WhiteHat Portal Onboarding

Synopsys

2024-02-16

Table of Contents

Chapter 1. WhiteHat Portal Onboarding

Synopsys' Customer Success unit will work with you to get your WhiteHat services up and running as quickly as possible, so that your web assets are being properly scanned and you are receiving accurate security information. The WhiteHat Portal Onboarding Processes document will outline how the onboarding process will work, and what you can do to expedite it.

Additional information about onboarding and about making the best use of Sentinel and Sentinel Source is available in our Customer Success Center; login information for the Customer Success Center will be sent to you in email on your contract start date. The Customer Success Center provides ready access to the customer success team, to your tickets, to Q&A information, and to downloadable reference and training material (including all user guides).

You will receive several emails from the WhiteHat Service Deployment Team on your contract start date—one providing you with your WhiteHat Portal interface login information, one providing your Customer Success Center login information, and one asking to schedule an introductory call. For that call, we will be asking you for the following information:

Service	Information Required
Sentinel Source (SAST)	• Source Code Repository and type(s) (e.g. SVN, CVS, Perforce) or Source Code Archive • URI(s) of the repositories or archives and any associated code bases • Read-only credentials or certificate information

WhiteHat Dynamic (DAST)	• Web application hostnames and any associated host names (if there are more than ten associated hostnames needed for a given asset, special arrangements will be required)
	• Web application credentials (one primary set with the highest available level of access and one backup set):
	  ◦ Any multi-factor authentication information
	  ◦ For PE licenses, two additional test accounts for each user level are needed for business logic testing
	• Weekly assessment schedule(s) (continuous, evenings and weekends, or specified days and times)

Service	Information Required
Sentinel Mobile	• All project files for your mobile application(s), both source code and build files • Two sets of credentials

The better prepared you can be at the beginning of the onboarding process, the more quickly the Synopsys team can get your scan services running in a continuous mode. For more details on the above information requirements and/or instructions for onboarding your assets, see the following sections:

Chapter 2. Sentinel Source (SAST) Onboarding

2.1. Required Information

For onboarding your static analysis services, we need to know the type of Source Code Repository that you are using (if any), the URIs of the repositories/code bases or binaries we will be assessing, appropriate credentials, and the assessment schedule that you want to use.

1. **Source Code Repository Type(s)**

   Synopsys will need to know what type of repository houses the application code you want us to assess, so that we can provision the correct connector for that repository within the Sentinel appliance that you must install prior to beginning an assessment. Information on the types of repositories that we currently support is available in the 'Adding a Code Base' section of the 'Managing Your Applications' .

2. **URI(s) of the Repositories and Associated Code Bases**

   You can add code bases that are part of the application to the scope of the Source scan. Doing this ensures a complete scan of the application's source code.

NOTE	Please ask your developers if there are any dependencies not declared within the application source code. If there are, please add these as additional code bases associated to the application within the WhiteHat Portal UI. This will ensure that our scanning engine can thoroughly test all source code related to the application.

3. **Read-Only Credentials**

   You will need to provide us with read-only credentials (if any) to the repositories on which your application resides. This allows our source code scanning engine to automatically log into the repository at the beginning of each schedule scan window.

2.2. Assessment Schedule

You can schedule scans of your source code on an as-needed basis. We recommend scheduling scan windows regularly to ensure a current view of your application's security status.

- **Scan Now** – Scans source code only once to completion
- **Daily** – Scans source code once per day to completion
- **Weekly** – Scans source code once per week to completion
- **Never Scan (Default)** – Source code will not be scanned until you allow it in the scan schedule

NOTE	Until you set a scan schedule, the default value used will be **Never Scan**.

2.3. Service Delivery Timeline and Setup

- **Source Appliance Download and Installation (1 Business Day)**

  The Source VM not only houses our Source scanning engine, but also creates a secure SSH tunnel from our servers to yours that allows us to verify potentially vulnerable code snippets. These snippets are the only pieces of your source code that will be passed via this secure connection to our TRC engineers.

  Follow the steps outlined in the **Source Appliance** guide, attached to your welcome email, to download and set up the VM Appliance within your network. Once you've installed the VM, we will verify the connection to your intended repositories is successful.

NOTE	We recommend having someone who has experience with ESX servers available for the setup process.

