Service Description for Cisco Secure Endpoint-Complete

This document (this "**Service Description**") describes the service features, components, and terms of the Cisco Secure Endpoint-Complete (the **"Services"**) that Cisco will provide to the designated customer listed in the order ("**Customer**"). The specific quantity and type of the Services purchased by Customer (directly or via an Authorized Reseller) will be documented in a service order, quote, or web order that is signed, click accepted, or other means of assent (e.g., issuing a purchase order) ("**Order**") between the parties. This Service Description should be read in conjunction with How Cisco Provides Services and the Cisco Secure Endpoint Offer Description for the Endpoint Licensing specific Offer Agreement. Appendix A to this Service Description has additional terms and conditions governing the Services.

1. Solution Overview

The Cisco Secure Endpoint-Complete is a combination of Cisco Secure Endpoint technology, Cisco Talos Threat Hunting capability, Cisco Talos Incident Response service and the Cisco Secure Managed Detection and Response (MDR) service which provides the Customer with (i) 24/7 threat monitoring through a combination of the Cisco Secure MDR service and the Cisco Talos threat hunting capability, and (ii) the Cisco Talos Incident Response service, which helps to prepare the Customer to respond to security breaches or compromises and which help support Customer during such incidents.

2. Solution Details

2.1. Cisco Secure Endpoint-Complete Services Features

Service Element	Description
Activation	Validation of Cisco Secure Technology Configuration: Cisco configures its MDR Platform, aligns runbooks and works with the Customer to help Customer configure and deploy the Covered Security Components (defined below in Section 2so that Cisco can actively monitor the Customer's environment in the manner described in this Services Description.
Detection	24x7x365 Security incident and alert monitoring: Cisco provides 24/7/365 monitoring of the Covered Security Components by experienced threat analysts, investigators, and incident responders. Quarterly Threat Briefing: Remote review meetings on a quarterly basis open to all Cisco Secure MDR Customers. This quarterly briefing will provide updates on current threat patterns and trending events. Threat hunting: For Customers with Cisco Threat Hunting enabled, Cisco will ingest Threat Hunting alerts, investigate them, and provide results to the Customer. Details on the Threat Hunting can be found here: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/secure-endpoint-offer-description.pdf.
Analysis	Investigation and response runbooks: Cisco uses its detection, investigation and response runbooks.
Investigation	Integrated Talos Threat intelligence: Cisco will correlate and prioritize security alerts with common threats, Talos Threat Intelligence and third-party threat intelligence using analytics, security orchestration, and automation response to help determine whether observed events and/or notifications are a breach or compromise
Response	Guided response actions: Cisco recommends responses to help contain, mitigate, remediate, or eradicate the threat. Threat advisories: Cisco issues threat advisories for new threats discovered helping Customer to proactively prevent incidents, or compromises through the implementation of mitigating controls.
Incident Response	Integrated Cisco Talos Incident Response Service: Cisco Talos Incident Response Services provide emergency response services and proactive services to help assess, strengthen, and evolve a Customer's incident readiness program.

2.2. Cisco Secure Technologies

The Services are dependent on the Customer configuring the Cisco cloud services and software products defined in documentation provided by Cisco as part of the Cisco Secure Endpoint Complete Service. Collectively, these Cisco cloud services, and software products shall be known as the "**Cisco Secure Technologies**".

The Cisco Secure Technologies are:

a) Cisco Secure Endpoint Premier
b) Cisco Secure Malware Analytics
c) Cisco SecureX Orchestrator

Customer must purchase the Cisco Secure Endpoint-Complete Service and the Cisco Secure Technologies together as part of the same ordering SKU in the quantities specified by Cisco in Cisco's quote. Customer is also required to obtain

and maintain all applicable Cisco support and maintenance agreements and any required infrastructure (i.e., compatible device types) in connection with Cisco Secure Endpoint-Complete and to support Customer's needs.

