Client Service Description

WhiteHat Managed Application Security

06 February 2021 | Document Version 1.0

Client Service Description

WhiteHat Managed Application Security

NTT contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Services Product Portfolio Director - Security, Phone: +1 203 446 4942

NTT Limited
☏ 000 000 00000
🖷 000 000 00000
✉ firstname.lastname@global.ntt

Please quote reference {Document Reference Number} in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of NTT Limited ('NTT'). {ClientFull} ('{Client}') may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that {Client} may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of {Client}'s evaluation of the document. {Client} agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as {Client}. As a condition of receiving this document, {Client} agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

NTT and {Client} acknowledge and agree is subject to NTT's standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by {Client}. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with NTT will be governed by {Law} Law and be subject to the exclusive jurisdiction of the {Law} courts.

Client Service Description

WhiteHat Managed Application Security

Document Preparation

	Name	Title	Date
Prepared:	Skip Taylor	Director	06 Feb 2021

Release

Version	Date Released	Pages	Remarks
1.0	06 Feb 2021		Internal DRAFT

This document is only a general description of the available Services. The Services to be supplied are subject to change. For each Client, the Services will be as set out in the contract entered into by the Client and NTT. If there is any conflict between this document and the contract, the contract will prevail.

Table of Contents

1. WhiteHat Services

Commented [EC(1]: Note to drafter:
If WhiteHat is **not** in scope, delete Appendix D in its entirety.

The use of the WhiteHat Security, Inc. ("WhiteHat") products and/or services purchased by Client under this SOW is subject to, and incorporates by reference, (i) the terms and conditions set forth in the existing services agreement executed by and between Client and WhiteHat, or (ii) where no such agreement has been executed, the terms and definitions set forth at https://www.whitehatsec.com/terms-conditions/general-terms/.

Client acknowledges and agrees that (a) Client is required to provide to WhiteHat in writing the hostnames representing the Web Application(s) to be tested by the Services, and (b) Client may not change the hostnames that represent a given Web Application during the Term without purchasing an additional Services subscription in connection with such change.

Client acknowledges and agrees that (i) WhiteHat Professional Services - DAST Quick Start may be performed only for Web Applications that are under an active subscription for WhiteHat Sentinel Baseline Edition, WhiteHat Sentinel Standard Edition or WhiteHat Sentinel Premium Edition and (ii) all DAST Quick Start subscriptions purchased by Client must be scheduled and completed prior to the end of the applicable Term.

At any time during the Term, if Client is using the Services to perform scans on a Source Application that exceeds the maximum allowable Uncompressed File Size and the number of Lines of Code (both as measured by WhiteHat) for such Source Application purchased by Client from an authorized WhiteHat reseller or distributor, WhiteHat has the right to cause its authorized reseller or distributor to invoice Client for the additional Fees to cover the actual Uncompressed File Size or number of Lines of Code of such Source Application used by Client. On such invoice, Client will be charged the applicable incremental Fee for the licenses required to bring Client into compliance with its actual usage for each Source Application, prorated over the remaining Term of the subscription for the Services. A Source Application in excess of 120MB in Uncompressed File Size and three million (3,000,000) Lines of Code will require the purchase by Client of multiple licenses (subject to pricing as agreed upon in writing by the parties) to fully license such Source Application.

Client acknowledges and agrees that (i)WhiteHat Professional Services – SAST Quick Start may be performed only for Source Applications that are under an active subscription for WhiteHat Sentinel Source and (ii) all SAST Quick Start subscriptions purchased by Client must be scheduled and completed prior to the end of the applicable Term.

WhiteHat Sentinel Quick Start Bundle or WhiteHat Sentinel Premium Edition or WhiteHat Sentinel Standard Edition or WhiteHat Sentinel Baseline Edition: Client acknowledges and agrees that (a) Client is required to provide to WhiteHat in writing the hostnames representing the Web Application(s) to be tested by the Services, and (b) Client may not change the hostnames that represent a given Web Application during the Term without purchasing an additional Services subscription in connection with such change.

