Service Description: Advanced Services – Fixed Price

Cisco Security Advisory Services: Blackbox Web Application Assessment (S)

ASF-CORE-BBAPP-30

This document describes the fixed price Cisco Security Blackbox Web Application Assessment (S) of up to 30 dynamic web pages.

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 www.cisco.com/go/legalterms. 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 www.cisco.com/go/legalterms. 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/.

Blackbox Web Application Assessment

Service Summary

Cisco will perform a Blackbox Application Assessment up to 30 dynamic web pages and three (3) authenticated roles, defined as common set of access privileges given to a set of users. The assessment identifies the application's immediate attack surface, and analyzes the attack surface for vulnerabilities using manual and automated testing techniques. When access credentials are provided, Cisco will perform authenticated testing. The primary focus of the testing is to identify application-layer vulnerabilities in the application code; however, the testing methodology may discover vulnerabilities in the application's immediate dependencies.

Location of Services

Services are delivered remotely.

Analysis

Cisco Responsibilities

- Conduct an analysis which includes a range of techniques intended to identify security vulnerabilities. Cisco will apply the following core strategies in performing the assessment:
  - Attack surface enumeration: attempts to identify application functionality by automated traversal of site hierarchy and permuting common variations on popular naming conventions
  - Manual fault injection: manual submission of malicious data to identify security vulnerabilities in request path
  - Automated fault injection: automated submission of a range of malicious data to identify security vulnerabilities in request path
  - Known vulnerability testing: identification of vulnerabilities in the hosting platform (web server, servlet container) using primarily automated analysis techniques
  - Candidate point: automated analysis to pinpoint known vulnerability patterns, followed by manual analysis to validate any vulnerability candidates

- Data correlation
- Research vulnerabilities
- Eliminate false positives
- Investigate the extent of the findings

Assessment

Cisco Responsibilities

- Conduct remote Kick-off call to review project plan and identify key stakeholders from Cisco and Customer.
- Perform an assessment, of up to 30 dynamic web pages and 3 roles, to identify security relevant issues including the following classes of vulnerabilities:
  - Injection vulnerabilities (command injection, SQL injection)
  - Cross-site scripting (XSS) and other script-based injection vulnerabilities
  - Cross-site request forgery (CSRF)
  - Memory management vulnerabilities
  - Input and output validation vulnerabilities
  - Session management vulnerabilities
  - Access control vulnerabilities
  - Path canonicalization vulnerabilities
  - Insufficient or ineffective use of encryption
  - Application related denial of service
  - Sensitive information exposure
  - Secure secrets storage
  - General data handling vulnerabilities
  - Object reference vulnerabilities
  - Design or logic that may introduce security weaknesses
  - Applicable issues not explicitly identified above, but covered by pertinent standards (OWASP top 10, SANS top 20)
  - Configuration weaknesses
  - Communication security weaknesses

Customer Responsibilities

- Ensure key individuals participate with Cisco in interviews and addressing technical questions.
- Provide Cisco with existing application diagrams and documentation, if available.
- Identify two (2) user accounts for each role to be tested during the assessment.
- Provide Cisco with URLs for applications being assessed (if applicable).
- Agree with Cisco on available window of hours for testing.
- Provide Cisco with administrative-level access to systems under assessment or access to Customer personnel capable of performing administrative actions in the event of technical difficulties.
- Provide debug and production builds of target software, when applicable.
- Allow Cisco equipment and tools to be placed on and used against the target environment.
- Ensure the application has been sufficiently populated with data to correctly access all features of the application.
- Provide details of any special numbers or data. This is unique information that that exists in the system that would be known by a real user but not necessarily Cisco.
- Provide any necessary authentication hardware.

Reporting

Cisco Responsibilities

- Provide Customer with the Blackbox Application Assessment Report, which includes:
  - Scope and approach
  - Prioritized list of findings
  - Details of vulnerabilities discovered, including:
- Schedule Executive Review call with identified executive stakeholders

Customer Responsibilities

- Identify stakeholders to attend Executive Review call with Cisco.
- Review with Cisco the completed Blackbox Application Assessment Report.
- Provide sign-off for Blackbox Application Assessment Services completion.

General Customer Responsibilities

- Customer represent and warrant that they have sufficient authority and the rights necessary for Customer to provide and/or facilitate Cisco's access to information, data, networks, systems, and media in connection with these Services.
- For all Customer requests under this Service Description that Cisco possess, access, or analyze particular media, computers, computer networks, communications networks, or other systems and equipment, to the extent Customer provides or facilitates Cisco's access thereto, Customer represents, warrants and covenants that they have all necessary right, title, license, and authority to make such requests and grant such access, including all necessary permissions from third-party owners of licensed or shared resources.
- CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL NECESSARY LICENSES, PERMISSIONS, AND CLEARANCES FOR CISCO TO ACCESS RESOURCES THAT ARE HOSTED, OWNED BY, OR SHARED WITH A THIRD-PARTY.
- Customer is responsible any delays in provision of necessary test access, environments, VPN connections, user accounts, administrative access, or other required technical assets.
- 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. Cisco 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.
- Customer will 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 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.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer understands that any web pages not assessed during the term of the Service will not result in any credit.
- 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 and any unused hours will expire.

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.

Assumptions and Exclusions

- Unless otherwise stated herein, Customer is responsible for provision of test equipment.
- Customer is solely responsible for determination and implementation of its network, design, business or other requirements and the implementation of any recommendations provided by Cisco. Cisco's recommendations are based upon Customer information provided to Cisco. Cisco shall not be liable for the accuracy or completeness of any Customer information contained in Cisco's recommendations.
- All documents will be provided in electronic form in the English language.
- Customer retains all responsibility for the security of Customer Technical Environment(s). Cisco shall have no responsibility for, or liability as a result of, any breach in security of Customer's Environment. Cisco cannot guarantee that Customer's security may or may not be vulnerable from any included, omitted or overlooked instances whether or not presented in the Services or Deliverables associated with this Service Description.
- Security assessment services will not definitively prove the absence of vulnerabilities.
- Customer understands and acknowledges that, where Cisco has exercised reasonable precautions in performing Services, Cisco is not responsible for system outages, degradation of performance, or other adverse technology environment consequences of tasks Customer has authorized Cisco to perform.
- Cisco recommends that Customer back up its environment and perform maintenance before the start of performance of Services and reminds Customer that such back up is its sole responsibility.