# Continuous Dynamic Service Definition

Black Duck Software, Inc.

2025-05-16

# Table of Contents

# Chapter 1. Continuous Dynamic Services Across the SDLC

Black Duck offers tools and services appropriate to each step of the Software Development Life Cycle (SDLC), each of which includes verified vulnerability results. We also have several training programs designed to support a variety of different roles across your security platform, teaching your team to integrate security practices into their daily job functions. Training is available on-site, via webinars, or as computer-based training (CBT).

Application security testing (AST) products and services are designed to analyze applications for security vulnerabilities. Ideally, an application would be tested using multiple approaches to ensure its security throughout the Software Development Lifecycle (SDLC).

Black Duck provides AST solutions to cover the entire SDLC.

| Production Stage | Description |
|---|---|
| Pre-Production | Sentinel Source (SAST), our Static AST technology, analyzes an application's source code for security vulnerabilities at the development and testing phases of the SDLC. |
| Staging and Live Production | Continuous Dynamic (DAST), our Dynamic AST technology, analyzes applications in staging and in production. We also offer API testing services. |
| Mobile Security | Sentinel Mobile, our Mobile AST, uses a combination of traditional SAST and DAST and behavioral analysis using static and dynamic techniques to discover malicious or potentially risky actions the app may be taking without the user's knowledge. |

# Chapter 2. Continuous Dynamic Testing Methodology

Black Duck offers vulnerability assessment throughout the software development life cycle; the testing methodology used depends on whether we are examining code or a site already in production.

## 2.1. Sentinel Source (SAST) Methodology

Sentinel Source offers vulnerability assessments for static code, even before it can be compiled. The Sentinel Appliance retrieves application code from a repository and, using rule-packs to define the conditions under which a vulnerability should be flagged, the scanning engine identifies vulnerabilities in the code. This requires that the TRC engineers work with the client to establish that the appliance has access to the correct repository, that the code is broken into applications correctly, and that it can be processed by the scanning engine. Once the scanning engine has identified potential vulnerabilities, the code snippets in question (which may include YAML configuration files) are passed to the TRC engineers for confirmation, ensuring that the customer only receives actual vulnerabilities.

## 2.2. Continuous Dynamic (DAST) Methodology

Continuous Dynamic offers vulnerability assessments for web applications in production or pre-production. The Continuous Dynamic scanner tests the application based on logical conditions established by the Threat Research Center; it discovers vulnerable behavior rather than being restricted to specific known issues. As new attacks are discovered, the TRC augments this testing to ensure that they are also detected, and those tests are created and updated on a daily basis.

The Threat Research Center will monitor and configure the scanner to ensure that the scanner can find every page, log in and maintain a session, support multi-step login, test every form that is safe to test and no form that is not safe to test, submit valid data, and will not loop and waste time testing identical pages. TRC engineers will examine each potential vulnerability discovered by the scanner to ensure that only actual vulnerabilities will be passed on to you for remediation, and will customize the risk, description, and solution associated with each vulnerability as needed; proofs of concept will be included appropriately. Unless a customer’s Continuous Dynamic Admin has deliberately requested tests that are not considered production safe, only production-safe tests will be run on production sites.

In addition to the service described above, Black Duck also offers Business Logic testing. Continuous Dynamic PE services include one or more Business Logic Assessments (BLAs) a year; in these assessments, experienced Threat Research Center security engineers focus on finding issues automated scanning is unlikely to find. This can include testing sensitive areas of production applications, looking for authentication and authorization issues, process logic flaws, and difficult-to-identify technical vulnerabilities such as blind cross-site scripting or blind SQL injection, as well as searching for vulnerabilities relating to the specific functionality of the application. To complete these tests, the engineer will reach out to the customer point of contact for any additional information that

may be needed.

## 2.3. API Testing Methodology

We also offer dynamic testing for standalone APIs. The difference is that, instead of the scanner crawling a site by parsing its HTML, testing depends on the customer providing documentation for a set of API calls. In our AutoAPI service, those become the basis for testing with the Continuous Dynamic engine. The testing is automated, but the results are human-verified. We also offer API Business Logic Assessments (BLAs), where a wider variety of issues are tested for by humans who can understand what the API calls mean.