WhiteHat Professional Services – DAST Quick Start – Complimentary: Client acknowledges and agrees that (i) WhiteHat Professional Services - DAST Quick Start may be performed only for Web Applications that are under an active subscription for WhiteHat Sentinel Baseline Edition, WhiteHat Sentinel Standard Edition or WhiteHat Sentinel Premium Edition and (ii) all DAST Quick Start subscriptions purchased by Client must be scheduled and completed prior to the end of the applicable Term.

WhiteHat Professional Services – SAST Quick Start: Client acknowledges and agrees that (i)WhiteHat Professional Services – SAST Quick Start may be performed only for Source Applications that are under an active subscription for WhiteHat Sentinel Source and (ii) all SAST Quick Start subscriptions purchased by Client must be scheduled and completed prior to the end of the applicable Term.

WhiteHat Sentinel Quick Start or WhiteHat Sentinel Source Essentials Edition: At any time during the Term, if Client is using the Services to perform scans on a Source Application that exceeds the maximum allowable Uncompressed File Size and the number of Lines of Code (both as measured by WhiteHat) for such Source Application purchased by Client from an authorized WhiteHat reseller or distributor, WhiteHat has the right to cause its authorized reseller or distributor to invoice Client for the additional Fees to cover the actual Uncompressed File Size or number of Lines of Code of such Source Application used by Client. On such invoice, Client will be charged the applicable incremental Fee for the licenses required to bring Client into compliance with its actual usage for each Source Application, prorated over the remaining Term of the subscription for the Services. A Source Application in excess of 120MB in Uncompressed File Size and three million (3,000,000) Lines of Code will require the purchase by Client of multiple licenses (subject to pricing as agreed upon in writing by the parties) to fully license such Source Application.

1 WhiteHat Services Scope and Descriptions.

Commented [EC(2]: Note to drafter:
If WhiteHat is in scope, only retain the service description(s) below for the products/services being purchased. Delete those that are not relevant.

1.1. SENTINEL BASELINE EDITION (WhiteHat)

1.1.1 Service Overview

1. WhiteHat Sentinel Baseline Edition (“Sentinel BE”) performs automated dynamic testing on Web Applications and is best suited for Web Applications that do not contain forms.
2. Sentinel BE includes the following components and services:
    1. Automated scanning of a Web Application: Scans with one user credential, using an automated login handler.
    2. Vulnerability verification and rating assignment: vulnerabilities identified are verified and rated by risk by WhiteHat prior to posting on the WhiteHat Sentinel User Interface (“Sentinel UI”) to assist Client with prioritization and the remediation process.

3. Ask-a-Question: Client may contact the WhiteHat Threat Research Center engineers (“TRC”) if they have questions or comments on any vulnerabilities found by Sentinel BE.
4. Automatic vulnerability retesting: vulnerabilities found during the automated scanning process are automatically retested during each scan to determine whether such vulnerabilities have been fixed. Customers can also retest vulnerabilities on demand.
5. Access to Sentinel interface and APIs: the designated Customer contacts have access to the Sentinel UI, including standard reports and the application program interface.

1.1.2 Service Delivery Process

1. Once a Web Application has been provisioned in Sentinel BE, Client is responsible for setting the schedule for the automated scanning process, including start and stop times, and for creating and managing all credentials needed to access the Web Application to be scanned.
2. When automated scanning has been completed, WhiteHat will be available to review the findings with any designated Client contact(s) via email or conference call.
3. Vulnerabilities are posted to the Sentinel UI as they are verified. Client is responsible for remediation of vulnerabilities.
4. Client is responsible for managing users and their access to Web Applications provisioned in Sentinel BE. Client can create an unlimited number of users in Sentinel BE.
5. Client is encouraged to continue to test the Web Application with a continuous or recurring scan schedule. New vulnerabilities may be discovered due to changes in the Web Application or new vulnerability research by WhiteHat or the security community.
6. As the Web Application changes throughout the term of the Client’s Sentinel BE subscription, the Sentinel BE service will discover and test any new or changed content. Automated scanning is updated at various times with new configurations to fully test the Web Application.

