Service Description: Security Posture Assessment Service

This document describes the Security Posture Assessment (SPA) Service.

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; and (3) Severity and Escalation Guidelines. 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, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services 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.

Cisco shall provide the Security Posture Assessment Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Service Summary

Security Posture Assessment Service provides a point-in-time assessment of the risk posed to an organization by vulnerabilities present in the organization's IP-networked systems and/or physical perimeter security controls. The service measures the extent to which identified vulnerabilities can be utilized to achieve unexpected or unauthorized access to the OS or applications on IP-connected endpoints (UNIX / Windows / network and security devices). The service comprises various activities including vulnerability discovery, manual and automated vulnerability confirmation, system- and/or site-level penetration, and presentation and reporting for each of six (6) vector-defined SPA services: Perimeter, Internal, Web Application, Client Side, Wireless and Physical. It is Cisco's policy to destroy these finding reports and to not store them anywhere on its network once these reports are delivered to the Customer and a delivery confirmation is received back.

Security Posture Assessment Service

Under this Service, Cisco shall provide the Security Posture Assessment Service during Standard Business Hours, unless stated otherwise. Cisco shall provide the following General Service provisions for any SPAs selected by Customer:

General Service

- Provide a single point of contact ("Cisco Project Manager") for all issues relating to the Services.
- Participate in regularly scheduled meetings with the Customer to discuss the status of the Services.
- Ensure Cisco employees and any Cisco subcontractors conform to Customer's reasonable workplace policies, conditions and safety regulations that are consistent with Cisco's obligations herein and that are provided to Cisco in writing prior to commencement of the Services; provided, however, that Cisco's personnel or subcontractors shall not be required to sign individual agreements with Customer or waive any personal rights.
- Supply Cisco project team personnel with a displayable form of identification to be worn at all times during activities at Customer facility.
- Cisco reserves the right to determine which of its personnel will be assigned to a particular project, to replace or reassign such personnel and/or subcontract to qualified third persons part or all of the performance of any SPA hereunder. Customer may request the removal or reassignment of any Cisco personnel at any time; however Customer shall be responsible for extra costs relating to such removal or reassignment of Cisco personnel. Cisco shall not have any liability for any costs, which may occur due to project delays due to such removal or reassignment of Cisco personnel.

1) Internal Security Posture Assessment ("SPA")

Cisco will provide an Internal SPA that will be conducted on-site at no more than **one (1)** Customer site. This SPA will provide information regarding security vulnerabilities

present on networked systems on the Customer's internal IP network(s). The following activities will be conducted as part of the Internal SPA:

- **Critical Network and Asset Identification Workshop:** Cisco Network Consulting Engineers (NCEs) will work with the Customer to identify business critical networks and assets (data, servers, applications, etc.). The critical networks and assets identified in the workshop will be used to qualify risk and prioritize recommendations and remediation efforts.

- **Discovery and Vulnerability Identification:** Cisco NCEs will identify live IP addresses, not to exceed the amount specified in the Quote from Cisco, on the Customer's internal network(s) from a list that the Customer provides. Specific activities performed during the discovery and vulnerability identification phase include:

  - Identify active (live) IP addresses in the targeted internal infrastructure using ICMP ping and TCP SYN scanning among other techniques as needed.

  - Scan a subset of the 65,535 potential TCP ports and a subset of potential UDP ports on the targeted live IP addresses to identify open ports and services.

  - Identify potential security vulnerabilities present on these live IP addresses.

- **Vulnerability Confirmation and Target Analysis:** Cisco NCEs will attempt to confirm the existence of potential security vulnerabilities identified during the previous activity using a variety of techniques up to and including system-level and secondary exploitation. This activity is designed to provide insight into the potential for successful attacks on the Customer's internal infrastructure by malicious individuals with internal network access and connectivity and the likelihood that the Customer's security and systems administrators would detect these attacks. Specific activities performed during the vulnerability confirmation and target analysis phase include:

  - Confirm vulnerabilities identified during the previous phase using validated and tested exploits and penetration testing techniques.

  - Analyze the risk posed by exploitable vulnerabilities to the Customer's environment via secondary exploitation and data mining of compromised systems.