## 2.4. Mobile Premium Methodology

Android or iOS mobile applications can be assessed like any other static code using Sentinel Source; in addition, Black Duck can provide a premium assessment from our dedicated team of mobile security experts in the Threat Research Center. For a premium mobile assessment, the customer will need to provide both the source code and the compiled version of the application directly to the Threat Research Center's mobile team. The mobile team will examine the application and the application code for issues around the configuration settings, authentication/authorization, session management, data handling and storage, anti-analysis, jailbreak/root detection, cryptography, data handling and storage, server-side controls, and secure coding best practices.

# Chapter 3. Production Safety

Continuous Dynamic services have been designed from the very beginning to be extremely safe for production web applications. Our maxim at Black Duck is "Do no harm" or, put more casually, we like to ask "Is this important?" before running a scan, rather than asking "Was that important?" afterward. By default, Continuous Dynamic operates "production-safe." This means that Continuous Dynamic only performs tests that will not permanently change the state of the system. So, you can be confident that we will safely scan your production business websites during business or high-traffic hours. To make sure we maintain little to no impact on your application, we'll need you to let us know if any of the following exists on your application:

- State-changing functionality performed via GET request
- Areas of the application or specific functionality you'd like us to refrain from testing

## 3.1. Key Features

In addition, we have implemented three key features that are unique to Continuous Dynamic that ensure that our testing remains completely safe for your production websites.

1. Customized Configuration

   The Black Duck Threat Research Center (TRC) manually reviews your web application and customizes Continuous Dynamic testing for safety and thoroughness. Every input, state changing request (POST request), or sensitive functionality is carefully analyzed by a human TRC engineer. Our engineers check this functionality first for safety, then for depth and coverage.

   This is especially applicable to administrative level functionality—things like create/delete users or groups. This kind of functionality is deemed unsafe to test in an automated fashion and Continuous Dynamic will be configured not to place these sensitive requests. Instead, a security engineer can check this functionality by hand in order to ensure little to no impact on the application. Examples of functionality that are commonly deemed unsafe:

   - Creation and deletion of users or data
   - Contact us features that involve sending email
   - Updating/Editing Profile or account data
   - Leaving comments or forum posts (Submit functionality)

     When an input or area of functionality is deemed safe for automated testing, a security engineer configures Continuous Dynamic to submit valid data in order to get further into the application.

     ***Customized Configuration Example:*** *A website has a "create user" page that requires a valid address and email address in order to successfully complete. A security engineer recognizes that these inputs are required and trains Continuous Dynamic to submit valid information in order to*

*get through this page. This action is repeated as long as the submitted request is deemed safe until the functionality is thoroughly covered. As part of the configuration process, TRC engineers also examine every link discovered by Continuous Dynamic to ensure overall coverage and to streamline the automated assessment for safe and efficient scanning.*

2. Non-Invasive Testing

   Many scanners bombard your site with hundreds or thousands of simultaneous requests, running the risk of negatively affecting or even bringing down the site being tested. Instead, Continuous Dynamic uses single-threaded requests during the automated portion of the web application assessment; much like a real user, Continuous Dynamic sends a request to your website and waits for a response before submitting the next request. In addition, by default Continuous Dynamic will place a maximum of four requests per second for a given set of credentials. (You can control this cap from the Continuous Dynamic Portal interface.) This approach ensures that your production sites never receive an unexpected heavy load of requests coming from our scanner.

3. Continuous Dynamic Will Not Execute Live Code

   By leveraging customized testing methodology unique to Continuous Dynamic in combination with our TRC's vulnerability verification process, Continuous Dynamic is able to detect vulnerabilities safely without executing live code on your web application. You are guaranteed that Continuous Dynamic will never execute live code in an automated fashion on your website. This greatly reduces the chance of negatively impacting the application.

## 3.2. Tracking Our Assessment Activities

As well as these production safety measures, we also provide clients with two easy methods of tracking all assessment activity:

**Custom Watermark** A "Black Duck Software" user agent header is added to all requests that originate from Continuous Dynamic. This allows you to create filters to monitor our activity, or to exclude certain alerts or warnings.

