Secureworks®

SERVICE DESCRIPTION

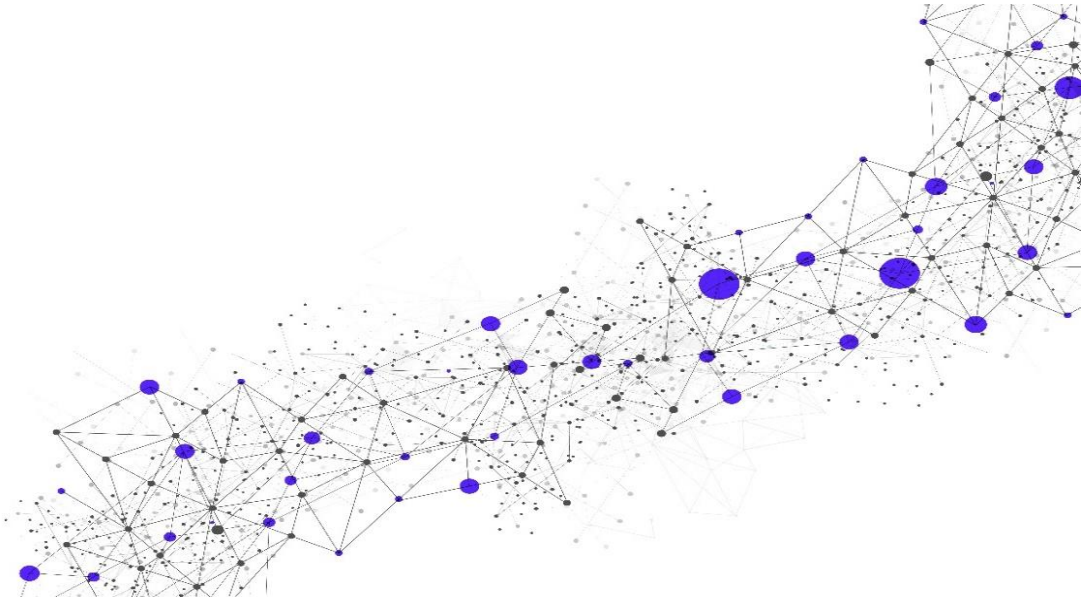
Adversary Emulation Exercise

Release Date

February 26, 2024

Version

4.3



www.secureworks.com

Global Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

Table of Contents

1 Service Introduction

This Service Description ("**SD**") describes the Adversary Emulation Exercise Service ("**Service**" or "**Exercise**"). All capitalized words and phrases shall have the meanings set forth herein, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement for direct or indirect purchases (individually referenced herein as "**CRA**"), that is incorporated herein by reference. For avoidance of doubt, the CRA available at www.secureworks.com/eula (or at www.secureworks.jp/eula-jp for Customers located in Japan) applies to Customer's purchases through an authorized Secureworks' reseller.

1.1 Overview

The Service uses threat intelligence to challenge Customer's organization's capabilities to detect, prevent, and respond to a defined threat actor that is known to target Customer's organization's industry.

Through emulating the tactics, techniques, and procedures ("TTPs") of the specific threat actor, the objectives of the exercise are as follows:

- Identify deficiencies in security controls and alerting that could allow the defined threat actor to act on their goals and objectives unimpeded.
- Train Customer's defenders to become familiar with and spot indicators of compromise from known threats and common TTPs.

1.2 Customer Obligations

Customer will perform the standard obligations listed below, and acknowledges and agrees that the ability of Secureworks 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 Secureworks, to permit Secureworks 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. Secureworks will evaluate these requests, and if approved for on-site activities, Customer will provide a suitable workspace for Secureworks personnel, and necessary access to systems, network, and devices. Secureworks 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 Secureworks to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Secureworks testing activities as needed, to prevent disruption to Secureworks business and performance of the Service (e.g., takedown requests, ISP deny list).
- Customer will provide to Secureworks all required information (key personnel contact information, credentials, and related information) at least two (2) weeks before initiating the Service.
- Customer's failure to retrieve and return all equipment (i.e., Adversary Emulation Exercise drop boxes, Wireless Remote Testing Appliance ("RTA"), and any other Secureworks-provided devices attached to a network to perform the Exercise) to Secureworks within two (2) weeks of the issuance of the Final Report will incur a $1,000 replacement fee per item of equipment.

