cisco SECURE

Offer Description: Cisco Security Analytics and Logging

This Offer Description (the **"Offer Description"**) describes Cisco Security Analytics and Logging SaaS ("**SAL SaaS**" or the "**Cloud Service**") and Cisco Security Analytics and Logging On-Premise ("**SAL OP**" or the "**Software**"**).** Your right to use the Software and/or Cloud Service is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (or similar terms existing between you and Cisco) (the **"Agreement"**). Capitalized terms used in this Offer Description and not otherwise defined herein have the meaning given to them in the Agreement.

1. Description

1.1. Cisco Security Analytics and Logging

Cisco Security Analytics and Logging ("SAL") provides Central Log Management (CLM) for streamlining IT operations, with added ability to analyze logs for enhanced visibility and advanced threat detection. SAL debuted with Cisco Firewall logs (FTD and ASA), with Network Flow Logs and other log sources being included progressively. Disparate logs types are covered by the same offer structure, which adopts a nested licensing model (i.e. with lower licenses nested in higher license capabilities). The licenses are:

(a) **Essentials**, formerly Logging and Troubleshooting (LT): Scalable central logging service with long-term retention options, with drill—down enabled through advanced viewer controls such as search, filer, download, etc.

(b) **Advantage**, formerly Log Analytics (LA): An optional capability to analyze logs for advanced threats using behavioral modelling techniques. These threat detection algorithms leverage existing Cisco Stealthwatch analytics, as well as trigger new alerts customized for SAL logs.

(c) **Premier**, formerly Total Network Analytics (TA): Aggregates log analysis with native Cisco Stealthwatch logs, for end-to-end analysis.

SAL SaaS licenses include the right to use the Cisco Defense Orchestrator (CDO) for firewall log viewing. In addition, Advantage (Log Analytics) and Premier (Total Network Analytics) licenses include the right to use Stealthwatch Cloud (SWC) for advanced threat detection. Please note that SAL SaaS does not require a separate subscription for either CDO or SWC, and neither is it mandatory for SAL logging firewall devices to be managed by CDO.

Similarly, SAL OP licenses leverage the Stealthwatch Enterprise (SWE) virtual and physical appliances, without the need for separate SWE flow rate licenses for SAL OP purposes. Flow rate licenses continue to be required for purposes of SWE.

1.2. Cisco SecureX

Your SAL subscription includes access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence (through SecureX threat response, also known as Cisco Threat Response), unifies visibility across various Cisco and third party security products, enables automated workflows, and more. Since SAL data triggers alerts in SWC and/or SWE, such alerts will be visualized in SecureX leveraging Stealthwatch's native integration with SecureX. For more information on SecureX, please see the SecureX Offer Description at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html.

2. Supplemental Terms and Conditions

2.1. Overage Billing

Security Analytics and Logging licenses are priced on log volume in gigabytes (GB) per day. For SAL SaaS offer only, 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 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. Disclaimers

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICE OR SOFTWARE 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 SERVICE OR SOFTWARE 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 OR SOFTWARE 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

The SAL, CDO, SWE, SWC and SecureX Privacy Data Sheet(s) (available here) describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services. For further detail on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center.

4. Support & Maintenance

A **Security Analytics and Logging (SaaS)** subscription includes basic support with online support only. 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.

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 Online Support	Web	Response to all cases within next Business Day during Standard Business Hours	

A **Security Analytics and Logging (On Prem)** subscription includes basic embedded SWSS support with phone and online support.

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 SWSS	24X7 access to Cisco Technical Assistance Center (online and phone)	Response within 1 hour	Response within next Business Day

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.