***Sample watermark:***

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0 Black_Duck_Software
```

For sites onboarded **before October 25, 2024**, the user agent header will contain the string `WhiteHat Security` and not `Black_Duck_Software` (the old header will not be changed retroactively).

If there is a specific watermark you would like us to use, let us know and we can customize the user agent header to include it.

### IP Address Allow List

All Continuous 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 Black Duck 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 |
| --- | --- |
| • 104.45.216.22<br>• 162.223.124.0/27 | • 3.72.175.49<br>• 3.76.244.88<br>• 18.194.206.33<br>• 54.93.186.146<br>• 54.229.46.147<br>• 148.253.176.50<br>• 194.46.129.108 |

# Chapter 4. Sentinel Source (SAST)

Sentinel Source is the SAST component of the Continuous Dynamic platform. We offer three levels of SAST testing to cover all your security needs.

- **Sentinel Source Standard Edition (SE)** is a full-service solution designed to incorporate security into your software development life cycle (SDLC). It enables you to assess your code as it is being developed and assists developers in identifying and remediating vulnerabilities before the code is pushed to production. As developers write code, containerize and upload it to a repository, Sentinel Source analyzes the code and identifies potential security vulnerabilities. Sentinel Source operates via our Sentinel Source engine housed on an installed VM image completely within your network. Any code snippets, including YAML configuration files, containing vulnerabilities identified by our automated Sentinel Source scanner are then sent to the Black Duck Threat Research Center (TRC) engineers to verify. Once verified, vulnerabilities are reported back to you either through the Sentinel Source user interface or directly into your bug-tracking system by integration with the Sentinel Source API.
- **Sentinel Source Essentials Edition (EE)** provides raw SAST findings as soon as a scan is completed, without any TRC services such as scan review, vulnerability verification to weed out false positives, Directed Remediation, or Ask-a-Question. The EE service provides a lower cost SAST service for non-mission critical apps, assuming that you have the knowledge to self-verify any findings.
- **SCA - Essentials (SCA)** rapidly and accurately identifies the third-party and open source components that have been integrated into your source applications. For each of these components, SCA identifies any open security common vulnerabilities and exposures (CVEs), licenses, and out-of-date library versions and age. SCA also creates a list of raw Unpatched Library findings, if any, for your source application as soon as a scan is complete. Applications onboarded using this service level will be limited to a maximum of 3M lines of code.

  This lower cost development tool does not include static analysis (SAST) or the following TRC services: Scan Review, Vulnerability Verification, Ask-a-Question, and Directed Remediation. SCA is suitable for non-mission-critical apps and for customers who have the competence to self verify these raw findings.

Each service level has features that make it uniquely appropriate for specific business needs.

## 4.1. Sentinel SCA Essentials Edition (SCA)

SCA is a standalone software composition analysis automated security testing service that rapidly and accurately identifies the third-party and open source components used in your source applications. For each of these components, SCA identifies:

- Any open security common vulnerabilities and exposures (CVEs)
- Licenses

- Out-of-date library versions and age

SCA also creates a list of raw Unpatched Library findings, if any, for your source application as soon as a scan is complete. Applications onboarded using this service level will be limited to a maximum of 3M lines of code.

This lower cost development service does not include static analysis (SAST) or the following TRC services: Scan Review, Vulnerability Verification,Ask-a-Question, and Directed Remediation. SCA is suitable for non-mission-critical apps and for customers who have the competence to self-verify these raw findings. The SCA service is included at no additional charge in Sentinel Source Standard Edition (SE) and Sentinel Source Essentials Edition (EE). Once you've purchased a license, you can add an SCA asset by going to the Assets Management page and selecting Add Application (SCA) from the Add Assets dropdown menu. For EE, select Add Application, and select Essentials Edition (EE) under service level.

SCA provides unverified findings that are identified by a gray V icon next to the Vulnerability ID, to differentiate them from verified findings, identified by a green V icon. These findings can be filtered by Verification Status on the Findings pages. If you determine that any of these unverified findings are false positives, you can mark them as Invalid by going to the Findings page, selecting them, and selecting Change Vulnerability Status from the Bulk Actions dropdown menu. SCA results for all your SAST and SCA applications are now available under a new Components tab, instead of under the Summary Dashboard.