Definitions: https://www.whitehatsec.com/terms-conditions/service-definitions/

1.2. BUSINESS LOGIC ASSESSMENT

1.2.1 Service Overview

1. A Business Logic Assessment (“BLA”) is a manual assessment of a Web Application (or Mobile Application) performed by the WhiteHat Threat Research Center engineers (“TRC”). This assessment focuses on uncovering vulnerabilities that are difficult or impossible for any automated testing to discover.
2. The primary credentials used for automated DAST scanning are also used as the basis for the BLA. Additional user roles and associated credentials (as provided by the Client) are used to interact with the content and security controls related to the

primary user role. For example, if the primary user role can create content that is visible to another user role, the TRC will test that interaction using both roles if they are provided by Client.

3. New content will be tested for business logic flaws once annually (or more frequently if Client has purchased additional BLAs).
4. Manual retest requests: for vulnerabilities that cannot be automatically retested, a manual retest of vulnerabilities identified during a BLA may be requested. The TRC will retest these types of vulnerabilities manually, and update the status in the Sentinel UI accordingly. This process is usually completed in approximately one business day.

1.3. SENTINEL PRENIUM EDITION

1.3.1 Service Overview

1. Sentinel Premium Edition ("Sentinel PE") performs dynamic testing on Web Applications and is best suited for complex, high-priority, or mission-critical Web Applications that use multi-step, form-based processes and role-based access controls.
2. Sentinel PE includes the following components and services:
    1. Automated scanning of a Web Application with one user credential, utilizing an automated login handler
    2. Configuration and customization of automated scanning process in order to:
        1. log in, maintain session, and log out using user credentials provided by Client;
        2. understand and use forms, application logic, and complete workflows;
        3. educe scanning of duplicated content and ensure complete coverage
    3. One BLA, as defined below, is conducted annually as part of Sentinel PE, using one user credential, to find logical flaws and to test parts of the Web Application that were excluded from automatic scanning due to production safety concerns.
    4. Vulnerability verification and rating assignment: identified vulnerabilities are verified and rated by risk by WhiteHat prior to posting on the Sentinel User Interface ("Sentinel UI") to assist Client with prioritization and the remediation process.
    5. Ask-a-Question: Client may contact the WhiteHat Threat Research Center engineers ("TRC") if they have questions or comments about any vulnerabilities found by Sentinel PE.
    6. Vulnerability retesting:
        1. Automatic Retest: vulnerabilities found during the automated scanning process are automatically retested during each subsequent scan to determine whether such vulnerabilities have been fixed. Clients can also retest vulnerabilities on demand.
        2. Manual retest requests: for vulnerabilities that cannot be automatically retested, a manual retest of vulnerabilities identified during a BLA may be requested. The TRC will retest these types of vulnerabilities manually, and update the status in the Sentinel UI accordingly. This process is usually completed in approximately one business day.

7. Access to Sentinel UI and APIs: the designated Client contacts have access to the Sentinel UI, including standard reports) and application program interface.
8. Business Logic Assessment ("BLA"): A BLA is a manual assessment of a Web Application (or Mobile Application) performed by the TRC. This assessment focuses on uncovering vulnerabilities that are difficult or impossible for any automated testing to discover. The primary credentials used for scanning are also used as the basis for the BLA. Additional user roles and associated credentials (as provided by the Client) are used to interact with the content and security controls related to the primary user role. For example, if the primary user role can create content that is visible to another user role, the TRC will test that interaction using both roles if they are provided by Client.

