# Service Description for Cisco Managed Detection and Response

This document (this "**Service Description**") describes the service features, components, and terms of the Managed Detection and Response services purchased by Partner ("**MDR Services**" or "**Services**") that Cisco will provide to the designated customer listed in the Ordering Documents ("**Customer**"). The specific quantity and type of the Services purchased by Partner will be documented in an Ordering Document between the parties. Appendix A to this Service Description sets forth the applicable terms and conditions governing the Services.

## 1. Service Summary and MDR Components

### 1.1 Service Summary

- The Services are a managed service that utilizes a set of Cisco security technologies that monitor the applicable portions of Customer's network and endpoints for indicators of compromise. Threats detectable by the technologies are correlated and analyzed. Based on the type of threat or indication of compromise, responses may include information, recommendations, or policy changes by Cisco.
- All Services will be delivered remotely from global Security Operations Centers (SOCs) and all services will be provided 24x7x365.
- The Services are dependent on Customer having specific software and cloud services and configuring it as defined in documentation provided by Cisco ("**MDR Components**"). This would include any required infrastructure (e.g., CPU, hard drives, and memory) to support typical Customer needs.


The Services provide an integrated Cisco security solution combining an expert team of researchers, investigators and responders with threat intelligence, and defined investigation and response playbooks supported by Talos threat research. The Services leverage key Cisco security technologies to advance the SOC's capabilities by delivering industry-leading threat detection and response to reduce mean time to detect and contain threats. The Services help detect, analyze, investigate, correlate against our threat intelligence research, allowing faster response to identify and thwart threats before they progress. The Services are based on Cisco the following technologies:

- Cisco Advanced Malware Protection (AMP) for Endpoints draws on Talos threat intelligence to continually adapt Customer's in-scope endpoints, network, email and web defenses. AMP correlates this data against Customer's environment telemetry data and known behavior, linking Customer defenses into a more integrated defense against emerging malware threats.

- Cisco Threat Grid combines advanced sandboxing with a context-rich malware knowledge base, configured for Customer's environment. It aligns to an industry framework that codifies threat-based Tools, Techniques, and Procedures (TTPs) so that Customers can evaluate severity and capability of the known threat.
- Cisco Stealthwatch Cloud applies the latest Cisco threat intelligence and analytics to proactively protect Customer's public cloud resources, internal network, and even certain types of encrypted traffic against new threats.
- Cisco Umbrella uses Talos intelligence to help identify new strategies malicious actors use to target end users and adapt Customer front-line Internet defenses to guard against them. Extending from the cloud to end points, it helps protect against new, previously unknown malicious destinations on the Internet.

**1.2 Required Products and Configuration**. In order to use the Services, Customer must purchase the applicable MDR Components (including maintaining support and maintenance services) and configure it to meet the Services requirements based on guidance provided by Cisco. **The Charges for the Services do not include the MDR Components, their support, maintenance, implementation or configuration, and are purchased separately.**

## 2. Features Summary. The key features of the Services (combined with the MDR Components) are:

**2.1 Detect.** Cisco uses a tested detection framework paired with research and investigations capabilities to foster fast triage of alerts, applying contextual observation, threat intelligence, and observed kill chain behavior**.** These capabilities include the following:

- Monitoring and providing escalated security incident alerting systems for known and emerging attacks.
- Intelligence to help detect and predict threats.
- Adaptive defenses to detect non-standard attacks.
- Detecting suspicious and anomalous activities using cloud native security analytics.
- Using early detection to support accelerating security operations to stop, prevent or contain the threat or attack.
- Utilizing Cisco Talos threat research and tools to collect data on new attack TTPs.

**2.2 Analyze.**

- Cisco AMP for Endpoints provides tracking and analysis of tagged suspicious files on endpoints, as they traverse the network, and across email and web content.
- Cisco Stealthwatch Cloud monitors for indicators of compromise on internal networks and cloud assets.
- Cisco uses analysts and automation to investigate certain categories of anomalous events and traffic where there isn't a known cause and may pose a material threat.

**2.3 Investigate.** Cisco will Investigate threats on endpoints, user behaviors, applications, and the network elements protected by the MDR Components.