## 4.2. Sentinel Source Essentials Edition (EE)

Essentials Edition (EE) is a new service level in Sentinel Source to provide raw SAST findings as soon as a scan is completed, without any TRC services such as scan review, vulnerability verification to weed out false positives, Directed Remediation, or Ask-a-Question. The EE service provides a lower cost SAST service for non-mission-critical apps, assuming that you have the knowledge to self-verify any findings.

You can now select the EE service level when adding a new asset. As before, license availability is checked and consumed when a Full Scan is requested. The selected service level will be displayed on the Asset Details page and unverified findings will be displayed on the Findings page with ability to filter them from other verified vulnerabilities. Finally, the Admin Account Overview page will show the license usage service level in addition to license type.

## 4.3. Sentinel Source Standard Edition (SE)

Sentinel Source SE is the full-service way to evaluate the security of your code as it is being developed.

# 4.4. Sentinel Source (SAST) Overview

| Feature | Details |
|---|---|
| Concierge Onboarding | The Black Duck Implementation Team will:<br>• Schedule a Webex welcome call to review all pertinent information and requirements for onboarding.<br>• Review all onboarding logistics (e.g. account set-up, purchase review) and verify and validate site specification(s).<br>• Deliver 'Welcome' documentation and review customer deliverables to ensure a successful onboarding and utilization. |
| Flexible Reports: | • Executive summary and unit level aggregation of data in flexible formats.<br>• Trend monitoring, including remediation rate, time to fix vulnerabilities, and age of vulnerabilities.<br>• Compliance reports (PCI) available at any time. |
| Access to Black Duck Engineers: | The Ask-a-Question feature gives direct access to TRC engineers. Questions can be submitted and responses received via the Continuous Dynamic Portal UI. If the Ask-a-Question feature is enabled, questions can also be asked through the Continuous Dynamic JIRA® plugins, allowing customers to integrate Continuous Dynamic information directly into their issue tracking software. (24 hour response.) |
| Access to Customer Support | Customer Support is available in the Black Duck Community, where customers can view their cases, submit cases, or access Continuous Dynamic documentation and tools.<br><br>You can also click here to email Customer Support. |
| Vulnerability Verification | When a Sentinel Source scan discovers a potential vulnerability, the potentially vulnerable code snippet is sent to our TRC engineers. Our engineers then personally verify that the vulnerability is real and actionable before posting it to your Portal interface, eliminating false positive alerts. |
| Code Coverage Review | Before Black Duck finalizes any assessment, we review the code coverage, complete operational checklists intended to ensure completeness, and perform business logic mapping. |
| Open XML and JSON API Integration | In addition to developing plugins that integrate Continuous Dynamic data with JIRA®, Black Duck offers a RESTful JSON XML-based Continuous Dynamic API that enables customers to create their own integrations with the Portal and utilize its data in their own applications. Support for Sentinel Source includes our API documentation and training (see http://apidocs.whitehatsec.com). |

| Feature | Details |
| --- | --- |
| Intellectual Property Preservation | Sentinel Source was designed to fit within the way organizations work. Therefore, Black Duck deploys a VM appliance at a customer's site. No code is removed from the network. Because assessments are done on the premises and only small code snippets are available to Black Duck engineers for verification, source code will not leave the developer's site—eliminating the possibility of IP loss or theft. (Note that a manual assessment of a mobile application will require a more complete code review, and therefore the Sentinel Source Mobile Manual Assessment is not included in this list.) |
| Flexible Assessment Scheduling | Sentinel Source allows for a flexible assessment schedule. An assessment may be scheduled as soon as code is put into the repository, to gather immediate feedback; assessments may also be scheduled at a specific time every day, to reduce the risk that assessments will be delayed until the last minute. (Note that a manual assessment of a mobile application will require the intensive involvement of a Threat Research Engineer, and therefore the Sentinel Source Mobile Manual Assessment is not included in this list.) |