1.3.2 Service Delivery Process

1. Once a Web Application has been provisioned in Sentinel PE, Client is responsible for setting the schedule for the automated scanning process, including start and stop times and for creating and managing all user credentials needed to access the Web Application to be scanned.
2. When automated scanning has been fully configured and the BLA has been completed, WhiteHat will designate the assessment as "Initial Assessment Complete". Most Web Applications require approximately two weeks for completion of the full initial assessment. After Initial Assessment Complete has been reached, WhiteHat will be available to review the findings with any designated Client contact(s) via email or conference call.
3. Vulnerabilities are posted as they are verified. Client is responsible for remediation of vulnerabilities.
4. Client is responsible for managing users and their access to Web Applications provisioned with Sentinel. Client can create an unlimited number of users in Sentinel.
5. Client is encouraged to continue to test the Web Application with a continuous or recurring scan schedule. After Initial Assessment Complete has been reached, additional scans may discover new vulnerabilities due to changes in the Web Application or new vulnerability research by WhiteHat or the security community.
6. As the Web Application changes throughout the term of the Client's Sentinel PE subscription, the Sentinel PE will discover and test any new or changed content. Automated scanning is updated at various times with new configurations to fully test the Web Application. New content will be tested for Business Logic Flaws once annually (or more frequently if Client has purchased additional BLAs) during the next BLA.

Definitions: https://www.whitehatsec.com/terms-conditions/service-definitions/

1.4. SENTINEL SOURCE (Microservices)

1.4.1 Service Overview

1. Sentinel Source ("Sentinel Source") is designed to incorporate security into the software development lifecycle (SDLC) by enabling the Client to assess their code as it is being developed and assisting developers in identifying and remediating vulnerabilities before the code is pushed to production. As developers write code and upload it to a repository, Sentinel Source analyzes the code and identifies security vulnerabilities. Sentinel Source operates via WhiteHat's Sentinel Source engine housed on an installed Sentinel Source Virtual Machine image ("VM"); the image may be completely within Client's network, or in some cases, may be hosted in the cloud by WhiteHat.
2. Sentinel Source includes the following components and services:
    1. Unlimited, automated & continuous scanning of source code
    2. Vulnerability verification and rating assignment: vulnerabilities identified are verified and rated by risk by WhiteHat prior to posting on the Sentinel User Interface ("Sentinel UI") to assist Client with prioritization and the remediation process.
    3. Ask-a-Question: Client may contact the WhiteHat Threat Research Center engineers ("TRC") if they have questions or comments on any vulnerabilities found by Sentinel Source.
    4. Vulnerability retesting: vulnerabilities found during the automated scanning process are automatically retested during each subsequent scan to determine whether such vulnerabilities have been fixed.
    5. Access to Sentinel UI and APIs: the designated Client contacts have access to the Sentinel UI (including standard reports) and application program interface.
    6. Access to plugins: Client can integrate Sentinel Source with a bug tracking tool (Jira), continuous build system (Jenkins), integrated development environments (Eclipse, Visual Studio, XCode, IntelliJ) to integrate security in the development life cycle.

1.4.2 Service Delivery Process

1. Prior to the initial scan by Sentinel Source, WhiteHat provides instructions and technical support to (i) assist Client in downloading and configuring the VM, (ii) establish the necessary connectivity to code repositories, build servers and dependency servers, (iii) add Source Applications, (iv) configure codebases, (v) configure and schedule static scans, and (vi) manage users/groups.
2. Client is able to run pre-scans to accurately determine the size of their Source Application(s) and exclude any files/folders from the scan configuration before initiating a full scan that will consume purchased license(s).
3. Client is responsible for setting the schedule for the automated scanning process, including start and stop times and for creating and managing all user credentials needed to access the Client Source Application to be scanned.
4. After the first full scan, WhiteHat will review configuration for full coverage, recommend configuration changes if needed, review the results, verify findings,

and be available for a review of the findings to explain the results to the designated Client contact(s) via email or conference call.

5. Vulnerabilities are posted to the Sentinel UI as they are verified. Client is responsible for remediation of all vulnerabilities.
6. Client is responsible for managing users and their access to Source Applications provisioned in Sentinel. Client can create unlimited number of users in Sentinel.
7. Client is encouraged to continue to test the application with a continuous or recurring scan schedule. After the first full scan, additional scans may discover new vulnerabilities due to changes in the Source Application or new vulnerability research by WhiteHat or the security community.

