

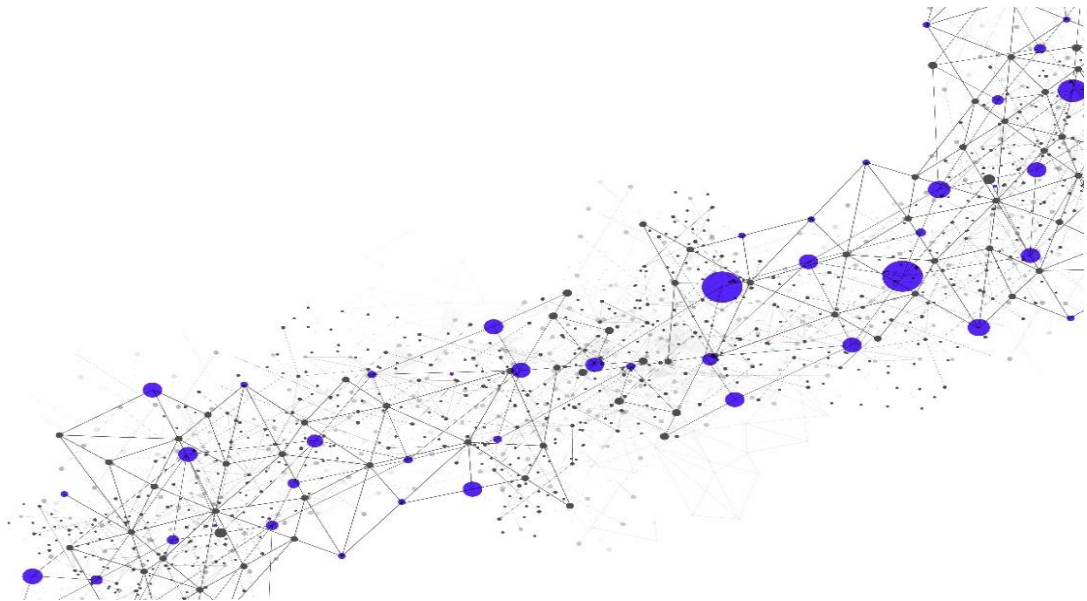
Threat Hunting Assessment

Release Date

October 23, 2023

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	4
1.1	Overview	4
1.2	Customer Obligations	4
1.3	Scheduling	4
1.4	Timeline	5
2	Service Details	5
2.1	Service Initiation	5
2.2	Service Scope	5
2.3	Service Methodology	6
2.4	Service Delivery	6
2.4.1	Delivery Coordination	6
2.4.2	Deliverables	7
2.5	Out of Scope	7
3	Service Fees and Related Information	8
3.1	Invoice Commencement	8
3.2	Expenses	8
3.3	Term	8
4	Additional Terms	8
4.1	On-site Services	8
4.2	Security Services	9
4.3	Record Retention	9
4.4	Compliance Services	9
4.5	Post-Engagement Activities	9
4.6	Legal Proceedings	9
4.7	Endpoint Assessment	10

Copyright

© Copyright 2007-2023. SecureWorks, Inc. or its affiliates. All Rights Reserved.

This publication contains information that is confidential and proprietary to Secureworks® and is subject to your confidentiality obligations set forth in your contract with Secureworks or its affiliates. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

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.

Secureworks® is a trademark or registered trademark of SecureWorks, Inc. or its affiliates. All other trademarks not owned by Secureworks that appear on this publication are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Secureworks.

1 Service Introduction

This Service Description (“SD”) describes the Threat Hunting Assessment 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

The Secureworks Threat Hunting Assessment is a 30-day comprehensive and intensive evaluation of the Customer environment to identify unknown compromise activity, visibility gaps, misconfigured security controls, hidden threats, and other unknown risks. The Service aims to help the Customer improve their cyber resilience with focused, tailored recommendations on security architecture, instrumentation, and security controls.

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.
- For on-site activities, Customer will provide a suitable workspace for Secureworks personnel, and necessary access to systems, network, and devices.
- Replies to all requests are prompt and in accordance with the delivery dates established between the parties.
- Customer’s scheduled interruptions and maintenance intervals allow adequate time for 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.

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.

Once scheduling of any on-site work at Customer facility has been mutually agreed to, any changes by Customer to the on-site work within two (2) weeks of the on-site work to be performed will incur a \$2,000

re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Secureworks.