- **Adding Applications and Code Bases**

  Since code checkout is done remotely via automation, Sentinel does not support browsing from a repository root, project listing, or web directory. If your application requires multiple repository projects to build, please add each project as a separate codebase. Remember that adding codebases that do not make up a single build may result in build errors that prevent scan completion.

  If your version control technology is not supported or if your application's build requires dependencies that are not available from a repository accessible by the Sentinel appliance, you may use a **mock codebase** to provide additional code to be used in the scan via a gzipped tarball. In addition, you may set an application up to have its binary files scanned, rather than its code.

  For more details on adding applications and code bases, see 'Managing Your Applications' .

- **Vulnerability Verification (Ongoing)**

  Any time Sentinel finds a vulnerability during a scheduled scan, it sends the potentially vulnerable code snippet to our TRC engineers. Our engineers then verify that the vulnerability is true and actionable before posting it.

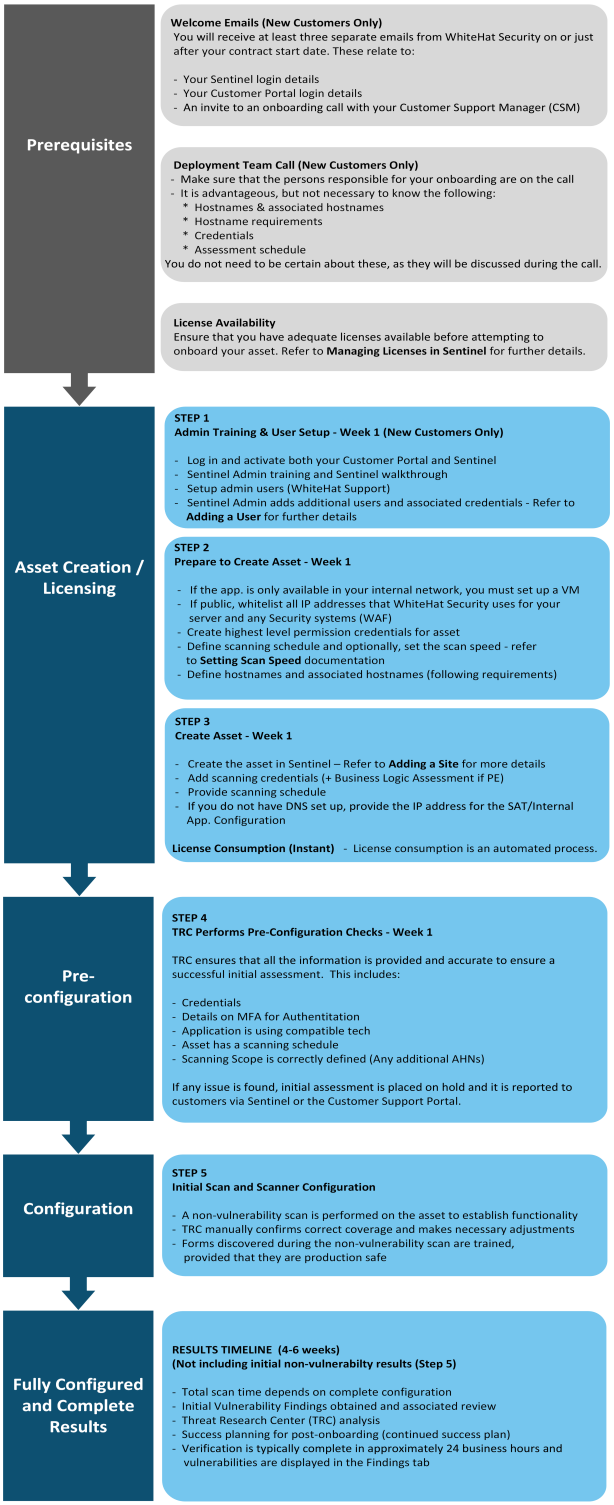
- **Initial Assessment Complete (1-2 Weeks)**

  When the first full scan completes successfully and all verified vulnerabilities have been reported, we recommend scheduling a Vulnerability Review call where our TRC engineers can discuss and explain vulnerabilities. This call includes a breakdown of each reported vulnerability class and their threat to your application's security using your vulnerabilities as examples.

  We encourage you and your security and development teams to request Vulnerability Reviews for specific vulnerabilities any time during your subscription term.

