| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-26** | HONEYPOTS | |
| **SC-26.1**  **SC-26.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of honeypots; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-8, SI-3, SI-4  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **SC-26.1.1.1** | | **Examine** system and communications protection policy, procedures addressing use of honeypots, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the components that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. |
| **SC-26.1.1.2** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed by the components identified in SC-26.1.1.1 to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. |
| **SC-26.1.1.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-26.1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-26.1.1.2. |
| **SC-26.1.1.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-26.1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **SC-26(1)** | | HONEYPOTS |
| **SC-26(1).1**  **SC-26(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system includes components that proactively seek to identify Web-based malicious code.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing use of honeypots; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms proactively seeking Web-based malicious code]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-8, SC-7, SI-3, SI-4  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SC-26(1).1.1.1** | | **Examine** system and communications protection policy, procedures addressing use of honeypots, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system components that proactively seek to identify Web-based malicious code. |
| **SC-26(1).1.1.2** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed by the information system components identified in SC-26(1).1.1.1 that proactively seek to identify Web-based malicious code. |
| **SC-26(1).1.1.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-26(1).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-26(1).1.1.2. |
| **SC-26(1).1.1.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-26(1).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |