Sophos Red Team Exercise – Full Spectrum Service – Service Description

This Service Description describes Sophos Red Team Exercise – Full Spectrum Service ("**Service**"). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined 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

The Service is delivered by Sophos Red Team and challenges Customer's organization's capabilities to detect, prevent, and respond to an unknown, sophisticated threat actor with specific goals and objectives that are tailored to Customer's environment and a realistic threat model. The Sophos Red Team adopts customized tooling and techniques as needed to assume the role of a unique threat actor. Through simulating a realistic attack by a unique adversary with non-attributable tactics, techniques, and procedures, the objectives of the Exercise are as follows:

- Identify deficiencies in security controls and alerting mechanisms that could allow a threat actor to pursue their goals without detection.
- Train Customer's defenders to recognize indicators of compromise from unknown threats.
- Test assumptions about detection and prevention against tactics and techniques that require deeper drilling into attack primitives.

1.2 Customer Obligations

Customer will perform the standard obligations listed below, and acknowledges and agrees that the ability of Sophos to perform the Service is contingent upon the following:

- Customer personnel are scheduled and available to assist as required for the Service(s).
- 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.

- This service is delivered remotely, but exceptions can be requested. Sophos will evaluate these requests, and if approved for on-site activities, Customer will provide a suitable workspace for Sophos personnel, and necessary access to systems, network, and devices. Sophos reserves the right to deny any and all on-site travel requests.
- 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 initiating the Service.
- Customer will prepare or assign a dedicated system and user to be used for the assumed breach phase of the engagement. This system must be domain joined if within an active directory environment or have VPN connectivity where applicable if it is part of a decentralized environment. Additionally, the user that is created or assigned should be one that is indicative of a typical employee or role within the organization and have realistic permissions for the environment.
- In the event that Exercise activities are discovered, Customer will inform personnel and third parties of Exercise activities immediately, in order to halt any actions that could cause harm or disruption to Sophos business activities outside of the Exercise. This includes, but is not limited to, takedown requests and Internet Service Provider (ISP) blacklisting.

In case physical testing or wireless testing components have been added to the Service, additional obligations apply to the Customer:

- Customer will inform all relevant law enforcement (e.g., county sheriff, municipal and state police, local FBI office) of activities prior to the start of work for the Exercise, and any private security not controlled by or paid for by Customer.
- Customer will complete and return the authorization letter, commonly called a "get out of jail letter," prior to start of the Exercise. Customer must always be available by phone during the Exercise to respond to security and law enforcement queries regarding the Exercise.
- Customer's failure to retrieve and return all equipment (i.e., Red Team Exercise drop boxes, Wireless Remote Testing Appliance ("RTA"), and any other Sophos-provided devices attached to a network to perform the Exercise) to Sophos within two (2) weeks of the issuance of the Final Report will incur a $1,000 replacement fee per item of equipment. Sophos will provide a detailed description of the location of the equipment, if applicable, upon completion of the Exercise.
- For wireless testing, Customer will accept shipment of a Wireless RTA and install it in a location that is suitable for wireless testing.

1.3 Scheduling

Sophos will contact a Customer-designated representative within five (5) business days after the execution of a Agreement to begin the Service Initiation activities described herein. These activities will ensure effective and efficient use of the Service.

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 downtime windows, Customer deliverable deadlines, and other Customer scheduling requests. Written confirmation of an agreed-upon schedule shall constitute formal acceptance of such schedule.

If an exception for on-site work is approved, and 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.

1.4 Timeline

- Remote work will occur Monday – Friday, 8 a.m. – 6 p.m. US Eastern time.
- Approved on-site work will be performed Monday – Friday, 8 a.m. – 6 p.m. Customer's local time or similar daytime working hours.
- To simulate real-world threat actors, goal-based testing, such as Penetration Tests and Red Team Tests, can occur at any time, within the testing dates, at Sophos' discretion.
- Work performed outside of the hours listed above, as requested or required by Customer, will incur additional service charges.

2 Service Details

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

2.1 Service Initiation

The rules of engagement for the Service are established during staging and introductory sessions. Items to be discussed include the following:

- Goals and objectives for the Exercise
- Definition of scope and validation of targets
- Rules of engagement, levels of effort, and risk acceptance
- Timelines and schedules for the Exercise
- Requirements, timelines, and milestones for reporting
- Key personnel, roles and responsibilities, and emergency planning
- Tools and techniques
- Assumed breach scenario planning

After the introductory teleconference, Sophos will send a confirmation email to ensure agreement on the above-listed items.

