Service Description
Cisco XDR Premier Services

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. Overview

The Cisco XDR Premier Service comprises:

1.1 The Cisco Managed Extended Detection and Response service ("Cisco MXDR"), where Cisco performs the activities summarized in Section 2.1 and described further in Section 3;

1.2 Cisco Technical Security Assessment (CTSA), where Cisco provides security assessments, validations, and enhancements; and

1.3 Cisco Talos Incident Response (Talos IR) services.

The Cisco XDR Premier Service uses a combination of Cisco's team of researchers, Incident handlers, integrated tool sets, and additional Cisco technologies to monitor for and respond to potential security threats and attacks.

This document does not describe the capabilities of the Cisco XDR platform or solution, which can be found on cisco.com.

2. Service Features (at a glance)

2.1 Cisco MXDR Services Features

Service Element	Description
Service Only Activation	Validation of Cisco XDR Premier Integrations: Cisco validates the integration of Customer's Cisco XDR Premier Supported Components (as defined in section 2.2 below) into Cisco MXDR.
Detection	24x7x365 security incident monitoring: Cisco monitors the Cisco XDR Premier Supported Components for events and alerts 24/7/365.
Analysis	Cisco XDR Platform Analysis: Cisco performs an analysis of data received by the relevant Cisco XDR Premier Supported Components on the XDR Platform and, where applicable, escalates the information to the Customer as a Security Incident.
Investigation	Incident Processes: Cisco MXDR SOC analyst will correlate, enrich, prioritize, and review all events through established SOC processes and, where applicable, the information to the Customer as a Security Incident. Cisco will determine the nature of the potential Security Incident, assign priority and determine potential impact, provide detailed examination results and contextual evidence, correlate network, hardware, and user information across available product sources, and provide detailed mitigation action recommendations

	for each Security Incident
Response	Guided response actions: Cisco recommends Security Incident responses to help the Customer contain, mitigate, remediate, or eradicate the threat. Response actions can be completed from the Cisco XDR Premier Service Portal directly. Threat advisories: Cisco issues threat advisories for new threats discovered helping Customer to proactively help prevent Security Incidents through the implementation of mitigating controls.

2.2 Cisco XDR Premier Supported Components

The Services are dependent on Customer (a) integrating Cisco XDR-supported security technologies, which are comprised of both Cisco security technologies (including the Cisco security products listed in Table 1 below) and certain eligible third party security technologies, as determined by Cisco (hereafter collectively referred to as "**Cisco XDR Premier Supported Components**")

3. Cisco MXDR Premier Service Elements

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.

3.1 Service Activation for MXDR Premier.

The purpose of the Service Activation activities is to work with the Customer to validate integration of Cisco XDR Premier Supported Components into Cisco MXDR in order to perform activities described in this Section 3.

Note: Although included within the definition of Cisco XDR Premier Supported Components, the following Cisco security products require specific onboarding activities in order for Cisco to be able to provide the Services:

Product	Tiers
Cisco Secure Endpoint	Advantage or Premier
Cisco Secure Malware Analytics	
Cisco Secure Cloud Analytics (Now included in Cisco XDR License)	On-premises network telemetry
Cisco Umbrella	DNS Advantage, SIG Essentials, or SIG Advantage

Table 1. Cisco security products which require specific onboarding activities

Cisco Responsibilities

- Work with Customer to validate that Customer has correctly installed and implemented Cisco XDR so that the Cisco XDR Premier Support Components can be monitored by Cisco.
- Provide technical and operational documentation to Customer to help Customer configure the Cisco security products listed in Table 1 above including the API and console interface requirements needed to enable the Services;
- Onboard the Cisco security products listed in Table 1 to the Cisco MXDR platform and perform testing to verify that they operate as expected and that all the Cisco playbooks have been correctly applied;
- Where applicable, work with the Customer to agree a list of "Identification" and "Containment" actions which Cisco may perform on Customer's behalf on the Cisco XDR platform (i) on a per-event basis or (ii) by action type (i.e. regardless of the

number of events). Accordingly Cisco will, in a response playbook ("Response Playbook"), document:

- the list of "Identification" and "Containment" actions which Cisco is hereby authorized by Customer to perform on Customer's behalf and those that Customer reserves for itself to perform, in each case whether on a per-event or per-action type basis; and
- the list of Cisco XDR Premier Supported Components for which Cisco may perform those actions on Customer's behalf; and

- Recommend initial configuration policies for the Cisco security products listed in Table 1.

Customer Responsibilities

- Ensure that Cisco XDR has been correctly installed and implemented in order to receive the Services;
- Provide the appropriate API tokens with the correct level of access for the Cisco products in Table 1;
- Approve the Response Playbook and, where applicable, configure Cisco XDR to ensure that Cisco is provided with authorization to perform the actions available to Cisco as documented in the Response Playbook;
- Configure and verify that the correct connectivity to the Cisco Security Operations Center (SOC) has been established, maintain the same for the duration of the Services, and be responsible for any future connectivity issues;
- Make necessary configuration and policy changes to the Cisco XDR Premier Supported 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;
- Provide and maintain access to the Cisco XDR Premier Supported Components for Cisco, as necessary for Cisco provide the Services. For example, Customer will not remove or limit access the API for each Cisco XDR Premier Supported Component nor the web-console interfaces.

Scope Limitations

- Service Activation does not include licensing, deployment, configuration, or integration of any security products outside of the Cisco XDR Premier Supported Components.
- Cisco does not require direct access to any security products other than Cisco security products in Table 1.

3.2 Detect.

Cisco will monitor the security alerts and events from the Cisco XDR Premier Supported Components for potential Security Incidents. Cisco will correlate and prioritize security events and alerts with known threats, Talos Threat Intelligence and third-party threat intelligence using analytics, security orchestration, and automated response playbooks to help determine whether observed events and/or notifications are a potential Security Incidents. Any detected security events which Cisco believes may pose a potential security threat will be escalated into a Customer-facing security incident ("**Security Incident**"), which details can be consulted by Customer from the Cisco XDR Premier Service Portal. All Security Incidents will be prioritized and categorized in order to help streamline Customer's review and response.

Cisco Responsibilities

- Monitor for and investigate security incident from the Cisco XDR Premier Supported Components;
- Utilize Cisco Talos Threat intelligence and Secure Malware Analytics to help identify the latest and most relevant threats that may be identified by the Cisco XDR Premier platform using indicators of compromise (observables), and inform Customer of potential mitigation best practices;
- Enrich security alerts with supporting contextual information;
- Collect data on new attack Tactics, Techniques, and Procedures (TTPs) to help identify security attacks or compromises;
- Analyze each Security Incident to determine and communicate recommended remediation or response actions to the Customer on the Cisco XDR Premier Service Portal, where applicable;
- Report all potential threats via detailed Security Incidents available on the Cisco XDR Premier Service Portal, including notifications for all new Security Incidents;

- Provide mitigation recommendations for all Security Incidents, including potential mitigation actions available as part of the Cisco XDR Premier Supported Components, as well as best practices, controls, and configurations which apply within the context of a Security Incident's impact;
- Provide 24x7x365 expert 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 known environment or operations;
- Notify Customer of major changes or new functionality within the Cisco security products within the Cisco XDR Premier Supported Components, as soon as reasonably practicable after they become available, including any recommended configuration or policy changes; and
- Notify Customer of any planned or unplanned outages related to:
    - the Cisco XDR Premier Service Portal; or
    - the Cisco MXDR platform monitoring capabilities.

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, as is seen required by the customer;
- Approve automated remediation actions in a timely manner, as deemed necessary by the customer;
- Maintain all required configurations, deployments, connectivity, and access to the Cisco XDR Premier Supported Components, understanding that if individual product licenses, API credentials, configuration, or deployment are not functioning as intended, the Cisco XDR Premier services may be adversely impacted.
- Ensure connectivity between the Cisco XDR Platform and all relevant Cisco XDR Premier Supported Components.

3.3 Analyze.

Cisco will analyze security events, alerts, and data detected pursuant to Section 3.2 above to identify potential threats utilizing the data available from Cisco XDR Platform. Cisco will also ingest the results of Cisco XDR Threat Hunting investigations, review and enrich them, and provide results to the Customer.

Cisco Responsibilities

- Utilize data from all configured sources available from the Cisco XDR Premier Supported 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 valid Cisco XDR Premier Support Component and valid API credentials, as configured as part of Service Activation. Ensure all expected data sources are reporting data into the Cisco XDR Premier Platform as expected and in acceptable timeframes, given the configuration and completed onboarding of the Customer. Investigate other available categories of events and/or traffic which may pose a material threat; and
- Perform analysis and effective investigation techniques, automated or manual, for any given Security Incident, utilizing the available data and all available practical expertise within the scope of the Cisco XDR Premier 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., outages, any maintenance activities, component removals, etc.); and

- Review active Incidents from the Cisco XDR Premier Service Portal to a degree necessary to interpret the breadth of the Incident, and to distill a plan to reach a more secure state.

3.4 Investigate.

Cisco will Investigate threats on Cisco XDR Premier Supported Components, applications, endpoints, identity, and the network elements protected by the Cisco XDR Premier Supported Components, where information on such threats is visible from within the Cisco XDR Premier Supported Component available logs, events, alerts, and incidents.

Cisco Responsibilities

- Use threat intelligence to research indicators of compromise (IOCs) to confirm threats, attacks, compromises or exploits;
- Create a Security Incident ticket on the Cisco XDR Premier Service Portal 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 available sources 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;
- Investigate Security Incidents that the 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. Cisco will set the priority level for these Security Incidents in accordance with the matrix set out in Appendix B and will include response action recommendations as well as available information that confirms, validates, or otherwise corroborates the detection of a potential Security incident. For these Security Incidents, Cisco will analyze Customer-provided threat information or logs, if Cisco deems the data to be sufficiently reliable and relevant. Incidents opened by the Customer do not have to originate from any of the Cisco XDR Premier Supported Components.

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 Customer-approved "Identification" and "Containment" actions within the Cisco XDR Platform, provide guided recommendations, and/or provide general recommended responses to help Customer contain, mitigate, prevent, or eradicate a Security Threat.

Cisco Responsibilities

- Perform Cisco XDR-supported "Identification" and "Containment" actions for events detected on the Cisco XDR Platform on Customer's behalf, as documented in the Response Playbook approved by the Customer during Service Activation;
- Provide guidance on how to mitigate, contain, or prevent a Security Threat 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 Cisco Security products identified in section 3.1 to help mitigate or respond to Security Incidents (Note: automated responses are limited to those documented in Cisco Secure Cisco XDR Premier response playbooks);
    - Where the Security Incident is an identified attack, recommend response actions to help mitigate the attack and provide guidance on how to help further remediate the Security Incident, leveraging the Cisco XDR Premier Supported Components and potential solutions outside of the Cisco XDR Premier Supported Components;
    - Where further validation of the threat is required, Cisco will provide recommendations on areas of focus for Customer investigation. This can include gathering additional information for the incident;

- Where response actions are outside of the Cisco XDR Premier Supported Components, Cisco will provide the client with recommendation for further Customer investigation and/or remediation, if possible;

- Create and maintain the Cisco XDR Premier response playbooks based on changing capabilities and integrations in the Cisco XDR Platform and the Cisco XDR Premier Supported Components, impacting processes described above;
- Release advisories as new information is obtained about new or novel threats (these advisories are not specific to Customer).

Customer Responsibilities

- Perform all actions on the Cisco XDR platform other than the specific "Identification" and "Containment" actions described in the Response Playbook (which Cisco will perform on Customer's behalf);
- Participate in diagnostic testing to help identify the source of the Security Incident;
- Perform Cisco recommended changes to the Cisco XDR Premier Supported Components and be responsible for acting on recommendations from Cisco, including determining any dependencies resulting from the recommended actions;
- Utilize the Cisco XDR Premier Service Portal to configure and approve response actions through Cisco APIs; and
- Utilize the resources on the Cisco XDR Premier Service Portal for support, knowledge base, incident management, latest threat intelligence, and communication with Cisco.

4. Talos IR and CTSA for XDR Premier

4.1 Talos IR and CTSA for XDR Premier Service Delivery

The Talos IR and CTSA for XDR Premier services provide remote-only emergency incident response and remote-only proactive services to XDR Premier Customers. Services may include one or more of the services in Table 2, subject to having a sufficient Service Hours balance (see Appendix A for more details).

Customer is eligible to use their Service Hours towards the following services:

Service	Minimal Hours
Intel on Demand	5
Breach Susceptibility Workshop	5
Organization Digital Footprint Assessment	10
Security Design Thinking Workshop	20
Emergency Incident Response	40
Penetration Testing	40
Threat Modeling	40
Device Configuration and Build Review	40
IR Plan	50
IR Playbooks	50
Tabletop Exercise	50
Security Architecture Assessment	80
IR Readiness Assessment	80
Compromise Assessment	80
Cyber Range	80
Proactive Threat Hunting	100
Red Team Threat Simulation	160
Purple Teaming	160
Security Operations Assessment	160

Table 2. Available Talos IR and CTSA for XDR Premier Services

Cisco Responsibilities

- Provide emergency incident response by escalating security incidents from the MXDR Premier Security Operations Center to the Cisco Talos Incident Response resources for eligible customers who have opted into receiving emergency incident response support from Talos IR.
- Provide the Customer with an estimate of Service Hours based on complexity of Customer request and scope of Customer request needed to perform the requested service(s).
- Create a Service Requirements Document ("SRD" to document the Service Hours, scope of Customer request and any specific deliverables for Customer approval for any requested proactive services.
- Perform the Talos IR and CTSA and provide the deliverables as documented in approved SRDs.

Customer Responsibilities

- Attend service delivery meetings as scheduled for emergency incident response and proactive services.
- Approve any SRDs within ten (10) business Days of sharing and no later than five (5) business days in advance of any proposed delivery start dates.
- Request proactive services at least ninety (90) days before service hours expire.
- Where Customer's Service Hours balance is insufficient to cover the services required from Cisco, purchase additional service hours to complete any emergency incident response or proactive services that exceed the available service hours (See Appendix A for more details).

4.2 Notes and Limitations

The following notes and limitations apply to the Talos IR and CTSA for XDR Premier services:

- Cisco will make efforts to allocate resources evenly throughout the Services subscription term.
- Once the number of Service Hours in the XDR Premier subscription term, as calculated from the order details, are used, Cisco may suspend work until additional hours are purchased or other written arrangements are made.
- The deidentified threat, indicator of compromise, vulnerability, attack, techniques used, vulnerability, weakness, and other related information that Cisco collects from Customer in relation to the Talos IR and CTSA for XDR Premier 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.
- Cisco will use commercially reasonable processes and technologies to assess Customer's cybersecurity, but Cisco does not guarantee that all vulnerabilities and weaknesses in Customer's environment will be detected.
- Talos IR and CTSA must be requested and scheduled at least ninety (90) days before the hours are set to expire per 12-month subscription term or end of subscription term.
- Customer expressly provides Cisco with permission to conduct penetration testing or other forms of simulated cyber-attacks on the Customer's environment as set forth in the SRD for that activity. Customer will provide Cisco a letter of authorization or similar documentation as proof of this permission upon Cisco's request.

- Customer may not report any of Cisco's testing activities, tools, or infrastructure used in connection with the Services as malicious to any third party.
- Customer will provide Cisco with prerequisites for each activity as set forth in the corresponding approved SRD. This may include connecting Cisco devices to networks, configuring devices to allow Cisco access, or providing requested credentials to access systems.
- If, during an activity, a serious fault or problem in Customer's environment is discovered that Cisco believes could affect the operational status of the environment or the delivery of the engagement, Cisco may generate a Security Fault Notice ("SFN"). In such event, Cisco may suspend activities until Customer has reviewed the SFN and Customer has instructed Cisco to resume activities. In this event, Cisco may generate a Change Request which may require additional Credits.
- Customer remains responsible for the security of its environment(s).
- Information on Cisco's corporate policy on the disclosure of Security Vulnerabilities discovered as part of Cisco's Services is posted at: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#dsvdpcsd

4.3 Service Terms Definitions

For the purposes of Section 4. Talos IR and CTSA for XDR Premier, the following definitions shall apply:

Term	Definition
Intel on demand	A service that provides research by Talos IR and/or Talos Intelligence for a Customer on latest threats and/or a Customer's specific contextual threat factors such as infrastructure, industry, and intellectual property.
Breach Susceptibility Workshop	A workshop that assesses the controls that exists for an organization that prevent breaches.
Organization Digital Footprint Assessment	A service that will take a list of internet accessible assets and provide a report detailing services that those systems offer.
Emergency Incident Response	An emergency service that assists a Customer with response to security incidents, which may include triage, coordination, investigation (such as analysis and forensics), containment, and guidance for remediation activities.
Security Design Thinking Workshop	A workshop where Cisco will use a Design Thinking methodology to help Customer identify security priorities and their alignment to the organization's priorities.
Pen testing	A service where Cisco uses their knowledge of security vulnerabilities and weaknesses to assess which a Customer is susceptible to and the impact should they be leveraged by an attacker.
Threat Modelling	A service that looks at Customer key operational functions, assets, and data to build models of how they might be impacted by a security incident.
Configuration and Build Review	A service that assesses the configuration and build of specific devices

Term	Definition
	against a standard to identify any vulnerabilities or weaknesses.
IR Plan	A service that reviews or creates a document to capture who is responsible for handling processes and communications when experiencing a security incident.
IR Playbooks	A service that reviews or creates document(s) to capture the steps that must be taken to detect, contain, and recover from a security incident that is threat specific.
Tabletop Exercise	A service that helps facilitate 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.
Security Architecture Assessment	A service that looks at the security controls that exist in an organization to identify any capability gaps, and where controls are not functioning as expected.
Compromise Assessment	A service that provides a high-level analysis and review of a Customer's environment to potentially determine whether the Customer's organization has been or is currently being 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 Talos IR.
Proactive Threat Hunting:	A service that provides a targeted analysis and review of a Customer's environment based on an agreed upon hypothesis to potentially determine whether the Customer's environment has signs of this hypothesis activity.
Red Teaming	A collaborative exercise where Cisco emulates adversary tactics, techniques, and procedures (TTPs) in a clandestine manner to simulate a real-world adversary.
Purple Teaming	A collaborative exercise where Cisco emulates adversary tactics, techniques, and procedures (TTPs) and partners with the Customer on event detection methods.
Security Operations Assessment	A service that assesses security operations that exist in an organization to identify any capability gaps, and where controls are not functioning as expected.

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 covered as a response action;
b) Connectivity, such as (for example) a local circuit;
c) Provision, configuration, support and/or management of any Cisco or third party elements or technologies

1.2 **Reporting.** Cisco will provide or make available via the Cisco XDR Premier Service Portal, the reports listed in the reporting documentation for the Detect and Response Services. Cisco reserves the right to add, change, or remove reports in its reasonable discretion. CTIR and CTSA reports will not be covered by Cisco XDR Premier Service Portal

1.3 **MXDR Logging.** Please see the product/service description and logging data for the Cisco XDR Premier Security Components. The Services retain Security Incident ticket data for one year and are then 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 that it will (i) prevent, detect, stop, or mitigate all Security Incidents, or (ii) always correctly identify an event as a Security Incident or otherwise.

1.6 **Cisco Talos Incident Response (Talos IR) and Cisco Technical Security Assessment (CTSA) for XDR Premier – Service Hours ("Service Hours").** Cisco XDR Premier Tier Service entitles Customer to a set number of Service Hours which can be called off against the Talos IR or CTSA services documented in Section 4.1.

Available Service Hours are determined by Cisco on the basis of the length of the Services Term and amount of Security Content Users (SCUs). Service Hours round up to the nearest whole number and are divided into 12-month period for each year of the Services Term. Hours do not roll over to subsequent 12-month period, nor can they pulled forward into any other 12-month period.

When Customer requests a Talos IR or CTSA service, Cisco will validate that Customer has sufficient Service Hours (See Appendix A: 1.6 for definition) for such services. If Customer's Service Hours balance is not sufficient, Customer will be required to purchase additional Service Hours, as documented by Cisco. Service Hours required will be proportional to length and complexity of the service being performed. For proactive services, Cisco will document activity scope, deliverables, and hours required to complete the service in a SRD to be approved by Customer before commencing any service.

1.7 **Cisco XDR Premier Technical Support.** The Services do not include technical support for the Cisco XDR Premier Supported Components or any other technologies. If Customer's issue requires technical support for Cisco XDR Premier Supported 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. If Customer requires technical support for any third party (or non Cisco-branded technologies), Customer should engage the relevant third party vendors. Customer shall, at all times during the Term:

1.7.1 Maintain all operational functionality (including Cisco user and API access) of the Cisco XDR Premier Supported Components, as required by Cisco to enable Cisco to provide the Services;
1.7.2 Notify the Cisco of any changes that will impact access to the in-scope data sources required to deliver the Services; and
1.7.3 Where applicable, engage third party vendors for support.

Appendix B – Priority Levels for Cisco XDR Premier Service

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

1. Impact and Urgency 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 Matrix

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. 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.

		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 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).

1.2 Priority Matrix

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. 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.

		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 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).

1.3 Service Level Objective ("SLO")

Time to Engage
DEFINITIONS Cisco will contact Customer's designated contact 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 within timeframes above for unresolved P1 and P2 Security 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 OBJECTIVE: On time escalation to Customer => 95%
MEASUREMENT PERIOD: Monthly (one calendar month)

If Cisco fails to meet the SLO above, it will review the reasons for its failure to meet the SLO and will use commercially reasonable efforts to remediate the cause of the failure. However, other than the obligation set out in the preceding sentence, Cisco will have no liability to Customer (whether financial or otherwise) if Cisco fails to meet the SLO.

The window to measure performance against the SLO is the Measurement Period. The first Measurement Period will begin 60 days after

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

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

Cisco's failure to achieve the SLO above will be excused if caused by (i) any mutually agreed schedule of activities, (ii) any Cisco technology being EoS (End of Sale) or EoL (End of Life) or otherwise not covered by maintenance, (iii) delays or faults caused by Customer, third party equipment, software, services, support, or vendors not under the control of Cisco, (iv) a Force Majeure Event or (v) failure by Customer to implement Cisco's recommendations necessary to remediate Security Incidents.