3. Service Delivery Model for Cisco Secure Endpoint-Complete

Cisco uses a standardized National Institute of Standards and Technology (NIST) aligned operational framework for the delivery of the Services, as more fully described in this Section 3. For the purposes of this Service Description, the Cisco Secure Technology specified in the Order as being within the scope of the Services is defined as a "**Covered Security Component**".

3.1. Service Activation.

The purpose of the Service Activation activity is to configure the Cisco MDR platform and work with the Customer to configure Covered Security Components in order to perform the other activities described in this Section 3.

Cisco Responsibilities

- Cisco will provide technical and operational documentation to Customer to help Customer configure the Covered Security Components, including the API interface requirements needed to enable the Services;
- Provided Customer has performed the required steps as described below correctly, Cisco will onboard the Covered Security Components onto the Cisco MDR platform and perform testing to verify that the Covered Security Components are operating as expected and that all the Cisco playbooks have been correctly applied; and
- Cisco will recommend initial configuration policies for the Covered Security Components

Customer Responsibilities

Customer will:

- Provide the appropriate API tokens with the correct level of access for Covered Security Components;
- Configure and verify that the correct connectivity to the Cisco SOC has been established and support any future connectivity issues;
- Make necessary configuration and policy changes to the Covered Security Components to align with the Cisco recommendations necessary for the delivery of the Services;
- Provide and maintain the necessary contact information for identified technical and operational contacts along with the escalation matrix for the organization; and
- Provide and maintain full admin access to the Covered Security Components for Cisco, as necessary for Cisco provide the Services. For example, Customer will not remove or limit access from either the API for each technology nor the web-console interfaces.

3.2. Detect.

Cisco will monitor the security alerts and notifications from the Covered Security Components for potential Security Incidents. Cisco will correlate and prioritize security alerts with common threats, Talos Threat Intelligence and third-party threat intelligence using analytics, security orchestration, and automation response to help determine whether observed events and/or notifications are a breach or compromise. Any detected security events which Cisco believes may pose a potential security threat will be escalated into a Customer-facing security incident ("**Security Incident**"), available from the Cisco Secure MDR Service Portal. All Security Incidents will be prioritized and categorized in order to help streamline Customer response.

Cisco Responsibilities

- Monitor for and investigate security events and alerts from the Covered Security Components through the Cisco Secure MDR platform, leveraging Talos Threat intelligence, SecureX Orchestrator and the capabilities of the Cisco Secure Endpoint:

- Utilize the capabilities of the Covered Security Components, in alignment with Cisco recommended configuration and policies. This includes security controls, response actions, query functionality, and detection techniques;
- Utilize Cisco Talos Threat intelligence and secure malware analytics to help identify the latest and most relevant threats, indicators of attack or compromise, and mitigation best practices;
- Leverage Cisco Talos Threat intelligence and Cisco MDR platform tools to enrich alerts with supporting information;
- Utilize threat research and tools to collect data on new attack Tactics, Techniques, and Procedures (TTPs) to help identify security breaches or compromises;
- Analyze each Security Incident to determine and then communicate recommended remediation or response actions to the Customer;
- Engage with the Customer on any high risk (P1 or P2) Security Incidents (verified true positive alert) with direct communication from the Cisco SOC to the Customer using the contact information provided by Customer. Cisco will provide context on the severity of the threat(s) and escalate the Security Incident in accordance with the agreed Security Incident response plan. Cisco provides the recommended remediation to the Customer for the Customer to complete the final remediation and resolution of the Security Incident;
- Report all potential threats detected in a timely manner to the Customer via detailed Security Incidents available on the Cisco Secure MDR Service Portal, including notifications for all new Security Incidents;
- Provide mitigation recommendations for all Security Incidents, including mitigation actions available as part of the Covered Security Components as well as best practices, controls, and configurations which apply within the context of a Security Incident's impact;
- Provide 24x7x365 expert SOC communication for all active Security Incidents as required;
- Follow up on Security Incidents as they evolve over time, adding additional context or detections to existing Security Incidents as needed and where possible;
- Respond to Customer inquiries related to active Security Incidents and related contextual information such as threat intelligence or overall impact to the Customer's environment or operations;
- Notify Customer of major changes or new functionality within the Covered Security Components, as they are available, in a timely manner, including any recommended configuration or policy changes; and
- Notify Customer of any planned or unplanned outages related to: the Cisco Secure MDR Service Portal, the Cisco MDR platform monitoring capabilities, or functionality related to Cisco's ability to monitor or respond to events coming from the Covered Security Components.

