Accenture Cyber Threat Intelligence ("CTI") as a Service

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 in the order confirmation issued by Accenture related to Client's purchase of Services of any similar document which further defines Client's rights and obligations related to the Services, 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 Accenture Cyber Threat Intelligence (CTI) as a Service. All capitalized terms in this description have the meaning ascribed to them in the Agreement or in the Definitions section.

Table of Contents

Accenture Cyber Threat Intelligence ("CTI") as a Service

Service Description

October 2020

1. Service Features and Definitions

Accenture shall provide the component or components of the Accenture CTI as a Service that are identified in the applicable Order Confirmation, each of which is more fully described below.

Service Features

The following table illustrates the features associated with each Service:

Service Feature	IntelGraph Client Portal	IntelGraph API Service	IntelGraph Threat Indicator API Service	IntelGraph Vulnerability API Service	Accenture CTI Analyst Service (Request for Intelligence)
IntelGraph Portal Access	X				
Threat Indicator Content	X	X	X		
Vulnerability Content	X	X		X	
Requests for Intelligence					X
API Calls		X	X	X	

Definitions

"**Accenture**" means the Accenture entity named in the Order Confirmation and/or its affiliates.

"**API**" means the application programming interface which consists of interface definitions, generated code libraries and associated tools and documentation.

"**API Key**" means one or more unique security keys, tokens, passwords and/or other credentials provided by Accenture and used by Client to access the applicable API Service.

"**Accenture Works**" means (a) all of Accenture's (or its licensors') Confidential Information, the Service, the IntelGraph Client Portal, the Content, documentation, APIs and other software, materials, tools, templates and technology developed by or on behalf of Accenture, or provided or made available by Accenture, pursuant to this Agreement or otherwise; (b) all other proprietary information of Accenture; (c) all customizations, modifications, enhancements, derivative works, configurations, translations, upgrades, and interfaces thereto; and (e) the ideas, concepts, techniques, inventions, processes, software or works of authorship developed, embodied in, or practiced in connection with the Services. For the avoidance of doubt, Accenture Works do not include Client's preexisting hardware, software, or networks.

"**Confidential Information**" has the meaning set out in the Online Terms and Conditions; provided, however, that, for purposes of this Service Description, Confidential Information includes Content and the documentation related to the Accenture Cyber Threat Intelligence as a Service.

"**Content**" means (a) Vulnerability Content; (b) Threat Indicator Content; and (c) any other cyber intelligence information, alerts, analytical tools, and interactive visualizations made available to Client as part of the Service via the IntelGraph Client Portal, an API Service, conference calls, emails, other electronic distribution or other means (as applicable). Accenture reserves the right to determine in its sole discretion the information which is made available as part of the Service.

"Client" means the client identified in the Order Confirmation.

"**Client Consultants**" means independent contractors and consultants providing services solely for Client's benefit.

"**Distributees**" means employees of Client and/or employees of Client Consultants.

"**IntelGraph Authorized Users**" means the number of employees of Client and/or employees of Client Consultants who are authorized to access the IntelGraph Client Portal, as set forth in the Order Confirmation.

"**IntelGraph API Service**" means the hosted API Service that allows Client to programmatically access the Content.

"**Accenture CTI Critical Intelligence Requirements**" or "**CIRs**" means Accenture-defined subject areas of cybersecurity identified in the IntelGraph Client Portal that may be changed from time to time by Accenture in its reasonable discretion.

"**IntelGraph Client Portal**" means a web-based portal (and/or any related interfaces or electronic tools that Accenture may provide from time to time under this Agreement) which provides Client with access to the Content.

"**Accenture Cyber Threat Intelligence as a Service**" or the "**Service**" means the services described in Section 2 herein and any other Accenture Works provided in connection therewith.

"**Indicator**" means a discrete data point that allows for identification or detection of a threat within an information technology infrastructure. Examples of Indicators include, but are not limited to, IP addresses, domain names and URLs.

"Online Services Terms and Conditions" means the Online Services Terms and Conditions located at or accessed through https://www.accenture.com/us-en/support/security/legal-terms.