Chapter 3. WhiteHat Dynamic Onboarding

3.1. DAST Onboarding Overview



Refer to the following useful links for more information:

- Managing Licenses in the WhiteHat Portal

- Adding a Site
- Adding a User
- Setting Scan Speed

3.2. Required Information

The following provides more detail to supplement the Site Onboarding Overview process diagram. For onboarding your dynamic analysis services, Synopsys needs to know the following information:

1. **Web Application Hostname(s) and Associated Host Names**

   The application hostname establishes the boundaries of the WhiteHat Dynamic assessment. WhiteHat Dynamic will only assess content that is specified by the hostname.

   Associated hostnames are those that are considered part of the same application where content is either accessible from a single login entry or without authentication. These hostnames can be added to the assessment scope under the same license, and will allow the assessment to encompass the entirety of the web application. For example:

   - Hostname: *www.site.com*
   - Associated hostnames: *secure.site.com, www.contact.site.com*

2. **Requirements for Associated Hostnames**
   - The current application and potential associated hostname should be similar in content and functionality.
   - There should be shared functionality between the current application and the potential associated hostname.
   - The content on the potential associated hostname goes with the content on the current application.
   - The associated hostname shares a session with the base domain.
   - The associated hostname cannot have a separate login function.

3. **Credentials**

   Though credentials are not required for your application assessments to begin, they're important to ensure we're able to access and test all functionality, specifically for sites that contain authenticated content. Please provide two sets of credentials with access to most or all functionality. One account serves as the primary account for automated testing, while the second account serves as a backup in case the primary account becomes invalid. For PE licenses, two additional test accounts for each user level are needed for business logic testing. For Example:

   - *Two administrator accounts*
   - *Two expert or special user accounts*

- *Two standard user accounts*

  This allows us to perform both horizontal and vertical privilege testing across the various user roles of the application. For Example:

- *Can Imani see Dar's account profile data?*
- *Can a non-administrative user escalate their privileges to an administrative account?*
- *Can Shashi rotate through user accounts and perform transactions as another user?*

4. **Assessment Schedule**

The assessment schedule is the recurring weekly date and time range where WhiteHat Dynamic is allowed to actively test your application. WhiteHat Dynamic saves its progress between scheduled windows, so if a scan is unable to complete before the scan window concludes, it can pick up where it left off at the beginning of the next scan window. You can set your weekly schedule within the WhiteHat Portal interface, and there are several scheduling options available:

- **Continuous** (highly recommended): Assessments run 24x7
- **Nights & Weekends** (recommended): Weekdays from 8pm to 6am (based on the time zone you select), and 24 hours a day on weekends
- **Custom Schedule**: You can choose to create a custom assessment schedule based on days of the week and hours of each day. If this option is chosen, please ensure at least 40 hours of scan time per week

5. **IP Address Whitelist** All WhiteHat Dynamic scans or manual work will come from one of our IP addresses or IP address ranges. Which IP addresses should you add to your allow list?
   - **Non-EU Customers**: If your company does not reside in the EU and you are not restricting access to US Synopsys employees, allowlist all IPs within this column.
   - **EU Customers**: If your company resides in the EU, allowlist all IPs within this column.

Non-EU Customers	EU Customers
• 52.204.38.40 • 104.45.216.22 • 162.223.124.0/27 • 162.244.4.2 • 162.244.4.5 • 162.244.5.2 • 162.244.5.5	• 3.72.175.49 • 3.76.244.88 • 18.194.206.33 • 54.93.186.146 • 54.229.46.147 • 148.253.176.50 • 194.46.129.108

3.3. Service Delivery Timeline and Setup

- **Initial URL Crawl (1-3 Weeks)**

  Once URLs and site credentials (if applicable) are received and a scan schedule has been entered, our TRC engineers create a customized login sequence that teaches WhiteHat Dynamic to assess authenticated portions of the web application. WhiteHat Dynamic will then begin crawling (also called "spidering") your application. Completion time for the initial crawl varies depending on the number and size of pages within the application. During the initial crawl, only GET requests are made.

- **Review of Site Coverage**

  After the initial URL crawl, TRC engineers will examine all links discovered by WhiteHat Dynamic. If there are pages known to exist that are missing from our scan coverage, an engineer will add them to our testing scope as entry points. Directories or files that are not directly accessible from a link connected to the web application are common examples of pages that may need to be added as entry points.