Customer Responsibilities

- Notify Cisco of planned activities or outages (e.g., software updates) or if it detects a possible Security Incident;
- Perform remediation actions recommended by Cisco's security analysts;
- Approve automated remediation actions in a timely manner; and
- Maintain an acceptable deployment configuration and deployment of the Covered Security Components, as required to enable Cisco to perform the Services in accordance with this Services Description.

3.3. Analyze.

Cisco will analyze anomalous events, alerts, and data to identify potential threats. Cisco will ingest Threat Hunting alerts, investigate them, and provide results to the Customer.

Cisco Responsibilities

- Utilize all sources of contextual and alert information available from the Covered Security Components to enable monitoring and detection of potential security threats. Correlate, analyze, and investigate each threat scenario presented with expert techniques and skillsets as applicable and practical for the given threat. Subject to Customer maintaining timely access to Cisco of the Covered Security Components (as configured as part of Service Activation), ensure all expected data sources are reporting data into the Cisco MDR Platform as expected and in acceptable timeframes, given the configuration and completed onboarding of the Customer. Investigate certain categories of anomalous events and traffic where there is not a known cause, where these events and/or this traffic may, In Cisco's opinion, pose a material threat;
- Utilize sources of non-Cisco specific contextual information as required, such as public DNS registration information, Virus Total, and more; and
- Perform analysis and effective investigation techniques, automated or manual, for any given Security Incident, utilizing the latest available contextual and correlative data and all available practical expertise within the scope of the Services, and use reasonable endeavors to deliver information within the Security Incident ticket that is actionable and easy for Customer to interpret.

Customer Responsibilities

- When requested, provide requested contextual data (e.g., systems running, any maintenance activities, etc.); and
- Review active Incidents from the Cisco Secure MDR Service Portal to a degree necessary to interpret the breadth of the Incident, and to distill a plan to reach a secure state.

3.4. Investigate.

Cisco will Investigate threats on Covered Security Components and user behaviors, applications, and the network elements protected by the Covered Security Components, where information on such threats is visible from within the Covered Security Components.

Cisco Responsibilities

- Use threat intelligence to research indicators of compromise (IOCs) and attack (IOAs) to confirm threats, attacks, compromises or exploits;
- Create an Incident ticket and notify Customer if a Security Incident is identified by Cisco or reported by Customer and verified by Cisco;
- Use established investigation methodology to add context from the Covered Security Components to help identify impact, severity, and scope of Security Incidents;
- Investigate the Security Incident for impact to the Customer, the attacker's level of success and their "Tactics, Techniques & Procedures"; and
- Investigate Security Incidents Customer has opened with Cisco using the same level of expert analysis as Cisco-discovered threats, including the same techniques and expertise available for a typical Security Incident. These Security Incidents will be prioritized and will include response action recommendations as well as information

(provided from available Cisco data sources) that confirms, validates, or otherwise corroborates the initial detection of a potential Security. For these Security Incidents, Cisco will analyze Customer-provided threat information or logs, if Cisco deems the data to be sufficiently reliable and relevant.

3.5. Respond.

Cisco will notify and update Customer of the status of the Security Incident and, based on the nature of the Security Incident: perform approved changes to the Covered Security Components, provide guided recommendations, and/or provide general recommendation responses to help contain, mitigate, remediate, or eradicate the Security Incident.