1.4 Timeline

- On-site work will be performed Monday – Friday, 8 a.m. – 6 p.m. Customer’s local time or similar daytime working hours.
- Remote work will occur Monday – Friday, 8 a.m. – 6 p.m. US Eastern time.
- 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

Prior to initiating the Service, Secureworks will provide Customer with a questionnaire to complete. Secureworks will work with Customer to identify the data sources necessary to complete the assessment, identify the available data sources, and construct a plan to obtain the required data. This questionnaire is integral in providing essential information that enables Secureworks to customize the assessment according to the specific environment. The initiation of the Threat Hunting Assessment will be contingent upon the completion of this questionnaire.

Customer environment may require additional host-based, network-based instrumentation, and cloud-based instrumentation to obtain the necessary data, in which case Secureworks will work with Customer to identify options for Customer to implement the instrumentation prior to the Assessment Phase of the Service, outlined herein.

Secureworks will provide an endpoint sensor for Customer to deploy in Customer environment if they do not have one. An endpoint sensor installation package will be provided to Customer, tailored to Customer's environment based on data provided during Service Initiation. Secureworks will assist Customer through a pre-deployment testing phase, in which Customer must deploy the endpoint sensor to a group of test systems that represent the majority of Customer-system functionality. The Threat Hunting Assessment will not commence until 75% of the endpoint sensors are deployed in Customer's environment.

Customers can utilize their own endpoint detection and response agent if supported by Secureworks Taegis XDR.

2.2 Service Scope

The Threat Hunting Assessment Service is available in the following scopes:

- Small Threat Hunting Assessment: One (1) Threat Hunting Assessment, up to one thousand (1,000) endpoints with thirty (30) days of storage
- Medium Threat Hunting Assessment: One (1) Threat Hunting Assessment, up to five thousand (5,000) endpoints with thirty (30) days of storage

- Large Threat Hunting Assessment: One (1) Threat Hunting Assessment, up to ten thousand (10,000) endpoints with thirty (30) days of storage

The Assessment Phase can last up to 30 calendar days, commencing on the date 75% of the endpoint sensors are deployed in the Customer environment.

2.3 Service Methodology

As part of the Threat Hunting Assessment, Secureworks will conduct an assessment in four (4) phases listed below:

Phase 1: Ingestion of environment telemetry into Taegis XDR platform. Secureworks processes this data through numerous countermeasures, threat intelligence, behavioral analytics, machine learning, and advanced detectors. Secureworks triages Critical and High alerts first to determine if there is an immediate threat undetected by previous security controls.

Phase 2: Deep hunt across all Taegis XDR alerts and Taegis XDR threat hunting leads where threat actors and malware often remain undetected.

Phase 3 (Requires additional Secureworks technology): During this phase, Secureworks analyzes forensic artifacts collected at the onset of the assessment for evidence of historical and unknown compromise, malicious user behavior, and potential security issues.

Phase 4: Secureworks will execute a series of proprietary Threat Hunting playbooks to identify visibility gaps, additional undetected threats, security misconfigurations, and other risks.

If Secureworks discovers ongoing or previous compromise activity during the assessment, Secureworks can provide Customer with Emergency Incident Response as a separate engagement.

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

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
Threat Hunting Assessment	Status Updates	Mutually agreed upon	Mutually agreed upon
	Final Report	Upon completion of service delivery	Mutually agreed upon

2.4.2.1 Status Updates

The Secureworks' team will provide periodic status updates to the Customer. Status updates, which may be verbal or written, may include the following:

- Summary of completed activities,
- Issues requiring attention,
- Planning for the upcoming work effort period.

2.4.2.2 Final Report

Secureworks will issue a report to the Customer designated point of contact within three (3) weeks of completing the assessment. The report may include the following:

- Executive summary, outlining key findings and recommendations,
- Methods, detailed findings, narratives, and recommendations,
- Attachments as needed for relevant details and supporting data.

Secureworks will issue a Final Report draft to the Customer-designated point of contact within three (3) weeks after delivering the Service. Customer shall then have three (3) weeks from Secureworks delivery of the Final Report draft to provide comments. Should Customer provide comments, the Final Report shall be deemed complete upon the earlier of the date which (1) Secureworks provides responses to these comments or (2) Secureworks delivers a revised Final Report. If no comments are received from Customer before the expiration of the review period, or upon Customer's written acceptance of the Report, the Final Report will be deemed complete and referred to as the "Completed Final Report".

2.5 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 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 Data Protection Addendum ("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 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.

4.5 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.

4.6 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.

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 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.