"**Term**" shall mean the term of the subscription of the Service(s) as specified in the applicable Order Confirmation.

"**Threat Indicator Content**" means up-to-date streams of Indicators that assist Client in detecting cyber-attacks within Client's network.

"**Vulnerability Content**" means information about both public and unpublished zero-day vulnerabilities derived from multiple public sources and internal research.

2. Entitlement and Subscription Information

Accenture grants to Client, during the Term, a limited, non-exclusive, non-transferable, non-assignable revocable right for IntelGraph Authorized Users to access and use, solely in accordance with the terms and conditions herein and any applicable instructions or documentation, the various components of the Accenture CTI as a Service as set forth below. This authorization shall include the right to distribute any authorized Content to Distributees, *provided* such Distributees agree to the restrictions relating to the Content set forth herein.

- IntelGraph Client Portal.
  (a) the IntelGraph Client Portal for the purposes of viewing and accessing the Content; and
  (b) the Content for the management and protection of Client's networks, systems and assets.

- IntelGraph API Services.
  (a) the IntelGraph API Service for the purposes of accessing and using the Content; and
  (b) the Content for the management and protection of Client's networks, systems and assets.

- IntelGraph Threat Indicator API Service.
  (a) the IntelGraph Threat Indicator API Service for the purposes of viewing and accessing the Threat Indicator Content; and
  (b) the Threat Indicator Content for the management and protection of Client's networks, systems and assets.

- IntelGraph Vulnerability API Service.
  (a) the IntelGraph Vulnerability API Service for the purposes of viewing and accessing the Vulnerability Content; and
  (b) the Vulnerability Content for the management and protection of Client's networks, systems and assets.

- Accenture CTI Analyst Service. If Client has purchased the Accenture CTI Analyst Service, Client may request additional information pertaining to the CIRs by submitting an RFI to Accenture via email or the IntelGraph Client Portal. Accenture may, in its reasonable discretion, decline to respond to an RFI if such RFI requires extensive research (more than four (4) hours) or does not fall under the CIRs.

Accenture may, in its sole discretion, discontinue any, all, or a material part of the Accenture CTI Services immediately, if necessary, to comply with the law or regulations or court or governmental order, decision or directive; provided Accenture promptly provides Client written notice of such discontinuation. Within thirty (30) days after receipt of notice by Accenture under this Section, Client shall have the right to terminate this Agreement, without penalty, in which case, Accenture shall refund to Client any pre-paid Fees for the terminated Accenture CTI Services based on a pro-rata portion of the Fees for Accenture CTI Services not yet rendered within ten (10) days after such notification by Client. Upon expiration of the foregoing sixty (60) day period, Client acknowledges and agrees that Client is responsible for connecting to the modified API Service, if applicable, in order to continue receiving the applicable Content.

3. Client Assistance and Technical Support

Client may contact Accenture support by telephone and by email on a 24x7 basis for technical support and assistance related to the Service. Accenture will (i) notify Client (email being sufficient) at least forty-eight (48) hours in advance of any planned maintenance; and (ii) use reasonable efforts to notify Client (email being sufficient) as soon as possible in the event of an emergency maintenance.

