Sophos Purple Team Exercise Service – Service Description

This Service Description describes Purple Team Exercise 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 allows your defenders to experience live-fire information security exercises designed to mimic real-world threat scenarios. Customer defends and/or hunts in Customer's own network, using its own tooling, against a live attack while maintaining a real-time, constant communication channel with the Sophos Red Team.

The Exercise is for organizations with established security monitoring, either in-house or third-party monitoring services that want to test assumptions about current detection, prevention, and response capabilities against common tactics, techniques, and procedures ("TTPs") of modern threat actors.

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.
- 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.

For cases where a Remote Testing Appliance (“RTA”) is necessary:

- Customer will provide a suitable hypervisor, outbound connectivity, and access to technical personnel for troubleshooting.
- Customer will assist with proper placement of the RTA virtual hosts and provide the necessary network connectivity to enable Service delivery.
- Customer will securely remove any RTA virtual hosts upon completion of the Service.
- For cases where a Customer’s dedicated endpoint system is necessary:
- Customer will provision a suitable non-production endpoint system, either laptop or Virtual Desktop Infrastructure (“VDI”) that is a good representation of Customer’s user endpoint systems.
- Customer will assist with proper placement of the dedicated endpoint system and ensure it has the necessary network connectivity to enable Service delivery.

1.3 Scheduling

Sophos will contact a Customer-designated representative within five (5) business days after the execution of an 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.

1.4 Timeline

- Remote work will occur Monday – Friday, 8 a.m. – 6 p.m. US Eastern time.
- For the purple team exercise, collaborative testing will be conducted at the start of the designated testing period. All activities will be executed in coordination with Blue Team members, and every action taken during the exercise will be openly communicated and broadcast in real time.
- 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

The real-time communication channel established during the introductory teleconference will be used during the Service delivery to relay information between Customer's Blue Team and Sophos Red Team members.

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

The Service is available in the following tier:

- **Standard -** The Purple Team Exercise allows organizations time to interact with the Red Team over the course of five (5) days. This exercise spreads out playbook tasks to give defenders ample time to hunt and validate detection and alerting capabilities, as well as communicate with the Red Team in real-time during activities to ask questions and discuss how to improve detection and alerting.

  One or more of the following playbooks can be selected:

  - Internal & Active Directory Exercise
  - Command and Control ("C2") Detonation and Network Detection Exercise
  - Ransomware Group Emulation Exercise
  - Cloud Compromise Exercise

Each exercise is based on common scenarios that emulate real-world TTPs with a goal of providing actionable events for the defenders so they can identify visibility deficiencies within security controls, and work with our consultants to improve detection capabilities.

Standard Purple Team exercises include **one built-in retesting day**, typically used to validate new or updated detections against **individual actions** performed during the exercise. This retest day focuses on confirming that specific visibility gaps identified earlier in the week have been addressed.

The optional **Post-Remediation Exercise Replay** add-on, however, is a **full playbook re-run**. When purchased, Sophos conducts a complete end-to-end replay of the entire exercise at a later scheduled date to ensure that all implemented remediations, detections, and security control improvements perform effectively across the full attack sequence, not just individual test actions.

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

2.3 Service Methodology

For each Exercise, Sophos will use pre-planned playbooks to provide actionable events for Customer's Blue Team to use to test detection and response capabilities. Activities and actions will be shared with Customer in advance so Customer's Blue Team is completely aware of what they should see during the Exercise. The value in the Exercise is not to fully execute as an attacker or Red Team engagement and thus, a grey box approach will be used.

Internal and Active Directory Testing Exercise:

This playbook is for testing detection of actionable events commonly employed by threat actors once an initial foothold has been established on the internal network. This activity includes the following actions against domain joined systems and services:

- Port Scanning - Internal - Top 5000 ports (TCP)
- Multicast/Broadcast Name Resolution Poisoning
- Discover Domain Controllers
- NetBIOS Null Session Enumeration
- Kerbrute - User Enumeration
- Internal Password Spraying (Kerberos)
- Internal Password Spraying (SMB)
- Group Policy Preferences Password Hunting
- LDAP User enumeration
- LDAP Domain enumeration
- Kerberoasting activity
- AS-REP roasting activity
- NTLM Relay attacks:
    - SMB Relay
    - LDAP Relay
- NTLMv1 Downgrade Attack
- Endpoint detection of BloodHound tooling
- Local Security Authority Subsystem Service (LSASS) dumping (Task Manager)
- Local Security Authority Subsystem Service (LSASS) dumping (Mimikatz)
- Disabling of endpoint protections (AV/EDR)
- Local Security Authority (LSA) Registry dumping
- Security Account Manager (SAM) dumping
- Pass-The-Hash (PTH)
- Network based Common Vulnerabilities and Exposure (CVE) exploit activity:
    - MS17-010 ETERNALBLUE
    - ZeroLogon (CVE-2020-1472)
    - PrintNightmare (CVE-2021-34527)
    - NoPAC (CVE-2021-42278 and CVE-2021-42287)
    - Log4Shell (CVE-2021-44228)
- Active Directory Certificate Services Privilege Escalation:
    - ESC1
    - ESC2
    - ESC3
    - ESC4
    - ESC6
    - ESC8