| Proof of Concept | For code vulnerabilities discovered via Sentinel Source, Black Duck will provide proof of concept for the vulnerability. |

# Chapter 5. Continuous Dynamic (DAST)

Our dynamic application testing services can be used to test production and pre-production web applications ("Sites"), using a combination of automated testing and manual assessments performed by our Threat Research Center (TRC) engineers. Black Duck has multiple Continuous Dynamic service lines providing varying degrees of application coverage. A Site in this context is understood as:

- One primary host name - This is the main domain associated with a site asset: for example, https://www.example.com.
- Up to ten associated host names - These are usually subdomains that cannot be crawled from the primary host but are essential to the function of the site being assessed.

## 5.1. Continuous Dynamic Portal-Supported Browsers

The Continuous Dynamic Portal provides full, certified support for the **Google Chrome** and **Mozilla Firefox** browsers.

Google Chrome

Mozilla FireFox

We test our products in the certified browsers and are committed to remediating defects identified during testing or reported by customers. Customers using non-supported browsers may experience incorrect functionality in some features. Black Duck encourages customers to use the supported browser versions, both for Portal functionality and for improved security.

Additional browsers may be supported on a case by case basis, depending on demonstrated business needs. For additional browsers, we will also identify and correct defects where a clear business case can be made for doing so. The same level of support guarantee offered with our Certified Supported browsers, cannot be offered for additional browsers. Some older browsers (e.g. IE11) will not be supported. For these browsers, we will not identify or remediate issues. The following is a summary of policies for certified browsers:

- Certified browsers are fully supported on all supported operating systems.
- Browser releases are evaluated quarterly and browser certifications for the Portal are updated accordingly.
- Discontinued versions of certified browsers will no longer be supported.

# 5.2. Continuous Dynamic (DAST) Service Detail

Black Duck offers three levels of Continuous Dynamic DAST services, each of which has features that are uniquely appropriate for specific business needs:

## 5.2.1. Continuous Dynamic DAST Baseline Edition (BE)

Baseline Edition (BE) is a basic unconfigured scan, designed to assess web applications that do not contain forms, like brochure-ware. This is our core offering, including automated scanning and vulnerability verification, and is ideal for identifying your sites and determining the degree of protection that is appropriate for each. Continuous Dynamic BE includes identification of technical vulnerabilities, verification of vulnerabilities to eliminate false positives, access to the Black Duck Threat Research Center (TRC) for support, and unlimited retesting to ensure your remediation strategies are effective.

| Overview Item | Details |
|---|---|
| Concierge Onboarding | The Black Duck Implementation Team will:<br>• Schedule a video welcome call to review all pertinent information and requirements for onboarding.<br>• Review all onboarding logistics (e.g. account set-up, purchase review) and verify and validate site specification(s).<br>• Deliver "Welcome" documentation and review customer deliverables to ensure successful on-boarding and utilization. |
| Continuous Dynamic Portal User Interface | The Portal user interface offers 24/7 Dashboard access to all your vulnerability information, including:<br>• **Flexible Reports**<br>◦ Executive summary and unit level aggregation of data in flexible formats.<br>◦ Trend monitoring, including remediation rate, time to fix vulnerabilities, and age of vulnerabilities.<br>◦ Compliance reports (PCI) available at any time.<br>• **Access to Black Duck Engineers**<br>The Ask-a-Question feature gives direct access to TRC engineers. Questions can be submitted and responses received via the Portal UI. If the Ask-a-Question feature is enabled, questions can also be asked through the Continuous Dynamic JIRA® plugins, allowing customers to integrate Continuous Dynamic information directly into their issue tracking software. (24 hour response.) |

| Overview Item | Details |
|---|---|
| Access to Customer Support | Customer Support is available in the Black Duck Community, where customers can view their cases, submit cases, or access Continuous Dynamic documentation and tools.<br><br>You can click here to email Customer Support. |
| Verified Vulnerabilities | When a scan discovers a potential vulnerability, the potential vulnerability is reviewed using more than 17 years of data intelligence and human verification. Only once we have verified that the vulnerability is real and actionable will it be posted to your Portal interface, eliminating false positive alerts. Automated retesting is available on demand. |
