Symantec™ Cyber Security: DeepSight™ Intelligence

Service Description

December 2018

Service Overview

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec which governs the use of the Service, or if no such signed agreement exists, the Symantec Online Services Terms and Condition (hereinafter referred to as the "**Agreement**").

Symantec™ Cyber Security: DeepSight™ Intelligence services are Symantec threat intelligence services comprising of either DeepSight™ Intelligence portal services ("Intelligence Portal") or DeepSight™ Intelligence datafeed services ("Datafeeds") (each a "Service" or collectively, "Services"), depending on the specific Service purchased by Customer. The Intelligence Portal Service is a threat intelligence service that allows Customer to view security information such as vulnerability data, malcode, cyber threats and adversary information. Datafeeds provide Customer access to one or more datafeeds containing various security data depending on the datafeed purchased.

Table of Contents

Technical/Business Functionality and Capabilities

Service Features

The following table illustrates the features associated with each Service.

Service Feature	Intelligence Portal – Standard	Intelligence Portal – Enterprise	Intelligence Portal – Advanced Enterprise	Datafeeds	Service Feature Description
Use Level	Up to two (2) Users	Per Managed User	Per Managed User	Per Managed User	Intelligence Portal – Standard is available on a per User basis up to a maximum of two (2) Users. Intelligence Portal – Enterprise and Advanced Enterprise and Datafeeds Services are available on a per Managed User basis.
Managed Services Portal	●	●	●	●	Access to the Managed Services Portal is limited to Authorized Personnel. Certain features and functionality of the Managed Services Portal may vary based on the Service purchased by Customer.
Administrators	2	5	5	1	The number of Administrators that Customer may Register (as defined below) to access and use the applicable Service, including access and use of the Managed Services Portal and Symantec Materials. Administrators may additionally designate a reasonable number of non-Administrators to access and use the Services, subject to the limitations set forth in the Agreement.
Alert Creation	●	●	●		Authorized Personnel may configure Alerts to receive notifications on new/updated vulnerabilities, malcode, security risks, and other security data available in the Global Intelligence Network (GIN).
Email Delivery	●	●	●		Authorized Personnel may designate their email address as an electronic delivery method for Alert Information through the Managed Services Portal.
XML Delivery		●	●		Authorized Personnel may designate XML as an electronic delivery method for certain Alert Information through the Managed Services Portal.
MATI Reports			●		See service feature description below.
Custom Reports		●	●		Authorized Personnel may access certain custom reports that Symantec may make generally available to all customers through the Managed Services Portal.

Service Feature	Intelligence Portal – Standard	Intelligence Portal – Enterprise	Intelligence Portal – Advanced Enterprise	Datafeeds	Service Feature Description
API Calls		●	●	● *	Provides access to intelligence content through API calls (up to a certain number each 24-hour period) without manually logging onto the Managed Services Portal or downloading the Datafeed. The number of API calls included and the type of intelligence content accessible by API calls are determined by Customer's subscription to DeepSight Intelligence services.
DeepSight Security Risk Datafeed				● *	Provides, in XML format, access to malicious code data and security risk data, including adware and spyware.
DeepSight Vulnerability Datafeed				● *	Provides, in XML format, access to vulnerability information, including mitigation guidance, impact analysis, SCAP related data, and links to security patches when available.
DeepSight IP Reputation Datafeed				● *	Provides, in XML, CSV or CEF format, access to reputation, hostility and confidence ratings of Internet protocol addresses, derived from threat analysis of data from the Symantec Sensor Network.
DeepSight Advanced IP Reputation Datafeed				● *	Provides, in XML, CSV or CEF format, access to reputation, hostility confidence ratings, (as well as ownership, geolocation, and industry, where such data is available) and malicious behavior details of Internet protocol addresses, derived from threat analysis of data from the Symantec Sensor Network.
DeepSight Domain Name & URL Reputation Datafeed				● *	Provides, in XML, CSV or CEF format, access to reputation, hostility and confidence ratings of domains, Universal Resource Locators, derived from threat analysis of data from the Symantec Sensor Network.
DeepSight Advanced Domain Name & URL Reputation Datafeed				● *	Provides, in XML, CSV or CEF format, access to reputation, hostility confidence ratings, (as well as ownership, geolocation, and industry, where such data is available) and malicious behavior details of domains and associated Universal Resource Locators, derived from threat analysis of data from the Symantec Sensor Network.