- Cisco uses threat intelligence to research indicators of compromise (IOCs) and attack (IOAs) to confirm threats, attacks, compromises or exploitation.
- Cisco uses investigation methodology to add context from integrated Cisco security products and help identify impact, severity and scope of Security Incident to the endpoint.
- Investigate the Security Incident for impact and attacker attributes.

### 2.4 Respond.

- Where applicable, perform Changes to the MDR Components defined within the MDR Response Catalog with the intent to prevent, mitigate or stop malicious activity.
- Create and modify the detection and response playbooks based on new information and threats from security events detected from the MDR Components and processes described above.
- Provide general (see below for details) guidance on how to mitigate, stop, or prevent a Security Incident based on the intelligence and advisories provided above, as relevant to customer's environment.

## 3. Service Elements.

| 3.1 **Service Transition - Planning and Support** | |
|---|---|
| **Summary:** Cisco and Customer will work together to provide details on the scope of the Services, and to define plan for establishing connectivity between Cisco and the MDR Components. | |
| **Cisco Responsibilities**<br>• Define the high-level scope of work required to transition the in-scope MDR Components, including assessing changes to the MDR Components, Network, and processes in order to Activate the Services<br>• Define the required API requirements necessary to Activate the MDR Components<br>• Identify a single point of contact (SPOC) to engage with Customer during the Service Transition<br>• Perform any other tasks designated as Cisco's responsibility in the Transition Plan by the date specified in the Transition Plan | **Customer Responsibilities**<br>• Unless as otherwise agreed in writing, provide the reasonably requested inventory and topology information by the dates provided in the Transition Plan<br>• Review and approve Transition Plan, including Activation date(s)<br>• Identify a SPOC to engage with Cisco throughout the Service Transition period<br>• Perform tasks specified as Customer's responsibility in the Transition Plan by the date specified in the Transition Plan |
| **Output**: Transition Plan | |

| 3.2 **Service Transition – Managed Component Activation** | |
|---|---|
| **Summary:** With Customer's assistance, Cisco will connect the MDR Components via APIs to the Cisco SOCs. Cisco will perform tests to confirm that the MDR Components meet technical readiness requirements and Activate the MDR Components onto the MDR Platform (MDRP). | |
| **Cisco Responsibilities**<br>• Provide Customer with general guidance on stabilization activities required to allow Activation.<br>• Implement MDRP and conduct tests to confirm that the MDR Components are Activated the Services are ready.<br>• Provide notification to Customer that Activation is complete.<br>• Provide a documentation to Customer to describe necessary steps to configure the MDR Components. | **Customer Responsibilities**<br>• Configure APIs and implement requirements as described in the Cisco documentation.<br>• Unless Cisco is performing installation services, perform any required hardware or software installations, configuration changes and other stabilization activities required to enable connectivity and communication between the MDR Components and MDRP. |

| | |
|---|---|
| | • Assist Cisco in establishing and validating bidirectional management connectivity between the MDR Components and MDRP.<br>• If desired, review and monitor Cisco's ready for use testing and results.<br>• Manage and resolve Security Incidents that pre-date Service Activation. |

## 3.3 Connectivity and Logging Incident Management

**Summary**: Cisco will help identify, troubleshoot, and restore normal operational functionality if an Incident related to connectivity, log receipts, data flow monitoring, is detected or reported by Customer between an MDR Component and the MDRP.

| Cisco Responsibilities | Customer Responsibilities |
|---|---|
| • Create Incident tickets from detected or reported Incidents.<br>• Manage Incidents by classifying, prioritizing, troubleshooting, and assisting in the restoration of telemetry or logging of the MDR Components.<br>• If Cisco is able to make the Changes to the MDR Components to restore connectivity or logging, make Changes with Customer's permission.<br>• Notify relevant parties about Incidents.<br>• Make recommendation to resolve Incident if the cause is out of scope our out of Cisco's control. | • Contact Cisco if Customer believes an Incident is in-progress or has occurred.<br>• Participate in diagnostic testing to identify the source of the Incident.<br>• Approve Cisco initiated Changes to help resolve Incidents.<br>• Perform Cisco or third-party recommended changes to MDR Components or third-party hardware, software or services to resolve the Incident. |