  You can expedite this phase by reviewing the pages found and tested within the WhiteHat Portal and notifying us if sections of your application are missing.

- **Custom Test Configuration (PE and SE only) (1-10 Business Days/Ongoing)**

  As WhiteHat Dynamic crawls your application, it alerts our Threat Research Center (TRC) of any forms your application contains, so an engineer can make custom test configurations that both allow WhiteHat Dynamic to safely test each form and permit the WhiteHat Dynamic scan to spider pages that lay behind each form. We refer to this step as “form training.” If your application contains several layers of forms, it may take several passes by WhiteHat Dynamic and several rounds of form training to reach all application pages.

  During this step, the TRC engineer may also enable URL rules for any template pages contained in your application. These rules instruct WhiteHat Dynamic to test a sample number of pages for each template used, which allows each WhiteHat Dynamic scan to complete more quickly while remaining thorough. As an example, an auction site that contains millions of products and is constantly adding additional products may use a common template. Instead of attempting to assess each individual product page, we will create a URL rule to assess only a subset of them. This reduces scan completion time without sacrificing quality.

3.4. Vulnerability Verification

Any time WhiteHat Dynamic finds a vulnerability, it flags the page and attack vector and sends a notification to the Threat Research Center. Using a combination of more than 17 years of data intelligence and human verification, the vulnerability is confirmed as true and actionable before it is posted. Vulnerabilities are grouped by the URL on which they are discovered, and then into the various vulnerability classes found within the Web Application Security Consortium V2 (WASC v2). The various

methods to exploit discovered vulnerabilities are categorized by vulnerability parameters known as “attack vectors”.

3.5. Business Logic Assessment (5 Business Days/Ongoing)

If you’ve purchased PE Service, you may schedule your BLA for any point during your license period. In the BLA, our TRC engineers will assess your application for vulnerabilities in its business logic. This testing is done by hand and can be scheduled in the WhiteHat Portal, under the "Services" subtab for the specific site.

3.6. Initial Assessment Complete

The initial assessment is understood to be complete when the Vulnerability Verification phase detailed above is completed.

At this point, we recommend scheduling a Vulnerability Review call where our TRC engineers can discuss and explain vulnerabilities. This call includes a detailed breakdown of each vulnerability, as well as a live demonstration of the vulnerabilities discovered, and is a great opportunity to involve other members of your security and development teams.

We encourage you to request a Vulnerability Review any time during your subscription term.

Chapter 4. Sentinel Mobile Onboarding

4.1. Required Information

For onboarding your mobile analysis services, we need to know the following information:

- Project files for your Mobile Application(s)
  - Source code
  - Build files

Our TRC engineers will need your application's project files, including source code and build files. You can upload these files to the SFTP account we create for you. Our Mobile Assessment Team securely downloads these files to conduct the assessment, and deletes them permanently when the assessment is complete.

