DeepSight™ Intelligence

Service Description

October 2020

This Service Description, with any attachments included by reference, is provided under the following terms and conditions in addition to any terms and conditions referenced on in the order confirmation issued by Accenture (or Symantec, as predecessor to Accenture) related to Client's purchase of Services or any similar document which further defines Client's rights and obligations related to the Services, such as a Symantec certificate (the "**Order Confirmation**") which incorporates this Service Description by reference (the Order Confirmation, this Service Description and any other documents referenced therein collectively, the "**Agreement**"). These terms shall be effective from the effective date of such ordering document. Any terms that are used but not defined herein shall have the meaning set forth in the Agreement.

This Service Description describes DeepSight™ Intelligence services comprising of either DeepSight™ Intelligence portal services ("**Intelligence Portal**") or DeepSight™ Intelligence datafeed services ("**Datafeeds**") (each a "**Service**" or collectively, "**Services**"). All capitalized terms in this description have the meaning ascribed to them in the Agreement or in the Definitions section.

Table of Contents

DeepSight™ Intelligence

Service Description

October 2020

1: Technical/Business Functionality and Capabilities

Service Overview

DeepSight™ Intelligence services are comprised of either Intelligence Portal or Datafeeds, depending on the specific Service purchased by Client. The Intelligence Portal Service is a threat intelligence service that allows Client to view security information such as vulnerability data, malcode, cyber threats and adversary information. Datafeeds provide Client access to one or more datafeeds containing various security data depending on the datafeed purchased.

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 Data feeds Services are available on a per Managed User basis.
Intelligence Portal	●	●	●	●	Access to the Intelligence Portal is limited to Authorized Personnel. Certain features and functionality of the Managed Services Portal may vary based on the Service purchased by Client.
Administrators	2	5	5	1	The number of Administrators that Client may Register (as defined below) to access and use the applicable Service including access and use of the Intelligence Portal and DeepSight 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 Intelligence Portal.
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 Accenture may make generally available to all clients through the Managed Services Portal.

DeepSight™ Intelligence

Service Description

October 2020

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 Client'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 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 Accenture threat analysis.
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 Accenture threat analysis.

*This Datafeed is only available to clients who have specifically purchased it, as indicated in the applicable Order Confirmation.

MATI Service Feature Description

The Managed Adversary 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 Clients can better respond to current and emerging threats. MATI is built upon our 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 clients 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 proprietary intelligence sources as well as from commercially available datasets and publicly available Internet resources, including limited-access marketplaces and forums.

Additional Available Services (Optional)

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

- **DeepSight Intelligence Directed Threat Research (DTR)**

  Clients that purchase DeepSight™ Intelligence Directed Threat Research will receive credit ("DTR Credit") in the amount paid and listed in the Order Confirmation, which allows Authorized Personnel to request certain custom reports from Accenture.

  - DTR Credit is valid for twelve (12) months from the date of purchase. Unused DTR Credit will expire after the validity period is over.
  - For Client to use unexpired DTR Credit, Client must have a current and valid ***Intelligence Portal – Advanced Enterprise*** license. Client must access the Managed Services Portal and submit requests for or view Directed Threat Research reports.
  - All costs (measured in DTR Hourly Rates) are per report. The estimated 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 Accenture for details. Once the report has been delivered, an amount equal to the number of hours spent by Accenture on the DTR request times the DTR Hourly Rate will be deducted from the DRT Credit.
  - Accenture reserves the right to decline all or any portion of a Directed Threat Research request.
  - Accenture will deliver Directed Threat Research reports when completed.

- **DeepSight Additional API Calls**

  Clients 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 Client to use additional API calls, Client 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	N/A	1,000	3,000
Standard	●		
Enterprise		●	
Advanced Enterprise			●
Datafeeds	**N/A**	**1,000**	**3,000**
Security Risk		●	
Vulnerability		●	
Adv. IP Reputation			●
Adv. Domain / URL Reputation			●

2: Client Responsibilities

Accenture can only perform the Service if Client provides required information or performs required actions, otherwise Accenture's performance of the Service may be delayed, impaired or prevented.