- **Results Analysis and Presentation:** Cisco NCEs will compile and analyze the results of the activities from the **Discovery and Vulnerability Identification** and **Vulnerability Confirmation and Target Analysis** phases. Specific activities performed during the results analysis and presentation phase include:

  - Identify critical deficiencies in the Customer's security posture by analyzing and reviewing the collected vulnerability information and comparing the internal assessment results with the Customer's operational requirements and recommended security practices and controls.

  - Correlate vulnerability data with network topology information and identify risk posed to critical networks and assets.

  - Provide an executive-level presentation summarizing the assessment findings and results in a prioritized manner along with recommendations to mitigate high-severity findings.

- **Assessment Report:** Cisco NCEs will provide an Internal SPA report. This report is typically provided in HTML format for easy navigation and includes: an assessment summary of the most critical findings; data and statistics regarding individual systems, and vulnerabilities; and recommendations for improvement.

2) Perimeter Security Posture Assessment ("SPA")

Cisco will provide a Perimeter SPA designed to assess vulnerabilities in the Customer's Internet-facing IP infrastructure and the effectiveness of email and browser security controls. Due to the global nature of the Cisco Advanced Services team that performs this testing, the Perimeter SPA may be performed at times outside of Standard Business Hours. The following activities will be conducted as part of the Perimeter SPA:

- **Discovery and Vulnerability Identification:** Cisco NCEs will identify and perform a vulnerability assessment and penetration test on IP addresses, not to exceed the amount specified in the Quote from Cisco, in the Customer's Internet-facing infrastructure from a list that the Customer provides. Specific activities performed during the discovery and vulnerability identification phase include:

  - Research and confirm IP and DNS registration of the targeted IP space.

  - Identify active (live) IP addresses in the targeted Internet-facing infrastructure using ICMP ping and TCP SYN scanning among other techniques as needed.

  - Scan all 65,535 potential TCP ports and a subset of potential UDP ports on the targeted live IP addresses to identify open ports and services.

- **Vulnerability Confirmation and Target Analysis:** Cisco NCEs will attempt to confirm the existence of potential security vulnerabilities identified during the previous activity using a variety of techniques up to and including system-level and secondary exploitation. This activity is designed to provide insight into the potential for successful attacks on the Customer's Internet-facing infrastructure by malicious individuals and the likelihood that the Customer's security and systems administrators would detect these attacks. Specific activities performed during the vulnerability confirmation and target analysis phase include:

  - Confirm vulnerabilities identified during the previous phase using validated and tested exploits and penetration testing techniques.

  - Analyze the risk posed by exploitable vulnerabilities to the Customer's environment via secondary exploitation and data mining of compromised systems.

- **Targeted Phishing Vulnerability Analysis:** Cisco NCEs will target internal users, not to exceed the amount specified in the Quote from Cisco, in order to assess the risk posed to the Customer by spear-phishing attacks. This activity is designed to provide insight into the potential for successful targeted phishing attacks on the Customer's internal users and infrastructure by malicious individuals and the efficiency of the Customer's patch management regimen, email filtering, anti-virus or host-based IPS controls and network-level access controls. Specific activities performed during the targeted phishing vulnerability assessment phase include:

  - Identify target email addresses. Customer can provide a list of email addresses for targeted individuals or alternately Cisco NCEs will identify potential targets using various Internet information sources such as public search engines.

  - Research targeted individuals using Internet information sources for personal information useful in crafting targeted spear-phishing emails.

  - Send individually crafted email(s) to targeted individuals using this personal information in order to convince the individual to take some action such as view an attached file or visit an external Internet-accessible website physically hosted in Cisco's SPA operations center in Austin, Texas USA. The file attachments and website are designed to exploit vulnerabilities in client applications such as a web browser or word processing application unless an appropriate patch is applied or another compensating control exists.

- **Results Analysis and Presentation:** Cisco NCEs will compile and analyze the results of the activities from the **Discovery and Vulnerability Identification**, **Vulnerability Confirmation and Target Analysis** and **Targeted Phishing Vulnerability Analysis** phases. Specific activities performed during the results analysis and presentation phase include:

  - Identify critical deficiencies in the Customer's security posture by analyzing and reviewing the collected vulnerability information and comparing the Perimeter SPA assessment results with the Customer's operational requirements and recommended security practices and controls.

  - Provide an executive-level presentation summarizing the assessment findings and results in a prioritized manner along with recommendations to mitigate high-severity findings.