Secureworks will provide a detailed description of the location of the equipment, if applicable, upon completion of the Exercise.

- 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.

1.3 Scheduling

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

Secureworks 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 Secureworks.

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 Secureworks' 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

- Emulation scenario planning

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

In the event that Secureworks RTA (as defined above) is used for the Exercise, a member of the Secureworks 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

Secureworks offers two tiers for the Exercise which allow organizations to focus on either a full spectrum of emulated threats through each phase of a cyber-attack or purely on the internal network from a post-breach context.

The following describes the differences between the two tiers:

- **Standard Tier** - Lasts 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 Exercise 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.
- 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.
-

Secureworks will execute the scope per Customer's requirements as outlined in a Transaction Document.

2.3 Service Methodology

The Exercise is conducted following each tactical phase of the MITRE ATT&CK framework and is in alignment with methodologies such as TIBER, CBEST, and iCAST, using a combination of proprietary, commercial, and open-source tools to ensure a complete assessment of detection, prevention, and response capabilities.

The phases of the Exercise are described in the subsections below.

Threat Intelligence Gathering

Secureworks begins by performing research via public sources, as well as leveraging information from the Secureworks Counter Threat Unit (CTU), for threat intelligence data to select an applicable real-world adversary which can be emulated for the Exercise.

Scenario Planning and Preparation

The data collected during the threat intelligence gathering phase is analyzed and used to develop an attack scenario that mimics the TTPs of the defined threat actor. Goals and objectives are appropriately formulated to match the adversary's motives.

Consultants will discuss the proposed scenario prior to the start of active operations to establish scope and any preparations needed to properly execute the Exercise.

Scenario Execution

Once the scenario is finalized and the TTPs are mapped out for emulation, execution of the plan begins. The subsections below explain the typical flow of activities for the Exercise.

Reconnaissance:

Reconnaissance often includes researching employee names and contact information, performing non-aggressive use of public services, and reviewing compromised documents via open-source intelligence ("OSINT") gathering. If on-site work is in-scope, Secureworks will also observe wireless traffic, and surveil employee activity from outside a customer property during this phase. Active reconnaissance is also performed to analyze exposed assets, resources, and services.

Examples of reconnaissance that are usually part of any Exercise include the following:

- Discovering networks owned by Customer
- Discovering exposed services and resources
- Discovering types of hardware and software used within the organization
- Identifying personnel within target organization who may have sensitive information

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
- Impersonating Customer-trusted individuals, such as its contractors and partners
- Asking a Customer's employee to perform tasks that compromise the target environment

Phishing and Vishing:

Phishing and Vishing, as employed in the Exercise, 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.

Execution and Follow-through on Goals and Objectives:

Immediately after bypassing the perimeter and gaining control of Customer's systems, Secureworks secures the stability of compromised hosts. The hosts are configured to provide persistence, maintaining a command-and-control channel with Secureworks.

After gaining persistent access, and ideally elevated privilege access, to a device on the target network, covert attack methods are performed to move toward the Service goals. Initially, low impact network monitoring is performed with the intent of obtaining additional network credentials and network information. Upon locating systems where compromised credentials are observed to be accepted, Secureworks will traverse the network and attempt to compromise that system. Once access to the new system has been obtained, the system is reviewed for critical information toward the Service goals and may be compromised if doing so leads to the goals. This process is repeated until the Service objectives and goals are achieved.

Assumed Breach:

Real world threat actors are typically not constrained by time limitations when planning attacks, and they are able to spend their time persistently exploring the perimeter and developing intricate social engineering ruses to gain initial access. As the Exercise is limited in time, to fully assess the detection, prevention, and response capabilities of Customer, an assumed breach model is used when the perimeter cannot be breached naturally, or if significant enough access is not gained to fully assess internal security controls.

