - leading practice and Cisco recommendations for network, applications, and security management tools.
- Work with Customer to schedule a summary review meeting, confirming a list of Customer stakeholders to attend the final meeting.
- Develop a summary presentation and final report.
- Conduct a review meeting to discuss the findings and recommendations contained in the Cloud Security Assessment Report.
- Conduct a final readout session to deliver the summary presentation.

Customer Responsibilities

- Confirm with Cisco the list of stakeholders to participate in the summary review meeting.
- Participate in the review meeting, reviewing with Cisco the Cloud Security Assessment Report, including all findings and recommendations
- Participate in the final readout session to deliver summary presentation.

General Customer Responsibilities

- Designate a single point of contact to act as the primary technical interface with the designated Cisco engineer.
- Provide documented Customer requirements (business and technical) and high-level network architecture design specifications.
- Provide documented information on Customer's existing infrastructure design including such as: features and services, network designs, call/data flow, security policies and operational processes, etc.
- Unless otherwise agreed to by the parties, Customer shall respond within two (2) Business Days of Cisco's request for any other documentation or information needed to provide the Service.
- Customer will create and manage an internal email alias for communication with the Cisco team.
- Customer will provide the required access to the network and required port connectivity for appliances and tools; and, Customer will provide the required IP addresses to connect the devices and the necessary DNS/NIS, Windows domain/Active directory configuration details.
- Notify Cisco about changes made to the Network such as Product(s) added/deleted and changes made to Product credentials, and any changes to Syslog, DNS, proxy and gateway servers IP address.
- Provide Cisco with a permission to utilize any Cisco or third-party software on the Network for the use of Data Collection Tools, network inventory and performance data gathering.
- Customer is responsible to implement system change requests (firewall, ACL configuration, user-id creation, etc.) to facilitate data gathering within one (1) business day of the initial request.
- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Customer will ensure that Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.