4.2. Service Delivery Timeline and Setup

- **SFTP Account Setup (1 Business Day)**

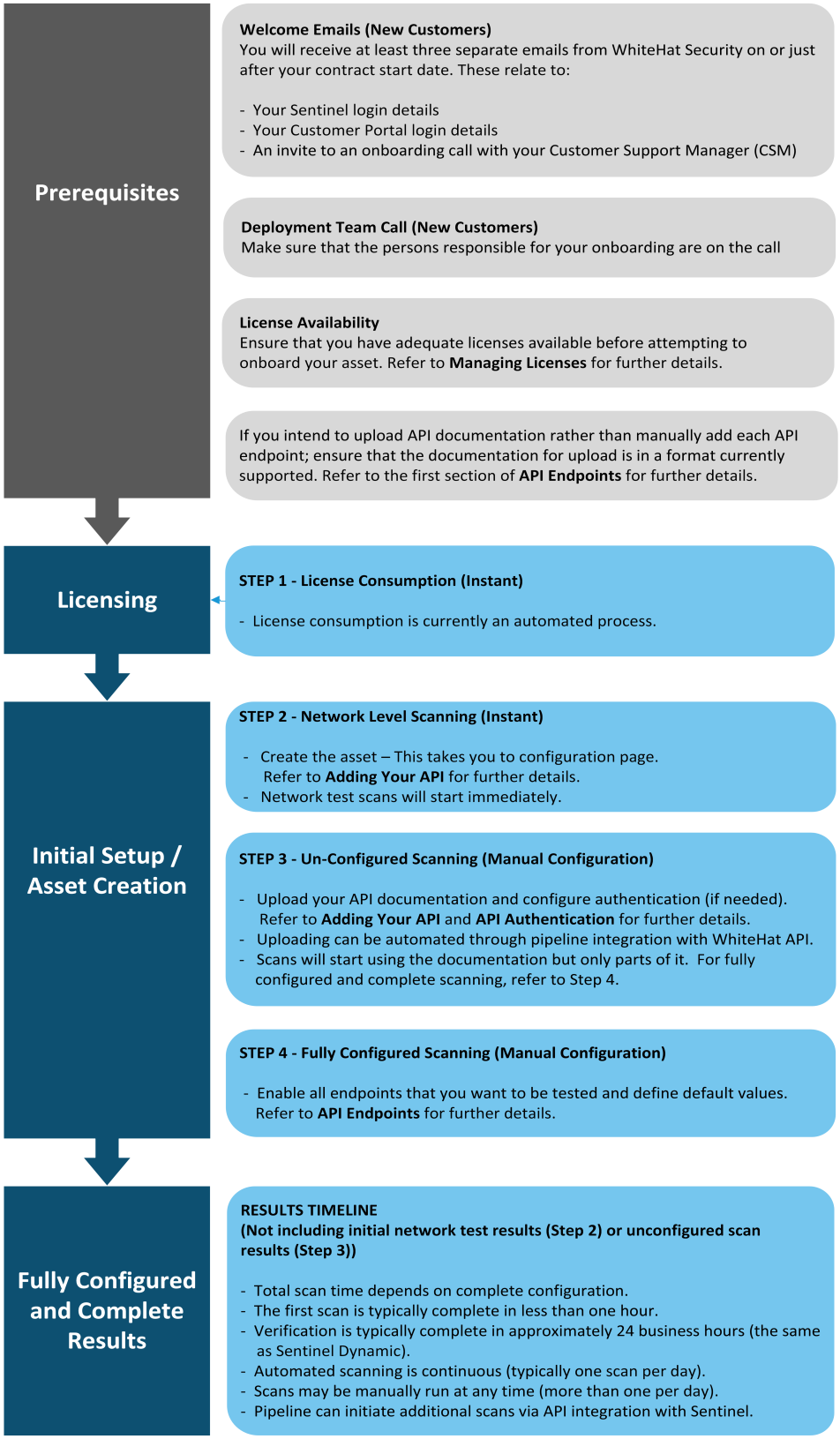
  Our Service Deployment Team will create an account for your team on our SFTP server and provide you with access details. This is where you'll need to upload your application's project files.

- **Assessment (10-15 Business Days)**

  During this time, TRC engineers will be assessing your mobile application for vulnerabilities.

Chapter 5. Sentinel API Onboarding

5.1. Onboarding Overview



5.2. Useful Links

Refer to the following useful links for more information

- Managing Licenses in the WhiteHat Portal
- Adding Your API
- API Endpoints
- API Custom Headers
- API Authentication

Chapter 6. Onboarding FAQ

6.1. General

1. **What does a "Site" asset refer to?**
   This refers to an asset tested by WhiteHat Dynamic (DAST).
2. **What does an "Application" asset refer to?**
   This refers to an asset tested by Sentinel Source (SAST).
3. **What is the difference between the dynamic service levels?**
   - **WhiteHat Dynamic BE** - The Basic (BE) service level is ideal for site discovery and for static sites.
   - **WhiteHat Dynamic SE** - The Standard (SE) service level is appropriate for permanent websites that use forms and logins but, are not necessarily mission-critical for your business.
   - **WhiteHat Dynamic PE** - The Premium (PE) service level is appropriate for complex mission-critical sites. It includes all the testing involved in the Standard service level, with the addition of business logic and multi-step form testing. PE is particularly appropriate for sites with rigorous compliance requirements and/or complex interactions.
4. **Are there video tutorials available for WhiteHat Portal fundamentals?**
   Video tutorials for the WhiteHat Portal are available from here: Video Tutorials.