**Output:** Incident Ticket; Change Request or recommendation to resolve Incident

## 3.4 Monitoring

**Summary**: Cisco will monitor the security alerts from the MDR Components for potential Security Incidents. Alerts are correlated against configured use cases, Talos Threat Intelligence and available third-party threat intelligence using analytics and security orchestration and automation response systems.

| Cisco Responsibilities | Customer Responsibilities |
|---|---|
| • Monitor alerts for indicators of compromise or attack against configured use cases.<br>• When an alert is generated Cisco will research and analyze against known and unknown threat vectors to determine if it is likely a Security Incident.<br>• Based on the Alerts and analysis create Security Incident tickets for known or reasonably suspected Security Incident. | • Contact Cisco if Customer believes an Incident is in-progress or has occurred, per Runbook.<br>• Participate in diagnostic testing to identify the source of the Incident.<br>• Notify Cisco in writing of any Customer change to the response policies for MDR Components or systems monitored by the Services. |

**Outputs:** Alert Settings; Security Incident Ticket.

## 3.5 Security Incident Response

**Summary**: When a Security Incident has been found, Cisco will recommend responses to help contain, mitigate, remediate, or eradicate the threat. Cisco MDR remote response actions are limited to actions defined within the MDR Response Catalog.

| Cisco Responsibilities | Customer Responsibilities |
|---|---|
| • Create Security Incident Ticket based on known or reasonably suspected Security Incident.<br>• Notify Customer of a Security Incident via approved method (high priority Security Incidents will be notified via email and phone).<br>• Based on the nature of the Security Incident, recommend response to Incident.<br>• Where Incident is a known attack, recommend response to mitigate or stop attack.<br>• Where applicable, and with Customer's permission (via click to accept or similar means), make Changes to the MDR Components to mitigate or stop the Security Incident.<br>• Where Incident is not fully discovered or known, recommend further analysis with focus on key areas.<br>• Where recommendations fall outside of the scope of MDR Component coverage, make recommendations to investigate or resolve the Incident (e.g., third-party hardware or software).<br>• When an Incident is P1, conduct additional investigations to provided recommendations to help resolve the Incident.<br>• Provide periodic reminder notifications to Customer according to defined priority, if indicators of a Security Incident remain after providing recommendations to Customer. Tickets will be closed at Customer request, or after 14 days if no action is taken by Customer. | • Participate in diagnostic testing to identify the source of the Incident.<br>• Designate appropriate persons to review and approve (if desired) Cisco's performance of recommended Changes to the MDR Components.<br>• Perform Cisco recommended changes to MDR Components.<br>• Act on recommendations from Cisco, including determining any dependencies resulting from the recommended actions.<br>• Notify Cisco if it believes the Security Incident has been resolved or if it will not act on the Cisco recommendations. |

**Output:** Incident Ticket; Recommendations to resolve, mitigate or research Security Incident; Change Request for MDR Components.

## 3.6 Quarterly Threat Briefing

**Summary**: Cisco Talos Incident Response will host a remote service review meeting on a quarterly basis open to all Customers (not private). This quarterly briefing will provide updates on current threat patterns, detection volumes, and trended events and similar relevant incident information.

# Appendix A- Terms

## 1. Services Terms.

1.1 **Scope of Additional Services.** Unless the Services are expressly provided for above, all other Cisco services are out of scope for this Service Description.

### 1.2 MDR Components

1.2.1 **MDR Components.** Customer or Partner is responsible for getting, installing, configuring and maintaining the MDR Components (using Cisco configuration guides) to allow for Service Activation by the requested Service Activation date and ongoing performance of the Services. This responsibility includes maintaining a valid support and maintenance agreement for all the MDR Components. Cisco is not responsible if Customer fails to do the above, and the Services and do not work or has errors. Cisco will not provide refunds if Customer fails to do the above and Cisco is unable to provide the Services as provided in this Service Description.

1.2.2 **Non-Standard MDR Components**. As part of Service Transition, Cisco and Customer will identify the limitations of the Services are a result of the type and configuration of the MDR Components. For example, certain configurations of the MDR Components may prohibit logging of certain telemetry data normally included in the Services.