*This Datafeed is only available to customers who have specifically purchased it, as indicated in the applicable Subscription Instrument.

MATI Service Feature Description

Symantec's Managed Adversary and Threat Intelligence ("MATI") team of global researchers and analysts is dedicated to understanding the cyber threat ecosystem and providing context-rich intelligence reporting on adversaries so that customers can better respond to current and emerging threats. MATI is built upon Symantec's deep experience tracking the world's most prolific and sophisticated cyber threat actors, and utilizes a wide array of research methodologies and sources to identify and assess adversary behavior and attempt to provide a future outlook on that behavior.

Intelligence Portal – Advanced Enterprise customers can access periodic MATI reporting ("MATI Reports") on the latest developments in significant cyber threat campaigns. MATI Reports may include:

- Narrative analysis of the latest campaign activities, patterns, and trends;
- Actor attribution and identifiers (*e.g.*, email addresses, Internet Protocol addresses, and usernames/accounts);
- Actionable technical details of campaign tools and adversary tactics, techniques, and procedures (*e.g.*, vulnerabilities exploited, hash values of malware deployed, traits of portable executables, and other indicators of compromise);
- Characteristics of malicious infrastructure (*e.g.*, domains, uniform resource locators, IPs, autonomous system numbers, and geo-location); and
- Target identifiers (*e.g.*, industries, job functions, and other traits).

The MATI team harvests cyber threat insights from Symantec's proprietary Global Intelligence Network as well as from commercially available datasets and publicly available Internet resources, including limited-access marketplaces and forums. All MATI research activities are governed by Symantec's internal protocols and oversight mechanisms intended to ensure they are conducted ethically and in accordance with applicable laws and regulations.

Additionally Available Service (Optional)

For additional fees, Symantec offers the following options to complement DeepSight Intelligence services:

- **DeepSight Intelligence Directed Threat Research**
  Customers that purchase DeepSight™ Intelligence Directed Threat Research will receive Tokens for each purchase, which allows Authorized Personnel to request certain custom reports from Symantec.
  - Tokens are valid for twelve (12) months from the date of purchase. Unused Tokens will expire after the validity period is over.
  - For Customer to use unexpired Tokens, Customer must have a current and valid ***Intelligence Portal – Advanced Enterprise*** license. Customer must access the Managed Services Portal and submit requests for or view Directed Threat Research reports.
  - All costs (measured in Tokens) are per report. The exact cost of any requests will be determined when the request is received by the MATI team based on the scope of the request. Various factors affect the cost of a request. Please contact Symantec for details. Once the scope and cost have been confirmed, Tokens will be deducted from your account, and further changes will not be accepted.
  - Symantec reserves the right to decline all or any portion of a Directed Threat Research request.
  - Symantec will deliver Directed Threat Research reports when completed.
  - Directed Threat Research reports are subject to the same protocols as MATI Reports, as described above.

- **DeepSight Additional API Calls**
  Customers that purchase additional API calls can increase the number of daily API call capacity included in DeepSight™ Intelligence services.
  - Additional API calls are available for purchase in increments of 1,000 (per day).
  - Additional API calls are valid for twelve (12) months from the date of purchase. Unused API call capacity will expire after the validity period is over.
  - For Customer to use additional API calls, Customer must have a current and valid DeepSight Intelligence services. (The API call functionality is not available with *Intelligence Portal - Standard*).
  - The number of daily API call capacity included in DeepSight Intelligence services are as follows:

Intelligence Portal	API Calls / Day			
	N/A	1,000	2,000	3,000
Standard	●			
Enterprise		●		
Advanced Enterprise				●
Datafeeds	**API Calls / Day**			
	N/A	1,000	2,000	3,000
Security Risk		●		
Vulnerability		●		
IP Reputation			●	
Domain & URL Reputation			●	
Adv. IP Reputation				●
Adv. Domain / URL Reputation				●

Customer Responsibilities

Customer acknowledges and agrees that Symantec can only perform the Services if Customer provides required information or performs required actions as set forth in the Agreement or as reasonably requested by Symantec. Accordingly, and without limitation, if Customer does not meet the following responsibilities, Symantec's performance of the Services may be delayed, impaired or prevented, as noted below:

- Customer must first register ("Register") the serial number(s) printed on the Subscription Instrument in the licensing section of the *MySymantec* portal located at https://my.symantec.com/ and appoint the Administrators associated with the Services ("Registration").
- Customer is solely responsible for acquiring and maintaining the Internet or telecommunications services and devices required to receive, access or use the Services or Symantec Materials.
- Datafeeds, any datasets within the Datafeeds and APIs to access them are Symantec's proprietary and confidential information. Customer must promptly notify Symantec after becoming aware of any unauthorized access to, acquisition, disclosure, loss, or use of the Symantec Datafeeds (including datasets thereof) or APIs.