6.2. Setup times

1. **What permissions are necessary for onboarding?**
   Permissions need to be enabled on the backend for an account to complete the onboarding process. If you need help with these permissions reach out to the support team or, if you're not the primary contact for the account, have the primary contact reach out on your behalf.
2. **What is the average time between initial setup and full scan results for DAST?**
   Currently the average time between configuration and full scan results for PE and SE DAST testing is two weeks.
3. **What is the average time between initial vulnerability assessment scan results for SAST?**
   Currently we aim for initial assessment of vulnerabilities to be completed in ten days for SAST: SE. Vulnerabilities found in subsequent scans should be reviewed within one or two business days.
4. **What is the average time between initial vulnerability assessment scan results for mobile SE (MAST)?**
   Currently the average time for mobile SE takes three days after initial configurations. On average it can take two weeks for both iOS and Android assets.

6.3. DAST

1. **What is the difference between DAST Parse Scan and vulnerability scan?**
   All DAST assessments start with a Parse Scan before moving to Vulnerability scans by default. The Parse Scan is a faster scan that is recommended for the initial assessment phase, during which TRC will verify your credentials once received and configure the site for authenticated scanning. TRC then manually adds entry points and tests any forms on the site, adding them to the scan if production safe, which results in proper site coverage. For Vulnerability Scans, within 24 business hours of the first vulnerability scan completing, you should have any scanner found vulnerabilities present in the **Findings** tab in the WhiteHat Portal. Vulnerability scans can be enabled at any time during the initial assessment if required, but this will result in getting full results being obtained more slowly.
2. **What could cause delays to my assessment timeline?**
   Potential delays to the assessment timeline can be caused by:
   - Not using a continuous scan schedule
   - Slow server response times
   - Site size
   - Access issues
   - Ignoring any open support cases from the TRC
3. **Can I enable vulnerability scans during initial assessment?**
   Users can enable vulnerability scans during initial assessments, however following our normal processes will provide scan results faster overall. If you require vulnerability scans to be enabled sooner than our normal recommended process, you should contact support.
4. **If my site is external, do I need to set up a virtual machine (VM) for DAST testing?**
   No, if the site is external, then no VM is necessary.
5. **If my site is internal, do I need to set up a VM for DAST testing?**
   Not necessarily, adding Synopsys' IP addresses to an allow list will provide Synopsys with access to your site.
6. **If my site is internal and only available on our internal network, do I need to set up a VM?**
   Yes, in this case a VM is necessary.

6.4. Base URL

1. **Do I need to provide a file path when onboarding the Base URL?**
   The Base URL needs to give a 200 OK response or similar, if that means including the filepath for the Base URL, the user will need to include it.
2. **Do I need to put a URL rule in place?**
   If you require us to only scan from a certain file path and not from the base URL, you will need to put a URL rule in place. If not, our scanner always tries to scan from the base domain.

3. **Can I swap URL once onboarding has started?**
   No, unless you have a Swap license you cannot swap the URL once onboarding has started.
4. **Can I make changes to my site's server port numbers after onboarding?**
   No, if you want to change server port numbers you have to re-onboard that asset.
5. **Is the scanning production safe?**
   Yes, Sentinel has been designed to be extremely safe for production. You can read more about Production Safety here.

6.5. Associated hostnames AHNs

1. **What are the requirements for adding an AHN?**
   The requirements for adding an AHN are as follows:
   - Logging into one login portal with the same set of credentials must allow a user to reach authenticated content on both the base domain and any AHN.
   - If the same session does not allow access to a proposed AHN, it must be considered a separate site for the purposes of licensing and assessment (i.e., a new license is required). A common example would be the login functionality being hosted on a different subdomain, such as: secure.example.com, but the main content of the application being www.example.com. It would still be possible to configure the scan to authenticate to www.example.com since we would only be requesting the resource found on secure.example.com for authentication purposes, but the login functionality itself and any other resources found on secure.example.com would be excluded from the assessment if not requested as an AHN.
   - An AHN or domain must be determined to be a **Necessary Hostname** if it seems to be a part of the main site and vital to how the main site functions. Requests must be made to it as a natural consequence of authenticating to or browsing the main site.
2. **Can I list a Single Sign On (SSO) site as an AHN?**
   Not usually. Single Sign On (SSO) sites usually do not meet the "Necessary Hostname" requirement as stated.
3. **How many AHNs can I add to the scope of a license?**
   Ten, we cannot make exceptions for more. If more are needed, you must purchase an additional license.

