Accenture Cyber Threat Intelligence

Service Description

December 2021

This Service Description, with any attachments included by reference, is provided under the following terms and conditions in addition to the Accenture Terms and Conditions or any other terms and conditions included or referenced in the order confirmation issued by Accenture related to Client's purchase of Services or 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 (ACTI). All capitalized terms in this description have the meaning ascribed to them in the Agreement or in the Definitions section.

1. Service Features and Definitions

Accenture shall provide the component or components of ACTI that are identified in the applicable Order Confirmation, each of which is more fully described below (the "**Service**"). During the Term, Accenture grants to Client a limited, non-exclusive, non-transferable, non-assignable revocable right for Client or its IntelGraph Authorized Users to access and use, solely in accordance with the terms and conditions herein and any applicable instructions or documentation, such Service solely for Client's internal use for the management and protection of Client's networks, systems and assets. This authorization shall include the right to distribute any in-scope ACTI Content to Distributees, *provided* such Distributees agree to the restrictions relating to the ACTI Content set forth herein.

Service Component	Service Description
ACTI IntelGraph Enterprise	Includes both ACTI IntelGraph Portal access and ACTI Full IntelGraph API service, each as defined below.
ACTI IntelGraph Portal	A web-based portal which provides Client's Authorized Users with access to the full ACTI Content.
ACTI Full IntelGraph API	An API service that provides Client with access to the full ACTI Content.
ACTI IntelGraph Threat Indicator API	An API service that provides Client with access to ACTI's streams of data points, such as IP addresses, domain names and URLs, that may be indicators of cyber threats (the "**Threat Indicator Content**").
ACTI IntelGraph Vulnerability API	An API service that provides Client with access to ACTI's streams of information about both public and unpublished vulnerabilities derived from multiple sources (the "**Vulnerability Content**").
Requests for Intelligence	A Service that allows Client to request additional information pertaining to the CIRs by submitting an RFI to Accenture via email or the ACTI IntelGraph 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 . Alternatively, if Accenture decides to respond to a Client request requiring extensive research then such request may count as more than one RFI.
Recon Darknet Detection (RDD)	A Service that provides Client with alerts ("**Alerts**") when certain Client information is detected on the dark web or other searched sources. In-scope components for alerting will be set forth in the Order Confirmation.
Recon Research Requests	A Service that allows Client to request additional research pertaining to the Alerts by submitting a request for additional research (**Recon Research**) to Accenture via email. Accenture will review the request and respond with an estimate of the effort that will be required to undertake the research. If Client authorizes the estimate, the research effort will be credited against pre-paid Recon Research Requests. Notwithstanding the

	foregoing, Accenture can decline to undertake any requested Recon Research at any time, before or after authorization of an estimate, if such research becomes infeasible.
Advanced IP Reputation Feed	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 (the "**Advanced IP Reputation Content").**
Advanced Domain/URL Reputation Feed	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 (the "**Advanced Domain/URL Reputation Content").**

Definitions

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

"**Accenture Cyber Threat Intelligence,**" "**ACTI**" or the "**Service**" means the services described in this Service Description and any other Accenture Works provided in connection therewith.

"**Accenture Works**" means (a) all of Accenture's (or its licensors') Confidential Information, the Service, the ACTI IntelGraph Portal, the ACTI 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 the 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 or Confidential Information.

"**ACTI Content**" means the (a) Vulnerability Content; (b) Threat Indicator Content; (c) Alerts; (d) Advanced IP Reputation Content; (e) Advanced Domain/URL Content and (f) any other cyber intelligence information, alerts, analytical tools, and interactive visualizations made available to Client as part of the Service via the IntelGraph Portal, an API service, RFIs, Recon Research, 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.

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

"**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.

"**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.

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

"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.

"Accenture Terms and Conditions" means the Accenture 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.

2. 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.

3. Client Responsibilities and License Restrictions

Accenture's grant of use rights under the Agreement is subject to the following Client responsibilities and restrictions:

- 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 Service components. 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 ACTI IntelGraph 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 ACTI IntelGraph 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 responsible for providing up-to-date key words or other information needed by Accenture in order to perform the Services.
- Client is solely responsible for its use of the ACTI 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 this Agreement, or its actions or inactions in response to the ACTI Content.
- If Accenture determines, in its sole but reasonable discretion, that any of the ACTI 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 ACTI Content promptly upon written notice from Accenture.
- Client acknowledges that Accenture Cyber Threat Intelligence 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 ACTI CONTENT WILL BE ACCURATE, RELIABLE, COMPLETE OR ACTIONABLE OR 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 ACTI CONTENT.
- The Service, the ACTI 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 this Agreement. Client will not remove any confidentiality, copyright, or other markings from the ACTI Content, and is responsible to keep the ACTI Content confidential, to only use the ACTI Content internally within its business for the purpose of protecting its networks, and to protect the ACTI 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 ACTI 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, 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 ACTI Content) or any copy thereof to any client, end-user, or other third party or display copies of all or any portion of the ACTI Content; (d) use the ACTI Content to provide services to any third party; (e) remove any confidentiality, copyright or other markings from the ACTI 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 ACTI 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 ACTI IntelGraph Portal and any of the API Services. Notwithstanding anything to the contrary in the Agreement, each party will remain fully liable (without any limits) for any use/mis-use of the other party's intellectual property in violation of the terms of this Agreement.
- Upon any expiration or termination of the Order Confirmation, (a) Client shall immediately cease using the ACTI Service; (b) the rights to use the Service and the ACTI Content will immediately terminate, provided, however, Client shall have a right to continue to use ACTI Content in its possession post expiration or termination in accordance with this Agreement.
- 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.

4. Service Updates

Accenture may, in its sole discretion, discontinue any, all, or a material part of the ACTI 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 ACTI Services based on a pro-rata portion of the Fees for ACTI Services not yet rendered within ten (10) days after such notification by Client. Upon expiration of the foregoing thirty (30) 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 ACTI Content.

5. Data Protection

Pursuant to the applicable data protection terms of the Agreement, Accenture will process on behalf of the Client the following categories of personal data as necessary to perform the Services: (i) the names and business email addresses of Client's Authorized Users, as communicated to Accenture by Client, in order to provide logon credentials; (ii) Personal Data that may be included in any key word data or information provided by Client and necessary to for the RDD Service (if applicable); (iii) any Personal Data that Accenture may, in the course of the Service, come into contact with and then share with Client, including business email addresses, passwords or other similar personal data of Client's personnel, vendors or clients, as well as of any other individuals whose data is returned as a result of searches pursuant to Client-provided names/key word data (Personal Data under (i), (ii) and (iii) collectively, in the context of the Services, (the "**Client Personal Data**").

Client acknowledges and agrees that 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 and warrants that it has and will maintain for the whole Term of the Agreement all necessary rights (including the existence of lawful legal basis for the processing, as applicable), authorizations and consents, and that it has provided all necessary notices, as required under applicable data protections laws, to provide Client Personal Data to Accenture, to entrust Accenture for the research of this Client Personal Data as necessary under the Services, as well as to receive and collect back this Client Personal Data under the Services.

Accenture agrees that it will: (a) only use the Client Personal Data to the extent that is necessary and proportionate to perform the Services, and in accordance with Client's instructions, 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 generically authorizes the engagement of Accenture's affiliates as subprocessors and specifically authorizes the engagement of other third parties as subprocessors as identified by Accenture and listed within IntelGraph 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 or any intended appointment of a new third party subprocessor and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes/appointment.

END OF SERVICE DESCRIPTION