Definitions: https://www.whitehatsec.com/terms-conditions/service-definitions/

1.5. SENTINEL SOURCE - ESSENTIALS EDITION

1.5.1 Service Overview

1. Sentinel Source Essentials Edition ("Source EE") is designed to incorporate security into the software development lifecycle (SDLC) by enabling the Client to assess their code as it is being developed and assisting developers in identifying and remediating vulnerabilities before the code is pushed to production. As developers write code and upload it to a repository, Source EE analyzes the code and identifies security vulnerabilities. Source EE operates via WhiteHat's Sentinel Source engine housed on an installed Sentinel Source Virtual Machine ("VM") image; the image may be completely within Client's network, or in some cases, may be hosted in the cloud by WhiteHat.
2. Source EE includes the following components and services:
    1. Unlimited, automated & continuous scanning of source code to find application security vulnerabilities using automated static application security testing.
    2. Vulnerability retesting: Vulnerabilities found during the automated scanning process are automatically retested during each subsequent scan to determine whether such vulnerabilities have been fixed.
    3. Access to Sentinel User Interface ("Sentinel UI") and APIs: the designated Client contacts have access to the Sentinel UI (including standard reports) and application program interface.
    4. Access to plugins: Client can integrate Sentinel Source with a bug tracking tool (Jira), continuous build system (Jenkins), integrated development environments (Eclipse, Visual Studio, XCode, IntelliJ) to integrate security in the development life cycle.

1.5.2 SERVICE DELIVERY PROCESS

1. Prior to the initial scan by Source EE, WhiteHat provides instructions and technical support to (i) assist Client in downloading and configuring the VM, (ii) establish the necessary connectivity to code repositories, build servers and dependency

servers, (iii) add Source Applications, (iv) configure codebases, (v) configure and schedule static scans, and (vi) manage users/groups.
2. Client is able to run pre-scans to accurately determine the size of their Source Application(s) and exclude any files/folders from the scan configuration before initiating a full scan that will consume purchased license(s).
3. Client is responsible for setting the schedule for the automated scanning process, including start and stop times and for creating and managing all user credentials needed to access the Client Source Application to be scanned.
4. After the first full scan, application security vulnerabilities are posted to the Sentinel UI after the scan is complete. Client is responsible for remediation of all vulnerabilities.
5. Client is responsible for managing users and their access to Source Applications provisioned in Sentinel. Client can create unlimited number of users in Sentinel.
6. Client is encouraged to continue to test the application with a continuous or recurring scan schedule. After the first full scan, additional scans may discover new vulnerabilities due to changes in the Source Application or new vulnerability research by WhiteHat or the security community.

Definitions: https://www.whitehatsec.com/terms-conditions/service-definitions/

1.6. SENTINEL STANDARD EDITION

1.6.1 Service Overview

1. Sentinel Standard Edition (“Sentinel SE”) performs dynamic testing on Web Applications and is best suited for applications that use forms and/or authentication but do not require the in-depth business logic testing provided by Sentinel Premium Edition.
2. Sentinel SE includes the following components and services:
    1. Automated scanning of a Web Application using one user credential.
    2. Configuration and customization of automated scanning process to:
        1. log in, maintain session, and log out with user credential(s) provided by Client;
        2. understand and use forms, application logic, and complete workflows;
        3. reduce scanning of duplicate content and ensure complete coverage.
    3. Vulnerability verification and rating assignment: vulnerabilities identified are verified and rated by risk by WhiteHat prior to posting on the Sentinel User Interface (“Sentinel UI”) to assist Client with prioritization and the remediation process.
    4. Ask-a-Question: Client may contact the WhiteHat Threat Research Center engineers (“TRC”) if they have questions or comments on any vulnerabilities found by Sentinel SE.
    5. Vulnerability retesting: vulnerabilities found during the automated scanning process are automatically retested during each scan to determine whether such vulnerabilities have been fixed. Clients can also retest identified vulnerabilities on demand.