6.6. Credentials

1. **What credentials do I need to provide for DAST scanning?**
   You must provide two sets of unique credentials of the highest user level that you want us to scan with.
2. **Are additional credentials needed for Business Logic Assessments (BLA)?**
   Yes, two additional sets of unique credentials for PE/BLA of the highest user level that you want us to test with.

3. **Can I scan unauthenticated?**
   Yes, you can disable credentials from the **Scan** tab in the WhiteHat Portal. You can also disable BLA credentials from the **Services** tab, find out more here.
4. **What if my site uses Captcha?**
   If your site uses Captcha it will need to either be disabled, which can be done via adding our IP addresses to an allow list, or by providing a static token that will always work to bypass the Captcha.
5. **Do you have the ability to self provision credentials?**
   Yes, if your site has a registration function, we can self-register credentials instead of provisioning them yourself. You can add a note to the **Additional Notes** section when onboarding if you'd like us to do this for you.
6. **What if my site uses two factor authentication?**
   If your site uses 2FA, we support Email and SMS authentications, or a static SMS token can be provided as a solution. Please note that the non-static SMS option requires an additional fee. The email address you must use for email authentication is provided on request through support.
7. **Can you scan more than one user level per license?**
   No, during a contract we can only scan a single user level. Additional user level scanning would require the purchase of additional licences.
8. **Can I use the same credentials between sites?**
   We highly recommend using completely unique credentials between sites. If not, depending on how your system is configured, it may result in credential lockouts and other issues.

6.7. BLAs

1. **Do I have to schedule BLAs myself?**
   Yes, you must schedule the BLA yourself, as they operate on a "use it or lose it basis".
2. **Will the BLA test more than one set of credentials?**
   The BLA will only test one set of credentials fully. Privilege level tests can be done on two other sets of credentials, i.e. a second admin level for horizontal testing, and one lower user level for vertical testing. By default, we fully test the highest privilege level provided unless otherwise specified.
3. **What happens if my BLA has been put on hold before the BLA has started?**
   If a BLA gets put on hold, you must respond to any support cases and stay in communication with us for the resolution of any issues. If not, the BLA will be canceled and you will have to reschedule it.
4. **What happens if I don't respond to my case if my BLA is put on hold after the BLA has started?**
   If you do not respond within two weeks for minor issues like credentials, or four weeks for major issues like the site is inaccessible or missing functionality, the BLA will be closed and marked complete. The BLA then cannot be reopened on this BLA license.
5. **Does the current state of my site matter?**
   Our manual assessors will need to know if the site contains live data and if they have permission to

test it.

6. **Do I have to provide dummy data for testing?**
   If dummy data will not work for testing forms, you must provide us with examples of information that will work e.g. employee ID. You can attach this via the **Notes** or **Attachments** in the **Services** tab in the WhiteHat Portal.

6.8. Virtual Machine Scanning

1. **What are the requirements for VM Scanning?**
   The installation and system requirements can be found here.
2. **If I'm using a DAST VM, do I need to have DNS resolution set up on my appliance?**
   We recommend that you have DNS set up. If you do not have DNS set up, you will need to provide the site's internal IP address.
3. **How many VM's will I need for SAST?**
   If your licensing totals more than five million LOC, you will likely be required to set up additional VMs.

6.9. Cloud Scanning

1. **Can I use Cloud Scanning instead of a VM?**
   Yes, cloud scanning can be used if you don't want to host a VM.
2. **Can I schedule a regular cloud scan?**
   No, with cloud scanning you cannot schedule a regular scan.

6.10. SAST

1. **Do I have to separate my application into smaller assets?**
   Potentially, depending on how you have your application set up, each asset should represent a single version of an application that runs in a single environment, on a single host. For example, the front end should be a separate asset from the backend.
2. **What is the difference between Pre Scan and Full Scan?**
   Pre Scan is a parse-only scan to check that we can access the site, ensure that you are within your license allotted LOC, and to check for missing dependencies. Pre Scan does not identify vulnerabilities or consume any WhiteHat licenses. Full Scan is a deep scan that identifies vulnerabilities which are then confirmed by Synopsys TRC. Full Scan requires and consumes an appropriate license.
3. **How can I tell if I'm getting full coverage?**
   You can use an LOC count or Extensions Scanned for a quick reference, or check the File Coverage section for a more in-depth coverage report.
4. **For SAST scanning, what happens if a vulnerability is raised that I have a fix for in a different part of my code?**

You may get a false positive as a result of Synopsys not having access to all of your code. If you have a remediation for a vulnerability located in a different part of your code, you can simply use the **Ask a Question** feature to explain this to us, so that we can review and close the vulnerability.

