Sophos Taegis™ Elite Threat Hunting – Service Description - Japan

This Service Description describes Sophos Taegis Elite Threat Hunting ("**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

This Service requires a subscription to Sophos® Taegis™ MDR, Taegis MDR Plus or Taegis MDR Enhanced ("**MDR**").

- **New customers of MDR:** For customers purchasing Elite Threat Hunting simultaneously with MDR, prior to onboarding, Sophos will activate Customer's Service by provisioning access to Customer's instance of 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:** For customers adding Elite Threat Hunting to an existing MDR subscription, Sophos will activate Customer's Service on the effective date of the Agreement for Elite Threat Hunting.

The Service provides Customer with a Threat Hunter, recurring threat hunting meetings, continuous human-led threat hunting, and tailored threat hunts.

Notes:

- Service and associated support shall be provided in Japanese language.
- "Endpoint" and "asset" are used interchangeably in this service description.
- **For Customers with more than one XDR tenant (i.e., Additional Managed Tenant)**, service components are applicable across all of Customer's tenants, unless otherwise specified below.

Service Components

Elite Threat Hunting

Sophos will conduct human-driven Threat Hunting, and relevant findings will be made available to Customer within Investigations in XDR. Lead by a Threat Hunter assigned to Customer, the Sophos proprietary methodology, expertise, threat analytics, and threat intelligence will be used to identify unknown Threats and undiscovered threat actors through their tactics, techniques, and procedures ("**TTPs**"), as well as to identify deficiencies in visibility, misconfiguration, or missing data sources discovered. Further, the Threat Hunter will inspect collected Customer telemetry to detect activity such as anomalous user activity, network communications, and application usage and persistence mechanisms.

The Sophos Threat Hunting team is generally available Monday – Friday, 9 a.m. – 17 p.m. JST (UTC +9), for support that is specific to Threat Hunting; however, Customer must contact the Sophos Security Operations Center ("**SOC**") for all support inquiries, and the SOC will engage the Threat Hunting team if needed. If Customer contacts the Sophos SOC for support during a time that is not within the above-listed time frame, and Threat Hunting-specific input is required to resolve Customer's issue, then the Threat Hunting team will be engaged as soon as possible during the above-listed hours.

Elite Threat Hunting includes the following:

- Assignment of a Threat Hunter who will collaborate with Customer to gain a thorough understanding of Customer's environment for purposes of effectively conducting Threat Hunting
- Continuous human-driven Threat Hunting across Customer's telemetry in XDR in search of undetected Threats and security exposure that jeopardizes Customer's security posture
- Up to two (2) touchpoint meetings each month with the Threat Hunter at a time as agreed with Customer, to discuss previously shared threat hunt findings and discuss and agree upon requested tailored threat hunts (described below) to align with Customer's risks and objectives.
- Up to four (4) tailored threat hunts performed each month as requested by Customer (maximum of one (1) per week and a minimum of 3 business days processing time to begin the requested hunt). Customer requests that Sophos researches but are deemed to be infeasible will count against the monthly limit. These hunts can include, but are not limited to:
- Artifact-Driven Threat Hunting
- Cloud and Network Threat Hunting
- Hypothesis-Driven Threat Hunting
- Threat Intelligence-Driven Threat Hunting
- Analysis and escalation to Customer via Taegis Investigation of all activity discovered during Threat Hunting that is deemed critical and could represent a confirmed Security Incident or Threat (e.g., misconfiguration, visibility deficiency)

Notes:

- **Note to Customers with more than one XDR tenant (i.e., Additional Managed Tenant):** Investigations created from Elite Threat Hunting activities as described above will be presented in the corresponding Customer XDR tenant. The maximum number of tailored threat hunts provided each month is four (4) regardless of the number of tenants. The maximum number of touchpoint meetings with the Threat Hunter is provided is two (2) regardless of the number of tenants.

  For clarity, if a Customer has four individual tenants, performing the same tailored threat hunts on each individual tenant counts as four tailored threat hunts, not one.

- Elite Threat Hunting cannot begin until after the specified Onboarding activities for the relevant MDR are completed and Customer enters steady state. (See relevant Service Description at https://www.sophos.com/en-us/legal/). In addition, Sophos highly recommends that Customer completely deploy supported Endpoint Agents on all endpoints—up to Customer's Licensed Volume—to maximize the effectiveness of this Service. Until completely deployed on all endpoints, Customer understands, agrees, and accepts the risk that this Service will have reduced capabilities for Customer's environment.
- Elite Threat Hunting customers who want to use CrowdStrike Endpoint must purchase the standard Falcon Data Replicator (FDR) directly from CrowdStrike or a CrowdStrike-authorized reseller.