| Proof of Concept | Black Duck will provide a proof of concept for vulnerabilities. |
| PCI Compliance | Continuous Dynamic (PE, SE, and BE) services exceed requirements of the PCI DSS providing on-going verified vulnerability assessments for both public and internal websites. |
| Open JSON and XML JSON and API Integration | In addition to developing plugins that integrate vulnerability data with JIRA®, Black Duck offers a RESTful JSON and XML-based API that enables customers to create their own integrations with Continuous Dynamic and utilize its data in their own applications. Support for Continuous Dynamic includes our API documentation and training (see http://apidocs.whitehatsec.com). |

### 5.2.2. Continuous Dynamic DAST Standard Edition (SE)

Standard Edition (SE) includes all the features described under Continuous Dynamic BE. In addition, Continuous Dynamic SE offers a configured scan, designed to provide assessment for permanent web applications that use forms or authentication but that do not require the in-depth business logic testing provided by Continuous Dynamic PE. Continuous Dynamic SE offers all the features of Continuous Dynamic BE, but also features the following:

- **Customized Authenticated Scanning** TRC engineers will configure your site to scan with one set of login credentials. While Continuous Dynamic BE includes authenticated scanning, no configuration is performed. With Continuous Dynamic SE, our engineers will configure our scanner to authenticate itself to even the most complicated login processes. If there is an issue with our scanner authenticating itself to the application, our engineers will take action to remedy the issue.
- **Full Configuration and Form Training** TRC engineers will configure the scanner to properly fill out any forms on the web application with valid inputs, as well as teach the scanner to avoid unsafe forms.
- **Faster Results from Parse Scans** A Parse Scan will be run on your site. This provides actionable results for certain vulnerability tests as soon as your onboarded application begins scanning. For details of the included tests, see Vulnerability Tests in Parse Scans.

Vulnerabilities found in Parse Scans are reviewed and verified in the same way as those found in full Vulnerability scans. For more information, see What is the difference between a DAST Parse Scan and a Vulnerability scan?.

### 5.2.3. Continuous Dynamic DAST Premium Edition (PE)

Premium Edition (PE) includes all the features described under Continuous Dynamic BE and SE. In addition, Continuous Dynamic PE includes business logic testing by our TRC engineers, and is designed to assess more complex, high-priority, or mission-critical web applications, including those using multi-step, form-based processes and authentication and those that require both technical and business logic testing.

- **Annual Business Logic Testing** In the annual Business Logic Testing, a team of security engineers will map out and test your web application's business logic and workflows, paying particular attention to privileges between and across roles and users. This additional testing by our engineers ensures that your business-critical applications are being thoroughly assessed against any form of attack a malicious user may attempt. Vulnerabilities discovered during the business logic assessment are reported in the Portal interface with specific details:
  - A custom description of the vulnerability and how it is exploitable.
  - Steps to reproduce the vulnerability.
  - The location of the vulnerability.
  - Request and response details.
  - A vulnerability score aligned with PCI and CVSS.
  - Recommended solutions and best practice.

## 5.3. Vulnerability Tests in Parse Scans

For SE and PE levels only, a subset of tests for the following DAST vulnerability classes is run in a Parse Scan:

- Abuse of Functionality
- Application Code Execution
- Application Misconfiguration
- Autocomplete Attribute
- Brute Force
- Content Spoofing
- Cross Site Request Forgery
- Directory Indexing
- Fingerprinting

- Frameable Resource
- HTTP Response Splitting
- Improper Input Handling
- Information Leakage
- Insufficient Transport Layer Protection
- Missing Secure Headers
- Server Misconfiguration
- SQL Injection
- Vulnerable Library

| **CAUTION** | Not all tests for the documented vulnerability classes are included in Parse Scans. |
|---|---|

## 5.4. Continuous Dynamic DAST Limitations

This service does not cover:

- APIs (Separate product)
- Client-side apps (Thick Clients)
- Windows/Mac native apps
- Plugin apps
- ActiveX Silverlight

Applications with heavy use of asynchronous POST requests cannot be fully scanned via automated testing. However, pairing with a business logic assessment (Continuous Dynamic PE) can mostly mitigate this issue. Applications with anti-automation functionality cannot be scanned:

- Dynamic links (links cannot be reused)