6.11. Mobile

1. **What are the requirements for Mobile onboarding?**
   More information on Sentinel Mobile onboarding can be found here. A video tutorial for onboarding mobile assets can be found here.
2. **Does Mobile BLA require me to set up Secure File Transfer Protocol (SFTP)?**
   Yes, you must upload both the Mobile Onboarding form and the binary to SFTP. When you are ready, Synopsys will provide SFTP credentials for you to use.

6.12. API SE (AutoAPI)

1. **Can I enable POSTs and PUTs to be scanned?**
   Yes, but these are not production safe.
2. **What if my API has POSTs and PUTs enabled?**
   These requests are not production safe.
3. **Are custom login configurations available for APIs?**
   No, custom login configurations are not supported, although custom headers can be added.
4. **Why is my POST request not working for the login configuration?**
   You may need to use a GET request instead.

6.13. API BLA

1. **How many operations can I test with one API BLA license?**
   Each license that you have represents one operation that Synopsys can test, i.e. if you have 10 API BLA licenses, Synopsys can test 10 operations.
2. **Do I have to provide any API documentation?**
   Documentation is required from you about your API. It must contain:
   - All of the endpoint URLs
   - All known parameters and values associated with each parameter
   - Any credentials or tokens required for authentication
   - Working examples in a full HTTP request form
   - Documentation for usage of the API
3. **Do I need to provide the documentation in a specific format?**
   Yes, provide the documentation in Postman-compatible or SoapUI-compatible collections. If it does not come in one of the following formats, the assessment could potentially take significantly longer

to complete.

- Postman-compatible documentation in JSON or YAML format:
  - Open API 3.0 specifications
  - Swagger 2.0 specifications
  - Postman Collection v2.1
- SoapUI compatible documentation:
  - WSDL format (file or URL)
  - REST API in XML format
  - SoapUI projects

4. **Can I schedule the BLA after I have sent the API documentation?**
   Once the documentation is sent to the Sales Engineer (SE) via a case to review, they confirm that it has the expected number of operations and everything needed for the assessment is present, after that we will onboard the site and schedule the BLA on your behalf.

6.14. Findings

1. **What is the difference between automatic and manual retesting?**
   The difference between automatic and manual retesting is that automatic retesting is denoted by a computer icon on the Findings tab and can be retested automatically within 30 minutes. Manual retesting is denoted by a person icon on the Findings tab and needs to be retested by a person which requires up to 24 business hours.
2. **I'm having trouble reproducing a finding. What might be wrong?**
   If you're having trouble duplicating a finding, make sure you're using the data from the Vulnerability Detail page's Description and Solution section. If a proof of concept (POC) is provided, make use of it. Also, ensure that you're accessing your site with the same configurations as Synopsys, otherwise you may get a different result. If you're still having problems, please use the Ask a Question feature to contact our customer support team. Please do not use this for retest requests as you can simply click the Retest button on the Findings tab or the Vulnerability Detail page.
3. **Can I see what request and response your scanner saw when testing a finding?**
   Yes, you can view the vector details by clicking the Vector ID on the Vulnerability Detail page. The Vector Detail page displays both the manipulated request sent, and the vulnerable response received.

6.15. Support

1. **How do I access the Customer Support Portal ?**
   Log in to the Synopsys Software Integrity Community here.
2. **How do I create a support case?**

We prefer if you use the Community Portal to create cases. You can either login to the Community Portal and create a case, or email support@whitehatsec.com, which will automatically create a case. Note that if you email support, please wait until we respond before emailing again so that we can attach a reference number to the email. This enables all further communication to be logged under the same case. Otherwise, each email would create a separate support case. Also, please note that a new support case should be used for each unique topic.

3. **What if I'd like to request a call with the support team?**
   If your question requires a subject matter expert, i.e. a vulnerability question, we require a minimum of 48 hours advanced notice, the longer the notice given, the better. When making the request for the call, please provide questions and/or as much detail as possible.

4. **How do I contact the support team?**
   You can log in to the Community Portal and contact them by creating or responding to a case. If you do not have Community Portal access you can email support@whitehatsec.com.