In the event that Sophos RTA (as defined above) is used for the Exercise, a member of the Sophos team will be involved between the initial session(s) and the start of the Exercise to help Customer complete any configuration tasks needed for exercise readiness.

If all pre-exercise tasks are not completed two (2) weeks before the Exercise is scheduled to begin, the Exercise will be rescheduled for a later date.

2.2 Service Scope

While the Service is largely geared towards organizations with a moderate amount of security maturity, Sophos offers two tiers for the Exercise to better help train defenders regardless of Customer's current level of security maturity. This allows for scalable sophistication as well as an option to focus only on the internal network from a post-breach context for organizations who are more interested in examining detection, prevention, and response capabilities from this standpoint only.

The following describes the differences between the two tiers:

- **Standard Tier** - Takes place over four (4) weeks and examines the detection, prevention, and response capabilities of Customer's organization covering all phases of an attack starting from an assessment of perimeter assets and external footprint, social engineering campaigns for initial access, and ultimately moving to the internal network where consultants will aim to act on goals and objectives established during a pre-engagement kickoff meeting.
- **Lite Tier** - Designed for organizations that are less concerned with their perimeter and social engineering defenses and who primarily would like to test assumptions about detection, prevention, and response capabilities for activity within the internal network. The Lite version of the Service takes place over two (2) weeks from an assumed breach context, such as starting from a compromised endpoint or compromised credentials through a VPN or virtual desktop environment.

Customer may also request the following add-ons to the Service (for an additional fee):

- Social Engineering: Phishing (Additional 2 weeks)
- Physical Testing (Additional 2 weeks)
- Wireless Testing (Additional 1 week)

Additional time in increments of one (1) week can be added to the exercise for an additional fee. Extra time will be a requirement if the goals and objectives of the exercise warrant additional time as determined during a scoping call.

Due to the unique nature of physical testing, additional scoping will be required. This includes a scoping teleconference with a member of the Sophos physical security testing team, and additional legal protections for both Customer and Sophos.

Sophos will execute the scope per Customer's requirements as outlined in an Agreement.

2.3 Service Methodology

The Service is conducted following each tactical phase of the MITRE ATT&CK framework using a combination of proprietary, commercial, and open-source tools to ensure a complete assessment of detection, prevention, and response capabilities.

The exercise methodology is summarized below:

Reconnaissance

During this phase, information is collected from public and compromised data sources by performing network probing, and by physical observation of target locations if applicable. In a process known as open-source intelligence gathering, Sophos uses commercial, open source, and proprietary tools to search public information sources for information about Customer. Sophos testers seek to identify assets that are associated with an organization, particularly those that an attacker may choose to exploit.

Reconnaissance often includes researching employee names and contact information, performing nonaggressive use of public services, and reviewing compromised documents. If on-site testing is in-

scope, then Sophos will also observe wireless traffic, and surveil employee activity from outside a Customer's property during this phase.

Examples of reconnaissance that are usually part of any Red Team Exercise - Full Spectrum include the following:

- Discovering networks owned by Customer
- Discovering types of hardware and software used within the organization
- Identifying personnel within target organization who may have sensitive information
- If on-site testing is in-scope, as described in the Scope section herein:
  - Reviewing aerial photographs of physical locations
  - Observing building security and personnel behavior at physical locations
  - Passively monitoring wireless networks

Planning and Preparation

Collected data is analyzed and potential vulnerabilities are mapped during planning and preparation. Interactions with the Service become more aggressive, though the goal is eliciting additional information, not exploiting vulnerabilities. Vulnerabilities are evaluated for their likelihood of success, risk of detection, and efficacy in furthering the objectives of the Exercise.

Specific to the external network perimeter, Sophos will explore hosts to look for potentially exploitable vulnerabilities. This type of vulnerability discovery may use automated scanning on a limited basis where it is most appropriate, but most work will be manual.

Sophos selects the most appropriate vulnerabilities and develops attack plans to exploit them, with the types of attacks chosen being dependent on the scope and objectives of the engagement.

