Vulnerability Assessment Request Form

*Note: This form to be used only if premium partner delivered customer(HEC).*

|  |  |
| --- | --- |
|  | **CUSTOMER** |
|  |  |
|  | **Company Name** | Click or tap here to enter text. |
|  | **Cloud Partner** | Click or tap here to enter text. |
|  | **AUTHORIZED CONTACT** |
|  |  |
|  | **Name** | Click or tap here to enter text. | **Department** | Click or tap here to enter text. |
|  | **E-Mail** | Click or tap here to enter text. | **Phone** | Click or tap here to enter text. |
|  | **Preferred Start** **Date** | Click or tap to enter a date. | **Preferred End****Date** | Click or tap to enter a date. |

|  |  |
| --- | --- |
|  |  |
|  | **SOURCE** |
|  |  |
|  | **Source IPs** | Click or tap here to enter text. |
|  |  |
|  | **Tester E-Mail** | Click or tap here to enter text. | **Phone** | Click or tap here to enter text. |
|  |  |  |

|  |  |
| --- | --- |
|  | **CLOUD SOLUTION** |
|  |  |
|  | **Solutions under Testing** | [ ]  HEC | [ ]  HCM | [ ]  S4H | [ ]  CC/CX | [ ]  IBP |
|  |  | [ ]  C4C | [ ]  SCI | [ ]  SCP EE | [ ]  SCP NEO | [ ]  SCP CF |
|  |  | [ ]  Ariba  | [ ]  Other  |  |  |  |
|  | **Please specify OTHER** | Click or tap here to enter text. |
|  | **Application under Testing** | Click or tap here to enter text. |
|  |  |
|  | **TARGET AND SCOPE** |
|  |  |
|  | **IP Addresses/Networks** | Click or tap here to enter text. |
|  | **URLs** |  |
|  | **Scanning Tools** |  |
|  | **Type and scope of testing planned** | Click or tap here to enter text. |

# Instructions to complete the form

Under **CUSTOMER**, please fill in accurately the full name of your company (“**Customer**”) as written in your Cloud Service contract. If the name does not match our records, we may deny your request. In this form, “**SAP**” refers to the local SAP entity that is responsible for performing your Cloud Service contract.

Premium partner delivered customer must specify cloud partner where SAP product is hosted.

Under **AUTHORIZED CONTACT**, please provide the individual authorized by Customer to be the single-point of contact for the security assessment. This individual shall be deemed fully authorized to act on behalf of Customer.

Under **SOURCE**, please provide the following information (if there are multiple items in each field, use a comma to separate each item):

* **Source IPs** – the IP addresses from which the tests will be conducted
* **Tester’s email and phone** – the email address and phone number of the individuals conducting the tests

Under **CLOUD SOLUTION**, please specify the Cloud solution Customer is testing.

* HEC – HANA Enterprise Cloud
* HCM – SuccessFactors Human Capital Management Cloud
* SCP – SAP Cloud Platform
* IBP – Integrated Business Planning
* SCI – SAP Cloud Integration
* CC/CX – SAP Commercer Cloud (Hybris Solution)
* OTHER – any other SAP Solution that Customer is testing, please specify in the dedicated field

Under **Components under Testing**, please specify the exact Cloud product or component being tested. For SFSF, this may be Employee Central, JAM, Recruiting, EC Payroll. For SAP Cloud Platform (SCP), this may be Portal, SAP Identity.

Under **TARGET AND SCOPE**, please specify the target IP addresses and URLs that are within the scope of the test. Please make sure the list is exhaustive. Testing outside of the approved scope is strictly prohibited. Please also provide:

* **Scanning Tools** – list of tools used in the security assessment (e.g. Burp, Nmap, Sqlmap, …)
* **Type and scope of testing planned** – e.g. OWASP TOP 10 (Manual), SSL Scan (Automated), Nessus Scan (Automated), Nexpose Scan (Automated), etc.

The completed form must be sent via email from the email account of Customer’s authorized administrator (as indicated on our records) to pentest@sap.com. Forms sent from any other email account will be disregarded. By sending the completed form to pentest@sap.com, Customer confirms to SAP that Customer has read, understood and accepted the RULES FOR VULNERABILITY ASSESSMENT set out next page.

# Rules For VULNERABILITY Assessment

1. The completed Vulnerability Assessment Request Form must be received by SAP at least 10 business days before the “Preferred Start Date” of the testing period. SAP operations team will review and notify the Authorized Contact of the approved testing period. Duration of testing period shall not exceed 3 weeks. Notwithstanding any approval of any testing period, SAP reserves the right at any time to reschedule, shorten or cancel such testing period for any reason, including for maintenance activities.
2. When planning for the test, please note that the permitted window for conducting tests is during non-business hours as follows:

|  |  |
| --- | --- |
| *Data Center’s Local Time Zone:* | *Permitted Window for Testing:* |
| US Data Centers | 9:00PM to 5:00AM Pacific Time |
| EU Data Centers | 9:00PM to 5:00AM Central European Time |
| Asia Pacific Japan/Greater China Data Centers | 9:00PM to 5:00AM Australian (EST) Time |

1. Testing outside of the above permitted windows is prohibited.
2. Customeris permitted to conduct no more than one test per major release of the Cloud product or component being tested.
3. Customer may only carry out vulnerability testing on its own Customer-specific Cloud solution landscape. Conducting scanning, penetration testing or other forms of security assessment on any other systems, including shared resources is strictly prohibited.
4. Each test request is unique and will be dealt with as such. A detailed scope of the testing plan must be provided and approved, before any testing can take place.
5. Vulnerability assessment must be non-load bearing. Denial of Service, Distributed Denial of Service and other destructive tests, including but not limited to DNS poisoning, root-kit installation are strictly prohibited.
6. Customer must not (and shall ensure that any third party performing the tests on its behalf must not) disclose the testing process, the test results or any issues found to any person or entity, except with the explicit written authorization from SAP. Such information must be treated as strictly confidential information. Nothing in this document authorizes the results to be released.
7. Customermust provide SAP with a test report containing results of testing and any issues found, as well as the descriptions of the tests and findings, the severity rating and instructions to reproduce the issues (if any). SAP may request that the results from the tests and issues found, if any, be summed up in the format provided by SAP (in an Microsoft Excel file).
8. SAP requires the IP address (one or two, but not a range) of the scanning source, to temporarily white-list this IP address in our monitoring stations. The source IP address must be specified in this form. If there is any change of IP address (be it source or target), Customer must immediately stop further testing, inform SAP, and wait for SAP to approve the change of IP address before continuing with testing.
9. If the testing cannot be completed within the permitted testing period, SAP must be notified by email and Customer must stop and wait for SAP’s approval to extend the testing period before continuing with testing.
10. Any deviation from the above will be considered an unauthorized attack against SAP infrastructure and be handled accordingly. This may result in a disruption of service to Customer. In certain jurisdictions, such actions may also be considered a criminal offence under computer misuse or similar legislations.
11. Product specific restrictions:
	* Business by Design (ByD) – Penetration testing approval only for non-production environment.
	* Success Factors (HXM) – Business hours testing request needs15 business days for processing.