- Provide guidance on how to help mitigate, stop, or prevent a Security Incident based on the intelligence and advisories provided, as relevant to Customer's environment. Cisco's recommended response to a Security Incident, may be one or more of the following:
  - With Customer's permission, perform approved policy or configuration changes to the Covered Security Components to help mitigate or respond to Security Incidents (Note: automated responses are limited to those documented in Cisco Secure MDR response playbooks);
  - Where the Security Incident is a known attack, recommend response actions to help mitigate the attack and provide guidance on how to help further remediate the Security Incident, leveraging the Covered Security Components;
  - Where further validation of the threat is required, Cisco will provide recommendations on areas of focus for Customer investigation;
  - Where response actions are outside of the Covered Security Components, Cisco will provide the client with recommendation for further Customer investigation and remediation;
- Create and/or modify the Cisco Secure MDR response playbooks based on new information and threats from security events detected from the Covered Security Components and processes described above; and
- Release advisories as new information is obtained about new or novel threats (these advisories are not specific to Customer).

Customer Responsibilities

- Participate in diagnostic testing to help identify the source of the Security Incident;
- Perform Cisco recommended changes to Covered Security Components and be responsible for acting on recommendations from Cisco, including determining any dependencies resulting from the recommended actions;
- Utilize the Cisco Secure MDR Service Portal to configure and approve response actions through Cisco APIs; and
- Utilize the resources on the Cisco Secure MDR Service Portal for support, knowledge base, incident management, latest threat intelligence, and communication with Cisco.

3.6. Cisco Talos Incident Response Service Delivery

Cisco Talos Incident Response provides remote reactive support and proactive services to help assess, strengthen, and evolve a Customer's incident readiness program.

Cisco Responsibilities

- Use commercially reasonable efforts to assign a resource via telephone for remote reactive incident response support of Cisco receiving notification by Customer of a security incident. Reactive support will be escalated from the Cisco Secure MDR Security Operations Center to the Cisco Talos Incident Response resources.
- Provide the following remote only reactive and proactive services by purchased endpoint volume:

Number of Endpoints	Remote Reactive (per 12 months)	Remote Proactive (per 12 months)
500 – 999	Up to 20 Hours of Incident Triage for up to one (1) incident	Cisco Secure Endpoint-Complete Incident Readiness Workshop.
1,000 – 4,999	Up to 20 Hours of Incident Triage for up to one (1) incident	Cisco Secure Endpoint-Complete Incident Readiness Workshop; and ***one (1)*** of the following: *one (1) Plan Created or reviewed/updated; *or Compromise Assessment
5,000 – 9,999	Up to 80 Hours of Emergency Incident Response	Cisco Secure Endpoint-Complete Incident Readiness Workshop, which may include review of existing Incident Response Plan; and ***one (1)*** of the following: * two (2) Playbooks Created or reviewed/updated; * or Tabletop Exercise; * or Compromise Assessment
10,000 – 24,999	Up to 80 Hours of Emergency Incident Response	Cisco Secure Endpoint-Complete Incident Readiness Workshop, which may include review of existing Incident Response Plan; and up to ***two (2)*** of the following: * Tabletop Exercise; * or Compromise Assessment; * or Cyber Range; * or two (2) Playbooks Created or reviewed/updated;
25,000+	Up to 120 Hours of Emergency Incident Response	Cisco Secure Endpoint-Complete Incident Readiness Workshop, which may include review of existing Incident Response Plan; and up to ***three (3)*** of the following: * Purple Team * or Tabletop Exercise; * or Compromise Assessment; * or Cyber Range; * or two (2) Playbooks Created or reviewed/updated

Customer Responsibilities

- Participate in the Cisco Secure Endpoint-Complete Incident Readiness Workshop within 30 (thirty) days of on-boarding
- Provide a primary point of contact and a list of members who can call for emergency response services
- Attend meetings as scheduled for proactive and reactive services

- Proactive Services need to be requested and scheduled at least ninety (90) days before the end date of the subscription.
- Purchase a full Cisco Talos Incident Response Retainer Service for any Emergency Incident Response hours or Proactive Services above what is provided in the table above.