- Web-based Common Vulnerabilities and Exposure (CVE) exploit activity:
    - Tomcat default credentials
    - MS-SQL default credentials
- Share Searching
- NTDS.dit Database Dumping

Command and Control (C2) Detonation and Network Detection Exercise:

This playbook is for testing the disk-level, execution, and network activity detection within your environment for common Command and Control frameworks at various levels of sophistication. This playbook includes the following frameworks and sophistication levels:

Command and control (C2) frameworks:

- Metasploit Meterpreter
- Sliver
- Cobalt Strike

Sophistication levels:

Level 1:

- Out-of-the-box binary
- No AV/EDR execution evasion
- Unencrypted communications to newly registered domain

Level 2:

- Microsoft MSBuild Project file
- Microsoft MSBuild AV/EDR execution evasion
- Encrypted communications using self-signed certificates to categorized domain

Level 3:

- Legitimate EXE with malicious DLL
- DLL Side-loading AV/EDR execution evasion
- Encrypted communications using legitimate certificates to categorized domains

Ransomware Group Emulation Exercise:

This playbook aims to test detection of Ransomware group activity on an endpoint system and within the network. 100 Simulated sensitive data files are provided that are deployed on a provisioned endpoint system and network share. In addition, a simulated encryption operation is performed over the network to a dedicated endpoint in a safe and controlled manner.

This exercise includes the following actions:

- Ransomware Command and Control - On Disk Detection
- Ransomware Command and Control - Execution Detection
- Ransomware Command and Control - Network Detection
- Scheduled Task Persistence
- Create Local Admin Accounts
- Account Discovery: Domain Accounts (Net Group)

- Account Discovery: Domain Accounts (ReconAD)
- Domain Trust Discovery
- System Network Configuration Discovery
- Network Service Scanning – 5 TCP Ports
- Network Share Discovery
- Disable Endpoint Defenses ○ Disable EDR/AV
- Disable Microsoft Defender via Powershell
- Credential Harvesting (ps-exec)
- Credential Harvesting (mimikatz)
- Kerberoasting
- Ransomware Payload - On Disk Detection
- Ransomware Payload - Execution Detection
- Ransomware Payload - Encryption Detection
- Ransomware Payload – Decryption

Cloud Compromise Exercise (for Azure Cloud):

This playbook is for testing detection of threat actor activity for attempting to breach, escalate privileges, and steal data from the Azure Cloud, including the following actions against target in-scope services:

- Azure recon activity
- Password spraying and brute-force activity
- Compromised credential checks
- Azure data collection
- Azure infrastructure sweeping of MFA protected assets
- Azure privilege escalation tests
- Data exfiltration through multiple Azure avenues

Post-Remediation Exercise Replay (if included in the Agreement):

During the Exercise, Customer may identify and remediate visibility gaps within existing security controls. If the Post-Remediation Exercise Replay add-on (“Replay”) is purchased, then Sophos will perform a replay of the entire in-scope Exercise to validate that any newly added remediations are working as expected.

The Replay can be scheduled at a later date within 180 days of completion of the Exercise and does not need to occur concurrently with the Exercise. The Replay requires a minimum of four (4) weeks of advance notification to schedule.

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
Purple Team Exercise	Final Report	Upon completion of the exercise	Email

2.4.2.1 Final Report

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

Reports generally include the following components:

- Executive Summary

- Technical Overview
- Actions Timeline
- Detection and Response Results Table, outlining outcomes from both Red and Blue Teams
- Recommendations, including:
    - Network Security Recommendations
    - Vulnerability Remediation Recommendations
    - Detection Gap Recommendations
- Actions Tables provide clear detail on actions performed, associated timestamps, commands executed, observed results, and corresponding MITRE ATT&CK mappings.
- For select playbooks, a separate Detection Guidance document is also provided to assist the Customer in tuning settings and controls to address identified detection gaps.

Sophos 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 the 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.

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 Agreement shall 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 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.

4.5 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.

4.6 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.

4.7 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.