### 1.3 Logging and Reporting.

1.3.1 **Reporting.** Cisco will provide, or make available via the Portal, the reports listed in the reporting documentation for MDR Services. Cisco reserves the right to add, change, or remove reports in its reasonable discretion. Customer may review any reports with Cisco as a part of Governance (described in Section 1.6 below). Customer is responsible for reviewing, analyzing, and if needed (e.g. reporting inaccuracies), discussing with Cisco the information contained in the reports provided.

1.3.2 **Logging.** The MDR Components contain their own logging capabilities. Please see the product/service description and logging data for the particular MDR Component. 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 **Portal**. Cisco will provide a web-based Portal that provides Customer at least the following core functionality:

a) Reports and information related to the Services; and

b) Submit and monitor Incident Tickets.

Requests submitted by Customer are deemed to be authorized by Customer.

1.5 **Cisco Recommendations.** To the extent that Customer fails to implement any reasonable Cisco recommendations or requirements with respect to the MDR Components or the Services, Cisco shall have no responsibility for any delays or failure(s) regarding the performance of the Services or its impact to the Customer.

1.6 **Services Management and Governance.**

1.6.1 Customer, not Cisco, is responsible for coordinating any complementary services (e.g. installation and management of MDR components, Security Incident response, Security Operations Center, etc.). If Partner wishes to directly receive customer data (e.g. Security Incident tickets) and/or perform responsibilities or complementary services on Customer's behalf, Partner will obtain written permission from Customer and if requested, provide Cisco with a Letter of Authorization from Customer, allowing this sharing of data and coordination of Services.

1.6.2 Cisco and Customer (and if requested and agreed, Partner) will implement a governance function with the following goals: discuss alignment of the services to Customer's business needs, identify opportunities to improve the Services (e.g., increase quality or reliability), and similar matters. The parties will conduct periodic governance meetings as mutually agreed. Both Cisco and Customer will make available appropriate members of its IT, business, and leadership organization for the governance meetings, as applicable.

1.7 **Detection and Response Capabilities**. **WHILE CISCO HAS IMPLEMENTED COMMERCIALLY REASONABLE TECHNOLOGIES AND PROCESSES AS A PART OF THE SERVICES, CISCO CANNOT GUARANTEE IT WILL PREVENT, DETECT, STOP, OR MITIGATE ALL SECURITY INCIDENTS.**

1.8 **General Customer Responsibilities.** Cisco's provision of the Services is dependent on Customer's compliance with its responsibilities listed in this Service Description. If Customer fails to perform its responsibilities, Cisco will be excused from performing the Services (including achieving any Service Levels) to the extent, and for the duration that Customer fails to meet its responsibilities or if an exclusion applies. In addition, Cisco reserves the right to charge Customer for expenses, costs, or time incurred, caused by Customer's failure to perform its responsibilities. In addition to the Customer responsibilities listed above, Customer will also be responsible for the following:

a) Promptly supply Cisco with reasonably requested and necessary technical data (e.g., network diagrams, IP addresses, and passwords) and other similar information to allow Cisco to provide the Services.
b) Provide reasonable cooperation and assistance to Cisco in performance of the Services (e.g., making Changes to MDR Components that cannot be done remotely, locally running tests, or diagnostics on MDR Components, enabling or updating APIs or configurations, etc.).
c) Maintain the locations and system requirements (e.g. power, HVAC, connectivity, physical and rack space, security, connectivity, and other requirements necessary for the proper operation of the MDR Components, Customer's other infrastructure, and applications in Customer locations, all as applicable.
d) Back-up and protect its own data against loss, damage, theft or destruction.
e) Comply with the terms related to the MDR Components.
f) Provide Cisco and Cisco personnel timely remote (logical) access to the MDR Components, as reasonably required for Cisco to perform all elements of the Services (e.g., opening ports, changing firewall settings, providing change windows, etc.). This responsibility includes obtaining any needed internal or third party approvals or licenses.
g) Manage all third-party products and/or services that are not in the scope of Services, including enforcing any third-party supplier contract terms (and Service Level Agreements, as applicable).
h) Notify Cisco in advance of any updates or changes planned in Customer's environment, including configuration or API changes to the MDR Components.

i) Identify any dependencies for out of scope hardware, software and/or services.

j) Provide and maintain connectivity (including, without limitation, any required local circuits, cross connects, and hardware) required to deliver the service.