3.6.1 For the purposes of this Section 3.6, the following additional definitions shall apply:

Term	Definition
Compromise Assessment	A service that that provides a high-level analysis and review of an organization's environment to help determine whether the customer's organization has been or is currently compromised.
Cyber Range	A multi-day training activity with an interactive Cisco lab environment for Customer employees to gain hands-on experience with digital forensic and incident response concepts from Cisco Talos Incident Response.
Emergency Incident Response	An emergency service that helps respond to cyber incidents, which may include triage, coordination, investigation (such as analysis and forensics), containment, and expert guidance to help remediation.
Incident Response Plan (or IR Plan or Plan)	A service that reviews or creates a document to capture who is responsible for handling processes and communications when experiencing a cyber incident.
Incident Response Playbook (or IR Playbook)	A service that reviews or creates document(s) to capture the steps that must be taken to detect, contain, and recover from a cyber incident that is threat specific.
Incident Triage	An initial scoping activity to evaluate if the Customer request aligns with the service and helps determine if there is a cyber incident. Incident Triage may include expert guidance on detection and containment with a plan of action.
Purple Team	A collaborative exercise where Cisco Talos Incident Response emulates adversary TTPs (tactics, techniques, and procedures) and partners with the Customer on detection.
Tabletop Exercise	A service that helps facilitate custom security incident scenario(s) to different levels of the Customer's organization and that provides an opportunity to practice and identify gaps within a Customer's incident response plan, processes, and procedures.

Appendix A – Terms

1. Services Terms.

1.1 **Scope of Services and Exclusions.** Unless the Services are expressly provided for above, all other Cisco services are out of scope for this Service Description. For clarity, the following are out of scope:

a) Change Management or implementation of changes not listed in the Services Catalog.
b) Connectivity, such as (for example) a local circuit.

1.2 **Reporting.** Cisco will provide or make available via the Cisco Secure MDR Service Portal, the reports listed in the reporting documentation for the Services. Cisco reserves the right to add, change, or remove reports in its reasonable discretion.

1.3 **Logging.** The Covered Security Components contain their own logging capabilities. Please see the product/service description and logging data for the Covered Security Components. The Services retain Security Incident ticket data for one year and then are deleted or overwritten on a rolling basis (oldest data first).

1.4 **Data Exchange.** Services-related data will be exchanged between Cisco and Customer only**.** If Customer wishes for a Partner or a third party to receive Incident data (e.g., Security Incident tickets) to provide complementary services on Customer's behalf, Customer will provide Cisco with a Letter of Authorization, allowing this sharing of data and coordination of Services.

1.5 **Detection and Response Capabilities.** While Cisco has implemented commercially reasonable technologies and processes as a part of the Service, Cisco cannot guarantee it will prevent, detect, stop, or mitigate all Security Incidents.

1.6 **Covered Cisco Security Component Technical Support.** The Services do not include technical support for the Covered Security Components. If Customer's issue requires technical support Covered Security Components, Cisco may perform initial triage and then direct Customer to Cisco's technical support services or direct Customer to contact Cisco technical support directly. Customer shall, at all times during the Term:

1.6.1 Maintain all operational functionality (including Cisco user and API access) of the Covered Security Components, as required by Cisco to enable Cisco to provide the Services; and

1.6.2 Notify the Cisco Secure MDR SOC of any changes that will impact access to the in-scope data sources required to deliver the Services.

2. Commercial Terms.

2.1 **Pricing Summary.** The Charges consist of a monthly fee based on the number and type of Security Components covered by the Services.

2.2 **Charges.** The charges for the Services ("**Charges**") and payment terms will be detailed in the applicable Order or the Agreement. Except as provided in the Orders or Cisco's material breach which gives Customer a right to terminate, all Charges paid are non-refundable. Cisco's rights to invoice for the Charges for the Services and Customer's obligation to pay will not be affected by (i) any delays caused by Partner or Customer (or anyone acting on their behalf), (ii) Customer's failure to perform or delay in performing its obligations under this Service

Description or any Supplement, or (iii) Customer's failure to issue a purchase order or Customer's delay or failure to pay an authorized reseller.