- WebSphere
- Anti-automation tokens
- Sites that enforce requests are sent in a certain order
- Other anti-automation techniques

Applications that require non-HTTP communication to use/authenticate:

- Physical token keys
- Two-factor authentication apart from Time-based One-time Password (TOTP), SMS, or email. SMS for authentication is supported provided texts come from a long-form number, e.g. 555-555-5555, and not a short-form number, e.g. 555-5555.

# Chapter 6. API Testing

Dynamic testing is available for standalone APIs, i.e., APIs without an HTML front-end for scanners to crawl. We rely on the client to provide API documentation, which is then used as the basis for testing.

## 6.1. AutoAPI

The **AutoAPI** feature of Continuous Dynamic is analogous to the Continuous Dynamic Standard Edition (SE) service level. It uses the same scanning engine, but learns what requests to make by parsing the customer-provided documentation instead of a website's HTML. All vulnerabilities are verified by a human engineer or well-trained machine learning model before getting posted to the portal. Proofs-of-concept are provided in vulnerability descriptions as appropriate. Retests are available on demand.

It shares a platform with our other services:

| Overview Item | Details |
|---|---|
| Concierge Onboarding | The Black Duck Implementation Team will:<br>• Schedule a video welcome call to review all pertinent information and requirements for onboarding.<br>• Review all onboarding logistics (e.g. account set-up, purchase review) and verify and validate site specification(s).<br>• Deliver "Welcome" documentation and review customer deliverables to ensure successful on-boarding and utilization. |
| Continuous Dynamic User Interface | The Continuous Dynamic user interface offers 24/7 Dashboard access to all your vulnerability information, including:<br>• **Flexible Reports**<br>◦ Executive summary and unit level aggregation of data in flexible formats.<br>◦ Trend monitoring, including remediation rate, time to fix vulnerabilities, and age of vulnerabilities.<br>◦ Compliance reports (PCI) available at any time.<br>• **Access to Black Duck Engineers**<br>The Ask-a-Question feature gives direct access to Black Duck Security Threat Research Center (TRC) engineers. Questions can be submitted and responses received via the Continuous Dynamic UI. If the Ask-a-Question feature is enabled, questions can also be asked through the Continuous Dynamic JIRA® plugins, allowing customers to integrate Continuous Dynamic information directly into their issue tracking software. (24 hour response.) |

| Overview Item | Details |
| --- | --- |
| Access to Customer Support | Customer Support is available in the Black Duck Community, where customers can view their cases, submit cases, or access Continuous Dynamic documentation and tools.<br><br>You can also click here to email Customer Support. |
| PCI Compliance | Continuous Dynamic (PE, SE, and BE) services exceed requirements of the PCI DSS providing on-going verified vulnerability assessments for both public and internal websites. |
| Open JSON and XML JSON and API Integration | In addition to developing plugins that integrate Continuous Dynamic data with JIRA®, Black Duck offers a RESTful JSON and XML-based API that enables customers to create their own integrations with Continuous Dynamic and utilize Continuous Dynamic data in their own applications. Support for Continuous Dynamic includes our API documentation and training (see http://apidocs.whitehatsec.com). |

## 6.2. API Business Logic Assessment

An **API Business Logic Assessment** (BLA) is analogous to the Continuous Dynamic Premium Edition (PE) service level. The difference from AutoAPI is that an API BLA is performed manually by TRC engineers, at a single point in time. It matches the vulnerability class coverage of AutoAPI, but includes additional testing for authentication/authorization issues, file upload issues, multi-step workflow bypasses, and more. Humans can understand the meaning of API responses in a way that computers cannot.

# Chapter 7. Sentinel Mobile

Our Mobile Application Security Testing involves a combination of both Dynamic Analysis (DAST) and Static Analysis (SAST) and a one-time manual assessment. Android or iOS mobile applications can be assessed like any other static code using Sentinel Source ; in addition, Black Duck can provide a premium assessment from our dedicated team of mobile security experts in the Threat Research Center.

**NOTE**

For a premium mobile assessment, Black Duck will need to have access to both the source code and the compiled version of the application. The mobile team will examine the application and the application code for issues around the configuration settings, authentication/authorization, session management, anti-analysis, jailbreak/root detection, cryptography, data handling and storage, server-side controls, and secure coding best practices.