1.9 **Exclusions.**Products and services that are not described in this Service Description are not part of the Services, including, but not limited to, the following examples:

a) Technical support for the MDR Components or related Cisco products (which may be provided under a separate service).

b) Software or hardware upgrades unless expressly referenced in this Service Description, Supplement(s) to this Service Description, or the applicable Ordering Document(s).

c) Change Management or implementation of changes not covered by the Service Catalog.

d) Providing Services on site or in any language other than English.

e) Troubleshooting Security Incidents that predate Service Activation.

## 2. Commercial Terms.

2.1 **Pricing Summary.** The Charges consist of a fixed monthly fee based on the number of endpoints covered by the Services and an overage fee if Customer exceeds that threshold. Volume Discounts may not apply to overages-Customer must increase its base number of endpoints covered.

2.2 **Charges.** The charges for the Services ("Charges") and payment terms will be detailed in the applicable Ordering Document or the Agreement. Except as provided in the Ordering Documents or Cisco's material breach, all Charges paid are non-refundable.

2.3 **Invoicing.**

2.3.1 Cisco will invoice on Service Activation (or deemed Service Activation).

2.3.2 Cisco will invoice the fixed monthly Charges in advance and the overage Charges from the previous month.

2.3.3 Cisco's rights to invoice for the charges for the Services and Partner'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) Partner's failure to issue a purchase order or Customer's delay or failure to pay Partner.

2.4 **Minimum Commitments and Minimum Term**. The Ordering Documents will contain any minimum term or minimum Charges commitment associated with the Services.

2.5 **Service Activation.** The Ordering Document will contain the requested Service Activation Date. Customer must activate the Services within 30 days of the requested Service Activation date, or it will be deemed activated. If Cisco is the primary cause of the delay in Service Activation, the Service Activation date will be delayed on a "day for day" basis.

2.6 **Endpoints and MDR Components**. Cisco will not provide Services for MDR Components (or its covered endpoints) and will not be responsible endpoints unless they are initially listed or referenced in the Ordering Document as in-scope. If

there are changes to the number and type of MDR Components or the number or type of endpoints covered by the MDR Components, the Charges will be adjusted accordingly.

### 2.7 Term, Termination, and Renewal.

2.7.1 **Term**. The term of the Services will be provided in the Ordering Documents. Unless provided in the Ordering Documents, the Term will begin upon the Effective Date of the Ordering Document.

2.7.2 **Termination**. Where an Ordering Document 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 Ordering Document. If the Ordering Document 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 Ordering Document. Rights to terminate for material breach are provided in the Agreement.

2.7.3 **Renewal**. If the automatic renewal selection is chosen, the Service will automatically renew for additional one-year terms at the same price, unless Cisco notifies Customer in writing at least ninety (90) days in advance of, or Customer notifies Cisco in writing at least forty-five (45) days in advance of, the expiration of the then-current term that it does not want to renew the Services.

## 3. Legal Terms.

3.1 **Order of Preference.** This Service Description is subject to the applicable reseller agreement between the parties ("Agreement"). If there is no reseller agreement in place, the following terms will apply: https://www.cisco.com/c/en/us/about/legal/terms-sale-software-license-agreement.html. If there is a conflict between this Service Description, an Ordering Document, the applicable Agreement, or any Supplement to this Service Description, the following priority will apply (from highest to lowest): (a) any Ordering Document, as applicable; (b) any Supplement(s); (c) the Service Description; and (d) the applicable Agreement. Defined terms will be as provided in this Service Description or as provided in the Glossary of terms found here: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/glossary-of-terms-for-cms.pdf

3.2 **Compliance with Laws.** Cisco will comply with applicable laws, rules and regulations, including, but not limited to, all applicable export control laws and regulations. Customer will comply with all applicable laws, rules, and regulations related to the receipt and use of the Services and will obtain all approvals and licenses required by any third parties related to the MDR Components, Customer's locations, systems, software, and network as are reasonably necessary for Cisco to provide the Services.

