Secureworks®

SERVICE DESCRIPTION

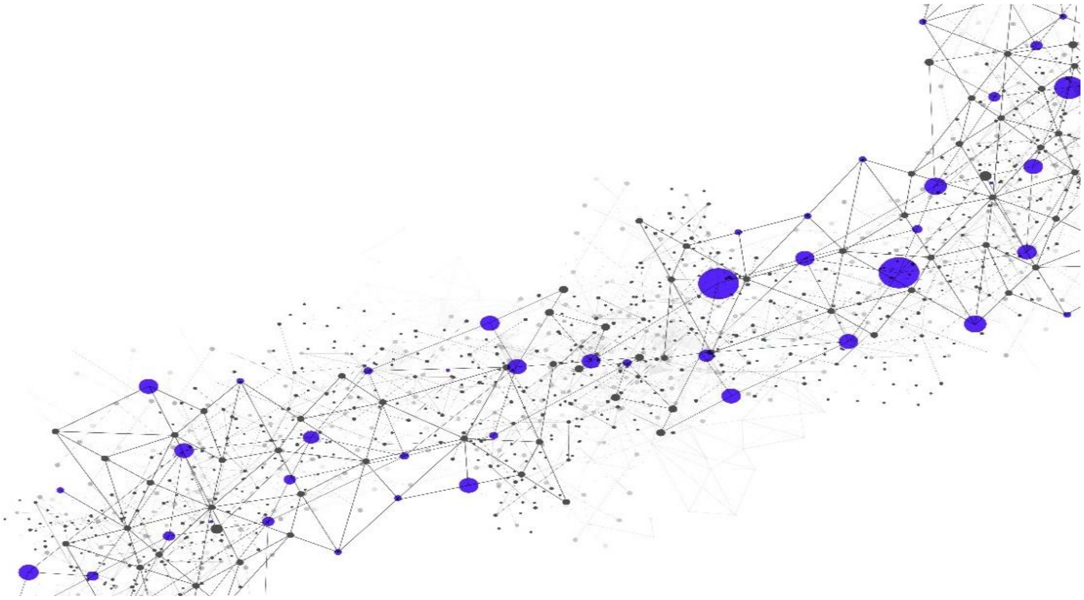
Penetration Test

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

Copyright

Due to continued service development, the information in this publication and related software may change without notice. Please refer to your contract with Secureworks for any provided warranty information.

1 Service Introduction

This Service Description ("**SD**") describes the Penetration Test Service ("**Service**"). 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

Secureworks will conduct a penetration test as defined in this Service Description. The objective of a Penetration Test is to demonstrate weaknesses in systems or network services (highlighting that "the chain is only as strong as the weakest link") and/or how to leverage the weaknesses to move through the network and gain access to target systems or data. The test includes exploitation of vulnerabilities, username and password discovery, lateral movement between systems inside and outside of the target environment, and pivoting through compromised hosts. The test exposes security flaws that vulnerability assessments do not usually detect.

1.2 Customer Obligations

Customer will perform the 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.

For assessments where a Remote Testing Appliance is necessary:

- Customer will provide a suitable hypervisor, outbound connectivity, and access to technical personnel for troubleshooting.
- Customer will assist in the proper placement of the RTA virtual machine, and provide the necessary network connectivity to enable service delivery.
- Customer will securely remove any RTA virtual hosts upon completion of the services.

For Adversarial Security Testing:

- 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 blacklisting).
- Customer agrees to whitelist Secureworks' source testing addresses and domains in any active security devices such as Network Access Control (NAC), Intrusion Prevention System (IPS), or a Web Application Firewall (WAF).

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 test
- Definition of scope and validation of targets
- Rules of engagement, levels of effort and risk acceptance
- Testing timelines and schedules

- Reporting requirements, timelines and milestones
- Key personnel, roles and responsibilities, and emergency planning
- Secureworks source Internet Protocol (“IP”) address ranges, and tools and techniques

After completion of all staging tasks and the introductory meeting, Secureworks will send a confirmation email to ensure agreement on the above-listed items.

A member of the Secureworks’ team will be involved between the introductory meeting and the start of testing to help Customer complete any pre-testing tasks. These tasks include collecting IP addresses / targets / scope, configuring any remote testing connectivity, and other mandatory pre-testing tasks.

2.2 Service Scope

- The Penetration Test Service is available in the following scopes:
- Small Internal Penetration Test: up to fifty (50) internal IP addresses
- Small External Penetration Test: up to fifty (50) external IP addresses
- Medium Internal Penetration Test: up to two hundred fifty (250) internal IP addresses
- Medium External Penetration Test: up to two hundred fifty (250) external IP addresses
- Large Internal Penetration Test: up to five hundred (500) internal IP addresses
- Large External Penetration Test: up to five hundred (500) external IP addresses

The Secureworks’ team will execute the scope per requirements as outlined in a Transaction Document.

Internal Test: Due to the goal-based nature of internal testing, all systems attached to the internal network are in scope. Any system not explicitly excluded from testing may be compromised and used during attempts to attack the target systems.