6. Access to the Sentinel UI interface and APIs: the designated Client contacts have access to the Sentinel UI, including standard reports and the application program interface.

1.6.2 Service Delivery Process

1. Once a Web Application has been provisioned in Sentinel SE, the Client is responsible for setting the schedule for the automated scanning process, including start and stop times, and for creating and managing all credentials needed to access the Web Application to be scanned.
2. When automated scanning has been completed, WhiteHat will designate the assessment as "Initial Assessment Complete". Most Web Applications require approximately two weeks for completion of the full initial assessment. After Initial Assessment Complete has been reached, WhiteHat will be available to review the findings with any designated Client contact(s) via email or conference call.
3. Vulnerabilities are posted as they are verified. Client is responsible for remediation of vulnerabilities.
4. Client is responsible for managing users and their access to Web Applications provisioned in Sentinel. Client can create an unlimited number of users in Sentinel.
5. Client is encouraged to continue to test the Web Application with a continuous or recurring scan schedule. After the scan has reached Initial Assessment Complete, additional scans may discover new vulnerabilities due to changes in the Web Application or new vulnerability research by WhiteHat or the security community.
6. As the Web Application changes throughout the term of the Client's Sentinel SE subscription, the Sentinel SE service will discover and test any new or changed content. Automated scanning is updated at various times with new configurations to fully test the Web Application.

Definitions: https://www.whitehatsec.com/terms-conditions/service-definitions/

1.7. WHITEHAT SENTINEL SCA - ESSENTIALS EDITION

1.7.1 Service Overview

1. Sentinel SCA Essentials Edition ("SCA EE") is designed to incorporate security into the software development lifecycle (SDLC) by enabling Clients to assess the third-party and open source components used by their own code and assisting developers in identifying and remediating vulnerable components used by their application, before the code is pushed to production. As developers write code and upload it to a repository, SCA EE analyzes the code and identifies third-party and open-source components that the code depends on and whether these components have security, license, or age related risks associated. SCA EE operates via WhiteHat's Sentinel Source engine housed on an installed Sentinel SCA Virtual Machine ("VM") image; the image may be completely within Client's network, or in some cases, may be hosted in the cloud by WhiteHat.

2. SCA EE includes the following components and services:
    1. Unlimited, automated & continuous scanning of source code to find security, license, and age related risks in third-party and open-source components used by the source code using automated software composition analysis.
    2. Vulnerability retesting: Vulnerabilities found during the automated scanning process are automatically retested during each subsequent scan to determine whether such vulnerabilities have been fixed.
    3. Access to Sentinel UI and APIs: the designated Client contacts have access to the Sentinel User Interface ("Sentinel UI") (including standard reports) and application program interface.
    4. Access to plugins: Client can integrate Sentinel Source with a bug tracking tool (Jira), continuous build system (Jenkins), integrated development environments (Eclipse, Visual Studio, XCode, IntelliJ) to integrate security in the development life cycle.

1.7.2 SERVICE DELIVERY PROCESS

1. Prior to the initial scan by SCA EE, WhiteHat provides instructions and technical support to (i) assist Client in downloading and configuring the VM, (ii) establish the necessary connectivity to code repositories, build servers and dependency servers, (iii) add Source Applications, (iv) configure codebases, (v) configure and schedule static scans, and (vi) manage users/groups.
2. Client is able to run a scan that will consume purchased license(s).
3. Client is responsible for setting the schedule for the automated scanning process, including start and stop times and for creating and managing all user credentials needed to access the Client Source Application to be scanned.
4. Vulnerabilities are posted to the Sentinel UI after the scan is complete. Client is responsible for remediation of all vulnerabilities.
5. Client is responsible for managing users and their access to Source Applications provisioned in Sentinel. Client can create unlimited number of users in Sentinel.
6. Client is encouraged to continue to test the application with a continuous or recurring scan schedule. After the first full scan, additional scans may discover new vulnerabilities due to changes in the Source Application or new vulnerability research by WhiteHat or the security community.

Definitions: https://www.whitehatsec.com/terms-conditions/service-definitions/