3.3 **Sale via Cisco Authorized Reseller**. Partner is responsible for obtaining appropriate agreements with Customer reflecting the applicable terms of this Service Description, including (without limitation) requiring the performance of Customer responsibilities. If Customer has purchased these Services through a Cisco Authorized Reseller and were not provided a Service Description by the Partner, then this Service Description is incorporated into the agreement between the Cisco Authorized Reseller and Customer governing the Authorized Reseller's provision of the Services to Customer (if applicable, the "Agreement").

3.4 **License.** Customer receives a limited, non-transferable, non-sublicensable, internal use, license to use the executable version of Portal, and any software provided by Cisco as part of the Services only to the extent and duration reasonably required to receive the Services. There are no warranties associated with these items outside of their use as part of the Services. Upon expiration or termination of the Services, the license to the Portal and any associated software will automatically terminate. Note, this license is separate from the licensing and rights associated with the MDR Components, which are licensed separately.

3.5 **Security and Data Privacy Program.** Cisco, Partner and Customer will maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any (i) unauthorized access, use, distribution, or deletion of Customer's data and (ii) compromise of the MDR Components or MDRP. More information on Cisco's security and privacy policy can be found here: http://www.cisco.com/c/en/us/about/trust-transparency-center/data-protection.html. If Cisco and Customer do not have a mutual data protection agreement in place (or equivalent privacy and data protection terms), the following Mutual Data Protection Agreement is incorporated into this Service Description: https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf

3.6 **Confidential Information.** The ticket information, including recommendations to resolve Security Incidents, Charges, Portal, , and Service Level performance information are Confidential Information. This information may not be used for any purpose other than in connection with Customer's use of the Services.

3.7 **Telemetry Data.** Cisco may collect data on Customer's usage of the Services in order to maintain, improve, market, or promote the Services. In addition, Cisco may use anonymized and aggregated data on Customer's use of the Services, Managed Component performance (Cisco products only), and network performance ("**Telemetry Data**") to create or improve its products and services. Cisco will comply at all times with applicable law related to Cisco's collection and use of the data above and will use reasonable physical, technical, and procedural means to protect the Telemetry Data that contains Personal Data in accordance with the Cisco Online Privacy Statement, which is made available at http://www.cisco.com/c/en/us/about/legal/privacy-full.html or such other site(s) as Cisco may publicly communicate from time to time.

3.8 **Subcontractors.** Cisco may use subcontractors to provide services to Customer on its behalf for the purposes of providing the Services. Cisco will remain responsible for its subcontractors' compliance with the obligations under this Service Description, any Supplement, and the applicable agreement between Cisco and Customer. References to Cisco in this Service Description and any Supplement shall include its subcontractors, as applicable.

## Appendix B- Priority Levels

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

**Priority Definition.** The Priority of an Incident is based on the Impact and Urgency of an Incident.

| **Impact:** An 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 an Incident is classified according to its impact on the monitored endpoints and impact to Customer's business. |
|---|---|
| There are four impact levels:<br>**Widespread:** Entire Service is affected.<br>**Large:** Multiple locations are affected.<br>**Localized:** A single location or an individual user at multiple locations are affected.<br>**Individualized:** A single user is affected. | There are four urgency levels:<br>**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.<br>**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.<br>**Minor:** Non-critical function is stopped or severely degraded. There is a possible financial impact to Customer's business.<br>**Low/Notice**: Non-critical business function is degraded. There is no material impact. Customer perceives the issue as low. |

**Priority Definitions**

Priority defines the level of effort that will be expended by Cisco and Customer to resolve the 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 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 Managed Detection and Response

1. Overview. This SLA describes the parties' responsibilities and sets Cisco's performance targets for the MDR 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").

2. SLA Scope. This SLA only applies to the Managed Detection and Response Services (MDR Services).

3. 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 MDR Services.

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

4.1 **Service Level Performance**. Subject to the terms of this SLA, Cisco will perform the MDR 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 failure to achieve certain Service Levels.

4.2 **Service Level Objectives (SLO).** For those Services Levels labelled as Service Level Objectives, they are objectives only. If Cisco fails to meet the Service Levels below, it will review the reasons it failed meet the Services Levels and will use commercially reasonable efforts to remediate the cause of the failure. However, other than the obligation above, there will be no financial or legal penalty if Cisco fails to meet the SLOs.

