Sophos Incident Management Retainer – Service Description

This Service Description describes Sophos Incident Management Retainer ("**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.

1.1 Overview

Sophos will provide Customer with services and capabilities intended to decrease the likelihood of a cyber incident, and to ensure timely and effective response efforts if Customer has a cyber incident.

Customer will choose a tier for the Service, which will appear on the Agreement. For ***all*** tiers, Customer will receive the following:

- SLAs for EIR
- Pre-negotiated rate for additional Service Units
- Access to the Sophos portfolio of Security Consulting and Professional Services through the Services Catalogs (Sophos Security Services Retainer Catalog and Incident Management Retainer Services Catalog); see the note below
- Pre-negotiated rate for EIR Hours
- Newsletters on a quarterly basis
- Access to Incident Response Hotline 24 hours a day, 7 days a week (Customer will receive information about the hotline during Service Initiation)

  Note: Alternately, Customers with access to the Taegis platform can submit requests through the Taegis Ticketing System instead of the Incident Response Hotline, if desired.

Depending on the tier Customer purchases, Customer will receive other service components as listed in the table below.

Tier	Summary of Service Components
1 – Value	• Four (4) Service Units ***Note:*** Customer can purchase a maximum ***additional*** number of four (4) service units—for a maximum ***total*** number of eight (8) Service Units for the Service Term
2 – Base	• Ten (10) Service Units ***Note:*** Customer can purchase a maximum ***additional*** number of fourteen (14) service units—for a maximum ***total*** number of twenty-four (24) Service Units for the Service Term

3 – Essential	• Annual Planning Workshop • Twenty-six (26) Service Units • Service Reviews (status updates and reports)

Tier	Summary of Service Components
4 – Essential Plus	• Annual Planning Workshop • Fifty (50) Service Units • Service Reviews (status updates and reports, End-of-Year Executive Briefing)

The in-scope locations for traveling to perform services are as follows: the European Union ("**EU**") member states, Japan, the Schengen Area, United Kingdom ("**UK**"), and the United States of America ("**USA**")—collectively referred to as the "**On-site Response Supported Locations**."

Sophos will work with Customer throughout the Service Term to define and execute a plan of action that is tailored to Customer's goals, needs, and overall cybersecurity strategy.

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above.

Notes:

- Sophos will not install third-party software on any appliance or system, unless explicitly indicated in Section 2 as being part of the Service.
- Each Customer-approved request for EIR, a Proactive Consulting or Professional Service is referred to as an Engagement. For example, one (1) Threat Hunting Assessment is a Proactive Consulting Service and is referred to as an Engagement.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Sophos to perform the Service, including meeting the Service Level Agreements ("**SLAs**") listed further below, is contingent upon the following:

- Customer personnel are scheduled and available to assist as required for the Service(s), and those attending enhancement sessions have user accounts within Taegis XDR.
- Customer will have obtained 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, Hosts, facilities or web applications.
- For on-site activities, Customer will provide a suitable workspace for Sophos personnel, and necessary access to systems, network, and devices.
- Replies to all requests are prompt and in accordance with the delivery dates established between the parties.
- Customer's scheduled interruptions and maintenance intervals allow adequate time for Sophos to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Sophos testing activities as needed, to prevent disruption to Sophos business and performance of the Service (e.g., takedown requests, ISP deny list).
- Customer will provide to Sophos all required information (key personnel contact information, credentials, and related information) at least two (2) weeks before an Engagement for a Proactive Consulting or Professional Service or prior to on-site arrival for Emergency Incident Response.

- Ensure that Customer's personnel have agreed to (i) maintain confidentiality of any Sophos Confidential Information and Sophos Materials used as part of the Service, and (ii) not to share such Confidential Information and Sophos Materials, including any recordings provided to Customer and its personnel in connection with the Service, outside the Customer's organization (including not to publish such recordings in public space or social media).
- When needed, provide support through Customer's personnel to make any changes to Customer's systems and infrastructure to enable the integrations to Taegis XDR.
- Customer is responsible for, and will promptly obtain, maintain, and comply with, any required licenses, approvals, permits, or consents necessary to receive and use the Services and for Sophos to provide the Services, including any rights, consents, or approvals needed to transfer the Customer Data to Sophos.

1.2.1 Communications

To initiate a request for an EIR Engagement, Customer will submit a request through the Incident Response Hotline (or the Taegis Ticketing System if Customer has access to the Taegis platform), which are available to Customer 24 hours a day, 7 days a week. To initiate a request for a Proactive Consulting or Professional Service or make any changes to the Proactive Consulting or Professional Services roadmap and schedule, Customer can send an email to SecurityServicesRetainer@sophos.com.

1.2.2 Ransomware Negotiation

- Customer will provide Sophos with access to personnel authorized to make decisions regarding Customer's position with respect to ransomware payments and instructions with respect to negotiation strategy. Customer will provide prompt feedback to any inquiries regarding ransomware by Sophos' negotiators.
- In the event that Customer decides to pay any demanded ransomware payment, Customer must conduct independent due diligence on the threat actor based upon any information that Sophos and Customer are able to ascertain during the performance of the Service. This information may be derived from data and information that is or will become available to Sophos and Customer during delivery of the Service. Customer agrees that Sophos is unable to provide recommendations or advice to Customer regarding its legal or regulatory compliance obligations with regard to any export or economic sanctions or other laws or regulations that would apply to either Sophos or Customer.
- Customer agrees that it shall indemnify, defend, and hold harmless Sophos, its Affiliates and subcontractors, and each of their respective directors, officers, employees, contractors, and agents from any damages, costs and liabilities, civil or criminal fines, and expenses (including reasonable and actual attorney's fees) actually incurred or finally adjudicated as to any claim, action, or allegation by a national government regarding alleged violations of export or economic sanctions regulations whereby Sophos is or was asked by Customer to perform or not to perform certain actions in connection with this Service.