Preparation includes network attacks, social engineering, and physical attacks, such as the following:

- Checking application versions to confirm vulnerability
- Cracking collected password hashes and preparing compromised authentication tokens
- Developing exploit methods for hardware and software
- If on-site testing is in-scope as indicated in the Scope section above, then the following is also part of preparation:
  - Identifying the building entry points and selecting techniques for bypassing controls
  - Customizing drop boxes and workstation-compromising payloads

Perimeter Breach

As the first step of compromise is bypassing the security perimeter, network, physical, or social vulnerabilities must be exploited according to the plans established in earlier phases. Successful exploitation yields privileged information, provides control of a target system, or grants access to a restricted area. Exploits are combined and cross-delivered, such as when a social engineering attack leads to the compromise of a workstation behind the perimeter firewall, providing a path for the remote tester's access to the internal network for further attacks.

Examples of attacks in this phase include:

- Exploiting a vulnerability on an internet-facing service to obtain control of the host server
- Using cracked passwords to gain control of new systems

- If the social engineering addon is purchased:
    - Asking a Customer's employee to perform tasks that compromise the target environment
    - Impersonating Customer-trusted individuals, such as its contractors and partners
- If on-site testing is in-scope, as described in the Scope section herein:
    - Bypassing physical security controls and entering sensitive areas inside the target environment

Phishing and Vishing (If included as an add-on)

Phishing and Vishing, as employed in the Service, differs significantly in content and delivery methods than the mass-distributed phishing common with Security Awareness Training. While phishing attempts may include the delivery of bulk messages or phone calls using general enticement, the approach for phishing during the Exercise focuses on highly specific social engineering attacks, potentially using personal information about the targets that was gathered during the OSINT phase.

Successful phishing and vishing attacks result in information useful for additional attacks, the collection of user passwords, or execution of malicious code that provides a temporary access point into Customer's internal network to enable attacks.

Physical Testing (if included in an Agreement)

Physical testing takes the form of active social engineering, passive social engineering, and physical control bypass. Active social engineering involves testers engaging with target individuals to gain specific information or access. Passive testing focuses on avoiding interaction while utilizing employees' normal actions to access and remain inside sensitive areas. Physical perimeter bypass makes use of tools and techniques designed to leverage flaws in physical control installation, design, or configuration.

Sophos uses all three forms of physical testing to access the targeted physical locations. Once testers breach physical security, they collect information for additional attacks, attach hardware to the network to provide a backdoor for remote testers, and leverage individual workstations, servers, and infrastructure to launch additional exploits.

Wireless Testing (if included in an Agreement)

During wireless security testing, Sophos will perform the following tasks:

- Run tests against the wireless access points
- Run tests against the wireless clients
- Attempt to bypass encryption usage and configuration
- Attempt to bypass overall security controls and gain access to a non-public network

Sophos uses a structured and iterative process, testing the network architecture, systems configurations, processes, and procedures that affect the ability to protect Customer's wireless assets from unauthorized access.

Sophos will attempt to detect, analyze, and compromise Customer's wireless networks.
Sophos will use wireless-specific security tools, such as Net Stumbler the Aircrack suite, Kismet, InSSIDer, etc. If the testers are successful in compromising the wireless network, they will then document the findings and provide information on how the compromise occurred.

Wireless clients are a critical part of the security of a wireless network; however, these clients are often overlooked during testing. Sophos will establish rogue access points and attempt to coerce clients to attach, to demonstrate the ability of an attacker to compromise laptops and other devices that connect to the wireless network.

Internal Access

Once breaching the perimeter and establishing a foothold, Sophos will attempt to set up persistence within the environment followed by lateral movement to other systems and resources to discover paths to escalate privileges which facilitate accomplishing goals and objectives.

As the exercise is constrained by time limitations unlike true adversaries, if Sophos is unable to find a way to breach the perimeter through exploitation or social engineering in a pre-determined timeframe, an assumed breach model will be adopted to progress the exercise to the internal access phase. The assumed breach scenario can be decided during the kickoff meeting scheduled well in advance of start of the engagement, and there are several potential options such as endpoint compromise with command-and-control malware or credential compromise with VPN access.