- **Assessment Report:** Cisco NCEs will provide a Perimeter SPA report. This report is typically provided in HTML format for easy navigation and includes: an assessment summary of the most critical findings; data and statistics regarding individual systems, and vulnerabilities; and recommendations for improvement.

3) Client Side Security Posture Assessment (SPA)

Cisco will do Client Side SPA to provide insight into the potential for successful targeted phishing attacks on the Customer's internal users and infrastructure by malicious individuals and the efficiency of the Customer's patch management regimen, email filtering, anti-virus or host-based IPS controls and network-level access controls. Cisco Advanced Services will target up to a predefined number of internal users as specified in Quote, in order to assess the risk posed to the Customer by phishing attack.

4) Web Application Security Posture Assessment (SPA)

Cisco Web Application PA assesses vulnerabilities in the Customer's web (HTTP/HTTPS) application(s). The Web Application SPA testing activities are sourced from Cisco's SPA operations center remotely. The scope of the Web Application Security Posture Assessment shall be limited number of hosts and Dynamic Page as specified in Quote.

Cisco Network Consulting Engineers (NCEs) will scan targeted web application to identify potential security vulnerabilities. This activity focuses on vulnerabilities defined as OWASP (Open Web Application Security Project) Top Ten: cross-site scripting (XSS), injection flaws, malicious file execution, insecure direct object reference, cross-site request forgery, information leakage and improper error handling, broken authentication and session management, insecure cryptographic storage, insecure communications, and failure to restrict URL access.

Cisco Network Consulting Engineers will identify potential security vulnerabilities present in the web applications within scope and will attempt to confirm the existence of these vulnerabilities using a variety of techniques up to and including system-level and secondary exploitation. This activity is designed to provide insight into the potential for successful attacks on the Customer's web application(s) by malicious individuals with access to the application(s) and the likelihood that the Customer's security and systems administrators would detect these attacks.

5) Wireless Security Posture Assessment ("SPA")

Cisco will provide a Wireless SPA designed to assess the security of the Customer's authorized 802.11 a/b/g/n wireless infrastructure and to identify and locate any unauthorized (rogue) 802.11 access points at Customer locations, not exceed the square meters specified in the Quote from Cisco. The following activities will be conducted as part of the Wireless SPA:

- **Site Survey:** Cisco NCEs will conduct a wireless site survey of the Customer location(s) to determine the number and location of deployed access points. Specific activities performed during the wireless site survey phase include:
  - Conduct an RF site survey of the interior area and outside perimeter (where feasible) of the site(s).
  - Compare the list of deployed access points identified during this survey with a list of authorized access points provided by the Customer in order to determine if any unauthorized access points are present.
  - Attempt to physically locate unauthorized access points so that their presence can be validated.
- **Wireless Security Testing:** Cisco NCEs will test the security controls implemented on both authorized and unauthorized 802.11 networks at the location(s) specified in order to (1) validate that the implemented controls meet Cisco and industry standards for 802.11 wireless security best practices and (2) provide adequate security against outside penetration. Specific activities performed during the wireless security testing phase include:
  - Attempt to penetrate authorized and unauthorized 802.11 wireless networks with potentially exploitable security controls such as WEP or WPA-PSK.
  - Take a sample packet capture of an 802.11 client authenticating to an authorized 802.11 network to validate that proper security controls are implemented.
- **Results Analysis and Presentation:** Cisco NCEs will compile and analyze the results of the activities from the **Site Survey** and **Wireless Security Testing** phases. Specific activities performed during the results analysis and presentation phase include:
  - Identify critical deficiencies in the Customer's security posture by analyzing and reviewing the collected information and comparing the wireless assessment results with the Customer's operational requirements and recommended security practices and controls.
  - Provide an executive-level presentation summarizing the assessment findings and results in a prioritized manner along with recommendations to mitigate high-severity findings.
- **Assessment Report and Recommendations:** Cisco NCEs will provide a Wireless SPA report. This report is typically provided in HTML format for easy navigation and includes: an assessment summary of the most critical findings; data and statistics regarding vulnerabilities; and recommendations for improvement.