2.3 **Services Start Date.** The Order will contain the Requested Start Date ("**Requested Start Date**") and Cisco will commence provision of the Services on the Requested Start Date.

2.4 **Term.** The Term will begin upon the Requested Start Date and Cisco will invoice the Customer for the Charges on that date.

2.5 **Termination.** Where an Order contains a minimum commitment or contract value, if Customer terminates the Services for convenience, Cisco will invoice the remainder of contract value or minimum commitment due under the Order. If the Order does not contain a minimum commitment, Customer may not terminate the Services for convenience, even if the Agreement allows it, unless expressly provided in the Order. Rights to terminate for material breach are provided in the Agreement.

2.6 **Renewal.** If automatic renewal for the Covered Security Components is enabled, the Services will also automatically renew on the same basis, unless the parties are notified that they do not wish to renew the Services as follows:

- **a)** Cisco must notify Customer in writing at least ninety (90) days in advance of the renewal date that it will not renew.
- **b)** Customer must notify Cisco in writing at least thirty (30) days in advance of the renewal date that it will not renew.

3. Legal Terms

3.1 **License**. Upon expiration or termination of the Services, the license to the Cisco Secure MDR Service Portal, Services, and any associated software will automatically terminate. Note, this license is separate from the licensing and rights associated with the Covered Security Components, which are covered by their applicable licenses.

3.2 **Data Protection**. Privacy Data Sheet(s) (available here) describe the Personal Data that Cisco collects and processes as part of the delivery of the Services and the data process by the Covered Security Components. The Privacy Data Sheets for the Covered Security Components are separate but found at the same location.

Appendix B – Priority Levels

This Appendix describes the methodology and associated terminology used in determining the priority level of a Security Incident.

1. Priority Definition

The Priority of a Security Incident is based on the Impact and Urgency of an Incident.

Impact: A Security Incident is classified according to the breadth of its impact on Customer's business (the size, scope, and complexity of the Incident).	**Urgency:** The Urgency of a Security Incident is classified according to its impact on the monitored Security Components and impact to Customer's business.
There are four impact levels: **Widespread:** Entire Service is affected. **Large:** Multiple locations are affected. **Localized:** A single location or an individual user at multiple locations are affected. **Individualized:** A single user is affected.	There are four urgency levels: **Critical:** Significant Security Incident causing primary function to be stopped, or significant loss, corruption, or unauthorized encryption of sensitive data. There may be a significant, immediate financial impact to Customer's business. **Major:** Primary function is severely degraded due to loss in functionality or data loss, corruption, or unauthorized encryption. There is a probable significant financial impact to Customer's business. **Minor:** Non-critical function is stopped or severely degraded. There is a possible financial impact to Customer's business. **Low/Notice**: Non-critical business function is degraded. There is no material impact. Customer perceives the issue as low.

1.1 Priority Definitions

Priority defines the level of effort that will be expended by Cisco and Customer to resolve the Security Incident. The Priority level is determined by applying the Impact and Urgency definitions to the chart below.

		IMPACT			
URGENCY		Widespread	Large	Localized	Individualized
	Critical	P1	P1	P2	P2
	Major	P1	P2	P2	P3
	Minor	P2	P3	P3	P3
	Low/Notice	P4	P4	P4	P4

- P1: Cisco and Customer will commit all reasonable resources 24x7 to assist in resolving the Incident (as provided above).
- P2-P4: Cisco and Customer will commit reasonable full-time resources during standard business hours to resolve the Security Incident, provide information, or provide assistance (as applicable).

Cisco will adjust the case priority in accordance with updated priority of impact or incident resolution. In addition, the ticket may be left open after containment or restoration for a prescribed period while remediation efforts are being assessed.

Appendix C- Service Level Agreement ("SLA") for Cisco Secure Endpoint-Complete

1. Overview

This SLA describes the parties' responsibilities and sets Cisco's performance targets for the Services ("Service Level(s)") and amounts Cisco will provide to Customer as a credit if Cisco fails to meet the performance objectives for the Service Levels set forth in this SLA ("Service Credits"). This SLA only applies to the Services.

