Offer Description: Cisco Defense Orchestrator and Cisco Security Analytics and Logging

This Offer Description (the **"Offer Description"**) describes Cisco Defense Orchestrator and Cisco Security Analytics and Logging (each a **"Cloud Service"** and collectively, the **"Cloud Services").** Your subscription is governed by this Offer Description and the Cisco Universal Cloud Agreement located at www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the **"Agreement"**). Capitalized terms used in this Offer Description and/or the Order not otherwise defined herein have the meaning given to them in the Agreement.

Table of Contents

1. Offer Description.

1.1. Cisco Defense Orchestrator.

Cisco Defense Orchestrator ("CDO") is a cloud-based security policy management application that allows the user to manage multiple Cisco security products with the following functionalities: policy change management, policy analysis and optimization, policy monitoring and reporting, orchestration of policy changes, and device and element management.

1.2. Cisco Security Analytics and Logging.

Cisco Security Analytics and Logging ("SAL") is an optional add-on product to CDO that provides greater visibility into network events and advanced threat detection and analytics utilizing (i) firewall event data and (ii) network telemetry through use of Stealthwatch Cloud Private Network Monitoring if the TA (defined below) license package is purchased.

The SAL Logging and Troubleshooting (LT) license package is generally available as of the publication date of this Offer Description. The SAL Firewall Analytics and Monitoring ("FA") and SAL Total Network Analytics and Monitoring ("TA") license packages are anticipated to be released in Fall 2019. FA and TA include the right to access and use certain Stealthwatch Cloud features.

Please see the Stealthwatch Cloud Offer Description at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html for more information regarding Stealthwatch Cloud .

2. Supplemental Terms and Conditions

2.1. SAL Overage Billing.

SAL subscriptions are priced on the firewall event log volume in gigabytes per day (GB/d). Cisco may bill for overages monthly in arrears. At the end of each calendar month, Cisco calculates the actual average daily firewall event log volume for the month and automatically invoices customers for any overage. For example, if a customer purchases a subscription for 10 GB/day, the customer is entitled to 300 GB of firewall event log volume for a 30 day calendar month. If at the end of such calendar month the customer actually used 330 GB, the average daily usage is 330/30 = 11, and Cisco shall have the right to bill the customer for an overage subscription 1 GB/day for that month.

2.2. Cisco Threat Content.

If Your use of a Cloud Service requires or permits You to use any Cisco Threat Content, then You (and Your agents acting on your behalf) may only use such Cisco Threat Content for Your use with such Cloud Service and with those third party products or services offerings that Cisco has identified as being compatible. You agree not to provide Cisco Threat Content to a third party.

2.3. Integration with Third Party Products.

The Cloud Service may allow you to integrate with third-party products. Cisco does not support or warrant third-party products and disclaims all responsibility and liability for third-party products used with the Cloud Service, including any responsibility for customer data transferred to such third-party product through Your use of the applicable integration. If You use a third-party product, the terms of use for that third-party product are between You and the provider. Some third-party products may contain tracking technology. Accordingly, it is Your responsibility to read the third party's disclosures, terms of use, and privacy policy before using such third-party products with a Cloud Service.

2.4. Disclaimers.

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD PARTY MALICIOUS ATTACKS. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS.

3. Data Protection

Cisco's data protection obligations are set forth in the Agreement. Additionally, the Cisco Defense Orchestrator and Cisco Security Analytics and Logging Privacy Data Sheet(s) (available here) supplement the Cisco Privacy Statement and describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services.

If You use a Cloud Service in China, You (1) acknowledge that You are the entity causing data to be transferred outside of China in connection with your use of the Cloud Service, and (2) acknowledge Your obligation to comply with China's cybersecurity requirements and other requirements related to the cross border transfer of data.

If You use a Cloud Service in Russia, You acknowledge that You are the data operator as defined under Russian law for purposes of Your users' personal data that is collected and processed in connection with the Cloud Service.

4. Support & Maintenance.

A CDO subscription includes basic support with online support and phone support. A SAL subscription includes basic support with online support only. Cisco will respond as set forth in the table below and may require information from you to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. Cisco will respond to a submitted case no later than the next business day during standard business hours.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. Cisco will respond within one (1) hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, Cisco will respond no later than the next business day.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic with Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day
Basic with Online Support	Web	Response to all cases within next Business Day during Standard Business Hours	

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

Severity 1 means the Cloud Service is unavailable or down or there is a critical impact to a significant impact to Case Submitter's business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

Severity 2 means the Cloud Service is degraded or significant aspects of Case Submitter's business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

Severity 3 means the Cloud Service is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

Severity 4 means minor intermittent functionality or performance issue, or information is required on the Cloud Service. There is little or no impact to Case Submitter's business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

Business Day means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

Local Time means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

Standard Business Hours means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

Your access to and use of the Cloud Services may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.

Definitions.

Cisco Threat Content means any Cisco provided threat intelligence, content or data including, but not limited to, rules, signatures, threat data feeds or suspicious URLs and IP address data feeds for use with any Cisco product or service.

Telemetry Data means Telemetry Data as defined in the Agreement and for the avoidance of doubt, includes without limitation: netflow data; origin and nature of malware; network security policies; the types of software or applications installed on a network or an endpoint; information related to the usage, origin of use, traffic patterns and behavior of the users of a network or cloud service; any geolocation data; or network traffic data such as cookies, web logs, web beacons, and other similar applications.