4. Client Responsibilities

Accenture can only perform the Service if Client provides the 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 Service, the Content, or the individual components of the Accenture CTI as a Service. Client will keep its connections to Accenture's systems secure (including safeguarding user credentials) and immediately notify Accenture of any breach of security related to such connections.
- Client is responsible for (i) appointing IntelGraph Authorized User(s) to access the IntelGraph Client Portal and/or applicable API Services; (ii) ensuring that its IntelGraph Authorized Users keep their usernames, passwords and the API Keys confidential and comply with the applicable terms of this Agreement; (iii) removing IntelGraph Authorized Users who leave Client's organization or who otherwise no longer require access to the IntelGraph Client Portal and/or API Services; (iv) all actions of the IntelGraph Authorized Users and Distributees as if such actions were those of Client; and (v) Client's use of its connections to Accenture's systems;
- Client is solely responsible for its use of the Content and any action or inaction in response to the Content. 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 Content.
- If Accenture determines, in its sole but reasonable discretion, that any of the Content contains 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, or make inaccessible any such Content promptly upon written notice from Accenture.
- Client acknowledges that the Accenture Cyber Threat Intelligence as a Service is 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 REPRESENT, WARRANT, OR GUARANTEE THAT THE CONTENT WILL BE ACCURATE, RELIABLE OR ACTIONABLE OR THAT USE OF THE SERVICES, OR ACCENTURE WORKS WILL BE UNINTERRUPTED OR ERROR FREE AND THAT USE OF THE SERVICES, OR ACCENTURE WORKS WILL BE UNINTERRUPTED OR ERROR FREE AND ACCENTURE SHALL NOT BE LIABLE FOR CLIENT'S ACTION, OR FAILURE TO ACT, IN RESPONSE TO ANY CONTENT.
- The Service, the Content, and the individual components of the Service, as well as the APIs to access them are Accenture's or its third-party licensors' proprietary and Confidential Information and shall be treated as such in accordance with the Online Terms and Conditions. Client will not remove any confidentiality, copyright, or other markings from the Content, and is responsible to keep the Content confidential, to only use the Content internally within its business for the purpose of protecting its networks, and to protect the Content 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 Service, the Content or the APIs.
- Except for any limited rights expressly granted in this Agreement, Client acknowledges that Accenture retains all right, title and interest in and to the Accenture Works. Except as otherwise expressly stated in the Agreement, nothing in the Agreement shall create any right of ownership or license in and to the other Party's Intellectual Property Rights, and each Party shall continue to independently own and maintain its Intellectual Property Rights. Client shall not: (a) attempt to create a substitute service or product for the Service through the use of the Service; (b) permit either direct or indirect use of the Service or any Accenture

Works by any third party; (c) transfer, distribute or sell any component of the Service (including the Content) or any copy thereof to any client, end-user, or other third party or display copies of all or any portion of the Content; (d) use the Content to provide services to any third party; (e) remove any confidentiality, copyright or other markings from the Content or any Accenture Works that it displays or copies in accordance with this Agreement; (f) create derivative works (as defined under U.S. copyright law) of the Content; or (g) modify, disassemble, decompile, reverse engineer, create derivative works (as defined under U.S. copyright law) of, or make any other attempt to discover or obtain the Intellectual Property which deliver the Service, including, but not limited to, the IntelGraph Client Portal and any of the API Services.

- 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.

5. Data Privacy Notice

Accenture will need the names and business email addresses of Client's Authorized Users in order to provide logon credentials, and 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**"). Accenture is a data processor and Client is the data controller with respect to the Client Personal Data under applicable data protection laws, including but not limited to the EU General Data Protection Regulation (GDPR). Client represents that it has all necessary rights and consents to provide Client Personal Data to Accenture.

Accenture agrees that it will: (a) only use the Client Personal Data in accordance with Client's instructions and in compliance with this Agreement, and only during the Term of this Agreement; (b) implement appropriate technical and organizational security measures to safeguard Client Personal Data, as set forth in Accenture's security procedures, which are available to Client upon request. Client has satisfied itself that Accenture's security procedures provide a level of security appropriate to the risk in respect of any processing of Client Personal Data under this Agreement; (c) provide assistance as reasonably requested by Client with respect to Client's obligations under applicable data protection laws (e.g. responding to requests by individuals, providing notice of breaches, consulting with regulators); (d) make available information as reasonably requested by Client to demonstrate Accenture's compliance with its obligations under this Section; and (e) return or destroy (at Client's direction) such Client Personal Data upon request of Client or termination of this Agreement.

Client specifically authorizes the engagement of Accenture's affiliates as subprocessors and generally authorizes the engagement of other third parties as subprocessors as identified by Accenture and listed within the IntelGraph Client Portal, which may be updated by Accenture from time to time. Accenture shall contractually require any such subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder. Accenture shall remain fully liable for the performance of the subprocessor. Accenture shall provide Client with written notice of any intended changes to the authorized subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes.

END OF SERVICE DESCRIPTION