Assistance and Technical Support

If Customer is entitled to receive assistance and technical support directly from Symantec, for Symantec™ Cyber Security: DeepSight™ Intelligence services, support is available on a twenty-four (24) hours/day by seven (7) days/week basis through *MySymantec* at https://my.symantec.com/ or by calling your local support line found at http://go.symantec.com/callcustomercare.

If Customer is entitled to receive assistance and technical support from a Symantec reseller, then refer to Customer's agreement with that reseller for details regarding support.

Service-Specific Terms

Service Conditions

- Customer warrants and represents that the quantity of Services purchased, as identified in the Subscription Instrument, reflects the total number of Users or Managed Users, as applicable, at the time of purchase. If, during the Service Period, Customer's number of Users exceeds two (2) for Intelligence Portal Service – Standard or Customer's Managed Users exceeds the banded amount in the Subscription Instrument for Intelligence Portal Service – Enterprise, Intelligence Portal Service – Advanced Enterprise, or Datafeeds, then Customer agrees to promptly, but no later than thirty (30) days following the increase in Users or Managed Users, as applicable, purchase additional Service entitlements to become compliant with such increase.
- While Symantec makes reasonable efforts as to the accuracy of Symantec Materials, Symantec disclaims all liability for any error or omission in Symantec Materials and makes no warranty as to the accuracy, reliability or completeness of Symantec Materials. Customer agrees that any reliance on Symantec Materials shall be strictly at Customer's sole risk.
- Except as otherwise specified in this Service Description, the Services may use open source technology and other third-party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/eulas/.
- The Services may be accessed and used globally, subject to applicable Use Levels, export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Symantec may update the Services at any time in order to maintain the effectiveness of the Services.
- Symantec will process information derived from the Services in accordance with, and for the purposes defined in, *Symantec's Global Privacy Statement* and *the Product Transparency Notice (DeepSight Intelligence)*, each available at www.symantec.com/privacy. Without limiting the generality of the foregoing, Symantec may additionally use certain information derived from the Services, once anonymized ("**Anonymized Information**") for the following purposes: (i) preparing and distributing statistical reports related to security trends and data patterns; (ii) distributing Anonymized Information to Symantec customers, in compiled or original formats, for the purposes of providing computer security information; and / or (iii) analysis; internal research, product or services development, or for providing general security related services.

Definitions

Capitalized terms used in this Service Description shall have the meaning given below. Any capitalized terms not defined in this Service Description shall have the same meaning as in the Subscription Instrument.

"**Administrator**" means an employee or third-party contractor designated by Customer to have administrative access to and use of the Services, including the Managed Services Portal and Symantec Materials, and are identified upon Registration or thereafter within the Managed Services Portal. In the event of a conflict, those Administrators identified within the Managed Services Portal will control over Administrators identified at the time of Registration.

"**Alert Information**" means the alert messages, data and/or information that Symantec provides or makes available pursuant to the Services.

"**Authorized Personnel**" means, collectively, Administrators and any additional personnel Administrators have designated as non-Administrators to access and use the Services, subject to the limitations set forth in the Agreement.

"**Managed Services Portal**" means Symantec's password-protected intelligence portal website, currently located at deepsight.symantec.com, including any Symantec subsites accessible via the Managed Services Portal, and all content accessible on such sites.

"**Managed Users**" means the total number of Customer's employees (excluding third party contractors), and is reflected in the banded amount in the SKU Description for Services set forth in the Subscription Instrument.

"**Symantec Materials**" means the materials provided in connection with the Services, including but not limited to the Alert Information, MATI Reports, Directed Threat Research reports, or Datafeeds, but not including any third party websites, or content thereon, that may be reached from any link contained in any such materials.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

"**Tokens**" means the total number of units purchased and redeemable for Directed Threat Research reports.

"**Use Level**" means the unit of measurement or model, by which Symantec measures, prices and sells the right to access and use a Service, as indicated in the Subscription Instrument.

"**User**" means a Customer employee or third-party contractor and is reflected in the SKU Description for Services set forth in the Subscription Instrument.

END OF SERVICE DESCRIPTION