

# Sophos Taegis™ MDR for OT -- Service Description

---

This Service Description describes Sophos Taegis MDR for OT (“**Service**”). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below) or in the Glossary section below.

This Service Description is part of and incorporated into, as applicable: (i) Customer’s manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at <https://www.sophos.com/legal> (collectively referred to as the “Agreement”). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to <https://www.sophos.com/legal>.

## Overview

- **New customers of MDR or MDR Elite:** For customers purchasing MDR for OT simultaneously with MDR or MDR Elite, prior to onboarding, Sophos will activate Customer’s Service by provisioning access to Customer’s instance of Taegis™ XDR, which will also provide Customer with access to: 1) online documentation; and 2) instructions to access and deploy the Taegis™ XDR Endpoint Agent.
- **Existing customers of MDR or MDR Elite:** For customers adding MDR for OT to an existing MDR or MDR Elite subscription, Sophos will activate Customer’s Service on the effective date of the Agreement for MDR for OT.

The Service provides Customer with access to a team of security professionals (the “OT Specialist Team”, herein referred to as the “Specialist Team”) to conduct in-depth analysis for investigations as well as consult on response and remediation related to Customer’s OT Environment.

The Specialist team is available 24x7 via chat, email, telephone and ticket. Customer **must** purchase the Taegis™ MDR service (“MDR”) in conjunction with this Service. (See the applicable MDR Service Description at <https://www.sophos.com/en-us/legal> ) As part of MDR, the MDR Security Analysts will review and investigate Threats detected within Customer’s Taegis™ XDR (“XDR”) tenant(s). Threats requiring further analysis as determined by Sophos will result in creation of an Investigation within XDR. The Specialist Team will conduct additional analyses of investigations identified in XDR related to assets associated with Customer’s OT environment. After analysis is completed for each Investigation, the Specialist Team will take appropriate action based on the documentation developed during Onboarding.

All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the applicable Sophos Agreement.

## Service Components

### 24x7 Access to OT Specialist Team

Customer will have access to the OT Specialist Team 24x7 via methods described above. From a remote location, the Specialist Team will conduct work on Customer's behalf and support Customer as defined herein. The Specialist Team will communicate with Customer through email and Sophos Ticketing System for support related to the activities described herein. The Specialist Team will also communicate with Customer through telephone solely for OT related investigations deemed by Sophos to be High or Critical.

### Threat Investigations

The Specialist Team will conduct Threat Investigations aligned to the following categories:

- OT-specific alert investigations: When event data is sent by supported OT Monitoring Technology and that data triggers an alert in Taegis XDR deemed by Sophos to be a Threat, the Specialist Team will perform an investigation with the goal of understanding the potential impact of the Threat to the Customer's OT Environment. The Specialist Team will also review and conduct analyses for Investigations that are automatically created through approved automation playbooks within Taegis XDR and add the findings to these Investigations.
- Non-OT-specific alert investigations: When event data from non-OT Monitoring Technology triggers an alert in Taegis XDR deemed by Sophos to be a Threat, initial triage, analysis, and investigation will be performed by MDR Security Analysts (as described in the Threat Detection and Investigation section of the MDR and MDR Elite service descriptions). At the conclusion of their investigation, the Specialist Team will conduct further analyses for these Investigations with the goal of understanding the potential impact of the Threat to the Customer's OT Environment.

For all Investigations, upon confirmation of a Threat by the Specialist Team, the Specialist Team will consult on responses and remediation with Customer, which includes communicating with responsible stakeholders and advising Customer about appropriate actions.

**Note:** The Specialist Team will focus solely on Cybersecurity threats identified or validated by Taegis XDR. Events generated by Customer OT Monitoring Technology related to health alerts, vulnerability scanning, or patching are not considered Threats by this service and will not be investigated. Such out-of-scope events may be data points included in the investigation of a Cybersecurity threat.

### Investigation Procedures

The Specialist Team will primarily operate within Taegis XDR as well as Sophos internal tools. The Specialist Team will investigate all Taegis XDR alerts determined by Sophos teams to be Threats. The Specialist Team will perform investigations based on Sophos best practices, the initial findings of MDR Security Analysts, and business context provided by the Customer during Onboarding and in an on-going fashion, as well as follow the escalation procedures for OT related Threats that will be developed by Customer and Sophos during Onboarding. Additionally, the Specialist Team will directly access Customer's supported OT Monitoring Technology, as needed, to enhance their investigations. Access for the Specialist Team to such platforms must be provided and maintained by the Customer. Customer acknowledges that not providing or maintaining this access for the Specialist Team limits the service that the Specialist Team can provide until the access is restored. The Specialist Team will use the Customer's OT Monitoring Technology to conduct analyses, identify additional business context, and determine their recommendations.

**Note:** The Specialist Team does not conduct any activities related to managing Customer's systems and tools (e.g., no software license or platform/configuration management).

## Service Phases

There are two primary phases for delivering the Service: Onboarding and Steady State.

### Onboarding

This phase will be managed by an assigned Program Manager (“PM”). The PM will coordinate the activities that must be completed during this phase. Sophos will guide Customer through multiple activities to help ensure that the Specialist Team has the access, familiarity, and context needed to deliver the Service to Customer. Onboarding is expected to be completed within 6-8 weeks; timeline will be based on dependencies and the project plan that will be agreed-upon during Onboarding.

### Steady State

Steady State commences when the Onboarding Checklist is completed and Customer has satisfied all Steady State requirements for the standard MDR service, which must accompany this Service (see [ManagedXDR Onboarding Guide](#)). During Steady State, the Specialist Team will conduct investigations and apply Customer’s business context based on their knowledge of OT security and information from Customer’s supported OT Monitoring Technology. When the Specialist Team confirms a Threat, they will help coordinate the response and remediation for Customer and will collaborate with Customer-designated personnel as appropriate.

The table below indicates timing and activities conducted by Sophos during the Service Phases. Please note that timing is approximate and predicated on Customer performing its responsibilities described herein.

Phase	Activities
Onboarding	<p><b>Timing: Upon start of Services Term</b></p> <ul style="list-style-type: none"> <li>• Ensure that the Specialist Team can access and use Customer’s supported OT Monitoring Technology.</li> <li>• Discuss and explain Specialist Team workflows and investigations strategies.</li> <li>• Discuss and document escalation processes for OT environment.</li> <li>• Discuss and implement Taegis custom alert and suppression rules.</li> <li>• Discuss OT Monitoring Technology tuning.</li> <li>• Discuss Endpoint tagging and Taegis Data Collector labelling for OT Environment.</li> <li>• Complete Endpoint tagging and Taegis Data Collector labelling for OT Environment.</li> <li>• Complete Onboarding Checklist to verify readiness for transitioning to Steady State</li> </ul>
Steady State	<p><b>Timing: 6-8 weeks after Onboarding begins</b></p> <ul style="list-style-type: none"> <li>• All Taegis MDR investigations and Taegis observed Threats from Customer OT Environment are reviewed by Specialist Team for OT risk</li> <li>• Engage Customer as needed for orchestrated response and remediation activities.</li> </ul>

## Customer Obligations

Customer is required to perform the obligations listed below and acknowledges and agrees that the ability of Sophos to perform its obligations hereunder are dependent on Customer’s compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result in limitations and reduced service capabilities or suspension of managed components of the Service.

Customer will do the following:

- Ensure that all MDR obligations are met (see [Customer Obligations for ManagedXDR](#)).
- Customer must acquire and maintain supported OT Monitoring Technology to provide telemetry from Customer OT environments.
- Provide and maintain Specialist Team access to Customer supported OT Monitoring Technology.

- Maintain proper tagging and labeling within Taegis XDR to ensure visibility into the OT portion of the Customer environment.
- Ensure list of Customer's authorized contacts remains current, including permissions and associated information.
- Obtain consent and authorization from the applicable third party, in form and substance satisfactory to Sophos, to permit Sophos to provide the Service if Customer does not own network resources such as IP addresses, tools, systems, hosts, facilities or web applications.

## Additional Information

Billing for the Service begins at the same time as billing for Taegis™ XDR. Contact account manager or refer to the official terms as stated on Customer's Agreement from purchase for the most up-to-date details. See the documentation within Taegis™ XDR (<https://docs.ctpx.secureworks.com/>) for information about compatible browsers, Integrations, detectors, dashboards, and training.

## Warranty Exclusion

While the Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Sophos makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer's systems.

## Glossary

Term	Description
Alert	Prioritized occurrences of suspicious or malicious behavior detected by a detector within XDR.
Investigation	A central location within XDR that is used to collect evidence, analysis, and recommendations related to a Threat that may be targeting an asset in a Customer's IT environment. Investigations are categorized into types, such as Security and Incident Response.
Parties	Customer and Sophos are referenced jointly using this term.
Security Analyst	A Sophos security expert who analyzes alerts deemed High and Critical for customers, and creates and escalates Investigations.  <b>Note:</b> A Security Analyst may also be referred to as a MDR analyst or an MDR analyst across other Sophos documentation.
Security Incident	An XDR-generated circumstance in which a compromise or suspected compromise has occurred involving a Customer's environment.
Services Term	Period of time identified in the Agreement during which Services will be delivered to Customer.
Threat	Any activity identified by XDR that may cause harm to an asset in a Customer's IT environment.