- Client is solely responsible for acquiring and maintaining the Internet or telecommunications services and devices required to receive, access or use the Services or DeepSight Materials.
- The DeepSight Materials and APIs to access them are Accenture or its third-party licensor's proprietary and confidential information. Client will not remove any confidentiality, copyright or other markings from the DeepSight Materials. Client is responsible to keep the DeepSight Materials confidential, to only use the DeepSight Materials internally within its business for the purpose of protecting its networks, and to protect the DeepSight Materials against disclosure to third parties. Client must promptly notify Accenture after becoming aware of any unauthorized access to, acquisition, disclosure, loss, or use of the Datafeeds (including datasets thereof) or APIs.
- Client is solely responsible for its use of the DeepSight Materials and any action or inaction in response to the DeepSight Materials. Client will indemnify and hold Accenture harmless against any claims arising from Client's breach of the Agreement, or its actions or inactions in response to the DeepSight Materials.
- If Accenture determines, in its sole but reasonable discretion, that any of the DeepSight Materials contain errors, or is, or could be, subject to a claim that it infringes any right of any person or entity, then Client will delete, correct make inaccessible any such DeepSight Materials promptly upon written notice from Accenture.
- Acceptable Use Policy: Client is responsible for complying with the Acceptable Use Policy, a copy of which is available at https://www.accenture.com/us-en/support/security/legal-terms or upon request to Accenture.
- Client acknowledges that the DeepSight Materials are provided "AS IS", "WHERE IS" AND "AS AVAILABLE" AND, TO THE MAXIMUM EXTENT PERMITTED BY LAW, ACCENTURE DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. ACCENTURE DOES NOT WARRANT THAT USE OF THE SERVICES, OR DEEPSIGHT MATERIALS WILL BE UNINTERRUPTED OR ERROR FREE.

3: Entitlement and Subscription Information

The Service(s) are non-cancellable and payments for the Service(s) are non-refundable.

Charge Metrics

The Service is available under one of the following Meters as specified in the Order Confirmation:

- 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 Data feeds Services are available on a per Managed User basis.
- "**User**" means an individual person and/or device authorized to use and/or benefit from the use of the Service, or that actually uses any portion of the Service.
- "**Managed Users**" means the total number of Client's employees (excluding third party contractors) and is reflected in the banded amount in the SKU Description for Services set forth in the Order Confirmation.

4: Client Assistance and Technical Support

Client Assistance

Accenture will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If Accenture is providing Technical Support to Client, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Client with configuration of the Service features and to resolve reported problems with the Service.
- Once a severity level is assigned to a Client submission for Support, Accenture will make every reasonable effort to respond. Faults originating from Client's actions or requiring the actions of other service providers are beyond the control of Accenture and as such are specifically excluded from this Support commitment.

Maintenance to the Service and/or supporting Service Infrastructure

Accenture must perform maintenance from time to time. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Accenture will provide forty-eight (48) hours notification.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for forty-eight (48) hours notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Accenture will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.

5: Data Privacy Notice

Client will need to supply the names and business email addresses of Client's authorized users in order to obtain logon credentials for the Intelligence Portal. In addition, Accenture may, in the course of its research of publicly available sources, come into contact with additional business email addresses, passwords or other similar personal data of Client's personnel or clients (collectively, the "Client Personal Data"). Client acknowledges that it is the controller of such Client Personal Data, and agrees that it is will take all necessary measures to ensure that it, and all of its employees or other third parties, are aware that their Personal Information may be processed as part of the Service(s) and that those individuals have given their consent to such processing, where required. Client will comply with its responsibilities as data controller in accordance with applicable laws and/or regulations. By providing Personal Information, Client consents, for itself, its users and contacts, to the following: Personal Information will be processed and accessible on a global basis by Accenture, its affiliates, agents and subcontractors for the purposes of providing the Service(s), to generate statistical information about the Service(s), for internal research and development, and as otherwise described in the Agreement, including in countries that may have less protective data protection laws than the country in which Client or its users are located. Accenture may disclose the collected Personal Information as required or permitted by law or in response to a subpoena or other legal process. Client understands and agrees that Accenture has no control or influence over the content of the Client Personal Data processed by Accenture and that Accenture performs the Service(s) on behalf of Client and that Accenture will only process the Personal Information in accordance with the instructions of Client, provided that such instructions are not incompatible with the terms of the Agreement. Accenture will also take appropriate technical and organizational measures to protect personal information against accidental loss or destruction of, or damage to, that Personal Information in the form of Data Safeguards, a description of which are available upon request.

6: Definitions

"**Administrator**" means an employee or third-party contractor designated by Client to have administrative access to and use of the Services, including the Managed Services Portal and DeepSight Materials, and are identified 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 Accenture 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.

"DeepSight Materials" means any 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.

"**Intelligence Portal**" means the password-protected intelligence portal website, currently located at deepsight.accenture.com , including any DeepSight subsites accessible via the Intelligence Portal, and all content accessible on such sites.

"**Service Infrastructure**" means any Accenture or licensor technology and intellectual property used to provide the Services.

"**DTR Credit**" means the total amount of pre-paid fees purchased and redeemable for Directed Threat Research reports, as set forth in the Order Confirmation.

"**DTR Hourly Rate"** means the hourly rate listed in the Order Confirmation for Directed Threat Research requests.

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

END OF SERVICE DESCRIPTION