Secureworks®

SERVICE DESCRIPTION

Taegis™ XDR Data Collection and Integration

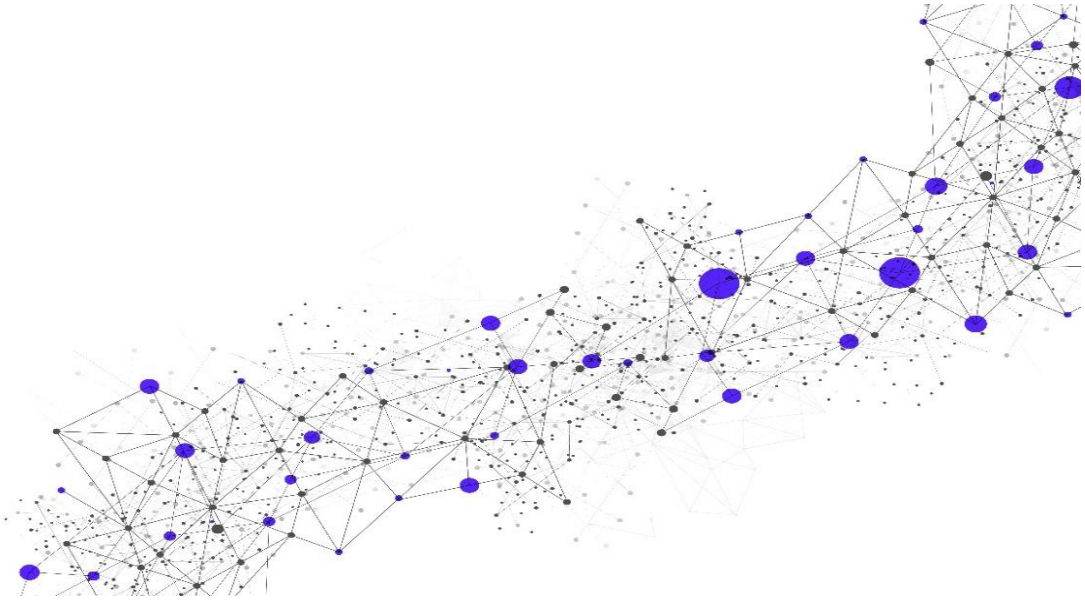
(XDR, ManagedXDR, and ManagedXDR Elite)

Release Date

January 14, 2022

Version

1.4



www.secureworks.com
A Dell Technologies Company

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 Taegis™ XDR Data Collection and Integration Service ("**Service**"). All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

1.1 Overview

Secureworks will assist Customer with integrating its data source into Taegis XDR ("**XDR**") for security analysis activities, thus enhancing the value of the information (data outputs) from XDR for Customer's unique needs. The Service includes the following:

- Provide one (1) XDR Data Collection and Integration ("**DCI**") Integration for custom parsing and ingesting data from one Customer data source (e.g., log, endpoint telemetry) into XDR to enhance the value and usefulness of XDR to meet Customer's unique needs
- Integrate Customer's data source according to the limitations listed below:
  - Up to eight (8) unique event types will be parsed (e.g., logon, logoff, user add, user delete, config save, connection open, connection close, signature detected)
  - Data source should be in one of the following data structures – JSON, CEF, LEEF, CSV, Key-Value Pairs, or unstructured Syslog (with vendor documentation)
  - Up to three (3) applicable Schemas (e.g., Schemas that exist in XDR such as Auth, DNS, Endpoint, HTTP, Netflow, NIDS); see https://docs.ctpx.secureworks.com/at_a_glance/, the "Detector Requirements" table for the most current information)

Notes:

- The Service provided within this SD is also referred to as an Engagement as described in Section 2.
- If Customer's needs exceed the above-defined scope, then a Statement of Work ("**SOW**") is required.
- This Service is also available to Customer with purchase of ManagedXDR or ManagedXDR Elite.
- This is a per-integration Service. If Customer has more than one tenant (i.e., **Additional Managed Tenant**), then Customer and Secureworks will collaborate and document the tenants in which the integration will be deployed.
- The number of unique event types correlates with the number of applicable Schemas. A custom parser will be developed to parse and ingest data into XDR from Customer's data source, and the data will be added to the applicable Schemas. For example, *logon* and *logoff* unique event types will be added to the Auth Schema, and *connection open* and *connection close* unique event types will be added to the Netflow Schema. Customer is required to complete a questionnaire about the data source during the Sales process to help determine the number of unique event types and applicable Schemas.

The Service will be delivered remotely from a secure location. See Section 2, Service Details, for details about the Service.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder are dependent on Customer's compliance with these obligations.

1.2.1 Application Program Interface ("API") Integration

Some vendors provide APIs to interact with their systems. Any script or code creation for, usage of, maintenance of, or Integration with other third-party tools are not included in this Service; Customer shall be responsible for all API Integration, and related activities and licenses not listed in this SD as part of the Service. Secureworks will not install any third-party software applications that use the API directly on the appliance.