The assumed breach is performed by Customer executing a customized payload to simulate situations such as a successful phishing campaign, the use of software which has been maliciously modified due to supply chain compromise, or direct access to internal systems to simulate a successful credential capture campaign or using leaked data. Any security solutions, such as EDRs and antivirus, should remain active to fully assess the efficacy of security controls.

2.4 Service Delivery

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

2.4.1 Delivery Coordination

Secureworks 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 Secureworks 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)

Secureworks solely reserves the right to refuse to travel to locations deemed unsafe by Secureworks or locations that would require a forced intellectual property transfer by Secureworks. Secureworks solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Secureworks. Customer will be notified at the time that services are requested if Secureworks refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Secureworks travel is arranged. In the event any quarantines, restrictions, or measures imposed by governmental authority or Secureworks restrict travel to any location, Secureworks 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, Secureworks 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. Secureworks will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Adversary Emulation Exercise	Final Report	Upon completion of the Exercise	Email

2.4.2.1 Final Report

Presentation of findings and deliverables compiled by Secureworks 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 Secureworks 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 a report. At the end of the TQA process, Secureworks 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 Secureworks. 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 Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Upon request, Secureworks

can provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document. Secureworks reserves the right to decline requests that:

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

3 Service Fees and Related Information

See Secureworks applicable CRA and Transaction Document 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.secureworks.com/legal/product-terms, as updated from time to time (the "Product Terms Page") or Transaction Document 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 Secureworks' reseller but instead shall be subject to Customer's agreement with its reseller.

3.2 Expenses

Customer agrees to reimburse Secureworks, 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 Secureworks agree that usage is necessary to complete Service delivery.

3.3 Term

The term of the Service is defined in the Transaction Document. Service will expire according to the Transaction Document 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 CRA shall be in full force and effect.

4 Additional Terms

4.1 For Approved On-site Services

Notwithstanding Secureworks' employees' placement at Customer's location(s), Secureworks 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 Secureworks 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 Secureworks completes testing.

4.3 Record Retention

Secureworks will retain a copy of the Customer Reports in accordance with Secureworks' record retention policy. Unless Customer gives Secureworks written notice to the contrary prior thereto and subject to the provisions of the applicable CRA and DPA, all Customer Data collected during the Services and stored by Secureworks will be deleted within 30 days from issuance of the final Customer Report. If Customer or its authorized agent requests that Secureworks retain Customer Data for longer than its standard retention policy, Customer shall pay Secureworks' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Secureworks 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

Secureworks shall have the right to terminate the provision of Service(s) to Customer under a Transaction Document and/or the 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 Secureworks proprietary or confidential data, information, software or other material, including, without limitation, information relating to Customer or other Secureworks customers, Secureworks IP, technology, code, cryptographic keys or access to encrypted material, trade secrets or security process secrets. Secureworks and Customer shall negotiate toward an agreement on reduction of future payments due to reduction in these Service(s). The Transaction Document and the Agreement and other Products purchased by Customer from Secureworks, directly or indirectly, shall continue in jurisdictions unaffected by Secureworks exercise of this right. This language shall not apply to jurisdictions where Secureworks Corp., Secureworks, Inc., or its subsidiaries are incorporated

4.5 Compliance Services

Customer understands that, although Secureworks' Services may discuss or relate to legal issues, Secureworks 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 Secureworks 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, Secureworks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Secureworks in the performance of the Services hereunder (the "**Engagement Media**"), unless prior to such commencement, Customer has specified in writing to Secureworks any special requirements for Secureworks to return such Engagement Media (at Customer's sole expense). Upon Customer's request, Secureworks will provide options for the transfer to Customer of Engagement Media and the related costs thereto. If so requested, Secureworks will provide a confirmation letter to Customer addressing completion and scope of these post-engagement activities, in Secureworks' standard form. Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Secureworks 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 Secureworks 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 Secureworks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks 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 Secureworks 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 Secureworks' 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 Secureworks from the software agent. Customer will uninstall the software agent as described in this Service.