1.3 Scheduling

Sophos will contact a Customer-designated representative within five (5) business days after the execution of the Agreement to begin the Service Initiation activities described herein. These activities will ensure effective and efficient use of the Service. For each Engagement, Sophos will provide a work order to Customer for review. Prior to scheduling and commencing work for each Engagement, Customer must provide written approval of the work order to Sophos. Below is information about scheduling and re-scheduling EIR, Proactive Consulting and Professional Services Engagements.

- **EIR:** Customer will request EIR using the Incident Response Hotline (or the Taegis Ticketing System if Customer has access to the Taegis platform). During Service Initiation, Sophos will provide Customer with information for the hotline (and Taegis Ticketing System if applicable). These communication methods are available to Customer 24 hours a day, 7 days a week.
- **Proactive Consulting Services:** The Proactive Consulting Services outlined within this SD require a minimum of eight (8) weeks advance notification to schedule services for completion within the Service Term. Sophos will use commercially reasonable efforts to meet Customer's requests for dates and times to deliver the Service(s), taking into consideration Customer-designated maintenance interval, Customer deliverable deadlines, and other Customer scheduling requests. Written confirmation of an agreed-upon schedule shall constitute formal acceptance of such schedule. If Customer requests multiple Proactive Consulting Services simultaneously, then Sophos will schedule the first request as described within this section, with additional requests scheduled as best-effort based on resource and personnel availability.
- **Professional Services:** The Professional Services listed in the Sophos Services Catalogs require a minimum of two (2) weeks advance notification to schedule and complete within the Service Term. Sophos will use commercially reasonable efforts to meet Customer's requests for dates and times to deliver the Service(s), taking into consideration Customer-designated maintenance interval, Customer deliverable deadlines, and other Customer scheduling requests. Written confirmation of an agreed-upon schedule shall constitute formal acceptance of such schedule. If Customer requests multiple Professional Services simultaneously, then Sophos will schedule the first request as described above, with additional requests scheduled as best effort based on resource and personnel availability.
- **Re-scheduling:** Once scheduling of any on-site work at Customer facility has been mutually agreed to, any changes by Customer to the on-site work within two (2) weeks of the on-site work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Sophos.
- **Cancellation/termination:** At any time before Sophos commences effort for an Engagement, Customer may terminate an Engagement and, as applicable to the Engagement being cancelled, reuse the Service Units for a Proactive Consulting or Professional Service or EIR Engagement. If Customer cancels the Engagement after Sophos commences effort, then Customer forfeits the Service Units as applicable to the Engagement being cancelled. If travel was booked, then Customer will incur a $2,000 termination fee.

2 Service Details

The subsections below contain details about the Service and how it will be initiated for each tier.

2.1 Service Initiation

The subsections below describe Service Initiation for each tier.

2.1.1 Tiers 1 and 2 – Value and Base

Service Initiation is when Sophos collects Service-specific information from Customer to ensure timely and effective response efforts if Customer has a cyber incident. The information collected and deliverables provided to Customer are explained in the subsections below.

Note: Service Units do not apply to Service Initiation.

2.1.1.1 Information Collection and Validation

In anticipation of an EIR and to prevent delays in response actions, Sophos will request Customer's information in the form of a survey. The survey will be sent to Customer within five (5) business days of the execution of the Agreement and shall be completed and returned to Sophos within ten (10) business days from the day received.

Requested information may include but is not limited to the following:

- Authorized Points of Contacts ("**POCs**") with respective contact information
- Roles and Responsibilities for Incident Response efforts

2.1.1.2 Deliverables

Upon completion of the activities described above, Customer will receive a welcome kit (usually through electronic methods) that includes the following:

- IMR Overview
- IMR Service Handbook
- Access to online videos about critical process and service information
- After the above activities are completed, Service Initiation will be concluded, and ongoing operations will commence.

2.1.2 Tiers 3 and 4 – Essential and Essential Plus

Service Initiation is comprised of two stages: Information Collection and Validation, and the Planning Workshop. Each stage is explained in the subsections below.

Note: Service Units do not apply to Service Initiation.

2.1.2.1 Information Collection and Validation

In anticipation of an EIR and to prevent delays in response actions, Sophos will request Customer's information in the form of a survey. The survey will be sent to Customer within five (5) business days of the execution of the Agreement and shall be completed and returned to Sophos within ten (10) business days from the day received.

Requested information may include but is not limited to the following:

- Authorized Points of Contacts ("**POCs**") with respective contact information
- Roles and Responsibilities for Incident Response efforts
- List of Customer's locations and countries in scope
- Cybersecurity controls
- List of technologies leveraged for Incident Response
- Incident Response preparedness and governance maturity

Results of the survey will also be used to facilitate discussions during the Planning Workshop explained in the next subsection.

2.1.2.2 Planning Workshop

Within two (2) weeks after the completed survey is returned to Sophos, Sophos will contact Customer to schedule an annual Planning Workshop ("Planning Workshop"). Upon Customer's request, the Planning Workshop can be conducted on-site at a Customer location (expenses, such as travel time and travel fees, will be Customer's responsibility if Planning Workshop is conducted on-site). EIR Fundamentals and Proactive Consulting Services Planning will be discussed as explained below.

EIR Fundamentals. In the event of an EIR Engagement, Sophos and Customer shall be prepared to work together to ensure effective coordination and prompt response. EIR Fundamentals is an open forum to discuss Customer's current IR plan to gain an initial understanding of Customer's IR process and practices, and to identify and discuss any areas that may hinder timely and efficient response during an EIR Engagement. Further, the forum is focused on building Customer's familiarity with core Sophos EIR processes and specific activities that Customer shall be prepared to handle during an EIR Engagement. Listed below are topics usually discussed during the forum.