1.2.2 General

- 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-scheduled interruptions and maintenance intervals will allow adequate time for Secureworks to perform the Service(s).
- Customer will provide sample logs to Secureworks before or during an introductory meeting as further described in Section 2.2.1 ("**Introductory Meeting**").
- Customer will ensure that the firmware or software that operates the in-scope devices for this Service is the same; otherwise, Secureworks may pause delivery of the Service, re-assess the work effort, and execute a new SO or SOW (depending on the work needed) with Customer for the additional fees specific to the increased work effort.

1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Service Order ("**SO**") to schedule the Introductory Meeting to start the Engagement.

Customer and Secureworks will designate respective points of contact ("**POC**") to facilitate communication and support ongoing activities related to delivering the Service.

2 Service Details

2.1 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

2.2 Engagement Process

The subsections below describe the process for delivering the Service.

2.2.1 Preparation

Secureworks will work with Customer to define objectives and deliverables for the Service. Both Customer and Secureworks will review the high-level requirements for delivering the Service (including reviewing the questionnaire that was completed during the Sales process), introduce key personnel, designate respective POCs, and establish communication channel(s). This phase includes the following activities:

- Introductory Meeting
  - Discuss Customer's goals for the Integration and key challenges that need to be addressed
  - Agree upon the Service delivery schedule
  - Collect artifacts necessary to facilitate Integration design activities
  - Document purpose of the Integration and include the following:
    - Key objectives of the Integration
    - Risks associated with the Integration
    - Audience who will be analyzing the data outputs related to the Integration
- Analyze Data
  - Collect and review sample logs
  - Review data transformation requirements
  - Review data output expectations

2.2.2 Design and Implementation

Secureworks will document the design requirements that will enable successful Integration with XDR. This phase includes the following activities:

- Discuss Integration Design
  - Confirm feasibility of the Integration with Secureworks XDR development team and modify as necessary
  - Communicate any limitations with Customer
- Implement Design
  - Implement the Integration per the agreed-to design. Any issues will be tracked and addressed.

2.2.3 Quality Evaluation and Wrap-Up

Secureworks will evaluate the Integration through sampling, review of steps completed during the DCI Integration, and/or automated techniques, and address defects observed by Customer and Secureworks. Elements to evaluate, as related to the design specifications, include the following:

- Adequacy
- Completeness
- Accuracy
- Effectiveness

Provided that the quality checks are completed satisfactorily, the deliverables listed in the Deliverables section of this SD will be completed and provided to Customer.

2.3 Deliverables

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

Service Name	Report	Delivery Schedule	Delivery Method
Custom XDR DCI Service	Integration Documentation	Upon Completion of Engagement	Email

2.3.1 Reports and Timing

Within two (2) weeks after completing the Engagement, Customer will receive Integration Documentation, which will include the following:

- Data Integration Strategy and Requirements specification
- Design specifications
- Quality checklist

2.4 Business Days and Business Hours

Business Days for Secureworks global headquarters are Monday – Friday and Business Hours are 8 a.m. – 5 p.m. US Eastern Time, excluding US holidays. Business Days and Business Hours for all other Secureworks locations vary according to local time zone and country. The Secureworks SOC is available 24 hours a day, 7 days a week, for questions and support. During non-Business Days and Hours, some SOC inquires may be sent to other support groups to address during Business Days and Hours.

2.5 Disclaimer: 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.

2.6 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. Items listed below are examples of services and activities that are out of scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate SO or SOW.

- Developing any detectors (e.g., detectors for XDR)
- Accessing Customer devices or directing data sources to the Secureworks® Taegis™ XDR Collector (this is a Customer responsibility)
- Re-parsing any of Customer's logs that have already been ingested into XDR (i.e., no retro-active parsing)
- Adding other event types and new event types that are discovered after completion of this Service
  Note: The custom parser will be developed based on Customer-provided sample logs and the above-defined scope. Should any additional event types be discovered ***before*** the custom parser development is completed by Secureworks, only up to five (5) of these additional event types will be added, up to the maximum of eight (8) for the Service.

- After deployment of the custom parser and completion of this Service, should any log format change due to factors not within the scope of this SOW (such as a firmware update), Customer will need to engage Secureworks for additional custom development work on the custom parser at a Time and Materials ("**T&M**") rate that is listed under Service Fees further below.

3 Service Fees and Related Information

Service Fees are based on a fixed fee; Customer is billed upon execution of Service Order. See Customer's MSA or CRA (as applicable), and SO or SOW (as applicable) for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

3.1 Invoice Commencement

See the Service-specific Addendum or SO for information about invoice commencement.

4 Glossary

Term	Description
Additional Managed Tenant	An add-on service for ManagedXDR and ManagedXDR Elite that provides Customer with more than one XDR tenant.
Integration	Application Programming Interface ("**API**") calls or other software scripts for conducting the agreed-upon Service(s) for the connected technology.
Schema	An organizational unit for log events ingested and parsed by XDR (examples: Authentication, DNS, Netflow, NIDS, HTTP, and Process).