2. Incident Priority Levels

Cisco will categorize and respond to Incidents according to the Priority level methodology described in Appendix B of the Service Description for Services.

3. Service Levels, Service Credits, Service Level Objectives, Key Performance Indicators.

Subject to the terms of this SLA, Cisco will perform the Services so that they will meet or exceed the performance targets Service Levels and Customer will be entitled to claim Service Credits for Cisco's unexcused failure to achieve the Service Levels.

4. Performance Measurement

a) Cisco will use its standard processes and tools for measuring its performance and determining whether the Service Levels were achieved.

b) The window to measure performance against the Service Levels is the Measurement Period. The first Measurement Period will begin 60 days after Service Activation.

c) Within thirty (30) days of the end of each Measurement Period, Cisco will make available to Customer data on the Service Level Performance for the relevant Measurement Period ("Performance Report").

d) If Customer disputes the Performance Report, the parties will review the matter, including providing underlying information to support or dispute the contents of the Performance Report.

5. Confidential Information

The Performance Reports and any underlying data provided to Customer to support the Performance Report are Confidential Information and may not be publicized.

6. Entitlement and Payment of Service Credits

Customer must submit a written claim to Cisco to receive Service Credits within sixty (60) days of receiving the Performance Report, or the right to receive them will be waived. Service Credits will be provided in the form of a Letter of Credit, which must be used during the term of the Services.

7. Limitations

a) Customer may not claim multiple Service Level breaches (and associated credits) where a single Incident has resulted in Cisco failing to achieve multiple Service Levels. If this happens, Customer will have a right to claim (1) Service Credit of its choosing.

b) Customer may not apply a Service Credit unless Customer has first paid remainder of the Charges (i.e., Charges minus the Service Credit Amount).

c) Customer may not sell, transfer, or assign any Service Credits or convert the Service Credit to cash.

d) The maximum and aggregate Service Credits will be (5%) of the recurring Charges paid by Customer for the Service for the relevant Measurement Period.

8. Exclusive Remedy

Cisco's issuance of Service Credits represents Cisco's sole liability to Customer, and Customer's sole and exclusive remedy against Cisco, for Cisco's failure to meet the Service Levels. Any Service Credits paid by Cisco under this SLA will count toward the limitation of Cisco's liability under the Agreement.

9. Customer Responsibilities

Customer will provide Cisco a point of contact to cooperate with Cisco and provide reasonably requested information to help verify Service Level Performance

10. Exceptions

Any failure by Cisco to achieve the Service Levels will be excused if caused by:

a) A material act or omission by Customer in breach of the terms and conditions of the Agreement, the Service Description, and/or the Order;

b) Customer's failure to comply with its responsibilities under the Service Description or this SLA or failure to implement Cisco's reasonable recommendations that would prevent the SLA failure;

c) Any delays or faults caused by Customer, third party equipment, software, services, support, or vendors not under the control of Cisco (e.g., Carrier cycle time);

d) Periods of maintenance where updates, patches, etc. are installed and configured (i.e., Maintenance Windows);

e) A Force Majeure Event;

f) The Covered Security Components being past the End of Support (EOS) date or not covered by support and maintenance.

g) Software defects that require installation of major software updates or reinstallation of the software on the Cisco equipment;

h) Changes in the Covered Security Components or network that were not validated or approved by Cisco or delays by Customer in implementing Changes requested by Cisco or otherwise agreed between Customer and Cisco;

i) Failure by Customer to provide a required response necessary for Cisco to meet the Service Levels (Please note: Incident Tickets will be on "hold" during the time Cisco is delayed in receiving required information from the Customer, the End User, or applicable third-party service providers);

j) Changes to the Covered Security Components that were not approved by Cisco.