- Review incident handling and escalation process
- Discuss communication and information exchange protocols
- Review and discuss existing IR plans, and processes and alignment for including Sophos Incident Response team in the event of an EIR Engagement
- Discuss core technical EIR processes

Proactive Services Planning. Focused on the proactive aspect of the Service, this session is for discussing objectives, goals, and broader strategy for Customer's cybersecurity program. In preparation for this session, Sophos will review the survey results and Customer's initial list of selected Proactive Consulting Services. Sophos shall contact Customer should additional information be needed from Customer prior to the scheduled session.

During the Proactive Consulting Services Planning session, Customer and Sophos will further discuss the initial plan for the selected Proactive Consulting Services, and mutually agree on the Proactive Consulting Services roadmap, delivery timeline for the Proactive Consulting Services, and ongoing periodic deliverables.

Customer will receive a welcome kit through electronic methods that includes the following:

- IMR Service Handbook
- Installation instructions for Taegis™ Endpoint Agent
- Access to online videos about critical process and service information

Within two (2) weeks after completion of the Planning Workshop, Customer will receive a finalized Proactive Consulting Services roadmap and schedule. Service Initiation will be concluded, and ongoing operations will commence.

2.2 Service Components

The subsections below contain information about the components of the Service that are provided during ongoing operations. To initiate a request for EIR (which is considered an Engagement), Customer must submit a request through the Incident Response Hotline (or Taegis Ticketing System if Customer has access), which are available to Customer 24 hours a day, 7 days a week. Customer will receive information about the hotline (and Taegis Ticketing System if applicable) during Service Initiation. To request changes to the schedule for the Proactive Consulting Services roadmap (each Proactive Consulting Service is considered an Engagement) or to request Professional Services, Customer can send an email to SecurityServicesRetainer@sophos.com. Customer can use or exchange the Service Units (as applicable to each tier) during the Service Term as explained below.

2.2.1 Emergency Incident Response ("EIR")

For ***all*** tiers, Sophos can provide EIR that can be conducted remotely or on-site. The activities conducted can include but are not limited to the following:

- Incident support and coordination
- Digital media handling guidance and support
- Deployment support for host-based, network-based, and log analysis technologies

- Network analysis services
- Incident response and digital forensic analysis of online and offline infrastructure and datasets from customer's on-premises and cloud assets
- Malware analysis and reverse engineering
- Containment planning guidance
- Negotiation with ransomware threat actor regarding return of data and potential ransom payment amount in the case of a ransomware incident based on Customer's feedback and instructions
- Periodic Engagement Status Updates, in accordance with the mutually agreed-upon communication plan for each Engagement
- Engagement-specific Deliverables, in accordance with the mutually agreed-upon deliverables for each Engagement

In the event of a cybersecurity emergency or need for Emergency Incident Response services, Customer may repurpose Service Units for an EIR Engagement. Only increments of one (1) Service Unit are acceptable for repurposing (e.g., partial Service Units cannot be repurposed). One (1) Service Unit is equal to four (4) EIR hours.

To provide clarification, information about some of the above-listed items is provided in the subsections below.

2.2.1.1 Digital Forensic Analysis

As part of EIR, Sophos may acquire and analyze a variety of formats for forensic analysis of digital media and artifacts to assess compromise activity, including but not limited to the following:

- Disk images
- Memory images
- Mobile devices
- Network packet captures
- Plain text log files

2.2.1.2 Malware Analysis and Reverse Engineering

As part of EIR, Sophos may perform static, dynamic, and reverse engineering analysis to assist in understanding the function of Customer-supplied files.

Sophos will provide analysis results, to include cyber threat intelligence based on correlation across Sophos datasets and will advise on mitigation actions to reduce the impact of the sample on Customer's infrastructure.

2.2.1.3 Ransomware Negotiation

As part of EIR, Sophos may negotiate on behalf of Customer with a ransomware threat actor regarding return or deletion of stolen data and potential payment of a ransom amount. The primary objective of ransomware negotiation is to negotiate a reduced price from the original ransom demand for the return or deletion of any stolen data to minimize Customer's risk pertaining to data leakage or further extortion.

2.2.2 Sophos Proactive Consulting and Professional Services

Sophos will provide Customer with Proactive and Professional Services to Taegis ManagedXDR Customers. Customer has a specified number of Service Units that are included (see the list in Section

1.1, Overview) for use towards Proactive Consulting and Professional Services. Customer can purchase additional Service Units at any time during the Service Term if desired. See the Services Catalogs (Sophos Security Services Retainer Catalog and Incident Management Retainer Services Catalog) for information about the available Proactive Consulting and Professional Services.

The scope for each Proactive Consulting and Professional Service in the Service Catalogs is fixed (standard Sophos scope will be used); however, Sophos can work with Customer to reasonably customize the scope. Any deviations from the Service Catalogs shall require a change order. Specific service description for Professional Services standard in scope are available at https://www.sophos.com/en-us/legal.

Each service request for a Proactive Consulting or Professional Service will be scoped and the number of required Service Units will be determined prior to Engagement start. See the **Operating Model Reference** section in the Incident Management Retainer Service Handbook (https://docs.ctpx.secureworks.com/ services/incident-response/imr-service-handbook/imr-servicehandbook/) for information about scheduling Proactive Consulting and Professional Services.

The first four subsections below explain the Proactive Consulting Services that are recommended for each tier. Customer does not have to adhere to the recommended usage; Customer can choose other Proactive Consulting Services listed in the Services Catalogs (explained below). The last two subsections provide information about Engagement-specific Deliverables and exchanging Service Units (both the included Service Units and any Service Units purchased during the Service Term) for other services in the Services Catalogs.

2.2.2.1 Tabletop Exercise (recommendation for Tiers 2, 3, and 4)

Sophos will conduct one Incident Response Tabletop exercise with Customer. Eight Service Units are used for this exercise. Sophos and Customer will perform a scripted incident scenario to proactively test Customer's existing incident response capabilities. See the Services Catalogs for details.

2.2.2.2 Threat Hunting Assessment (recommendation for Tiers 3 and 4)

Sophos will conduct one Threat Hunting Assessment for up to 5,000 endpoints in Customer's environment and provide thirty (30) days of storage for data. 16 Service Units are used for this assessment. Sophos will review traces that persist in endpoint agents/sensors, network sensors, and retained logs to identify indicators and behaviors of compromise. See the Services Catalogs for details.

Note: This Service requires deployment of the Sophos or Taegis Endpoint Agent.

2.2.2.3 Penetration Test (recommendation for Tier 4 only)

Sophos will conduct one Penetration Test for up to 50 Internet Protocol ("**IP**") addresses within Customer's environment. Eight Service Units are used for this test. The test demonstrates weaknesses in systems or network services in Customer's environment. See the Services Catalogs for details.

2.2.2.4 Incident Response Plan Review (recommendation for Tier 4 only)

Sophos will conduct one Incident Response Plan Review ("**IRP Review**") for a maximum of 50 pages of incident response plan documentation. Eight Service Units are used for this review. Sophos will Customer's existing incident response ("**IR**") posture – current IR capabilities, processes, and practices – and apply its expertise and breadth of experience to provide prioritized recommendations for improving Customer's IR practices. See the Services Catalogs for details.

2.2.2.5 Engagement-specific Deliverables

Upon completion of each Proactive Consulting Service, Customer will receive final Engagement-specific Deliverables (e.g., a Final Report) that will include information about the completed Proactive Consulting Service. See the Services Catalogs for details.

2.2.2.6 Proactive Consulting Services

The Services Catalogs contain the Proactive Consulting Services available to Customer through use of the Service Units. Below are descriptions of the categories of Proactive Consulting services listed in the Services Catalogs.

Incident Readiness and Advisory Services – Sophos will assess and/or design an incident response plan that enables effective and efficient response to a cyber incident. Cybersecurity assessments are available to help Customer strengthen its cybersecurity posture and align cybersecurity program efforts with strategic objectives.

Testing and Validation Services – Sophos will conduct testing to discover any previously unknown issues, vulnerabilities, or threats in Customer's environment that could lead to a compromise.

Threat Intelligence Services – Sophos will provide threat and brand surveillance services such as an information brief for Enterprise Brand Surveillance.

Workshops and Exercises – Sophos will conduct or provide training modules that teach an incident responder core skills and key activities to perform during an incident. The workshops and exercises provide practical, hands-on experience in performing tactical incident response tasks, validate defined IR processes, and allow practice of the concepts outlined in Customer's existing IR plan in real-world cyber event scenarios. The workshops and exercises can be customized based on Customer's specific needs.

Programs – Sophos will work with you to identify the most appropriate path to maximize your readiness to respond to a ransomware attack and test your resilience.

Technical Assistance Services – Sophos will provide services for fixed scope technical requests such as conducting malware analysis.

2.2.2.7 Professional Services for Taegis ManagedXDR Customers

For Taegis ManagedXDR Customers, Sophos Services Catalogs include a list of Professional Services in the following categories:

Taegis Enablement Core — A Consultant guided engagement designed to establish a strong security monitoring foundation from the beginning of your Taegis journey with sessions designed to deliver a variety of activities including enablement assistance sessions, administrator and analyst training, environment discovery, standard Taegis playbook deployment, custom alert rule creation, and proactive response enablement.

Taegis Enablement Plus — A joint Project Manager and Consultant guided engagement which builds on the Core offering with expanded enablement assistance sessions, additional playbook deployment and rule creation, plus additional sessions for report creation, custom parser training and scenario-based training. This offering also includes governance and planning services from project management resources highly experienced in Taegis adoption.

Taegis Health Check — Sophos will assess and measure adoption and reinforce confidence on how Taegis automated processes, custom rules, reporting, and technology integrations are contributing to the customer's overall security posture. Outcomes include platform actionable recommendations, along with a three-hour session to review and implement identified recommendation to further enhance adoption of Taegis and drive increasing return on solution investment.

Taegis Training — Expand Taegis knowledge with additional training sessions, delivered by a Sophos security consultant. Outcomes include four hours of ad-hoc training, and a choice of role, scenario and skill-based sessions.

Data Collection and Integration — Sophos will assist Customer with integrating the identified data source into Sophos Taegis™ XDR, thus enhancing the value of the information (data outputs) from XDR for your unique needs. The service provides one XDR Data Collection and Integration ("DCI") for custom parsing and ingesting of data from one customer data source (e.g., log, endpoint telemetry) into XDR to enhance the value and usefulness of XDR to meet your unique needs.

Taegis Customizations — There are many opportunities to meet business-specific use cases using the customization options within Sophos Taegis™ XDR. Sophos Professional Services consultants can create outcomes specific to your use cases, or alternatively guide, teach, and assist you in their creation.

If Customer does not have enough Service Units to exchange for services, then Customer will need to purchase additional Service Units as indicated in the Additional Service Fees section. Within sixty (60) days of the Effective Date of the Agreement, Customer can exchange the services listed above for any of the services listed in the Services Catalogs.

2.2.3 Service Reviews (Tiers 3 and 4)

For Customers purchasing Tiers 3 (Essential) and 4 (Essential Plus), Sophos will conduct activities to facilitate periodic communication and interaction with Customer as described in the subsections below.

Note: Service Units do not apply to Service Reviews.

2.2.3.1 Status Update

Sophos will conduct a Status Update remotely through teleconference with Customer each quarter. The teleconference will not exceed two (2) hours and topics include Engagement results, Proactive Consulting Service Roadmap, and trends.

2.2.3.2 Status Report

Sophos will document each Service Review in the form of a quarterly Status Report and provide the report to Customer using a mutually agreed-upon method. The report will include a summary of completed Engagements, Customer's remaining Service Units, summary of scheduled (upcoming) Engagements, and recommendations for Engagements.

2.2.3.3 Executive Briefing (Tier 4 only)

For Customers purchasing Tier 4 (Essential Plus), Sophos will conduct one Executive Briefing per Service Term, delivered remotely through teleconference at a time agreed to by Customer and Sophos that is not earlier than month ten (10) of the Service Term. Upon Customer's request, the Executive Briefing can be conducted on-site at a Customer location (expenses, such as travel time and travel fees, will be Customer's responsibility if Briefing is conducted on-site). The Executive Briefing will include lessons learned from Engagements, current state of Customer's IR capabilities, insights into trends, and recommendations.

Note: Service Units do not apply to the Executive Briefing.

2.2.4 Quarterly Newsletters

For ***all*** tiers, Customer will receive quarterly communication in the form of a newsletter. The newsletter will provide insights into cybersecurity trends, emerging cyber threats, notable cyber threat intelligence, and other knowledge to support Customer's proactive approach and informed cybersecurity decisions.

Note: Service Units do not apply to newsletters.

2.3 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.3.1 Delivery Coordination

Sophos will provide coordination for the Service(s) with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics for people, processes, and tools as well as timeline and meeting facilitation.

The scope of delivery coordination includes the following:

- Develop delivery timeline with Customer and with Sophos personnel
- Work with Customer to identify and address issues or concerns that impact service delivery
- Periodic, high-level updates on progress
- Confirm delivery and procure project sign-off

Services will be delivered from Customer's site(s) and/or remotely from a secure location. Sophos and Customer will determine the location of the service(s) to be performed herein.

Sophos solely reserves the right to refuse to travel to locations deemed unsafe by Sophos or locations that would require a forced intellectual property transfer by Sophos. Sophos solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Sophos. Customer will be notified at the time that services are requested if Sophos refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Sophos travel is arranged. In the event any quarantines, restrictions, or measures imposed by governmental authority or Sophos restrict travel to any location, Sophos may at its election (i) deliver the Services remotely or (ii) postpone the Services until travel is permitted. If neither option (i) nor (ii) in the preceding sentence is feasible, Sophos may terminate the affected Services and provide Customer with a refund of any unused, prepaid fees.

2.3.2 Deliverables

Listed in the tables below are the standard deliverables for each tier. Sophos will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Tier 1 – Value

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Emergency Incident Response and Proactive Consulting Service Engagements	Engagement Status Updates and Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon
Professional Services		Mutually agreed upon	Mutually agreed upon

Tier 2 – Base

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Emergency Incident Response and Proactive Consulting Service Engagements	Engagement Status Updates and Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon

Professional Services	Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon

Tier 3 – Essential

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Onboarding	Planning Workshop(s)	Within thirty (30) days of contract commencement or agreed-upon intervals	Mutually agreed upon
	Proactive Consulting Services Roadmap	Two (2) weeks after completing the planning activities	Mutually agreed upon
Service Reviews	Status Updates	Quarterly	Remotely through teleconference
	Status Report	Quarterly	Mutually agreed upon
Emergency Incident Response and Proactive Consulting Service Engagements	Engagement Status Updates and Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon
Professional Services	Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon

Tier 4 – Essential Plus

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Onboarding	Planning Workshop(s)	Within thirty (30) days of contract commencement or agreed-upon intervals	Mutually agreed upon
	Proactive Consulting Services Roadmap	Two (2) weeks after completing the planning activities	Mutually agreed upon
Service Reviews	Status Updates	Quarterly	Remotely through teleconference
	Status Report	Quarterly	Mutually agreed upon

Service	Deliverable(s)	Delivery Schedule	Delivery Method
	Executive Briefing	One per Service Term (not earlier than month 10 of the Service Term)	On-site meeting or remotely through teleconference
Emergency Incident Response and Proactive Consulting Service Engagements	Engagement Status Updates and Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon
Professional Services	Engagement-specific Deliverables	Mutually agreed upon	Mutually agreed upon

2.3.2.1 Engagement-specific Deliverables and Timing

For ***all*** tiers, deliverables and presentation of findings compiled by Sophos in the performance of the Service(s) (the "**Engagement-specific Deliverables**") are tailored to work performed, and to Customer's needs.

2.3.2.1.1 Periodic Engagement Status Updates

Periodic Engagement Status Updates, which may be verbal or written, will be provided to Customer during the Engagement and may include the following:

- Summary of completed activities
- Issues requiring attention
- Planning for the next work effort period

2.3.2.1.2 Final Report

The Final Report may include the following:

- Executive summary, outlining key findings and recommendations
- Methods, detailed findings, narratives, and recommendations
- Attachments providing relevant details and supporting data

During the beginning phases of an Engagement, if a Final Report has been mutually agreed upon as an Engagement-specific Deliverable, then Sophos will issue a Final Report draft to the Customer designated point of contact within three (3) weeks of completing an Engagement. Customer shall then have three (3) weeks from Sophos delivery of the Final Report draft to provide comments. Should Customer provide comments, the Final Report shall be deemed complete upon the earlier of the date which (1) Sophos provides responses to these comments or (2) Sophos delivers a revised Final Report. If no comments are received from Customer before the expiration of the review period, or upon Customer's written acceptance of the Report, the Final Report will be deemed complete and referred to as the "Completed Final Report".

2.3.3 Customer and Sophos Responsibilities

The responsibility assignment matrix below describes the participation required by both Customer and Sophos in completing tasks or deliverables for a project or business process to facilitate successful

service delivery. Sophos uses standard RACI role criteria for managing Customer projects and deliverables. These roles are defined as follows:

- R – Responsible: Role(s) assigned to do the work.
- A – Accountable: Role(s) that make the final decision and has ultimate ownership.
- C – Consulted: Role(s) consulted as the subject matter expert ("**SME**") before a decision or action is taken.
- I – Informed: Role(s) updated with status of work being done, status of ongoing work, and results of work completed.

Note: The table below contains only high-level tasks for the Taegis Incident Management Retainer. Tasks for other services and activities (e.g., Threat Hunting Assessment) are not included.

Taegis Incident Management Retainer			
Activity	**Task**	**Customer**	**Sophos**
Service Initiation	Provide survey to Customer for completion	I	R, A
	Provide information for authorized users who need access to the Taegis Ticketing System (if applicable)	R, A	I
	Return completed survey to Sophos	R, A	I
	Provide Customer's authorized users with access to the Taegis Ticketing System (if applicable)	C, I	R, A
	Provide welcome kit to Customer	I	R, A
	Work with Sophos to determine date and time for the Planning Workshop	R, A	C, I
	Facilitate the Planning Workshop		R, A
	Ensure appropriate Customer personnel participates in the Planning Workshop	R, A	I
	Provide Customer with Proactive Consulting Services roadmap and schedule	I	R, A
	Request changes to Proactive Consulting Services roadmap and schedule through sending an email to SecurityServicesRetainer@sophos.com	R, A	C, I

2.4 Out of Scope

The information in Section 2 comprises the Sophos standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Upon request, Sophos can provide out-of-scope technical support on a time and materials basis pursuant to a separate Agreement. Sophos reserves the right to decline requests that:

- Are beyond the scope of the Service(s) described herein
- Are beyond the capability of Sophos to deliver within the contracted service levels
- Might violate legal or regulatory requirements

Customer acknowledges that payment, facilitation, or fronting of any ransom payment on behalf of Customer is out of scope for this Service. The facilitation of such ransomware payment is exclusively the obligation of Customer. If Customer needs assistance identifying a third party to facilitate and make any such ransomware payment, then Sophos may recommend a third party.

---

3 Service Fees and Related Information

Service Fees are based on the tier purchased. If Customer purchases additional Service Units and/or EIR Hours, then Customer will have additional Service Fees. See Sophos applicable Agreement for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Service Term

Billable effort for Proactive Consulting and Professional Services Engagements will be calculated using Service Units. Billable effort for EIR Engagements will be calculated on an hourly basis. Customer may stop an Engagement by providing 24-hour advance notice to stop all work against the Agreement. Notice for stop of an Engagement must be sent by email to SecurityServicesRetainer@sophos.com. See the Scheduling section above for additional information about terminating an Engagement. Notwithstanding the foregoing, Service Units and EIR Hours will not be refunded and are not transferable to Sophos services not listed in the Services Catalogs.

3.1 Invoice Commencement

See the Service-specific Addendum incorporated herein by reference at https://www.sophos.com/legal/-terms, as updated from time to time (the "Product Terms Page") or Agreement for information about invoice commencement. Provisions related to the term of the Service and payment terms within the Product Terms Page shall not apply to Customer's consumption of Services in case of purchases through a Sophos' reseller but instead shall be subject to Customer's agreement with its reseller.

3.2 Additional Service Fees and Other Information

Customer has a specified number of Service Units that are **included** (see the Table in Section 1.1, Overview), and Customer can purchase additional Service Units at any time during the Service Term if desired. In addition, Customer can purchase Emergency Incident Response Hours ("**EIR Hours**") at a pre-negotiated rate at any time during the Service Term. Additional Service Units and/or EIR hours will be co-termed with the related contract term. For multi-year contracts, co-terming will be done on an annual basis. Customer's approval for EIR Hours and Service Units shall be sent through email to SecurityServicesRetainer@sophos.com. Customer acknowledges and agrees that receipt of such email will be from a Customer representative authorized to commit Customer to the purchase of additional Service Units and/or EIR Hours and email notification is binding upon Customer. Total Fees for Service

Units are 100% billable upon Customer's approval through email. Total Fees for EIR Hours are billed monthly in arrears as hours are consumed.

Customer acknowledges and agrees that if Purchase Orders (P.O.s) are required for the transaction with Sophos to extend or add to the originally purchased service(s), then an updated P.O. will be issued to Sophos for the extended/added service(s) specified in the authorizing email within seven (7) calendar days from the date of the acknowledged receipt of the email by Sophos. If an updated P.O. is not received within 7 calendar days, then Sophos may terminate the service(s) and/or Engagement as applicable and, notwithstanding the foregoing, Customer acknowledges and agrees that it remains responsible for any additional work performed by Sophos until such P.O. is received.

3.3 Expenses

Customer agrees to reimburse Sophos, directly or indirectly (in case of purchases through an authorized reseller), for all reasonable and actual expenses incurred in conjunction with delivery of the Service.

These expenses include but are not limited to the following:

- Travel costs related to transportation, meals, and lodging to perform the Services, including travel to Customer location(s)—e.g., traveling for Engagements and the performance of **optional** onsite planning workshops. Additionally, time spent traveling to/from Customer location(s) will be billed to Customer. For Emergency Incident Response Engagements, up to eight (8) hours per travel day for each participating Sophos employee will be billed, and for Proactive Incident Response engagements two (2) Service Units will be added to the scope of the engagement for each participating Sophos employee requested by Customer to travel onsite.
- Digital media storage, Engagement-specific equipment, or licensing necessary for tailored digital forensic analysis work.
- Monthly fees for other purchased infrastructure to support service delivery (e.g., public cloud computing services) may apply, if Customer and Sophos agree that usage is necessary to complete the Engagement.

3.4 Term

The Service Term is defined in the Agreement. Any service units and/or EIR hours specified for any twelve-month period beginning on the Effective Date of the Agreement and each anniversary thereof (each twelve-month period, a "Contract Year") that are not used within such Contract Year shall be forfeited.

Upon expiration of the initial term of the Service Term, the Service Term shall automatically renew for successive periods of twelve months (each, a "Renewal Term") as outlined in the Consulting Services Addendum, unless either Party provides at least 60 days' prior written notice of its intent not to renew.

4 Service Level Agreements ("SLAs")

The tables below contain the SLAs that are applicable to each tier for the Service.

4.1 Tier 1 – Value

Service	SLA Description	Credit

Engagements for Emergency Incident Response	• **Initial Contact:** Sophos will make initial contact with Customer within four (4) hours for Customer requests regarding Emergency Incident Response submitted through the Incident Response Hotline (or Taegis Ticketing System if Customer has access and uses this system). Discussion with Customer will be scheduled to discern the nature, scope, and action plan for the request. • **Remote Support:** Sophos will commence work remotely within 24 hours of agreement on scope for EIR. Sophos effort for events deemed to be of a non-crisis nature will occur during	5 EIR Hours for each business day that the SLA is not met

Service	SLA Description	Credit
	business days with extended hours (8 AM – 8 PM based on event geographical location), as determined by Sophos. • **In-Transit to Provide On-site Support:** If mutually deemed necessary, Sophos will have personnel in-transit to Customer's location on a best effort basis. • Customer requests submitted without using the Incident Response Hotline (or Taegis Ticketing System if applicable) will be addressed on a best-effort basis and are excluded from the scope of this SLA. • Any Emergency Incident Response Engagements that are requested within the first fourteen (14) calendar days of the Effective Date of the Agreement will be addressed on a best-effort basis and are excluded from the scope of this SLA.	

4.2 Tier 2 – Base

SLA	Definition	Credit

Engagements for Emergency Incident Response	• **Initial Contact:** Sophos will make initial contact with Customer within four (4) hours for Customer requests regarding Emergency Incident Response submitted through the Incident Response Hotline (or Taegis Ticketing System if Customer has access and uses this system). Discussion with Customer will be scheduled to discern the nature, scope, and action plan for the request. • **Remote Support:** Sophos will commence work remotely within 24 hours of agreement on scope for EIR for Customer locations within the European Union ("**EU**") member states, the Schengen Area, United Kingdom ("**UK**"), and the United States of America ("**USA**"). Sophos effort for events deemed to be of a non-crisis nature will occur during business days with extended hours (8 AM-8 PM based on event geographical location), as determined by Sophos. • **On-site Support:** If mutually deemed necessary, Sophos will have personnel ***on-site*** in On-site Response Supported Locations (see the "Overview" section of this SD for an explanation of On-site Response Supported Locations) within 48 hours of agreement on scope for EIR. o For a location that is not within the On-site Response Supported Locations, Sophos will have personnel ***intransit*** to the location within 48 hours of agreement on scope for EIR, unless Sophos deems those locations unsafe. • Customer requests submitted without using the Incident Response Hotline (or Taegis Ticketing System if applicable) will be addressed on a best-effort basis and are excluded from the scope of this SLA.	5 EIR Hours for each business day that the SLA is not met
SLA	**Definition**	**Credit**
	• Any EIR Engagements that are requested within the first 14 calendar days of the Effective Date of the Agreement will be addressed on a best-effort basis and are excluded from the scope of this SLA.	

4.3 Tier 3 – Essential

SLA	Definition	Credit

Engagements for Emergency Incident Response	• **Initial Contact:** Sophos will make initial contact with Customer within two (2) hours for Customer requests regarding Emergency Incident Response submitted through the Incident Response Hotline (or Taegis Ticketing System if Customer has access and uses this system). Discussion with Customer will be scheduled to discern the nature, scope, and action plan for the request. • **Remote Support:** Sophos will commence work remotely within 12 hours of agreement on scope for EIR for Customer locations within the European Union ("**EU**") member states, the Schengen Area, United Kingdom ("**UK**"), and the United States of America ("**USA**"); and within 24 hours for other Customer locations. Sophos effort for events deemed to be of a noncrisis nature will occur during business days with extended hours (8 AM-8 PM based on event geographical location), as determined by Sophos. • **On-site Support:** If mutually deemed necessary, Sophos will have personnel ***on-site*** in On-site Response Supported Locations (see the "Overview" section of this SD for an explanation of On-site Response Supported Locations) within 36 hours of agreement on scope for EIR. o For a location that is not within the On-site Response Supported Locations, Sophos will have personnel ***in transit*** to the location within 48 hours of agreement on scope for EIR, unless Sophos deems those locations unsafe. • Customer requests submitted without using the Incident Response Hotline (or Taegis Ticketing System if applicable) will be addressed on a best-effort basis and are excluded from the scope of this SLA. • Any EIR Engagements that are requested within the first 14 calendar days of the Effective Date of the Agreement will be addressed on a best-effort basis and are excluded from the scope of this SLA.	5 EIR Hours for each business day that the SLA is not met