External Test: External testing will be limited to pre-defined target systems or network ranges. Any modifications to scope will be discussed and documented with Customer before proceeding, and may incur additional fees through a Change Order.

Remote Retest: Secureworks will conduct one (1) remediation validation (“RV”) for only the high- and critical-severity findings listed in the final report.

After primary test completion, Customer has ninety (90) days in which to remediate issues, schedule the RV, and have Secureworks perform the RV. Customer must submit the RV request through email to the Secureworks point of contact for the assessment within thirty (30) days of delivery of the final report or the RV is forfeited.

- For external penetration tests, findings discovered after pivoting and post-exploitation can be difficult to validate and are therefore not included in RV.
- For internal penetration tests, RV can only be performed if the original test used the Secureworks RTA.

Secureworks will issue a brief report summarizing the results of the RV, which will include information about whether Customer successfully remediated the issues.

Note: Secureworks only conducts RVs remotely, regardless of whether the assessment was conducted on-site.

2.3 Service Methodology

The Secureworks' team employs a multi-phase approach to advanced network security testing, based on an internally developed methodology, derived from industry best practice and Secureworks extensive experience. Secureworks works closely with Customer to determine in-scope and out-of-scope targets.

Network Discovery

Secureworks performs port-scans of the provided IP ranges to identify live hosts. This includes activities such as the following:

- Scanning a range of IP addresses to identify top TCP ports in use
- Identifying certain applications and potential version information through banner grabbing

For external tests, scan data is delivered after testing is complete, detailing live hosts and top open ports. Port-scan data is not included with internal test reports.

Open Network Services Enumeration

Secureworks interrogates network services to determine additional information about Customer network that could lead to compromise. Examples include the following:

- DNS host name lookups, brute force zone transfers and DNS relays
- SNMP operating system, software, and network and user enumeration
- SMTP open mail relays and user enumeration
- NetBIOS/SMB domain policy disclosure, including password policy
- LDAP domain policy disclosure and enumeration
- Network service banners for exploitable software
- Web servers for default usernames and passwords and file upload vulnerabilities
- Unknown services to locate potential backdoors

Open Network Services Exploitation

Secureworks will use information from "Open Network Services Enumeration" to attempt compromise of network services. Examples of techniques used include the following:

- Brute-forcing of password protected, network-based services
- Authentication bypass of vulnerable network services
- Exploiting outdated vulnerable services using public exploits
- Identifying and exploiting network backdoors

Note: Use of captured credentials, while not a software vulnerability, is a common vector of attack. Use of captured credentials and publicly disclosed password dumps are considered in-scope. The use of any exploits with high risk of Customer service impact will be discussed prior to use.

Post Exploitation and Lateral Movement

Secureworks will attempt to identify compromise vectors for the wider network and domain infrastructure. The following techniques may be used to show the impact of compromise from earlier phases:

- Exploiting domain trusts, network routes, and bridged networks exposed by compromised systems

- Evading antivirus and end-point protection on compromised systems, further exploiting compromised hosts without detection
- Retrieving additional network and domain passwords and elevating privileges to achieve Domain Administrator or root-level access
- Using gathered credentials and access tokens to compromise additional systems
- Searching for business-critical data

3 Service Delivery

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

3.1.1 Remote Testing Appliance

Secureworks created a system that facilitates remote testing, which is the Remote Testing Appliance (“**RTA**”). This virtual machine allows Secureworks to establish a point-of-presence on Customer’s internal network and provide remote, internal testing capabilities. Using the RTA eliminates on-site travel expenses and provides scheduling flexibility while providing the same quality as an on-site test.

The RTA implementation process is as follows:

- Secureworks works with Customer to pre-configure the RTA, determine the best source-network placement, and provide Customer with a download link for the RTA image
- Customer downloads the RTA, and with Secureworks assistance, deploys the RTA to the source network
- Secureworks verifies connectivity before testing begins, and works with Customer to resolve any connectivity issues

3.1.1.1 Remote Testing Appliance Requirements:

- Outbound internet connectivity to the secure Secureworks testing environment. The RTA creates an encrypted, outbound connection over port 443 using an SSL VPN protocol.
  - Note: At no point can a direct connection be initiated to the RTA from outside Customer network. All outbound connections are initiated by Customer, from within the virtual machine, to the Secureworks secure testing facilities
- A virtual machine hypervisor that supports OVA, OVF, or VMX virtual machine images. The RTA runs in most hypervisors, including free and licensed versions of VMware and VirtualBox, as well as AWS.
- Each RTA virtual machine requires a minimum of 2 virtual CPUs, 4 GB RAM, and 32GB hard disk space.

3.1.2 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.

3.1.3 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
Penetration Test	Final Report	Upon completion of testing	Email

3.1.3.1 Final Report

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 the 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.

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.

3.2 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

Web Applications: If web applications are detected within the range of Customer’s in-scope IP addresses that will be assessed for this Service, then Secureworks will perform generic (also known as black box) testing of those web applications; however, this testing is not considered a comprehensive test of Customer’s web application. Customer can purchase Secureworks web application testing services separately.

4 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

4.1 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.

4.2 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.

4.3 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.

5 Additional Terms

5.1 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.

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 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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 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.