6) Physical Security Posture Assessment ("SPA")

Cisco will provide a Physical SPA designed to assess the implemented physical security controls at Customer sites and cities, based on the amounts specified in the Quote from Cisco**.** The goal of the Physical Security SPA is to evaluate the effectiveness of the implemented controls using reconnaissance and penetration testing techniques and assess the risk that physical penetration poses to the security of the Customer's IT assets. The following activities will be conducted as part of the Physical SPA:

- **Reconnaissance and Information Discovery:** Cisco NCEs will remotely conduct zero-knowledge site reconnaissance using publically available information resources. Specific activities performed during the reconnaissance and information discovery phase include:
  - Review of the site layout, entrances, access routes and topology using Internet-accessible information.
  - Profiling of site personnel in order to create a dossier of information useful for social engineering attempts.
- **Site Survey:** Cisco NCEs will conduct a black-box physical site survey of the Customer location(s) in order to identify deployed physical security controls. Specific activities performed during the site survey phase include:
  - Conduct a site perimeter survey of the site(s) (where feasible) and identify and document

physical security controls and access procedures.

- **Physical Site Penetration:** Cisco NCEs will conduct active testing of the security controls implemented at the Customer location(s) specified in order to (1) validate that the implemented controls adequately prevent or inhibit physical access by unauthorized individuals and (2) measure the impact of unauthorized physical access to the Customer's IT assets if physical access is achieved. Specific activities performed during the wireless security testing phase include:
  - Attempt to penetrate the site's physical perimeter and gain access to the location's interior. Myriad methods may be employed to conduct this penetration testing, including but not limited to, social engineering, impersonation, tail-gating authorized employees as they enter the site, and access through improperly secured entrances.
  - If access to the location is achieved, Cisco NCEs will attempt to connect to the Customer's internal IP network(s) and create a back-channel connection between a Cisco-controlled server on the Customer's network and a Cisco-controlled network accessible via the public Internet.
- **Results Analysis and Presentation:** Cisco NCEs will compile and analyze the results of the activities from the **Reconnaissance and Information Discovery**, **Site Survey** and **Physical Site Penetration** phases. Specific activities performed during the results analysis and presentation phase include:
  - Identify critical deficiencies in the Customer's security posture by analyzing and reviewing the collected information and comparing the physical security assessment results with the Customer's operational requirements and recommended security practices and controls.
  - Provide an executive-level presentation summarizing the assessment findings and results in a prioritized manner along with recommendations to mitigate high-severity findings.
- **Assessment Report and Recommendations:** Cisco NCEs will provide a Physical SPA report. This report will include an assessment summary of the most critical findings; data and statistics regarding vulnerabilities; and recommendations for improvement.

Service Responsibilities of Customer

Customer shall comply with the following the obligations.

- Customer shall designate a person to whom all Cisco communications may be addressed and who has the authority to act on all aspects of the Services. Customer shall also designate a back up when the Customer contact is not available who has the authority to act on all aspects of the Services in the absence of the primary contact.
- Customer shall ensure its site is ready for the date scheduled for performance of Services.
- Provide Cisco with such access to Customer facility and facilities as required to enable Cisco to comply with its obligations, including where applicable, computers, telecom equipment, facilities, workspace and telephone for Cisco's use during the project.
- Unless otherwise agreed to by the parties, Customer shall respond within two (2) business days of Cisco's request for documentation or information needed for the project.
- Customer shall be responsible for making the decision to implement all or any portion of the SPA and for any implementation of the SPA. Customer shall retain all responsibility for the security of its Networks. Cisco shall have no responsibility for, or liability as a result of, any breach in security of Customer's Network. 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 SPA or deliverables associated with the applicable SPA.
- Provide proper security clearances and/or escorts as required to access the Customer facility.
- Customer understands and acknowledges that it is Cisco's policy to destroy Customer specific finding reports and to not store them anywhere on its network once these reports are delivered to the Customer and a delivery confirmation is received back.
- Supply the workplace policies, conditions and environment in effect at the Customer facility.
- Customer shall ensure that all information provided by Customer concerning the design, topology, and other features of its Network is materially accurate, and shall not materially change between the date of Customer's issuance of purchase order of the Services and the completion of all Services contemplated hereunder.
- Customer agrees that it will not hire a current or former employee of Cisco, who is involved in the Services under this Service Description, during the term of the Service and for a period of one (1) year after the termination of the Service. As liquidated damages, and not as a penalty, should Customer hire a current or former Cisco employee

who is involved in the Services under this Service Description, Customer shall pay to Cisco three (3) times the annual compensation of such employee on the date the employee is hired. If payment is not made on such date, the liquidated damage payment shall be six (6) times the annual compensation of such employee.