4.4 Tier 4 – Essential Plus

SLA	Definition	Credit

Engagements for Emergency Incident Response	• **Initial Contact:** Sophos will make initial contact with Customer within two (2) hours for Customer requests regarding Emergency Incident Response submitted through the Incident Response Hotline (or Taegis Ticketing System if Customer has access and uses this system). Discussion with Customer will be scheduled to discern the nature, scope, and action plan for the request. • **Remote Support:** Sophos will commence work remotely within 12 hours of agreement on scope for EIR for Customer locations within the European Union ("**EU**") member states, the Schengen Area, United Kingdom ("**UK**"), and the United States of America ("**USA**"); and within 24 hours for other Customer locations. Sophos effort for events deemed to be of a noncrisis nature will occur during business days with extended hours (8 AM-8 PM based on event geographical location), as determined by Sophos. • **On-site Support:** If mutually deemed necessary, Sophos will have personnel ***on-site*** in On-site Response Supported Locations (see the "Overview" section of this SD for an explanation of On-site Response Supported Locations) within 36 hours of agreement on scope for EIR. o For a location that is not within the On-site Response Supported Locations, Sophos will have personnel ***in transit*** to the location within 48 hours of agreement on scope for EIR, unless Sophos deems those locations unsafe. • Customer requests submitted without using the Incident Response Hotline (or Taegis Ticketing System if applicable) will be addressed on a best-effort basis and are excluded from the scope of this SLA. • Any EIR Engagements that are requested within the first 14 calendar days of the Effective Date of the Agreement will be addressed on a best-effort basis and are excluded from the scope of this SLA.	5 EIR Hours for each business day that the SLA is not met

The SLAs set forth above are subject to the following limitations:

- The SLAs shall not apply if any act or omission by Customer prohibits or otherwise limits Sophos from providing the Service or meeting the SLAs, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information.
- The SLAs shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD.

For Customer to receive an SLA credit, subject to the limitations above, the notification of the SLA failure must be submitted to Sophos within thirty (30) days of the date of such SLA failure. Sophos will research the notification and respond to Customer within thirty (30) days from the date such notification is received. The total amount credited to Customer in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. The foregoing SLA credit(s) shall be Customer's sole and exclusive remedy for failure to meet or exceed the foregoing SLAs.

5 Additional Terms

5.1 On-site Services

Notwithstanding Sophos' employees' placement at Customer's location(s), Sophos retains the right to control the work of such employees. For international travel, on-site Services may require additional documentation, such as visas, visitor invitations, and related documentation, which may affect timing of the Services and reimbursable expenses.

5.2 Security Services

Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding Customer's systems and accepts those risks and consequences. Customer hereby consents and authorizes Sophos to provide any or all of the Security Services with respect to Customer's systems. Customer further acknowledges that it is Customer's responsibility to restore network computer systems to a secure configuration after Sophos completes testing.

5.3 Record Retention

Sophos will retain a copy of the Customer Reports or recordings of any training sessions or workshops provided to Customer in accordance with Sophos' record retention policy. Unless Customer gives Sophos written notice to the contrary prior thereto and subject to the provisions of the applicable Agreement and DPA, all Customer Data collected during the Services and stored by Sophos will be deleted within 30 days from issuance of the final Customer Report. If Customer or its authorized agent requests that Sophos retain Customer Data for longer than its standard retention policy, Customer shall pay Sophos' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Sophos shall be entitled to retain Customer Data as necessary to comply with its own legal, regulatory, judicial, audit, or internal compliance requirements.

5.4 Sophos Proprietary Rights

As between Customer and Sophos, Sophos will own all right, title and interest in and to the Service and Sophos Materials used for the delivery of the Service, including any recordings of the deliverables hereunder. Sophos does not transfer or convey to Customer or any third party, any right, title or interest in or to the Service or any associated IP rights, but only a limited right of use as granted in and revocable in accordance with the applicable Agreement. Any copies of the Service's presentation's recordings and related materials provided to Customer upon request represent Sophos Materials and are subject to copyright.

5.5 No Reproduction of Sophos Materials

No part of Sophos Materials may be reproduced or distributed to the public or press or reproduced or transmitted by the Customer or any of its personnel in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without the express written permission of Sophos. Each of Customer's personnel who has received a copy of the Service's presentation and related materials or viewed a recording of such presentation is deemed to have agreed not to reproduce or distribute such Sophos Materials, in whole or in part, without the prior written consent of Sophos.

5.6 No Reliance by Third Parties

The Service's presentation and all information and any documents in any oral, hardcopy or electronic form has been prepared specifically for Customer in connection with the Service and is subject to Sophos' ownership in any Sophos Materials. Sophos disclaims all liability for any damages whatsoever to any unaffiliated third party arising from or related to its reliance on such presentation or any contents thereof.

5.7 Compliance Services

Customer understands that, although Sophos' Services may discuss or relate to legal issues, Sophos does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Sophos in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

5.8 Post-Engagement Activities

Subject to any applicable legal or regulatory requirements, thirty (30) days after the completed delivery of the Service, Sophos will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Sophos in the performance of the Services hereunder (the "**Engagement Media**"). Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Sophos shall, in its sole discretion, dispose of the Engagement Media on or after the engagement conclusion and only maintain a copy of the completed engagement-specific deliverables.

5.9 Legal Proceedings

If Customer knows or has reason to believe that Sophos or its employees performing Services under this Service have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require Sophos or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Sophos, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Sophos for (a) its employees' time spent as to such response, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and Sophos as to the Service.

5.10 Endpoint Assessment

Unless otherwise agreed upon in writing, if a software agent has been deployed as part of an Engagement, within thirty (30) days following the date of the Completed Final Report (the "**Thirty Day Period**"), Customer shall uninstall any and all copies of the software agent used for the Engagement. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Sophos' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Sophos from the software agent. Customer will uninstall the software agent as described in this Service.

6 Glossary

Term	Definition

Service Level Agreement (“**SLA**”)	A legally-binding arrangement to meet defined standards for the Service.
Taegis Ticketing System	The system within the Sophos Taegis platform that Customer can use to submit requests as related to the Service if Customer has an active license for Taegis platform.