4.3 **Key Performance Indicators (KPI).** KPIs are performance indicators only and there are no financial or legal penalties if Cisco does not achieve them.

5. Performance Measurement.

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

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

5.3 Within thirty (30) days of the end of each Measurement Period, Cisco will provide to Customer a report on the Service Level Performance for the relevant Measurement Period ("**Performance Report**").

5.4 Within 30 days of receiving the Performance Report ("**Review Period**"), Customer should review the report and submit a written claim for Service Credits or dispute the report.

5.5 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.

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

7. Entitlement and Payment of Service Credits.

7.1 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.

7.2 Service Credits will be provided in the form of a Letter of Credit, which must be used against an invoice for the MDR Services within three (3) months of receiving the Letter of Credit or the Service Credit is void and of no value.

## 8. Limitations.

8.1 Customer may not claim Services Credits for multiple breaches of multiple Service Levels 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.
8.2 Customer may not apply a Service Credit unless Customer has first paid remainder of the Charges (i.e. Charges minus the Service Credit Amount).
8.3 Customer may not sell, transfer or assign any Service Credits or convert the Service Credit to cash.
8.4 The maximum and aggregate Service Credits will be (5%) of the recurring Charges paid by Customer for the Service for the relevant Measurement Period.

9. **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.

## 10. Customer Responsibilities.

10.1 Customer will provide Cisco with a single point of contact to cooperate with Cisco and respond to any Cisco requests to help verify Service Level Performance
10.2 Customer will such information and assistance that Cisco reasonably requests to help Cisco verify Service Level Performance.
10.3 Customer will comply with all of its responsibilities as described in the Service Description for MDR Services, including any referenced documents.

11. **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 Ordering Document;

b) Customer's failure to comply with its obligations or responsibilities under the Service Description or this SLA;

c) Any mutually agreed schedule of activities that causes service levels to fall outside of measured and defined Service Level obligations set forth in this SLA;

d) 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);

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

f) A Force Majeure Event;

g) Any Cisco or third-party hardware dispatch and replacement, which may be covered under a separate agreement;

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

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

j) Changes in the MDR 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;

k) Failure to implement Cisco's recommendations necessary to remediate Incidents;

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

m) Any conditions existing prior to Cisco management of the MDR Components, including any incident, problem, error or other event subject to an open support ticket from a legacy or other third-party service provider; and/or

n) Changes to the MDR Components that were not approved by Cisco.

12. Security Audit. If there are repeated Security Incidents that Cisco reasonably believes can be prevented through the proper use of the MDR 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.

13. 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.

## Annex 1 - Service Levels, Service Level Objectives and Key Performance Indicators

**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.

**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**

| Portal Availability | Service Credit (% of the Fixed Monthly Service Charges for the Measurement Period) |
|---|---|
| <99% and ≥ 98.5% | 1% |
| <98.5% and ≥ 98% | 2% |
| <98% and ≥ 97.5 | 3% |
| <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 ≥ 75% | 3% |
| <75% | 5% |

**Measurement Period:** Monthly (one calendar month)

## Service Level Objectives

| Containment Service Level Description | Service Level Target | Customer Requirements |
|---|---|---|
| **Definition:** Provide response, or if no automatic response is possible, provide response recommendations, to resolve, stop, prevent, or mitigate a Security Incident<br>P1: 4 hours<br>P2: 8 hours<br>P3: 1 business day<br>P4: 3 business days | 99% | Customer will provide information about impact and threat |

## Key Performance Indicators

| Description | Requirements/ Dependencies |
|---|---|
| **Containment/Eradication**: Cisco will work to create automated responses to resolve, prevent, or mitigate known Security Incident causes and add them to the standard Response Catalogue for faster delivery to Customer. | |
| **Situational Awareness**: Create or modify existing detection and response playbooks based on new information and threats<br>P1: 5 business days<br>P2: 10 business days<br>P3: 15 business days<br>P4: 1 calendar month | Dependent on receiving sufficient data about the threat (including from Customer) |