Service Phases

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

Onboarding

Once steady state for MDR has been achieved (according to the definitions set forth in the applicable MDR service description that can be found at https://www.sophos.com/en-us/legal/), an initial meeting between Customer and their Threat Hunter will be coordinated. During this initial meeting, the Threat Hunter will explain their hunting methodology and initial strategy and the Customer will inform the Threat Hunter about Customer's environments and their hunting priorities.

Steady State

Following the initial meeting with the Threat Hunter, steady state service will begin assuming that Customer's MXDR service is also in steady state. As a reminder, MDR is considered steady state when Customer deployed at least 40% of its Licensed Volume (i.e., deployed compatible Endpoint Agents to endpoints) **and** Customer has acknowledged completion of the training videos within parts one and four of the MDR Onboarding Overview (www.secureworks.com/legal/product-terms).

Phase	Activities

Onboarding	**Timing: Once MDR is in steady state**
	
	• Facilitate the Elite Threat Hunting introductory teleconference to discuss with Customer the following:
	    ○ Overview and deliverables
	    ○ Roles, responsibilities, and scope
	    ○ Bi-weekly (up to twice a month) operational teleconference

Bi-weekly Meetings	**Timing: Approximately two (2) weeks after Steady State service begins** • Review notable Alerts, Investigations, and Threat Hunts created for Customer • Discuss Customer environment and posture changes • Discuss threat landscape developments and hunting strategy
Quarterly Updates	**Timing: Quarterly after the baseline meeting is conducted** • Summary of recent hunting initiatives and findings will be sent to Customer CSM for inclusion in executive reporting

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.

Note to Customers with more than one XDR tenant (i.e., Additional Managed Tenant): The Customer Obligations listed below are required and applicable to **each** of Customer's XDR tenants.

Customer will do the following:

- Respond to their Threat Hunter in scheduling bi-weekly meetings
- Respond for making tailored threat hunting requests according to the timing guidance provided above (maximum of one (1) per week and a minimum of 3 business days processing time to begin the requested hunt)
- Acknowledge recommendations and findings provided by the Threat Hunter

Warranty Exclusion

While this 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 network.

Additional Information

See the documentation within XDR (https://docs.ctpx.secureworks.com/) for information about compatible browsers, integrations, detectors, dashboards, and training. Other information is also available, including release notes.

Glossary

Term	Description
Artifact-Driven Threat Hunting	This proactive approach begins with a focus on specific artifacts, such as mailbox rules or persistent mechanisms, to uncover potential threats. It's a reactive method focusing on analyzing existing data to find known malicious activities.
Additional Managed Tenant	An add-on for MDR that provides Customer with more than one XDR tenant.
Alert	Prioritized occurrences of suspicious or malicious behavior detected by a detector within XDR.
Endpoint Agent	An application installed on an endpoint that is used to gather and send information about activities and operating system details of the endpoint to XDR for analysis and detection of Threats. Use this link to access the list of Endpoint Agents that are compatible with XDR: https://docs.ctpx.secureworks.com/at_a_glance/#endpoints.
Hypothesis-Driven Threat Hunting	This proactive method involves forming hypotheses about potential threats based on knowledge of the environment and attacker behavior. Hunters

Term	Description
	design specific investigations to test these hypotheses and uncover hidden threats.
Integration	Application Programming Interface ("**API**") calls or other software scripts for conducting the agreed-upon Services for the connected technology.
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.
Proactive Risk Identification	The process of proactively searching for potential security risks, miss-configurations, poor security controls, within an organization's IT environment before they can be exploited by attackers.
Security Analyst	A Sophos security expert who analyzes alerts deemed High and Critical for customers, and creates and escalates Investigations. ***Note:*** 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.
Security Investigation	A type of Investigation that is conducted for a Critical or High alert or event in XDR after a Security Analyst completes preliminary investigative procedures to determine whether a Threat is valid.
Services Term	Period of time identified in the Agreement during which Services will be delivered to Customer.
Tailored Threat Hunt	A threat hunt requested by Customer. Feasibility and execution of requested threat hunt is determined by the Threat Hunter.
Threat	Any activity identified by XDR that may cause harm to an asset in a Customer's IT environment.
Threat Hunter	A designated Sophos security expert focused on Threat Hunting.
Threat Hunting	To proactively and iteratively discover current or historical threats that evade existing security mechanisms and to use that information to develop future countermeasures and increase cyber resilience.
Threat Intelligence-Driven Threat Hunting	A type of reactive threat hunting using indicators of compromise (IOCs) to search within the network.