

SPI-09: Test a system for vulnerabilities using an automated service

A **service provider** or **campus IT administrator** needs to use an automated vulnerability scanning service to test their system for vulnerabilities.

In most cases, the service provider wants to experience it as follows.

1. First, the service provider visits the community's website (or website section) for service providers, and locates the vulnerability scanning service.
2. Then, the service provider enters the address of the system to be scanned and initiates the scan.
3. Then, the scanning service scans the system, either providing a progress indicator in the interface or promising to notify the service provider when the scan completes.
4. Finally, the scan completes and the scanning service provides a report to the service provider noting any vulnerabilities and (ideally) a list of what was checked.

We'll take any solution, as long as...

1. In Steps 1 and 2, the vulnerability scanning service can be accessed and used with nothing more than a standard web browser and an internet connection.
2. In Step 2, the address can be either an FQDN (fully-qualified domain name) or an IP address.

SPI-10: Obtain expert help with resolving a system vulnerability

A **service provider** needs to obtain help from an expert who can help resolve a vulnerability detected in a system.

In most cases, the service provider wants to experience it as follows.

1. First, the service provider visits the community's website (or website section) for service providers, and locates the vulnerability assistance section.
2. Then, the service provider fills out and submits a form requesting assistance with a specific vulnerability on a specific system.
3. Finally, the service provider receives a response to the request, either indicating that assistance isn't available or providing contact information for assistance.

We'll take any solution, as long as...

1. In Steps 1 and 2, the vulnerability assistance request can be accessed and used with nothing more than a standard web browser and an internet connection.
2. In Step 2, the form prompts the service provider for all information required to provide a response. (The response shouldn't be contingent on information that wasn't initially requested.)
3. In Step 3, the response is provided no more than one business day after the request was received.

SPI-11: Host a repository of files so it can be accessed on many resources and manually populated by authorized individuals

A **service provider** needs to host a repository of files so it can be accessed on many resources. The contents of the repository will be populated manually by authorized individuals. We assume a group within the service provider's community is prepared to maintain the contents of the repository.

In most cases, the service provider wants to experience it as follows.

1. First, the service provider receives a request from a group in the service provider's community asking for a repository the group can maintain and use.
2. If the service provider doesn't already maintain repositories, the service provider visits the community's website (or website section) for service providers, locates and reviews the documentation on hosting repositories, then installs and configures the necessary hardware and software. If the service provider encounters any issues, the service provider files a support ticket with the community's support service.
3. Then, the service provider allocates storage for the repository on the service provider's systems.
4. If the service provider doesn't already maintain repositories, the service provider initializes the hosting service(s) by generating host information and credentials as described in the documentation on hosting repositories.
5. Then, the service provider uses the repository hosting software to initialize the repository using the information provided by the requesting group.
6. Then, the service provider configures the system to enable and permit the requesting group members to maintain the contents of the repository.
7. Finally, the service provider notifies the requesting group members that the repository is available for their use.

We'll take any solution, as long as...

1. In Step 2, any software required by the instructions is available under a license that permits free use by the service provider within the community.
2. In Step 4, any service provider in the community can generate (or obtain) the required credentials to host a repository.
3. In Step 6, the interfaces used to maintain the repository are ideally interfaces used for other community purposes. E.g., one or more of: the login interface described in use case [CAN-04](#) and the file transfer interfaces described in [DM-12](#) and [DM-13](#).

SPI-12: Host a repository of files so it can be accessed on many resources and automatically populated

A **service provider** needs to host a repository of files so it can be accessed on many resources. The contents of the repository will be populated automatically by pulling from another repository. Examples of source repositories include: DockerHub, a GitHub project, a StashCache service.

In most cases, the service provider wants to experience it as follows.

1. First, the service provider receives a request from a group in the service provider's community asking for a repository the group can maintain and use.
2. If the service provider doesn't already maintain repositories, the service provider visits the community's website (or website section) for service providers, locates and reviews the documentation on hosting repositories, then installs and configures the necessary hardware and software. If the service provider encounters any issues, the service provider files a support ticket with the community's support service.
3. Then, the service provider allocates storage for the repository on the service provider's systems.
4. If the service provider doesn't already maintain repositories, the service provider initializes the hosting service(s) by generating host information and credentials as described in the documentation on hosting repositories.
5. Then, the service provider uses the repository hosting software to initialize the repository using the information provided by the requesting group.
6. Then, the service provider configures the system to automatically populate the repository by pulling from the requested repository.
7. Finally, the service provider notifies the requesting group members that the repository is available for their use.

We'll take any solution, as long as...

1. In Step 2, any software required by the instructions is available under a license that permits free use by the service provider within the community.
2. In Step 4, any service provider in the community can generate (or obtain) the required credentials to host a repository.
3. In Step 6, the mechanisms for pulling contents from other repositories are included in the materials in Step 2 and do not compromise the security of the hosting system.
4. In Step 6, source repository types can include, at minimum: GitHub repositories, DockerHub repositories, and StashCache services.