11. Security Audit

If there are repeated Security Incidents that Cisco reasonably believes can be prevented through the proper use of the Covered Security Components and Services, Cisco may conduct, at its own expense and discretion, a review of Customer's security environment. Customer will reasonably cooperate with this review. Following any such review, Customer will make commercially reasonable efforts to implement any reasonable Cisco recommendations. If Customer fails to do so, this SLA will not apply.

12. Governance and Escalation

Cisco and Customer will hold regular meetings to review and assess Service Level Performance, address any Customer concerns, and work in good faith to resolve any disputes between the Parties with respect to Service Level Performance.

Appendix D – Service Levels, Service Level Objectives, and Key Performance Indicators

13. Overview

Cisco Secure MDR Service Portal Availability

Definitions

"**Availability**" means the following, converted to a percentage:

Calculation: (Number of minutes in the month – Outage Time) / Number of minutes in the month.

Cisco Secure MDR Service Portal Availability - is the availability of the web accessible portal made available to Customer to view reports and submit tickets.

Outage Time shall commence upon the earlier of: (1) Cisco's detecting the outage and logging an Incident ticket or (2) Cisco's logging an Incident ticket upon Customer's notice to Cisco of the outage, which notice contains sufficient information to confirm that the outage is occurring in the System. The Outage Time ends when the System is returned to a usable level of service. The duration of Outage time shall be rounded to the nearest minute. Cisco will log an Incident ticket promptly following notification from Customer or its own detection of an outage.

Service Level

Platform Availability: 100%

Portal Availability: 99%

Service Credit

Platform Availability	Service Credit (% of the fixed monthly services charges for the Measurement Period)	Portal Availability	Service Credit (% of the Fixed Monthly Service Charges for the Measurement Period)
> 100% and < 99.9%	1%	<99% and ≥ 98.5%	1%
> 99.9% and < 99%	2%	<98.5% and ≥ 98%	2%
> 99% and < 98.5%	3%	<98% and ≥ 97.5	3%
>98.5%	5%	<97.5%	5%

Measurement Period: Monthly (one calendar month)

Time to Engage

Definition

Cisco will contact Customer's designated contact by phone or MSS Chat within 30 minutes of prioritizing a P1 Security Incident (45 minutes for a P2) if a recommendation to mitigate, stop, research, etc. has already not been provided by this time.

Calculation: Cisco contacts customer in timeframes above for unresolved P1 and P2 Incidents / Total number of P1 and P2 Security Incidents in the month that require engagement after prioritization (i.e., no automatic recommendation provided).

Service Level: On time engagement 95%

Service Credit

Time to Engage	Service Credit (% of the Fixed Monthly Service Charges for the Measurement Period)
<95% and ≥ 90%	1%
<90% and ≥ 80%	2%
<80% and ³ 75%	3%
<75%	5%

Measurement Period: Monthly (one calendar month)

Appendix E – Notes and Limitations of the Incident Response Delivery

The following notes and limitations apply to the Cisco Talos Incident Response Services as part of the Cisco Secure Endpoint-Complete:

- Once the number of hours in the reactive services (as specified in Section 2.6) are used, Cisco may suspend reactive service work until additional hours are purchased or other written arrangements are made. Any unused hours expire at the end of a subscription term.
- The deidentified threat, indicator of compromise, vulnerability, attack, and techniques used (e.g., ATT&CK), and other related information that Cisco collects from Customer in relation to the Services is considered Systems Information, and we will treat it according to our security and privacy program referenced in How Cisco Provides Services.
- Given the variety of situations and issues that may be encountered, incidents may require a variety of other services or capabilities to complement this Service. For example, incidents may require specialized tools to provide deeper visibility or access into the Network.
- There is no guarantee that root cause analysis will result in a root cause being identified or confirmed for an incident.
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan.
- Security incident analysis activities may require additional hours to be purchased by Customer.
- Incident Response Services can provide insight into deficiencies of an Incident Response plan for resolving an incident; however, executing the plan may require the purchase of follow-on Services.
- Work may occur after Standard Business Hours, as reasonably determined by Cisco.