## 7.1. Sentinel Mobile Service Detail

Sentinel Mobile uses both Source and Dynamic testing to evaluate the security of your application both at the development level and in production. Manual Assessment is also available to customers using Sentinel Mobile.

### 7.1.1. Sentinel Mobile (Only)

- **Preservation of Intellectual Property** Sentinel Source was designed to fit within the way organizations work. Therefore, Black Duck deploys a VM appliance at a customer's site. No code is removed from the network. Because assessments are done on the premises and only small code snippets are available to Black Duck engineers for verification, source code will not leave the developer's site—eliminating the possibility of IP loss or theft. (Note that a manual assessment of a mobile application will require a more complete code review, and therefore the Sentinel Source Mobile Manual Assessment is not included in this list.)
- **Flexible Assessment Scheduling** Sentinel Source allows for a flexible assessment schedule. An assessment may be scheduled as soon as code is put into the repository, to gather immediate feedback; assessments may also be scheduled at a specific time every day, to reduce the risk that assessments will be delayed until the last minute. (Note that a manual assessment of a mobile application will require the intensive involvement of a Threat Research Engineer, and therefore the Sentinel Source Mobile Manual Assessment is not included in this list.)

### 7.1.2. Sentinel Mobile Manual Assessment (Only)

- **Annual Business Logic Testing** In the annual Business Logic Testing, a team of security engineers will map out and test your web application's business logic and workflows, paying particular attention to privileges between and across roles and users. This additional testing by our engineers ensures that your business-critical applications are being thoroughly assessed against any form of

attack a malicious user may attempt. Vulnerabilities discovered during the business logic assessment are reported in the Continuous Dynamic Portal interface with specific details:

- A custom description of the vulnerability and how it is exploitable
- Steps to reproduce the vulnerability
- The location of the vulnerability
- Request and response details
- A vulnerability score aligned with PCI and CVSS
- Recommended solutions and best practice

### 7.1.3. Sentinel Mobile and Sentinel Mobile Manual Assessment

| Feature | Details |
|---|---|
| Concierge Onboarding | The Black Duck Implementation Team will:<br>• Schedule a video welcome call to review all pertinent information and requirements for onboarding.<br>• Review all onboarding logistics (e.g. account set-up, purchase review) and verify and validate site specification(s).<br>• Deliver “Welcome” documentation and review customer deliverables to ensure successful on-boarding and utilization. |
| Continuous Dynamic Portal User Interface | The Portal offers 24/7 Dashboard access to all your vulnerability information, including:<br>• **Flexible Reports**<br>◦ Executive summary and unit level aggregation of data in flexible formats.<br>◦ Trend monitoring, including remediation rate, time to fix vulnerabilities, and age of vulnerabilities.<br>◦ Compliance reports (PCI) available at any time.<br>• **Access to Black Duck Engineers**<br>The Ask-a-Question feature gives direct access to Black Duck Threat Research Center (TRC) engineers. Questions can be submitted and responses received via the Portal UI. If the Ask-a-Question feature is enabled, questions can also be asked through the Continuous Dynamic JIRA® plugins, allowing customers to integrate Continuous Dynamic information directly into their issue tracking software. (24 hour response.) |

| Feature | Details |
| --- | --- |
| Access to Customer Support | Customer Support is available in the Black Duck Community, where customers can view their cases, submit cases, or access Continuous Dynamic documentation and tools.<br><br>You can also click here to email Customer Support. |
| Vulnerability Verification | When a Sentinel Source scan discovers a potential vulnerability, the potentially vulnerable code snippet is sent to our TRC engineers. Our engineers then personally verify that the vulnerability is real and actionable before posting it to your Portal interface, eliminating false positive alerts. |
| Code Coverage Review | Before Black Duck finalizes any assessment, we review the code coverage, complete operational checklists intended to ensure completeness, and perform business logic mapping. |
| Open JSON and XML JSON and API Integration | In addition to developing plugins that integrate vulnerability data with JIRA®, Black Duck offers a RESTful JSON and XML-based API that enables customers to create their own integrations with Continuous Dynamic and utilize its data in their own applications. Support for Continuous Dynamic includes our API documentation and training (see http://apidocs.whitehatsec.com). |