Follow-through on Goals and Objectives

After expanding influence in the target environment through lateral movement and privilege escalation, adversaries will begin to act on their goals and objectives. Sophos will attempt to covertly achieve the goals and objectives that were established prior to the exercise. This includes attaining intellectual property, exfiltrating sensitive data, compromising and subsequently poisoning development operations pipeline, and other objectives for which an adversary would target Customer's organization.

The exercise assesses whether current security controls and personnel can mitigate and evict adversaries before they are able to follow-through on their goals and objectives. If Sophos consultants are successfully evicted from the environment, as opposed to using the remaining time attempting to re-gain access, it is encouraged to proceed into a phase that only monitors subsequent activities to gain a full picture of the latter portions of the kill chain, and to identify potential security gaps.

2.4 Service Delivery

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

2.4.1 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 remotely from a secure location or, if an exception has been approved then from the Customer's site(s).

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.

2.4.2 Deliverables

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

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Red Team Exercise - Full Spectrum	Final Report	Upon completion of the Exercise	Email

2.4.2.1 Final Report

Presentation of findings and deliverables compiled by Sophos in the performance of the Service(s) are tailored to work performed, and to Customer's needs.

A report generally contain:

- Executive summary
- Methods, detailed findings, narratives and recommendations if any •
  Attachments as needed for relevant details and supporting data

During the three (3) weeks after delivering the Service, the Sophos Technical Quality Assurance ("TQA") process for reporting may require validation and investigation of issues raised in a report. This will result in a small amount of testing outside the primary testing interval that will stop prior to delivery of the report. At the end of the TQA process, Sophos will issue a formal report to the Customer-designated point of contact.

Customer shall have one (1) week from delivery of the report to provide comments to be included in the final report. If there are no comments received from Customer before expiration of the review period, the report will be deemed final ("Final Report").

Upon completion of the Service, the Customer-designated contact will receive a secure/encrypted email confirmation from Sophos. Unless otherwise notified in writing to the contrary by Customer-designated contact, within five (5) business days of such email confirmation, the Service shall be deemed complete.

2.5 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

3 Service Fees and Related Information

See Sophos applicable Agreement for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses

- Services Term

3.1 Invoice Commencement

See the Service-specific Addendum incorporated herein by reference at https://www.sophos.com/legal, 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 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 fees related to transportation, meals, and lodging to perform the Services, including travel to Customer location(s)
- Digital media storage, specific equipment necessary for delivering the Service, 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 Service delivery.

3.3 Term

The term of the Service is defined in the Agreement. Service will expire according to the Agreement provided that, if there is currently an in-progress delivery of the Service at the time of expiration, then the term shall automatically extend and expire upon completion of such in-progress delivery of the Service. During such extended term (if applicable), the terms and conditions of the Agreemeshall be in full force and effect.

4 Additional Terms

4.1 For Approved 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.

4.2 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.

4.3 Record Retention

Sophos will retain a copy of the Customer Reports 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.

4.4 Proprietary IP Termination Right

Sophos shall have the right to terminate the provision of Service(s) to Customer under an Agreement with immediate effect in regard to any specific country or jurisdiction upon written notice to Customer in the event that the specific country or jurisdiction demands access to any Sophos proprietary or confidential data, information, software or other material, including, without limitation, information relating to Customer or other Sophos customers, Sophos IP, technology, code, cryptographic keys or access to encrypted material, trade secrets or security process secrets. Sophos and Customer shall negotiate toward an agreement on reduction of future payments due to reduction in these Service(s). The Agreement and the Agreement and other Products purchased by
Customer from Sophos, directly or indirectly, shall continue in jurisdictions unaffected by Sophos exercise of this right.

4.5 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.

4.6 Post-Engagement Activities

Subject to any applicable legal or regulatory requirements, thirty (30) days after completing 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 prior to such commencement, Customer has specified in writing to Sophos any special requirements for Sophos to return such Engagement Media (at Customer's sole expense). Upon Customer's request, Sophos will provide options for the transfer to Customer of Engagement Media and the related costs thereto. If so requested, Sophos will provide a confirmation letter to Customer addressing completion and scope of these post engagement activities, in Sophos' standard form. 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.

4.7 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.

4.8 Endpoint Assessment

Unless otherwise agreed upon in writing, if a software agent has been deployed as part of the Service, 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 Service. 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.